Twiin Afsprakenstelsel 1.4.1

Publicatiedatum: 28 mei, 2026

Inhoud

Dit is de voorlaatste versie van het Twiin Afsprakenstelsel. De actuele normatieve versie is te vinden via https://afsprakenstelsel.twiin.nl/normatief/

28 May 2026 Dit is de vastgestelde release 1.4.1 voor publicatie.

Wat is het Twiin Afsprakenstelsel?

Het Twiin Afsprakenstelsel is een set samenwerkingsafspraken voor het delen en beschikbaar maken van gezondheidsgegevens; veilig en betrouwbaar, tussen zorgaanbieders, zorgnetwerken en voorzieningen. Het stelsel bevat afspraken voor zorgaanbieders en hun dienstverleners en leveranciers.

Opbouw Twiin Afsprakenstelsel

Het afsprakenstelsel bevat afspraken op alle lagen van het Nictiz-vijflagenmodel. Het afsprakenstelsel is onderverdeeld in een generiek deel en een specifiek deel met daarin de zorgtoepassingen. Het generieke deel bevat alle afspraken die van toepassing zijn op alle zorgtoepassingen.

Het generieke deel van het Twiin Afsprakenstelsel bevat onder andere het vertrouwensmodel en een technische kern. Het vertrouwensmodel is een essentieel onderdeel van het Twiin Afsprakenstelsel en is de basis voor veilige en betrouwbare landelijke elektronische uitwisseling en beschikbaarheid van medische gegevens. Het vertrouwensmodel beschermt het beroepsgeheim van de zorgverlener en de privacy van de cliënt bij de uitwisseling van gezondheidsgegevens, ook al vindt deze uitwisseling tussen knooppunten van verschillende infrastructuren plaats. De technische kern bevat generieke communicatiepatronen die ingezet kunnen worden voor één of meer zorgtoepassingen.

Het specifieke deel van het afsprakenstelsel bevat de implementatiewijzers voor de implementatie van specifieke zorgtoepassingen. Er is ruimte om het specifieke deel uit te breiden met implementatiewijzers van nieuwe zorgtoepassingen. Hierbij geldt telkens als eis dat de implementatiewijzer de afspraken volgt die zijn opgenomen in het generieke deel.

Landelijk afsprakenstelsel

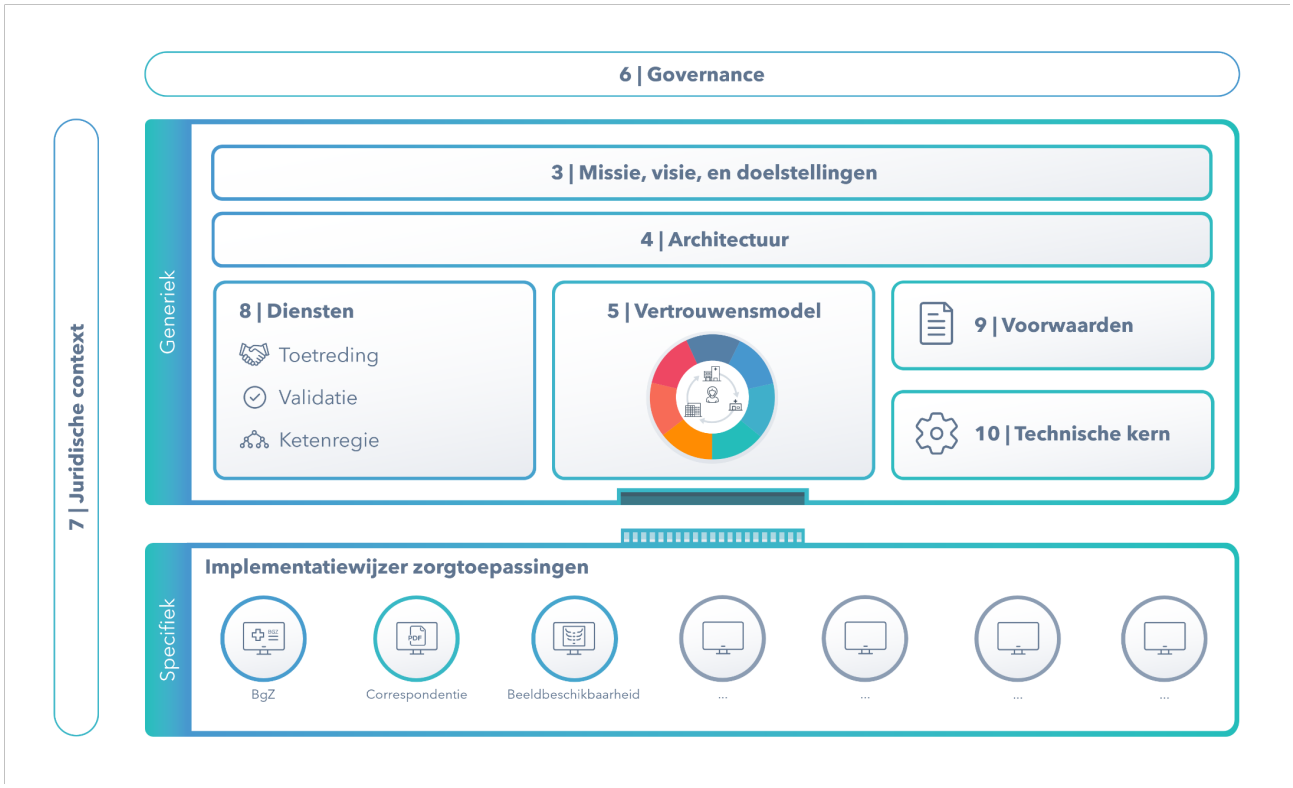
Het Ministerie van Volksgezondheid, Welzijn en Sport heeft het Twiin Afsprakenstelsel gekozen[1] als dé **centrale plek** voor de vastlegging van geharmoniseerde en gestandaardiseerde vertrouwensafspraken in de zorg. De transitie naar een landelijk afsprakenstelsel met Twiin als fundament, biedt structuur en samenhang tussen alle afspraken.

1. https://www.datavoorgezondheid.nl/landelijk-vertrouwensstelsel

1 | Leeswijzer

Het Twiin Afsprakenstelsel kent een logische opbouw. Onderstaand overzicht toont een overzicht van de verschillende onderdelen van het afsprakenstelsel. Centraal hierbij is het onderscheid tussen het generieke en het specifieke deel. In het hoofdstuk Doelgroepen (see page 3) is per doelgroep aangegeven welke onderdelen vooral relevant zijn.

Opbouw Twiin Afsprakenstelsel



1.1 | Doelgroepen

Relevante onderdelen afsprakenstelsel per doelgroep

In dit hoofdstuk is per doelgroep aangegeven welke onderdelen van het Twiin Afsprakenstel vooral relevant zijn.

Doelgroep	Rol	Relevante onderdelen
Zorgaanbieders	Bestuurders	3 | Missie, visie en doelstellingen (see page 35) 5 | Vertrouwensmodel (see page 56) 6 | Governance (see page 80)
	ICT Management	2 | Release-informatie (see page 9) 3 | Missie, visie en doelstellingen (see page 35) 4 | Architectuur (see page 37) 5 | Vertrouwensmodel (see page 56) 6 | Governance (see page 80) 8 | Diensten (see page 119) 9 | Voorwaarden (see page 142) Twiin Implementatiewijzer Zorgtoepassingen (see page 294)
	Juristen	5 | Vertrouwensmodel (see page 56) 6 | Governance (see page 80) 7 | Juridische context (see page 102) 9 | Voorwaarden (see page 142)
	Security & Privacy officers	5 | Vertrouwensmodel (see page 56) 7 | Juridische context (see page 102) 9 | Voorwaarden (see page 142) 10 | Technische kern (see page 164)
	Projectleiders	5 | Vertrouwensmodel (see page 56) 8 | Diensten (see page 119) Twiin Implementatiewijzer Zorgtoepassingen (see page 294)
	Architecten, Ontwerpers, Beheerders	2 | Release-informatie (see page 9) 4 | Architectuur (see page 37) 5 | Vertrouwensmodel (see page 56) 9 | Voorwaarden (see page 142) 10 | Technische kern (see page 164) Twiin Implementatiewijzer Zorgtoepassingen (see page 294)
Zorgverleners		3 | Missie, visie en doelstellingen (see page 35) 5 | Vertrouwensmodel (see page 56)
Cliënten		5 | Vertrouwensmodel (see page 56)
Leveranciers		4 | Architectuur (see page 37) 5 | Vertrouwensmodel (see page 56) 9 | Voorwaarden (see page 142) 10 | Technische kern (see page 164) Twiin Implementatiewijzer Zorgtoepassingen (see page 294)
Regio's		4 | Architectuur (see page 37) 5 | Vertrouwensmodel (see page 56) 8 | Diensten (see page 119) 9 | Voorwaarden (see page 142) 10 | Technische kern (see page 164)
Overig		2 | Release-informatie (see page 9) 3 | Missie, visie en doelstellingen (see page 35)5 | Vertrouwensmodel (see page 56)

1.2 | Begrippen

Algemene begrippen

Het Twiin Afsprakenstelsel volgt de begrippen uit toepasselijke wet- en regelgeving. Waar mogelijk sluit het Twiin Afsprakenstelsel aan bij begrippen uit de DIZRA (Duurzaam Informatiestelsel in de Zorg Referentie Architectuur)[2] en de Nationale Visie en Strategie (NVS)[3].

Twiin-begrippenlijst

In de Twiin-begrippenlijst zijn enkel Twiin-specifieke begrippen opgenomen.

- (TA141) Begrip: Afsprakenstelsel

  Een afsprakenstelsel is een samenhangend geheel van juridische, organisatorische, semantische en technische afspraken, inclusief afspraken over besturing en beheer. Het beschrijft hoe partijen onderling op een veilige, betrouwbare en doelmatige manier gegevens delen.
- (TA141) Begrip: Beheerovereenkomst

  Twiin Deelnemers die een GtK Beheerder inschakelen, sluiten een beheerovereenkomst met de GtK Beheerder. In deze overeenkomst staan formele afspraken tussen een Twiin Deelnemer en de betrokken GtK Beheerder waarin wordt vastgelegd hoe het beheer van een Gevalideerd Twiin Knooppunt (GtK) wordt georganiseerd en uitgevoerd, waaronder incidentbeheer, wijzigingsbeheer en operationele ondersteuning. De Twiin Organisatie stelt een modelbeheerovereenkomst beschikbaar die partijen kunnen gebruiken om passende afspraken met elkaar te maken.
- (TA141) Begrip: Bewijs van Validatie

  Een bewijs dat wordt verstrekt na het succesvol doorlopen van het Proces Validatie. Er zijn twee typen: het Bewijs van Validatie Twiin Deelnemer voor de Twiin Deelnemer en het Bewijs van Validatie GtK voor het GtK.
- (TA141) Begrip: Deelnemersovereenkomst

  De overeenkomst tussen de Twiin-organisatie en een Twiin-deelnemer, waarin de deelnemer zich committeert aan deelname aan het Twiin-afsprakenstelsel en onder vastgestelde voorwaarden toewerkt naar validatie, met inachtneming van de geldende afspraken en verplichtingen..
- (TA141) Begrip: Dienstverleningsovereenkomst

  De overeenkomst die Twiin Deelnemers sluiten met een Twiin Dienstverlener.
- (TA141) Begrip: Dossierhouder

  Een zorgaanbieder die verantwoordelijk is voor het (laten) onderhouden van het dossier van een cliënt en in het kader daarvan beschikt over gezondheidsgegevens van die cliënt.
- (TA141) Begrip: Dossierontvanger

  Een zorgaanbieder die gezondheidsgegevens van een cliënt ontvangt van een dossierhouder.
- (TA141) Begrip: Dossierraadpleger

2. https://dizra.gitbook.io/dizra
3. https://www.datavoorgezondheid.nl/nationale-visie-en-strategie/visie

Een zorgaanbieder die bij een dossierhouder gezondheidsgegevens raadpleegt van een cliënt.

- (TA141) Begrip: Gemeenschappelijke voorziening

  Een product of dienst gericht op het ondersteunen van een generieke functie.
- (TA141) Begrip: Governance

  De inrichting van de rollen, taken, verantwoordelijkheden en spelregels die nodig is voor de besturing van de Twiin Organisatie als stelselhouder van het Twiin Afsprakenstelsel.
- (TA141) Begrip: GtK

  Een GtK (Gevalideerd Twiin Knooppunt) is een door Twiin gevalideerde oplossing die onderdeel uitmaakt van een keten voor beschikbaarheid en uitwisseling van gegevens voor één of meer zorgtoepassingen voor één of meerdere Twiin Deelnemers. Een GtK hoeft niet per se uit één uitwisselingssysteem of uit één (aparte) applicatie te bestaan. Een GtK kan gevormd worden door meerdere onderdelen. Het GtK bestaat minimaal uit een koppelvlak op een regionale infrastructuur, een landelijke infrastructuur, een leveranciersnetwerk of een platform.
- (TA141) Begrip: GtK Beheerder

  Een organisatie die namens de Twiin Deelnemer invulling geeft aan het technisch beheer van het GtK, zoals omschreven in de Voorwaarden GtK Beheer.
- (TA141) Begrip: GtK Leverancier

  Leverancier van een GtK.
- (TA141) Begrip: Incident

  Een ongeplande onderbreking van een IT-dienst, een vermindering van de kwaliteit van een IT-dienst, beveiligingsincidenten en/of een een inbreuk in verband met persoonsgegevens als bedoeld in artikel 4 onder 12 AVG.
- (TA141) Begrip: Regio

  Een geografisch afgebakend deel van Nederland dat eventueel valt onder de verantwoordelijkheid van een regionale samenwerkingsorganisatie (RSO).
- (TA141) Begrip: Samenwerkingsvoorwaarden

  De invulling die de Twiin Deelnemer geeft aan de Twiin Voorwaarden zolang de Twiin Deelnemer nog niet is gevalideerd. Deze invulling is gebaseerd op het groeimodel met als doel om tot validatie te komen.
- (TA141) Begrip: Servicedesk Twiin Deelnemer

  De servicedesk die iedere Twiin Deelnemer zelf inricht, inclusief contract met ondersteunende leveranciers, of laat inrichten door een GtK Beheerder.
- (TA141) Begrip: Tijdlijn

  Een tijdlijn is een integraal overzicht van statussen en resultaten dat plaats- en tijdonafhankelijk is en over de grenzen van zorginstellingen heen gaat.

  Het biedt binnen de werkomgeving van de zorgverlener een samenhangende chronologische weergave van alle voor het zorgproces relevante gegevens. Per situatie wordt bepaald of er een tijdlijn nodig is en welke soort gegevens de tijdlijn bevat.
- (TA141) Begrip: Twiin Beheerorganisatie

Organisatie die in opdracht van de Twiin Organisatie beheertaken uitvoert in het kader van het Twiin Afsprakenstelsel.

- (TA141) Begrip: Twiin Bestuur

  Het organisatieonderdeel van de Twiin Organisatie dat eindverantwoordelijk is voor het beheer en de doorontwikkeling van het Twiin Afsprakenstelsel.
- (TA141) Begrip: Twiin Casemanager

  Persoon werkzaam voor de Twiin Organisatie met inhoudelijke kennis voor het proces dat hij/zij begeleidt.
- (TA141) Begrip: Twiin Deelnemer

  Organisatie die de Twiin Deelnemersovereenkomst voor het Twiin Afsprakenstelsel heeft getekend. Vooralsnog zijn dit enkel zorgaanbieders zolang niet anders wordt besloten op basis van het reglement.
- (TA141) Begrip: Twiin Dienstverlener

  Een partner die begeleidt bij de implementatie en de ontwikkeling van zorgtoepassingen en die Twiin Deelnemers helpt om te voldoen aan het Twiin Afsprakenstelsel.
- (TA141) Begrip: Twiin Organisatie

  Eindverantwoordelijke voor het Twiin Afsprakenstelsel met de rol van stelselhouder.
- (TA141) Begrip: Twiin Samenwerkingsverband

  Het samenwerkingverband van de Twiin Organisatie en partijen die zijn aangesloten (see page 119) bij het Twiin Afsprakenstelsel.
- (TA141) Begrip: Twiin Serviceportaal

  Een communicatieplatform voor ketenregie met contactgegevens, versiebeheer en gemelde incidenten. De Twiin Organisatie zorgt voor de inrichting van het serviceportaal.
- (TA141) Begrip: Twiin Vertrouwensmodel

  Het vertrouwensmodel is het geheel van afspraken voor het vertrouwen in de landelijke elektronische uitwisseling van medische gegevens. Deze afspraken zien toe op de invulling van zeven verschillende onderdelen: identificatie, authenticatie, autorisatie, behandelrelatie, toestemming, logging en transparantie. Deze afspraken zijn noodzakelijk voor het onderlinge vertrouwen tussen zorgaanbieder, zorgverlener en personen. Het vertrouwensmodel borgt de vertrouwelijkheid van het medische dossier.
- (TA141) Begrip: Twiin Voorwaarden

  De voorwaarden waaraan Twiin Deelnemers zijn gehouden door ondertekening van de Twiin Deelnemersovereenkomst.
- (TA141) Begrip: Verklaring GtK Beheerder

  De verklaring tussen de Twiin Organisatie en een GtK Beheerder, waarin de GtK Beheerder zich committeert aan deelname aan het Twiin Afsprakenstelsel en het voldoen aan de vastgestelde voorwaarden, geldende afspraken en verplichtingen.
- (TA141) Begrip: Verklaring GtK Leveranciers

De verklaring tussen de Twiin Organisatie en een GtK Leverancier, waarin de GtK Leverancier zich committeert aan deelname aan het Twiin Afsprakenstelsel en het voldoen aan de vastgestelde voorwaarden, geldende afspraken en verplichtingen.

- (TA141) Begrip: Verklaring Twiin Dienstverlener

  De verklaring tussen de Twiin Organisatie en een Twiin Dienstverlener, waarin de dienstverlener zich committeert aan deelname aan het Twiin Afsprakenstelsel en het voldoen aan de vastgestelde voorwaarden, geldende afspraken en verplichtingen.
- (TA141) Begrip: Zorgtoepassing

  Een (deels) geautomatiseerde oplossing voor gegevensbeschikbaarheid die een specifiek zorgproces ondersteunt.

2 | Release-informatie

Onderstaande tabel toont de belangrijkste wijzigingen die zijn doorgevoerd in deze gepubliceerde release van het Twiin Afsprakenstelsel ten opzichte van de vorige versie. Per wijziging is er ook een verwijzing naar de desbetreffende pagina. Beperkte redactionele wijzigingen zoals herstel van typfouten en evidente verschrijvingen worden niet apart benoemd.

Release – Nr	Betreft	Verwijzing
	Minor release 1.4.1	
1.4.1 – 2	Eis 5.030 / BgZ-2a-NS-03 is aangepast omdat ChaCha20-Poly1305 niet voldoet aan de Amerikaanse eisen van het NIST en daarmee niet altijd ondersteund wordt door leveranciers.	PvE | Netwerkbeveiliging (see page 213)
1.4.1 – 1	`http://fhir.twiin.nl/fhir/CodeSystem/TaskCode` en `http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile` zijn voor consistentie doorgevoerd.	Twiin-07 | Token Request (see page 270) 10.5.1 | Twiin-01 | Send Notification Task (see page 217) 10.5.2 | Twiin-02 | Cancel Notification Task (see page 225) Z1.4.2 | BgZ: FHIR Workflow Task implementation (see page 347) Z1.4.3 | BgZ: FHIR examples (see page 363)
	Minor release 1.4.0	
1.4.0 – 44	GtK Beheer voorwaarde 4.4 over het beheer van de logging verwijst nu expliciet naar Logging eis Log-02. Zolang er nog geen landelijke procedures en afspraken zijn opgesteld over de uitwisseling van de logging tussen GtK's zal dit in de (uitzonderlijke) gevallen wanneer dit toch nodig is op ad hoc basis gedaan moeten worden.	9.3 | Voorwaarden GtK Beheer (see page 155) PvE | Logging (see page 209)
1.4.0 – 43	Aan de Risicoanalyse is toegevoegd dat de Twiin Deelnemers de risicoanalyse kunnen delen met hun Dienstverlener	8.4 | Risicoanalyse (see page 138)
1.4.0 – 42	GtK Leverancier is gewijzigd in GtK Beheerder in de uitgangspunten bij Ketenregie. De Beheerder is het eerste aanspreekpunt voor incidentmeldingen, niet de leverancier.	8.3 | Ketenregie (see page 136)

Release – Nr	Betreft	Verwijzing
1.4.0 – 41	Waar in het Twiin Afsprakenstelsel gedoeld wordt op een leverancier van een GtK dat nog niet gevalideerd is, is het begrip GtK Leverancier gewijzigd in aspirant GtK Leverancier.	8.1.2 | Aansluiten Twiin Dienstverlener (see page 121)
1.4.0 – 40	Missie, visie en doelstellingen die beschreven zijn gelden breder dan alleen voor de Twiin Deelnemers.	3 | Missie, visie en doelstellingen (see page 35)
1.4.0 – 39	Tabel over de communicatiepatronen is aangepast. De initiator van de communicatie is toegevoegd.	4.4 | Logische architectuur (see page 46)
1.4.0 – 38	Principes zijn aangescherpt. Principe 1: omschrijving is aangepast: meer focus op primair gebruik Bij principe 6 is bij de implicatie EHDS toegevoegd en is de implicatie dat Dienstverleners kennis moeten hebben van leveranciers verwijderd.	4.2 | Twiin Principes (see page 38)
1.4.0 – 37	Eisen BgZ-3-5 en BgZ-3-6 verwezen nog naar niet meer actuele BgZ medisch-specialistische zorg Technical Implementation Guide 1.0, dit is gewijzigd naar link naar de 1.1 versie	Z1.5 | BgZ: PvE (see page 377)
1.4.0 – 36	10.4.1 | TTA – Identification & Authentication (see page 203) voorzien van een inleidende tekst	10.4.1 | TTA – Identification & Authentication (see page 203)
1.4.0 – 35	De beschrijving van gemeenschappelijke voorziening is herschreven in lijn met de definitie van NVS	10.2 | Kern Volume 0b – Generieke functies (see page 179)
1.4.0 – 34	Vaak is er een keuze om bepaalde functionaliteit in het XIS dan wel het GtK te beleggen. In de diagrammen en beschrijvingen van communicatiepatronen in 10.1 | Kern Volume 0a – Communicatiepatroon Overview (see page 169) lijkt het dat hier al keuzes in gemaakt worden. Het is in de tekst toegelicht dat keuzes mogelijk zijn.	10.1 | Kern Volume 0a – Communicatiepatroon Overview (see page 169)

Release – Nr	Betreft	Verwijzing
1.4.0 – 33	Header hygiëne toegevoegd. Hierin is ook de W3C Trace Context toegevoegd om invulling te geven aan de NEN7513 qua traceerbaarheid van logging.	HTTP-header hygiene (see page 289) 10.2.4 | Generieke functie – Logging (see page 182)
1.4.0 – 32	Vernieuwingen van technische kern doorgevoerd in de voorbeelden van BgZ.	Z1.4.2 | BgZ: FHIR Workflow Task implementation (see page 347) Z1.4.3 | BgZ: FHIR examples (see page 363)
1.4.0 – 31	Lijst gemarkeerd voor verwijdering in volgende release.	Z1.4.1 | BgZ: FHIR Task reference codes (deprecated) (see page 345)
1.4.0 – 30	Verwijzingen naar Nictiz implementatiegids 1.0 vervangen door 1.1. Geen verdere wijzigingen noodzakelijk.	Z1 | BgZ: Implementatiewijzer Basisgegevensset Zorg (see page 294) Z1.1.1 | Uitwisseling BgZ bij verwijzing of overdracht (see page 297) Z1.1.2 | Opvraging BgZ bij eerdere behandelaar (see page 299) Z1.4 | BgZ: Volume 3 – Content (see page 345)
1.4.0 – 29	Aanscherping van de tekst en eisen in 10.4.7 | Network level security (see page 211) vanwege een update van de NCSC richtlijnen[4] van juni 2025. • Certificate Verification: ECDSA of RSA en zijn afgewaardeerd van goed naar voldoende met oog op de quantumdreiging, maar er zijn (nog) geen alternatieven op beveiligingsniveau goed beschikbaar. EdDSA is ook van het niveau 'voldoende' • Key exchange: ECDHE is zijn afgewaardeerd van goed naar voldoende. Met X25519MLKEM768, SecP256r1MLKEM768, SecP384r1MLKEM1024 zijn er alternatieven, maar deze algoritmes zijn (relatief) nieuw en maken nog geen deel uit van de TLS standaarden. ECDHE moet daarom nog gebruikt worden.oldoende' met AES-256-GCM en ChaCha20-Poly1305 zijn er nog 2 alternatieven met niveau 'goed'	10.4.7 | Network level security (see page 211), eis **5.030 /** BgZ-2a-NS-03 PvE | Netwerkbeveiliging (see page 213)

4. https://www.ncsc.nl/documenten/publicaties/2025/juni/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2025-05

Release – Nr	Betreft	Verwijzing
1.4.0 – 28	In hoofdstuk 8 wordt verwezen naar de vindplaats van achterliggende procedurebeschrijvingen.	8 | Diensten (see page 119)
1.4.0 – 27	In hoofdstuk 8 zijn dubbele teksten verwijderd. Bij de diensten *Aansluiten* en *Valideren* is in de tabellen duidelijker benoemd welke processtappen doorlopen worden en welke organisatie verantwoordelijk is voor een processtap.	8 | Diensten (see page 119) 8.1 | Aansluiten (see page 119) 8.2 | Valideren (see page 128)
1.4.0 – 26	Update aan de parameters voor de input in de Notification Task.	10.5.1 | Twiin-01 | Send Notification Task (see page 217)
1.4.0 – 25	Er is een dienst toegevoegd genaamd *Risicoanalyse*.	8.4 | Risicoanalyse (see page 138)
1.4.0 – 24	Hoofdstuk 7 (*Juridische Context*) is opgesplitst. De juridische context bevat het schematische overzicht van de wet- en regelgeving. In paragraaf 7.1 (*Juridisch kader*) is de korte samenvatting en toepassing van de wet- en regelgeving opgeschreven. Het onderdeel *Toelichting verwerkingsverantwoordelijkheid* (7.2) heeft een eigen paragraaf gekregen. De normen hebben een eigen paragraaf gekregen (7.3). Deze onderdelen zijn daarbij ook geüpdatet. Het *Informatiebeveiligingsbeleid* (7.4) is toegevoegd.	7 | Juridische context (see page 102) 7.1 | Juridisch kader (see page 104) 7.2 | Toelichting verwerkingsverantwoordelijkheid (see page 113) 7.3 | Toepasselijke normen (see page 115) 7.4 | Informatiebeveiligingsbeleid (see page 117)
1.4.0 – 23	Hoofdstuk 4 *Architectuur* is geredigeerd. Er is een andere structuur aangebracht, reeds bestaande teksten zijn ingekort en er is meer onderlinge samenhang aangebracht. Inhoudelijk wordt er geen andere invulling gegeven aan de architectuur.	4 | Architectuur (see page 37)

Release – Nr	Betreft	Verwijzing
1.4.0 – 22	In het reglement is verduidelijkt dat de Overlegtafels het recht hebben, maar niet de plicht, om adviezen te geven. Toegevoegd is dat deze adviezen zien op uitvoeringsvragen en gegeven worden binnen het kader van de strategische besluiten op basis van de NVS. Toegevoegd is dat de Twiin Organisatie kan besluiten beide Overlegtafels gezamenlijk bijeen te laten komen. Toegevoegd is dat het Twiin Bestuur binnen dertig dagen een reactie geeft op adviezen en op verzoek deze reactie mondeling toelicht. Dit in plaats van de regeling over negatieve adviezen. Toegevoegd is dat de Twiin Dienstverlener de partij is die een Twiin Deelnemer kan vertegenwoordigen. Vervallen is het vooraf schriftelijk inbrengen van standpunten bij de voorzitter.	6.6 | Reglement (see page 98)
1.4.0 – 21	Aangepast dat een post-fix hoort bij een release van het afsprakenstelsel als geheel. De post-fix met de status 'review' is komen te vervallen aangezien voor iedere nieuwe release eerst een review georganiseerd wordt voorafgaand aan publicatie. De post-fix met de status 'uitgefaseerd' is toegevoegd. Ook is verduidelijkt dat de status van een implementatiewijzer volgt uit status van de versie van het Twiin Afsprakenstelsel waarin deze implementatiewijzer is gepubliceerd en dat in aanvulling daarop aan een implementatiewijzer nog de status 'trial' kan worden toegekend.	6.5 | Releasebeleid (see page 97)
1.4.0 – 20	Technische uitwerkingen TTA SOAP – Indexed Pull, TTA SOAP Push en TTA FHIR Pull voldoen nog niet volledig aan het Twiin Afsprakenstelsel en zijn naar het ontwikkelsupplement verplaatst.	Het ontwikkelsupplement wordt separaat gepubliceerd. Zie www.twiin.nl[5] voor een verwijzing.

5. http://www.twiin.nl

Release – Nr	Betreft	Verwijzing
1.4.0 – 19	De volgende eisen samengevoegd omdat voor zowel GtK verzender en GtK ontvanger dezelfde eis was opgesteld of omdat de eis op meerdere plekken in min of meer dezelfde vorm voor kwam. • BgZ-2a-AA-07 en BgZ-2a-AA-12 • BgZ-2a-AA-01 en BgZ-2a-AA-02 • BgZ-2a-TANP-04 en BgZ-2a-TANP-05 • 5.030 en BgZ-2a-NS-03 • 5.010 en BgZ-2a-NS-02 • 5.050 en BgZ-2a-NS-04 • 5.060 / BgZ-2a-NS-05	• BgZ-2a-AA-07 en BgZ-2a-AA-12PvE | Notified Pull (see page 193) • BgZ-2a-AA-01 en BgZ-2a-AA-02 PvE | Identificatie en authenticatie (see page 204) • BgZ-2a-TANP-04 en BgZ-2a-TANP-05PvE | Adressering (see page 210) • 5.030 en BgZ-2a-NS-03 PvE | Netwerkbeveiliging (see page 213) • 5.010 en BgZ-2a-NS-02 PvE | Netwerkbeveiliging (see page 213) • 5.050 en BgZ-2a-NS-04PvE | Netwerkbeveiliging (see page 213) • 5.060 / BgZ-2a-NS-05 PvE | Netwerkbeveiliging (see page 213)
1.4.0 – 18	De eisen aan communicatiepatronen en generieke functies zijn van de zorgtoepassing (BgZ) naar PvE pagina's in de kern verplaatst. De eisen zijn qua identificatie en inhoud niet aangepast, tenzij dit expliciet als ander item in de release-informatie is opgenomen.	Z1.5 | BgZ: PvE (see page 377) en 10.4 | Kern Volume 1b – Technical Agreements – GF (see page 203)
1.4.0 – 17	**Id-01** aangevuld met de eis dat een id uniek moet zijn en blijven in lijn met wat er al in het vertrouwensmodel stond.	PvE | Identificatie en authenticatie (see page 204)
1.4.0 – 16	Correctie systeem-identifiers in de *Authorization scope*.	Twiin-07 | Token Request (see page 270)
1.4.0 – 15	Correctie systeem-identifiers voor **requester.onBehalfOf.identifier** en **owner.identifier** in de *Send Notification Task*.	10.5.1 | Twiin-01 | Send Notification Task (see page 217)
1.4.0 – 14	De naam valueString bij verschillende comments bevatte een slash ("/"). Dit was incorrect en is aangepast om verwarring te voorkomen.	Z1.4.2 | BgZ: FHIR Workflow Task implementation (see page 347)

Release – Nr	Betreft	Verwijzing
1.4.0 – 13	Het hoofdstuk *Missie, visie en doelstellingen* is aangevuld met uitleg over de missie en verduidelijking van de doelstellingen. De tekst in dit hoofdstuk over het verbinden van zorgnetwerken door middel van knooppunten en generieke functies is weggelaten om dubbeling te voorkomen met het hoofdstuk *Architectuur*. De subpagina over de relatie tot EHDS, Wegiz, NVS, LVS en LDN is weggelaten. Voor EHDS en Wegiz om dubbeling te voorkomen met het hoofdstuk *Juridische context*. De tekst over NVS, LVS en LDN is verplaatst naar de website. Uitleg over deze ontwikkelingen kan beter worden gegeven via de Twiin-website. Beslissingen over eventuele aanpassing van het Twiin Afsprakenstelsel op basis van deze ontwikkelingen worden bovendien uitsluitend genomen conform het reglement en het releasebeleid.	3 | Missie, visie en doelstellingen (see page 35)
1.4.0 – 12	Hoofdstukken 1-3 zijn geredigeerd. Teksten zijn ingekort en dubbelingen zijn verwijderd. Uitleg is toegevoegd dat het afsprakenstelsel is onderverdeeld in een generiek en een specifiek deel. Verduidelijkt is dat redactionele wijzigingen niet worden benoemd als deze beperkt zijn zoals bij herstel van typfouten en evidente verschrijvingen. Het overzicht met relevante hoofdstukken per doelgroep is verduidelijkt.	Twiin Afsprakenstelsel 1.4.1 (see page 1) 1 | Leeswijzer (see page 3) 1.1 | Doelgroepen (see page 3) 2 | Release-informatie (see page 9) 3 | Missie, visie en doelstellingen (see page 35)
1.4.0 – 11	Het proces incidentmelding is aangepast met een plicht om een root cause analysis te verstrekken. Aanvulling over AVG-verzoeken.	8.3.1 | Incidentmelding (see page 137)
1.4.0 – 10	Bij de afspraken over Token Request ontbrak het punt 'Aanscherping voor het bepalen van de scope wanneer de patiëntcontext wel of niet bekend is: gebruik van system of patiënt' in de releasenotes v1.3.1. Dit is nu toegevoegd.	Twiin-07 | Token Request (see page 270)
1.4.0 – 9	Tekstuele verduidelijkingen aangebracht en diagramstijl in de beschrijving van het communicatiepatroon Notified Pull gelijk getrokken.	10.1.4 | Communicatiepatroon: Notified Pull (see page 177)

Release – Nr	Betreft	Verwijzing
1.4.0 – 8	De pagina met functionele use cases in de kern is verwijderd. Het voegde daar niet veel toe. De beschrijving van functionele use cases staan beschreven in de zorgtoepassingen.	
1.4.0 – 7	Verwijzing naar de BgZ zoals beschreven staat in de technische implementatie gids van Nictiz geüpdatet naar versie 1.1.	Z1.4 | BgZ: Volume 3 – Content (see page 345)
1.4.0 – 6	Enkele aanpassingen op de *Begrippenlijst*: • Verwijzing naar externe bronnen is herzien • Definitie van het begrip *Bewijs van Validatie* is toegevoegd, met differentiatie voor GtK en voor Twiin Deelnemer. • Begrip *Twiin Beheerorganisatie* is toegevoegd. • Begrip *Twiin Samenwerkingsverband* is toegevoegd. • Begrip *Verklaring Twiin Dienstverlener* is toegevoegd. • Begrip *Verklaring GtK Beheerder* is toegevoegd. • Begrip *Verklaring GtK Leverancier* is toegevoegd. • Begrip *Geïdentificeerde Patiënt* is komen te vervallen. • Begrip *Governance* is komen te vervallen. • Begrip GtK Leverancier is korter omschreven als Leverancier van een GtK. Zie ook 1.4.0 – 46. • Diverse begrippen zijn aangescherpt.	1.2 | Begrippen (see page 5)
1.4.0 – 5	De inleiding *Communicatiepatroon Overview* is licht herschreven.	10.1 | Kern Volume 0a – Communicatiepatroon Overview (see page 169)

Release – Nr	Betreft	Verwijzing

1.4.0 – 4	Voorwaarden Twiin Deelnemer herschreven:
	• Eerst kon de tekst geïnterpreteerd worden dat ook andere zorgverleners en zorgaanbieders door de deelnemer geïdentificeerd moesten worden. Dat hoeft de deelnemer niet te doen, daar zijn de andere partijen verantwoordelijk voor. Ook is de identificatie van de zorgverlener en die van de deelnemer zelf (zorgaanbieder) gesplitst over 5.8 en 5.9.
	  • 5.8 De Twiin Deelnemer zorgt voor het eenduidig identificeren van de eigen zorgverleners bij gebruik van het GtK. Deelnemer zorgt voor identificatie van zorgverleners op basis van UZI als dit mogelijk is. Als dit niet kan is een ander identifier van de zorgverlener ook toegestaan (bijvoorbeeld het eigen medewerkernummer i.c.m. het URA. Deze identifier moet uniek voor de zorgverlener zijn én blijven).
	  • 5.9 De Twiin Deelnemer identificeert zichzelf met het UZI-Register Abonneenummer (URA).
	• Voorwaarde 5.15 is aangepast. Deze verwijst niet langer naar Mitz als verplichte oplossing voor lokalisatie. Als gevolg is voorwaarde 5.16 komen te vervallen. Na de aanpassing van 5.15 waren beide voorwaarden namelijk identiek zodat er geen reden was om 5.16 te behouden.
	• Voorwaarde 5.11 is aangepast. 5.11 kon worden geïnterpreteerd dat de Twiin Deelnemer (de zorgaanbieder) zelf een identificatiemiddel dat voldoet aan eIDAS hoog moest gebruiken. De bedoeling is dat de zorgverleners deze identificatiemiddelen gebruiken.
	• Waar eerder gesproken werd over gebruikers van het GtK, wordt nu specifiek gesproken over zorgverleners om verwarring met beheerders te voorkomen.
		9.1 | Voorwaarden Twiin Deelnemer (see page 142)

Release – Nr	Betreft	Verwijzing
1.4.0 – 3	Hoofdstuk 5 over het vertrouwensmodel is geredigeerd. Er zijn afbeeldingen toegevoegd om de onderlinge samenhang van de zeven vertrouwensfuncties te duiden. Ook is er in het hoofdstuk meer aandacht voor de samenhang tussen het vertrouwensmodel en de andere hoofdstukken van het afsprakenstelsel. Het schema is aangepast. Het bevat niet langer een samenvatting van de zeven vertrouwensfuncties om dubbeling met de onderliggende hoofdstukken te voorkomen. In het schema is per vertrouwensfunctie de relevante NEN-norm en de relevante voorwaarde vermeld.	5 | Vertrouwensmodel (see page 56)
1.4.0 – 2	In de onderdelen van het vertrouwensmodel stond in iedere tabel eerst 'principe' waar 'vereiste' was bedoeld. Dat is nu aangepast. Bij 'verantwoordelijkheid' staat nu '(verwerkings)verantwoordelijkheid' aangezien het ook om de AVG verantwoordelijkheid gaat.	5.1 | Vertrouwen: Identificatie (see page 62) 5.2 | Vertrouwen: Authenticatie (see page 65) 5.3 | Vertrouwen: Autorisatie (see page 70) 5.4 | Vertrouwen: Behandelrelatie (see page 72) 5.5 | Vertrouwen: Toestemming (see page 74) 5.6 | Vertrouwen: Logging (see page 76) 5.7 | Vertrouwen: Transparantie (see page 78)

Release – Nr	Betreft	Verwijzing
1.4.0 – 1	Herstructurering van de technische kern. De technische kern is voorbereid op het kunnen integreren van landelijk afgesproken generieke functies, waar de samenwerkingspartners van Twiin nu nog eigen afspraken maken over een tijdelijke invulling. Volume 0 : De functionele, technologie-agnostische beschrijving van communicatiepatronen en generieke functies Volume 1 : De technische implementatie afspraken (Technical Agreements) van communicatiepatronen en generieke functies. Let op dat er mogelijk meerdere technische implementaties kunnen zijn van één communicatiepatroon of generieke functie (SOAP of REST, SAML of oAuth). Volume 2: De individuele transacties die gebruikt worden in de TA's. Let hierbij op dat sommige transacties eerst onder de uitwerking van een communicatiepatroon stonden nu verplaatst zijn naar het kopje transacties generieke functies. De structuur van de Twiin Implementatiewijzer Zorgtoepassingen is ook aangepast om dezelfde structuur te volgen.	10 | Technische kern (see page 164) 10.1 | Kern Volume 0a – Communicatiepatroon Overview (see page 169) 10.2 | Kern Volume 0b – Generieke functies (see page 179) 10.3 | Kern Volume 1a – Technical Agreements – CP (see page 185) 10.4 | Kern Volume 1b – Technical Agreements – GF (see page 203) 10.5 | Kern Volume 2a – Transactions – CP (see page 217) 10.6 | Kern Volume 2b – Transactions – GF (see page 264) Twiin Implementatiewijzer Zorgtoepassingen (see page 294)
	Patch Release 1.3.1	
1.3.1 – 11	Tijdelijke afspraken zijn toegevoegd voor de plek van de activity definition in de dikke en dunne notificatie in afwachting tot expliciete afspraken in de TA Routering.	10.5.1 | Twiin-01 | Send Notification Task (see page 217) en 10.5.3 | Twiin-03 | Get Workflow Task (see page 228)

Release – Nr	Betreft	Verwijzing
1.3.1 – 10	Voor de token request zijn nieuwe aanvullende afspraken gemaakt: • Een acces token mag maximaal 15 minuten geldig zijn. • Gebruik van jti (JWT ID) is omschreven: hergebruik is niet toegestaan • Een client assertion mag maximaal 5 minuten geldig zijn. • Drie signature algoritmes zijn gespecificeerd voor gebruik binnen Twiin met de expliciete eis om andere algoritmes af te wijzen. • Formaat voor OID en URA als identifier is scherper gesteld bij de user_role, authorizer en patient claims • Parameter voor scope en bijbehorende URL-encoding zijn toegevoegd bij het acces token request	Twiin-07 | Token Request (see page 270)
1.3.1 – 9	Details rondom transacties zijn van 10.2.5 verplaatst naar en geconsolideerd in 10.3.7	10.4.2 | TTA FHIR – Authorization (see page 206) en Twiin-07 | Token Request (see page 270)
1.3.1 – 8	Input:authorization:base kent nu een kardinaliteit van 1..1	10.5.1 | Twiin-01 | Send Notification Task (see page 217)
1.3.1 – 7	European Health Dataspace (EHDS) is toegevoegd aan het overzicht van wet- en regelgeving	7 | Juridische context (see page 102)
1.3.1 – 6	Externe link geüpdatet over lokatie PKIo certificaat gegevens (CRL)	PvE | Netwerkbeveiliging (see page 213) eis 5.070
1.3.1 – 5	Afspraken over de cancel notification beter toegelicht (in navolging van change 1.3 – 25). • Het versturen van een cancel notification is optioneel en niet verplicht • Het ontvangen van een cancel notification en het bevestigen hiervan is wel verplicht • Over de inhoudelijke verwerking van een cancel notification doet Twiin momenteel geen uitspraak.	Z1.1.1 | Uitwisseling BgZ bij verwijzing of overdracht (see page 297) aangevuld met een alinea over het annuleren van het verzoek om de BgZ op te vragen. BgZ-2b-trans-06 is optioneel gemaaktZ1.5 | BgZ: PvE (see page 377) 10.5.2 | Twiin-02 | Cancel Notification Task (see page 225) en daarmee ook Z1.3.2 | Twiin-02 | Cancel BgZ Notification Task (see page 324)

Release – Nr	Betreft	Verwijzing
1.3.1 – 4	Aanscherping gebruik TLS-algoritmes. Er wordt enkel gebruik gemaakt van TLS-versies en -algoritmen die zijn geclassificeerd als "goed". Algoritmes van het niveau “voldoende” mogen niet meer gebruikt worden. Ook alle genoemde algoritmes dienen ondersteund te worden.	Wijziging van eis 5.030 in PvE | Netwerkbeveiliging (see page 213) Aanvulling in 10.4.7 | Network level security (see page 211) dat het Twiin afsprakenstelsel aangepast zal worden als genoemde algoritmes worden gedeclassificeerd naar “voldoende” of “uit te faseren”.
1.3.1 – 3	DNSSEC dient ondersteund te worden. Nieuwe eisen in PvE | Netwerkbeveiliging GTK: 5.080 en 5.090	PvE | Netwerkbeveiliging (see page 213)
1.3.1 – 2	9.4 nieuwe eis 1.4: De GtK Leveranciers hebben beleid m.b.t. reguliere scans van stacks en het beleid m.b.t. encryptie conform NEN 7510:2024.	9.4 | Voorwaarden GtK (see page 162)
1.3.1 – 1	Scherper beschreven naar welke onderdelen van de autorisatierichtlijn BgZ wordt verwezen. Het gaat om een samenvoeging van twee tabellen uit de autorisatierichtlijn: de autorisatiematrix uit paragraaf 3.5.3 en de arts-specialisaties (rolcode 01.*) uit tabel uit paragraaf 3.4.	Z1.4.4 | BgZ: Autorisatie (see page 374)
	18 Dec 2024 Minor Release 1.3.0	
1.3 – 26	Formaten systeem-identifiers toegevoegd.	10.4.2 | TTA FHIR – Authorization (see page 206)
1.3 – 25	Verduidelijkt dat Cancel Notification Task wél ontvangen moet kunnen worden, maar niet verwerkt hoeft te worden.	10.5.2 | Twiin-02 | Cancel Notification Task (see page 225)
1.3 – 24	De term GtK Beheerder aangepast. De Twiin Deelnemer is verantwoordelijk voor het beheer. De beheerder is uitvoerder (in opdracht van de Twiin Deelnemer).	(TA141) Begrip: GtK Beheerder

Release – Nr	Betreft	Verwijzing
1.3 – 23	Routering. • In het notified pull communicatiepatroon kan een parameter opgenomen worden die aangeeft voor welke afdeling een notificatie bedoeld is. • Partijen die dit nodig achten zullen de parameterlijst met hun mede deelnemers moeten delen. Dit is een tijdelijke oplossing totdat de bouwsteen Technische Afspraak Routering (Routing) in het Twiin Afsprakenstelsel is opgenomen. • Het proces van het informeren van de Twiin Beheerorganisatie over GtK endpoint informatie opdat deze in in ZORG-AB gepubliceerd kunnen worden.	10.2.5 | Generieke functie – Adressering (see page 184) 10.4.5 | TTA – Addressing (see page 210) 10.5.1 | Twiin-01 | Send Notification Task (see page 217) 9.1 | Voorwaarden Twiin Deelnemer (see page 142) 5.19 Z1.5 | BgZ: PvE (see page 377) BgZ-3-10
1.3 – 22	Nieuwe begrippen toegevoegd aan de begrippenlijst: (TA141) Begrip: Servicedesk Twiin Deelnemer, (TA141) Begrip: Incident, (TA141) Begrip: Twiin Serviceportaal	1.2 | Begrippen (see page 5)
1.3 – 21	Verwijzing naar eIDAS betrouwbaarheidsniveau's toegevoegd.	7 | Juridische context (see page 102) (onder eIDAS)
1.3 – 20	Maximale termijn waarbinnen BgZ nog geraadpleegd mag worden bij een verwijzing of overdracht: 1 jaar.	Z1.1.1 | Uitwisseling BgZ bij verwijzing of overdracht (see page 297) Z1.5 | BgZ: PvE (see page 377) eis BgZ-3-9
1.3 – 19	Technische kern – logging geactualiseerd n.a.v. status NEN7513:2024. In deze nieuwe versie van de norm is een tabel toegevoegd met te loggen items in de expliciete context van gegevensuitwisseling. Verder is de norm in lijn gebracht met de internationale ISO norm, dit kan ook impact hebben op de logging voor lokale toegang op het medisch dossier (maar dat ligt buiten de scope van het Twiin afsprakenstelsel).	10.2.4 | Generieke functie – Logging (see page 182) PvE | Logging (see page 209)
1.3 – 18	Zorgtoepassingen Verpleegkundige overdracht en Geboortezorg zijn verplaatst naar het ontwikkelsupplement. De toelichtende tekst is geactualiseerd.	[Publicatie van het ontwikkelsupplement volgt bij publicatie van release 1.3] Zie ook: 6.5 | Releasebeleid (see page 97)

Release – Nr	Betreft	Verwijzing
1.3 – 17	GZN-eisen voor verbindingen tussen de GtK's vervalt en zijn vervangen door neutrale eisen voor veilig-netwerk die volgen uit NEN7512. Zie specifiek de vijf punten in Voorwaarden GtK nr. 1.3. Deze eisen zijn omschreven als minimum-eisen waarbij per Zorgtoepassing aanvullende eisen kunnen worden gesteld. De Voorwaarden GtK Beheer zijn aangepast als volgt: • Voorwaarde nr. 2.3 is aangevuld. SLA moet ook zien op beschikbaarheid; • Voorwaarde nr. 5.1 is aangevuld. SLA moet ook zien op incidentafhandeling en beschikbaarheid zoals uitgewerkt per zorgtoepassing; • Voorwaarde nr. 5.2 is daarmee komen te vervallen. Inleiding generieke functie – netwerkbeveiliging toegevoegd	9.1 | Voorwaarden Twiin Deelnemer (see page 142), 9.4 | Voorwaarden GtK (see page 162), 9.3 | Voorwaarden GtK Beheer (see page 155) Z1.5 | BgZ: PvE (see page 377) BgZ-3-11, 10.2.7 | Generieke functie – Netwerkbeveiliging (see page 185)
1.3 – 16	Reglement geüpdatet op een aantal punten: leden overlegtafels zijn geïnformeerd, onafhankelijk voorzitter, aanpassing Reglement via nieuwe release, jaarlijkse evaluatie overlegstructuur, notulen binnen twee weken beschikbaar, bij afwezigheid eventuele input schriftelijk indienen, geen bezwaar tegen besluiten in geval van vertegenwoordiging, jaarlijkse agendapunten zijn de nieuwe release en release roadmap.	6.6 | Reglement (see page 98)
1.3 – 15	Deelnemersovereenkomst aangepast op de volgende punten: • In artikel 1.a zijn de definities GtK en GtK Beheerder meer in lijn gebracht met de uitleg van de begrippen in hoofdstuk 1.2 Afsprakenstelsel; • In artikel 2.a en 7.b is een link gemaakt naar Reglement om duidelijk te maken dat dit het kader is voor (inspraak op de) doorontwikkeling van het afsprakenstelsel; • In artikel 10.a is expliciet verwoord dat deelnemers zelf niet alleen hun eigen kosten dragen, maar ook zelf verantwoordelijk blijven en daarmee dus ook aansprakelijk en moeten zorgen voor een adequate verzekering.	6.1 | Deelnemersovereenkomst (see page 84)

Release – Nr	Betreft	Verwijzing
1.3 – 14	De bestaande Verklaring GtK Leverancier toegevoegd aan hoofdstuk governance en een proces toegevoegd voor het verkrijgen van die verklaring.	6.4 | Verklaring GtK Leverancier (see page 95) 8.1.4 | Aansluiten GtK Leverancier (see page 126)
1.3 – 13	Uitgewerkt dat de communicatiepatronen twee typen kennen: verzenden en raadpleegbaar maken, waarbij er per type communicatiepatroon verschillende eisen gelden in het vertrouwensmodel en in de Voorwaarden Twiin Deelnemer. Uitleg toegevoegd aan het hoofdstuk juridische context dat deze typen bepalen of sprake is van een elektronisch uitwisselingssysteem zoals bedoeld in de Wabvpz.	5 | Vertrouwensmodel (see page 56), 7 | Juridische context (see page 102), 9.1 | Voorwaarden Twiin Deelnemer (see page 142) 10.1 | Kern Volume 0a – Communicatiepatroon Overview (see page 169)
1.3 – 12	Definitie van identificatie aangescherpt. Ook is aangepast dat het wetsvoorstel Diaz inmiddels in behandeling is. Aangepast dat op basis van een organisatiespecifiek medewerkersnummer andere partijen niet *zelfstandig onafhankelijk* de identiteit van de gebruiker kunnen verifiëren	5.1 | Vertrouwen: Identificatie (see page 62), 5 | Vertrouwensmodel (see page 56)
1.3 – 11	Verhelderd dat veronderstelde toestemming is toegestaan bij de use case verwijzen en daarnaast in een beperkt aantal andere situaties waaronder in een noodsituatie. Verder verhelderd dat WGBO-toestemming nodig is bij de use case opvragen dossier.	5.5 | Vertrouwen: Toestemming (see page 74), 9.1 | Voorwaarden Twiin Deelnemer (see page 142)
1.3 – 10	Het hoofdstuk met de juridische context is aangevuld met een overzicht van de actuele stand van zaken van de NEN EGIZ normen en met de Begiz.	7 | Juridische context (see page 102)

Release – Nr	Betreft	Verwijzing
1.3 – 9	Nr. 1.2 van de Voorwaarden Twiin Deelnemer aangevuld ter verduidelijking dat de (sub)verwerkersovereenkomst moet voldoen aan artikel 28 AVG. Nr. 2.4 aangepast om duidelijk te maken dat Deelnemer beschikt over een NEN7510 of een andere vergelijkbare verklaring. Nr. 2.6 aangepast dat een deelnemer de patiënt met een verkeerd geadresseerd AVG-verzoek 'zo mogelijk' doorverwijst naar de juiste deelnemer in plaats van 'onverwijld'. De voorwaarden 5.12 en 5.13 samengevoegd in één nieuwe voorwaarde 5.12 ter verduidelijking dat de autorisatieafspraken worden gevolgd zoals beschikbaar voor de Zorgtoepassing. De voorwaarde 5.15 aangepast om duidelijk te maken dat vastleggen van veronderstelde toestemming niet verplicht is.	9.1 | Voorwaarden Twiin Deelnemer (see page 142)
1.3 – 8	Update H3.1 Twiin in relatie tot Wegiz, NVS,LVS en LDN	3.1 | OUD Twiin in relatie tot EHDS, Wegiz, NVS, LVS en LDN
1.3 – 7	Autorisatieafspraken aangepast. De verzendende partij moet de autorisatierichtlijn BgZ toepassen (was eerst de ontvanger). De GtK-verzender mag vervolgens wel vertrouwen op de interne autorisatieregels bij de GtK-ontvanger. Wijziging van: • Functionele beschrijving Z1.5 | BgZ: PvE (see page 377) ; preconditie toegevoegd dat de behandelend arts geautoriseerd is; • Autorisatie BgZ https://vzvz.atlassian.net/wiki/pages/resumedraft.action?draftId=205554695 : toelichting gegeven. • Eis BgZ-2a-AA-11 • User_ID is verplicht om altijd mee te sturen. User_role en subrole zijn conditioneel verplicht: 10.4.2 | TTA FHIR – Authorization (see page 206) • Aanscherping vertrouwensmodel: https://vzvz.atlassian.net/wiki/pages/resumedraft.action?draftId=29630159	Z1.1.1 | Uitwisseling BgZ bij verwijzing of overdracht (see page 297) , Z1.4.4 | BgZ: Autorisatie (see page 374) , Z1.5 | BgZ: PvE (see page 377) ,10.2.2 | Generieke functie – Autorisatie (see page 180) , 10.4.2 | TTA FHIR – Authorization (see page 206) ,5.3 | Vertrouwen: Autorisatie (see page 70)

Release – Nr	Betreft	Verwijzing
1.3 – 6	De eerdere lijst met uitgangspunten voor gemeenschappelijke voorzieningen is nu een lijst met voorwaarden en daaraan is toegevoegd dat er eisen gelden voor het beheer van die gemeenschappelijke voorzieningen. Aan principe 8 de uitleg toegevoegd dat internationale standaarden in lijn moeten zijn met toepasselijke wet- en regelgeving.	4 | Architectuur (see page 37) 4.2 | Twiin Principes (see page 38)
1.3 – 5	Toegevoegd dat het hervalideren van Twiin Deelnemer ook kan plaatsvinden als dat nodig is op basis van het proces handhaving. Link toegevoegd naar het proces handhaving. Er is verschil aangebracht in het Bewijs van Validatie Twiin Deelnemer en het Bewijs van Validatie GtK. Verduidelijkt dat de Twiin Dienstverlener de relevante documentatie voor validatie kan aanleveren voor de Twiin Deelnemer.	8.2.1 | Validatie Twiin Deelnemer (see page 128)
1.3 – 4	Begrip Bewijs van Validatie GtK is toegevoegd om onderscheid te kunnen maken met het Bewijs van Validatie Twiin Deelnemer. Toegevoegd dat het hervalideren van GtK ook kan plaatsvinden als dat nodig is op basis van het proces handhaving. Link toegevoegd naar het proces handhaving.	8.2.2 | Validatie GtK (see page 132)
1.3 – 3	Proces incidentmelding en proces handhaving toegevoegd ter uitwerking van de dienst ketenregie. Indien sprake is van handhaving zullen de Overlegtafels geïnformeerd worden vanuit het oogpunt van transparantie.	8.3.1 | Incidentmelding (see page 137), 8.5 | Handhaving (see page 140)
1.3 – 2	Proces ketenregie is herzien: • Verhelderd dat de rol van de GtK Beheerder ondersteunend is aan die van Twiin Deelnemer. • Hoe eenduidige naamgeving is geborgd voor de vindbaarheid. • Link gelegd tussen ketenregie en het proces handhaving en het proces incidentmelding.	8.3 | Ketenregie (see page 136)

Release – Nr	Betreft	Verwijzing

1.3 – 1	ZT BB: Aanpassing Functioneel Overzicht,
	• functionele usecases gelijk getrokken met de meest recente Infomatiestandaard BB van Nictiz
	  • enkel de usecases die relevant zijn voor Twiin zijn opgenomen
	  • push usecases verwijderd, in afwachting van Nictiz voor uitwerking van deze usecase
		Z2.1 | BB: Volume 0 – Functioneel overzicht (see page 416)

	02 Jun 2024 Patch Release 1.2.1. In deze patch release zijn enkele teksten en begrippen aangescherpt en verbeterd.	
1.2.1 – 25	Aanscherping verhouding Twiin tot gemeenschappelijke voorzieningen met de toevoeging dat de Twiin Organisatie zich inspant om op landelijk niveau te participeren in de discussies zoals in het DTO, het IB en bij de normerkingstrajecten van de NEN en deze te ondersteunen door kennis in te brengen. De pagina Architectuur is geredigeerd; specifiek de paragraaf over Generieke Functies en Gemeenschappelijke voorzieningen. Daar stond ook een verwijzing naar landelijke ontwikkelingen wat een onnodige dubbeling was.	4 | Architectuur (see page 37) 3.1 | OUD Twiin in relatie tot EHDS, Wegiz, NVS, LVS en LDN
1.2.1 – 24	Fouten in de autorisatietabel hersteld betreffende rolcodes i.r.t. autorisatierichtlijn. De volgende rollen waren abusievelijk overgenomen uit de autorisatierichtlijn BgZ: • Gezondheidszorgpsycholoog (25.000) • Klinisch psycholoog (25.061) • Klinisch neuropsycholoog (25.063) • Verpleegkundige (30.000) Deze rollen zijn allen **niet** geautoriseerd om de BgZ te versturen of op te vragen.	Z1.4.4 | BgZ: Autorisatie (see page 374)
1.2.1 – 23	Toepassen juiste terminologie (Resource Server → Responding GtK)	10.5.3 | Twiin-03 | Get Workflow Task (see page 228)
1.2.1 – 22	URA moet in de notificatie staan. [Red. Dit was nog een oud issue en was al doorgevoerd in de 1.2.0 versie.]	10.3.1 | TTA FHIR – Notified pull (see page 185)

Release – Nr	Betreft	Verwijzing
1.2.1 – 21	Toetreden deelnemer toegelicht in de zin dat deelnemer aangeeft welke Twiin Dienstverlener is betrokken.	8.1.1 | Aansluiten Twiin Deelnemer (see page 120)
1.2.1 – 20	Releasebeleid toegelicht (vaststellen omvat ook release roadmap voor onderwerpen die nog in ontwikkeling zijn)	6.5 | Releasebeleid (see page 97) , 6.6 | Reglement (see page 98)
1.2.1 – 19	Tekstuele aanpassing: Mitz kan gebruikt worden voor lokalisatie, maar dat is voor patiënttoestemming niet relevant. Deze tekst is verwijderd.	5.5 | Vertrouwen: Toestemming (see page 74)
1.2.1 – 18	Aanscherping: Zorgmedewerkers worden geïdentificeerd met een landelijk uniek nummer (die ook uniek blijft).	5.1 | Vertrouwen: Identificatie (see page 62) 9.1 | Voorwaarden Twiin Deelnemer (see page 142)
1.2.1 – 17	Naast URA ook de optionele mogelijkheid om andere identificatienummers te gebruiken. Ook toegevoegd dat men de codestelsels waaruit de identificatiecodes komen moeten worden toegevoegd.	5.1 | Vertrouwen: Identificatie (see page 62) , IHE ITI-40 | Provide X-User Assertion (see page 265) , 10.4.2 | TTA FHIR – Authorization (see page 206)
1.2.1 – 16	Principe P4 aangepast met één extra zin bij de rationale van dit principe om duidelijk te maken dat ook bij validatie gezorgd wordt dat de belasting zo beperkt mogelijk is.	4.2 | Twiin Principes (see page 38)
1.2.0 – 15	Implementatiewijzer Verpleegkundige overdracht bevat een informatieve toelichting.	OUD: Zx | VO: implementatiewijzer Verpleegkundige overdracht – 1.2.0 Informative
1.2.0 – 14	Implementatiewijzer Zorgtoepassing Geboortezorg bevat een informatieve toelichting.	Z5 | IGD: implementatiewijzer Geboortezorg 1.2.0 Informative
1.2.0 – 13	Implementatiewijzer Zorgtoepassing Beeldbeschikbaarheid herschreven in 3 volumes voor beproeving (status trial) inclusief PvE.	Z2 | BB: Implementatiewijzer Beeldbeschikbaarheid – Trial (see page 414)
1.2.0 – 12	Implementatiewijzer Zorgtoepassing Correspondentie toegevoegd in 3 volumes voor beproeving (status trial) inclusief PvE.	Z3 | COR: Implementatiewijzer Correspondentie (see page 469)

Release – Nr	Betreft	Verwijzing
1.2.0 – 11	Implementatiewijzer Zorgtoepassing BgZ herschreven in 3 volumes voor beproeving (status trial) inclusief PvE.	Z1 | BgZ: Implementatiewijzer Basisgegevensset Zorg (see page 294)
1.2.0 – 10	TA Notified Pull (Technical Agreement) Notified Pull opgenomen in het Twiin Afsprakenstelsel en zorgtoepassing BgZ.	10.3.1 | TTA FHIR – Notified pull (see page 185) Z1.2.1 | TTA Exchanging BgZ – FHIR Notified Pull (see page 302)
1.2.0 – 9	Zorgtoepassingen onderdeel afsprakenstelsel naast de " generieke kern" met eigen versienr.	Twiin Implementatiewijzer Zorgtoepassingen (see page 294)
1.2.0 – 8	Aansluit en implementatiewijzer herschreven in Technische Kern en onderverdeeld in 3 Volumes: • Volume 1 Uitwisselpatronen • Volume 2: Technical Agreements en Transacties (dit onderdeel is vanwege de doelgroep in het engels) • Volume 3: Content en metadata	10 | Technische kern (see page 164)
1.2.0 – 7	Diensten zijn geactualiseerd en herschreven. Processen zijn ondergebracht bij de bijbehorende diensten waardoor het onderdeel processen is vervallen.	8 | Diensten (see page 119)
1.2.0 – 6	Onderdeel Architectuur • Uitwerking uitwisselconcepten is verhuisd naar de Technische kern en heten nu uitwisselpatronen • Twiin als verbindend afsprakenstelsel toegelicht • Databeschikbaarheid uitgelegd	4 | Architectuur (see page 37)
1.2.0 – 5	Onderdeel Grondslag hernoemd naar Visie en volledig herschreven	3 | Missie, visie en doelstellingen (see page 35)
1.2.0 – 3	Begrip GtK verduidelijkt	(TA141) Begrip: GtK

Release – Nr	Betreft	Verwijzing
1.2.0 – 2	Voorwaarden (voorheen onderdeel van de aansluit- en implementatiewijzer) op het hoogste niveau gebracht en verbeterd, verduidelijkt, beknopter en concreter gemaakt nav ervaringen met release 1.1 bèta. Begrip en voorwaarden GtK-netwerk is vervallen en is opgenomen als eis aan het GtK.	9 | Voorwaarden (see page 142)
1.2.0 – 1	Releasebeleid toegevoegd	6.5 | Releasebeleid (see page 97)

Releasebeleid

Het releasebeleid is een onderdeel van de governance, zie 6.5 | Releasebeleid (see page 97)

Vorige versies

21 Dec 2023 **Wijzigingen Twiin Afsprakenstelsel release 1.2**

Doelstelling voor release 1.2 is dat de toevoeging bèta niet meer nodig is als:

- [x] De deelnemersovereenkomst getekend kan worden en er zijn partijen bereid om deelnemersovereenkomst te tekenen
- [x] Releasebeleid is vastgesteld
- [x] Duidelijk onderscheid maken in het afsprakenstelsel tussen het generieke deel (de core) en de zorgtoepassingen
- [x] Zorgtoepassingen hebben een eigen versie gerelateerd aan een release van het afsprakenstelsel
- [x] Update / compleet maken technische kern incl. PVE's (techniek)
- [x] De TA Notified Pull is verwerkt in het Twiin Afsprakenstelsel
- [x] Twiin afsprakenstelsel breed is geconsulteerd

Wijzigingen Release 1.1 beta

Schoning afsprakenstelsel

- Het afsprakenstelsel is geschoond. De toegepaste schoningscriteria zijn:
  - Een afsprakenstelsel is een bindende samenwerkingsovereenkomst tussen verschillende partijen waarin beschreven is aan welke afspraken en eisen wordt voldaan.
  - Een afsprakenstelsel bevat het nu, niet de toekomst. Het is dus geen doelarchitectuur. Deze wordt buiten het afsprakenstelsel vastgelegd, zodat verbeteringen op het afsprakenstelsel met RFC's kunnen worden ontwikkeld en doorgevoerd.

- Voorbeelden van schoning:
  - Meer informatie over het programma Twiin is verplaatst naar de website, zie https://www.twiin.nl/over-twiin/wat-doet-twiin
  - Conceptuele oplossingsrichtingen naar Toolkit, zie https://www.twiin.nl/twiin-afsprakenstelsel/toolkit
  - Minder submenu's
  - Andere onderdelen zijn compacter beschreven

Doelstelling afsprakenstelsel aangescherpt.

In de doelstelling van het afsprakenstelsel is nadrukkelijker beschreven dat Twiin een verbindend afsprakenstelsel is tussen bestaande zorgnetwerken, platformen, stelsels en voorzieningen

Governance

Nieuwe governance (see page 80) en daaruit voortvloeiende aanpassing in https://vzvz.atlassian.net/wiki/spaces/Twiin/pages/29594422, voorwaarden (see page 142)en GtK beschrijvingen

- Tussen Twiin en zorgaanbieder bestaat er een deelnemersovereenkomst
- Tussen de zorgaanbieder en de GtK-dienstverlener en GtK-beheerder bestaat er een dienst- c.q. beheerovereenkomst met daarin opgenomen de taken en verantwoordelijkheden van de dienstverlener respectievelijk de beheerder
- Zorgaanbieders, GtK-applicaties en GtK-netwerk worden gevalideerd
- GtK-dienstverlener en GtK-beheerders tekenen met Twiin onderling een verklaring
- In eerdere versies van het afsprakenstelsel stond GtK voor Gekwalificeerd Twiin Knooppunt. Vanaf versie 1.1 bèta worden de GtK-dienstverlener en GtK-beheerder niet meer gekwalificeerd maar volstaat een verklaring. De applicatie en het netwerk van het knooppunt wordt gevalideerd. Zie voor meer info de pagina Governance Het begrip GtK staat vanaf versie 1.1 synoniem voor een Twiin knooppunt.

Groeimodel geïntroduceerd

Twiin introduceert een groeimodel om zorgaanbieders en GtK-dienstverleners te ondersteunen bij de implementatie van het Twiin Afsprakenstelsel.

Het groeimodel zelf is GEEN onderdeel van de Twiin release 1.1 bèta. We nemen het model op in de Toolkit op https://www.twiin.nl/twiin-afsprakenstelsel/toolkit . Bij de generieke functies verwijzen we naar het groeimodel.

Navigatiekaart

Om het Twiin Afsprakenstelsel overzichtelijker te maken en eenvoudiger door het afsprakenstelsel te navigeren, is een Navigatiekaart opgenomen.

Opbouw architectuurrepository

Met release 1.1 bèta hebben we een eerste stap gemaakt met het opzetten van een architectuurrepository. Hiermee willen we de ontwikkeling en het beheer van Twiin beheersbaar maken en de samenhang en consistentie van de architectuur bevorderen. Dit gebeurt achter de schermen. In Release 1.1 bèta zie je nieuwe bijgewerkte applicatie- en transactiediagrammen bij de uitwisselconcepten.

Actueler en compacter

Verschillende onderdelen van het afsprakenstelsel zijn geactualiseerd en compacter gemaakt, onder andere:

- Juridische context en Juridisch kader (see page 102)
- Vertrouwensmodel (see page 56)geactualiseerd
- https://vzvz.atlassian.net/wiki/spaces/Twiin/pages/29608689
-
    - In lijn gebracht met het uitwisselingskompas
    - Wat in R1.0 bèta nog de gewenste situatie is genoemd bij de generieke functies heet nu “Invulling Twiin”
    - Paragraaf groeipad is verwijderd. Daarvoor in de plaats is het groeimodel gekomen
- Twiin Implementatiewijzer Zorgtoepassingen (see page 294) zijn geactualiseerd

Concreter

- Aanscherping en concretisering voorwaarden Twiin. Taken, verantwoordelijkheden, voorwaarden en eisen van de GtK rollen en de zorgaanbieder.
- Aanscherping Uitwisselconcepten en de rol van Mitz bij Push en Notified Pull

Verbeterd

- Taalkundig verbeterde teksten
- Begrippen (see page 5) zijn aangescherpt
- Twiin principe 10 aangescherpt
- Homepagina verbeterd De landingspagina is aansprekender gemaakt en geeft direct antwoord op:
    - Wat is Twiin?
    - Wat is het Twiin Afsprakenstelsel?
    - Waarom is er een Twiin Afsprakenstelsel?
    - Voor wie is het Twiin Afsprakenstelsel?
    - Hoe gebruik ik het Twiin Afsprakenstelsel?
    - Waar vind ik wat?

Technische implementatiewijzigingen

- MITZ als toestemmingvoorziening speelt geen rol meer in de uitwisselconcepten Push en Notified pull
- Op enkele tekstuele wijzigingen na, zijn er verder geen inhoudelijke wijzigingen aangebracht

Wijzigingen release 1.0 beta

Algemeen

- Release en versie beheer toegevoegd onder menu releaseinformatie (see page 9)
- Algehele tekst en lees verbeterslag op alle onderdelen en een minder diep geneste menustructuur
- PDF download afsprakenstelsel
- Aanscherping begrippenlijst (see page 5)
- Verbeterde leeswijzer (see page 3) en leeswijzer per doelgroep (see page 3)

Inhoudelijk

- Governance (see page 80)Twiin op hoofdlijn
- Uitwerking Vertrouwensmodel (see page 56)
- Gehele revisie van het onderdeel https://vzvz.atlassian.net/wiki/spaces/Twiin/pages/29608689 (gewenste situatie obv vertrouwensmodel, de huidige situatie is geschetst en een mogelijk groeipad)
- Uitwerking dienstenmodel (see page 119)
    - Implementatiediensten; Toetreding en validatiediensten (see page 128)
    - https://vzvz.atlassian.net/wiki/spaces/Twiin/pages/29601697
    - Ketenregie
- Uitwerking https://vzvz.atlassian.net/wiki/spaces/Twiin/pages/29594422
    - https://vzvz.atlassian.net/wiki/spaces/Twiin/pages/29631714
    - https://vzvz.atlassian.net/wiki/spaces/Twiin/pages/29630099
- Aanscherping, nuancering en decompositie GtK Gevalideerd Twiin Knooppunt in GtK dienstverlener, GtK beheerder, GtK applicatie en GtK-netwerk
- Aanpassing Voorwaarden (see page 142) (nav Vertrouwensmodel en aanscherping GtK)

Technische implementatiewijzigingen

- Op enkele tekstuele wijzigingen na, zijn er geen grote wijzigingen aangebracht in de implementatiewijzers.

Wijzigingen release 0.8

Ten opzichte van release 0.7 zijn de volgende zaken gewijzigd:

- Zorgtoepassing BgZ is toegevoegd
- De implementatiehandleiding Beeldbeschikbaarheid is een onderdeel gemaakt van het Twiin afsprakenstelsel. Delen zijn verplaatst naar de aansluit en implementatiewijzer kern en naar de zorgtoepassing Beeldbeschikbaarheid. Op deze manier is maximale hergebruik, beschikbaarheid, consistentie en integriteit beter geborgd.
- De indeling van het onderdeel architectuur is logischer en intuïtiever gemaakt met minder klikken
- Er is een eerste opzet gemaakt voor de diensten die Twiin gaat aanbieden.

- De aansluitvoorwaarden GtK zijn aangescherpt aan de hand van versnellingssessies eind 2020 en inzichten uit projecten Knoop. en Beeldbeschikbaarheid. Eventuele tegenstrijdigheden zijn verwijderd.
- Er is een korte termijn oplossing beschreven voor autorisatie
- De definitie van het vertrouwensmodel is toegevoegd (Governance & Vertrouwensmodel[6])
- Toegevoegd is een uitleg van hoe we omgaan met lokalisatie zolang nog niet iedereen is aangesloten op Mitz als gemeenschappelijke voorziening (Lokalisatie & toestemming)

6. https://confluence.vzvz.nl/pages/viewpage.action?pageId=56766747

3 | Missie, visie en doelstellingen

Inleiding

Zorgaanbieders wisselen onderling gegevens uit voor verschillende zorgprocessen. Hiervoor maken zij gebruik van diverse infrastructuren en koppelvlakken. Wanneer veel zorgaanbieders samenwerken, bijvoorbeeld in een netwerk, ontstaan er veel onderlinge relaties.

Sinds de Eerste Kamer in 2011 het wetsvoorstel voor het landelijke EPD heeft verworpen is er lange tijd geen regie meer geweest op het zorginformatiestelsel. Hierdoor zijn er in de loop van de jaren verschillende initiatieven ontstaan om de zorg te ondersteunen bij gegevensuitwisseling en databeschikbaarheid. Deze initiatieven sluiten veelal niet goed op elkaar aan door verschillen in de werking en inrichting van digitale oplossingen. Het Twiin Afsprakenstelsel is bedoeld om deze verschillen te overbruggen, zodat gezondheidsgegevens uiteindelijk veilig onderling gedeeld kunnen worden.

Voor goede databeschikbaarheid en gegevensuitwisseling zijn afspraken nodig – op bestuurlijk, organisatorisch, juridisch, procesmatig, semantisch en technisch niveau. Kortom: afspraken op alle lagen van het interoperabiliteitsmodel van Nictiz. Het is essentieel om op alle lagen afspraken te maken zodat uitwisseling volledig interoperabel is. Het Twiin Afsprakenstelsel voorziet hierin en behandelt alle lagen van dit model.

De Twiin Organisatie verbindt verschillende nationale en Europese initiatieven en volgt de ontwikkelingen in wet- en regelgeving, normen en standaarden. Het gaat onder meer om wet- en regelgeving rond databeschikbaarheid voor het verlenen van zorg (zie 7 | Juridische context (see page 102)) en de Nationale Strategie voor het Gezondheidsinformatiestelsel. De Twiin Organisatie volgt alle strategische besluiten die op basis van deze strategie worden genomen. Zo sluit Twiin bijvoorbeeld aan bij de Wegiz en ook bij de EHDS zodra de specificaties daarvoor beschikbaar zijn. Deze ontwikkelingen bepalen de keuzes van de Twiin Organisatie voor de doorontwikkeling van het Twiin Afsprakenstelsel.

Missie

De missie van de Twiin Organisatie is zorgen voor een afsprakenstelsel op basis waarvan zorgaanbieders onderling gezondheidsgegevens kunnen uitwisselen (delen en benaderen) en waarmee de betrouwbaarheid en de vertrouwelijkheid van die gegevens goed wordt geborgd. Hoe meer zorgaanbieders samenwerken in een keten of netwerk, hoe meer uitwisseling van gezondheidsgegevens noodzakelijk is tussen deze zorgaanbieders. Voorafgaand aan iedere uitwisseling van gezondheidsgegevens is het noodzakelijk om nadere afspraken te maken over privacy, informatiebeveiliging en het gebruik van technische standaarden. Deze afspraken moeten voortbouwen op en invulling geven aan het bestaande kader van wet- en regelgeving en normen. Het Twiin Afsprakenstelsel bevat alle noodzakelijke afspraken over de uitwisseling van gezondheidsgegevens: lokaal, regionaal en landelijk.

Visie

De visie van de Twiin Organisatie is landelijke beschikbaarheid van gezondheidsgegevens. Databeschikbaarheid draagt bij aan hogere kwaliteit van zorg, vermindert de administratieve last van zorgaanbieders en voorkomt dat kostbare tijd van zorgverleners verloren gaat aan het zoeken naar de juiste gezondheidsgegevens. Zo blijft er meer tijd over voor aandacht voor de cliënt. De zorgaanbieder heeft toegang tot alle gezondheidsgegevens die nodig zijn voor het verlenen van goede zorg. Bovendien draagt databeschikbaarheid bij aan betere samenwerking tussen zorgaanbieders.

Doelstellingen

De doelstellingen van de Twiin Organisatie zijn:

- Het maken van een afsprakenstelsel dat voortbouwt op en invulling geeft aan het bestaande kader van wet- en regelgeving en normen. De Twiin Organisatie volgt hierbij de landelijke strategische besluiten.
- Het maken van een afsprakenstelsel dat helder, toegankelijk en bruikbaar is voor zorgaanbieders, hun leveranciers en dienstverleners. Helder zodanig dat de afspraken begrijpelijk en duidelijk zijn. Toegankelijk houdt in dat het stelsel publiek beschikbaar is via Twiin.nl[7]. Bruikbaar betekent dat de afspraken daadwerkelijk toepasbaar zijn in de praktijk.
- Het maken van een afsprakenstelsel waarin alle noodzakelijk afspraken zijn opgenomen die nodig zijn om bestaande infrastructuren en voorzieningen met elkaar te verbinden en het aanbieden van ondersteunende diensten bij het gebruik van het afsprakenstelsel.
- Het maken van een afsprakenstelsel waarmee de veiligheid en betrouwbaarheid geborgd wordt, bij het beschikbaar stellen van gezondheidsgegevens met gebruik van bestaande infrastructuren en voorzieningen op basis van het Twiin Afsprakenstelsel.
- Het betrekken van zorgaanbieders, hun leveranciers en dienstverleners bij de (door)ontwikkeling en de toepassing van het Twiin Afsprakenstelsel.

7. http://Twiin.nl

4 | Architectuur

Dit hoofdstuk beschrijft de architectuur van Twiin, bestaande uit drie onderdelen: gegevensuitwisseling via Gevalideerde Twiin Knooppunten (GtK's), de structuur en samenhang van het afsprakenstelsel, en de organisatie van het (TA141) Begrip: Twiin Samenwerkingsverband. Achtereenvolgens worden achtergrond en uitgangspunten toegelicht 4.1 | Context (see page 37), de principes 4.2 | Twiin Principes (see page 38), de verwachtingen van het te bereiken resultaat 4.3 | Conceptuele architectuur (see page 45), de componenten die hiervoor nodig zijn 4.4 | Logische architectuur (see page 46) en de structuren die gebruikt worden 4.5 | Fysieke architectuur (see page 53). Wat betreft de fysieke architectuur beschrijft het Twiin Afsprakenstelsel overigens geen fysieke ICT-componenten, maar wel de organisatie van Twiin en het product: het Twiin Afsprakenstelsel. Deze indeling (contextueel, conceptueel, logisch en fysiek) komt voort uit het Integrated Architecture Framework (IAF). Sinds versie 10 onderscheidt TOGAF expliciet dezelfde abstractieniveaus.

4.1 | Context

De context beschrijft het doel van de architectuur, de verwachtingen en de uitgangspunten. De missie, visie en doelstellingen uit hoofdstuk 3 (see page 35) maken een belangrijk onderdeel uit van de context. Aanvullend daarop beschrijft deze pagina de visie op het uitwerken van architectuur en komen in hoofdstuk 4.2 (see page 38) de Twiin Principes aan bod.

Doel

De architectuur van het Twiin Samenwerkingsverband en het Twiin Afsprakenstelsel draagt bij aan realisatie van de missie, visie en doelstellingen van de Twiin Organisatie.

Architectuurvisie

Hoe meer zorgorganisaties en zorgverleners gaan samenwerken in een keten of netwerk, hoe meer relaties er ontstaan. Deze partijen wisselen informatie uit, delen gegevens, gebruiken voorzieningen en maken afspraken. De relaties die ontstaan zijn bestuurlijk, organisatorisch, juridisch, procesmatig, semantisch en technisch van aard, en beslaan daarmee alle lagen van het interoperabiliteitsmodel.

Verbinden

Het gaat om een complexe situatie met vele zorgaanbieders, verschillende processen, informatiestromen, verschillende infrastructuren en koppelvlakken. Twiin is ontstaan om deze verschillen te overbruggen. Om dit te kunnen doen, is het belangrijk om partijen te betrekken bij het maken en doorontwikkelen van de afspraken: niet alleen voorzieningen en infrastructuren moeten verbonden worden, maar ook organisaties en mensen. De architectuur van Twiin kijkt naar het gehele zorgveld, niet alleen aangesloten deelnemers.

Interoperabiliteit

Twiin sluit aan bij het interoperabiliteitsmodel van Nictiz. Het is belangrijk om op alle lagen afspraken te maken zodat uitwisseling volledig interoperabel is. Ook Twiin onderschrijft dit model. In het afsprakenstelsel komen alle lagen van het interoperabiliteitsmodel aan bod.

Herbruikbaarheid, haalbaarheid en betrokkenheid

Het is belangrijk om de grote complexiteit bij de uitwisseling van gegevens beheersbaar te houden. Dit kan onder andere door op overeenkomsten te richten en verschillen te overbruggen. Het Twiin Afsprakenstelsel is erop gericht om zoveel mogelijk generieke, herbruikbare afspraken te maken en te zorgen voor afspraken die haalbaar zijn.

Verschillen overbruggen gaat niet vanzelf. Het is van belang dat betrokken partijen actief deelnemen aan het opstellen en doorontwikkelen van de afspraken.

4.2 | Twiin Principes

De Twiin Principes zijn fundamentele uitgangspunten, afgeleid van de missie, visie en doelstellingen, en architectuurvisie van Twiin. Ze geven richting en structuur aan het ontwerp van het afsprakenstelsel. De principes zijn voorzien van een rationale, waarin de belangrijkste ontwerp afwegingen zijn opgenomen met bijbehorende implicaties. De rationale beschrijft de reden waarom het principe van belang is. De implicatie geeft aan wat er moet gebeuren om dit principe te realiseren, vaak op organisatorisch vlak.

Titel	Omschrijving	Rationale	Implicatie
P1. Landelijke beschikbaarheid en hergebruik van gezondheidsgegevens	Landelijke en zorgbrede (domeinoverstijgende) beschikbaarheid van gegevens door zorginfrastructuren te verbinden met afspraken op alle lagen van het interoperabiliteitsmodel. Het doel is deze gegevens in te zetten voor preventie, zorg en welzijn en secundair gebruik. In eerste instantie zal de focus van Twiin vooral gericht zijn op beschikbaarheid en hergebruik binnen de zorg.	Zorg vindt steeds meer plaats in meerdere instellingen vaak over de regio's heen. Personen zijn mobiel en hebben onafhankelijk van waar ze zich bevinden binnen Nederland recht op de juiste zorg. Momenteel is de reikwijdte van de zorg vaak nog beperkt tot regionaal, lokaal of categoraal niveau.	Afstemming op alle lagen: politiek, bestuurlijk, bij (beroeps-)verenigingen, op gebied van informatiestandaarden en infrastructuren op landelijk niveau en in samenwerking met regionale en lokale organisaties. Twiin is schaalbaar en bruikbaar voor landelijke uitwisseling. Uitwisseling via knooppunten, gebruikmakend van (bestaande) gemeenschappelijke voorzieningen. Uit te breiden naar meerdere zorgtoepassingen. De architectuur van Twiin moet flexibel genoeg zijn om toekomstige (nieuwe) zorgtoepassingen te ondersteunen.

Titel	Omschrijving	Rationale	Implicatie
P2. Twiin is een vertrouwd netwerk van organisaties	Twiin is een verzameling van autonome actoren die van elkaar afhankelijk zijn om een gemeenschappelijk probleem op te lossen. Door afspraken met elkaar te maken over hoe we elkaar kunnen vertrouwen (het vertrouwensmodel (see page 56)) en deze te borgen door middel van validatie (see page 128) en technische maatregelen ontstaat onderling vertrouwen.	Om problemen op te lossen die door een enkele organisatie moeizaam of helemaal niet kunnen worden opgelost.	Twiin kent een governancestructuur met rollen, taken, verantwoordelijkheden en bevoegdheden om besluiten te nemen voor ontwikkeling en beheer. Twiin kent een afsprakenstelsel dat bestaat uit een set van samenhangende afspraken, procedures en regels op gebied van organisatie, besturing, toezicht, beheer, architectuur, toepassingen, techniek met als doel het realiseren en borgen van het vertrouwen binnen het Twiin-netwerk.
P3. Het Twiin Afsprakenstelsel leeft en blijft zich ontwikkelen	Het Twiin Afsprakenstelsel is een levend document. We groeien door ervaringen en verwerken deze in het afsprakenstelsel.	Om doorontwikkeling mogelijk te maken én te kunnen leren van tussentijdse ervaringen, volgt het afsprakenstelsel een groeipad. Om voortgang te laten zien, te gebruiken wat er al is en z.s.m. oplossingen te integreren. Daarbij is ook de haalbaarheid van realisatie, waaronder de aansluiting op de huidige ontwikkelingen in de markt, een criterium. Daar waar duidelijkheid nodig is in de afspraken die pas op termijn van kracht zijn, maar die op enig moment nog niet haalbaar zijn, kan een groeipad worden afgesproken.	Het doel van Twiin is het faciliteren van meerdere zorgtoepassingen en generieke afspraken voor het landelijk beschikbaar maken en/of uitwisselen van gegevens. Twiin heeft als ambitie om zorgdomeinbreed te faciliteren. De meerjarenagenda van de Wegiz wordt gevolgd, waarbij ook gekeken wordt naar de aanpassingen vanuit LDN, IGF en EHDS.

Titel	Omschrijving	Rationale	Implicatie
P4. De functionele behoeften van zorgverleners, zorgaanbieders en cliënten zijn leidend	De functionele behoeften van zorgverleners, zorgaanbieders en cliënten zijn leidend voor het Twiin Afsprakenstelsel.	De voornaamste drijfveer van Twiin is om invulling te geven aan de functionele behoeften van zorgverleners en cliënten op zodanige wijze dat landelijke dekking en maximaal hergebruik mogelijk is en daardoor de zorgverlener te ontlasten van registratielast en de zorg te verbeteren. Ook validatie wordt zo ingericht dat de belasting zo beperkt mogelijk is.	Keuzes die gemaakt worden bij de doorontwikkeling van Twiin worden getoetst aan de functionele behoeften van zorgverleners en zorgaanbieders.

Titel	Omschrijving	Rationale	Implicatie
P5. Deelname aan Twiin is vrijwillig, maar niet vrijblijvend	*Vrijwillig* Een zorgaanbieder besluit zelf om wel of niet aan te sluiten en voor welke zorgtoepassing dit gebeurt. *Niet vrijblijvend* Deelnemende zorgaanbieders dienen te voldoen aan de afspraken van het afsprakenstelsel.	Zorgaanbieders die aansluiten moeten er op kunnen vertrouwen dat andere aangesloten zorgaanbieders conform het afsprakenstelsel werken.	Op basis van Wegiz kunnen zorgaanbieders verplicht zijn om bepaalde gegevens digitaal uit te wisselen. Zodra de implementatietermijn is verlopen zal de EHDS zorgaanbieders verplichten om – voor de prioritaire categorieën – gegevens digitaal en gestandaardiseerd uit te wisselen. Door aansluiting bij Twiin kan dit vervolgens in de praktijk worden gerealiseerd. Elke deelnemende zorgaanbieder beoogt uitwisseling met alle deelnemers van de infrastructuur binnen de zorgtoepassing waarin wordt deelgenomen. Het afsprakenstelsel verplicht deelnemers niet om daadwerkelijk gegevens uit te wisselen. Dat is uiteindelijk aan de zorgaanbieder/cliënt. Zorgaanbieders die aansluiten hebben een inspanningsverplichting om gegevens beschikbaar te stellen.

Titel	Omschrijving	Rationale	Implicatie
P6. Keuzevrijheid voor zorgaanbieders en leveranciers	Zowel de 'bewegingsvrijheid' van zorgaanbieders, als de keuzevrijheid van beheerders en leveranciers moet zo veel mogelijk in stand worden gehouden.	De zorgaanbieder moet de vrijheid hebben in de keuze van leveranciers die het beste bij de bedrijfsprocessen past of economisch gezien het meest voordelig is. Zorgaanbieders moeten eenvoudig kunnen aansluiten, met zo min mogelijk drempels. Leveranciers hebben gelijke kansen om deel te nemen.	Twiin levert een overzicht van aansluitvoorwaarden voor zorgaanbieders, GtK Beheerders, Twiin Dienstverleners en GtK's.
P7. Privacy en Security by Design	Voor Twiin zijn privacy en informatiebeveiliging randvoorwaardelijk.	Privacy en security zijn randvoorwaardelijk en worden dan ook vanaf het begin meegenomen in het ontwerp en de ontwikkeling.	Principes en best practices van Security en Privacy by Design worden gehanteerd bij het maken en doorontwikkelen van het Twiin Afsprakenstelsel en architectuur. Informatiebeveiliging en privacy worden vanaf het begin en bij doorontwikkeling meegenomen in het vertrouwensmodel en de technische uitwerking hiervan in de kern. Ze hebben impact op alle onderdelen van het afsprakenstelsel. Iedere Twiin Deelnemer zorgt dat wordt voldaan aan de beveiligingsnormen, waaronder met name NEN 7510, NEN 7512 en NEN 7513.

Titel	Omschrijving	Rationale	Implicatie
P8. Gebruik van internationale standaarden	Hantering van internationale standaarden boven Europese en nationale standaarden Om technische interoperabiliteit te realiseren, gaat Twiin zoveel mogelijk uit van open (internationale) standaarden. Twiin maakt gebruik van bestaande en in beheer zijnde standaarden, normen en agreements.	Door gebruik van open internationale standaarden wordt de afhankelijkheid van een leverancier grotendeels voorkomen. De uitwisselbaarheid en herbruikbaarheid wordt verhoogd. Per zorgtoepassing zijn andere partijen betrokken en worden andere gegevens uitgewisseld, waardoor keuze voor een vaste techniek niet altijd de meest passende is. Open internationale standaarden worden breed gedragen en zullen in samenhang met nieuwe standaarden blijven werken (robuust). Zorg is internationaal en leveranciers van informatietechnologieën zijn internationaal.	De keuze is niet gebaseerd op één enkele techniek. Er wordt gekeken wat de juiste keuze is per 'zorgtoepassing' en naar wat mogelijk is, uitgaande van vorige principes en al in gebruik zijnde standaarden. Standaarden moeten implementeerbaar zijn in de Nederlandse setting door meerdere leveranciers en in lijn zijn met toepasselijke wet- en regelgeving. Indien nodig kan er gebruik gemaakt worden van nationale extensies of kunnen nationale extensies ontwikkeld worden. Twiin verwijst naar andere organisaties als het gaat om standaarden, zoals kwaliteitsstandaarden of informatiestandaarden. Hierdoor ontstaat een afhankelijkheid van deze standaarden. De verantwoordelijkheid voor deze standaarden ligt bij de organisaties die deze standaarden creëren en/ of beheren. Ook een eventuele kwalificatie om te voldoen aan deze standaarden ligt bij deze organisaties.

Titel	Omschrijving	Rationale	Implicatie
			Voor elke zorgtoepassing zal door het veld geanalyseerd worden of de bestaande informatiestandaard landelijk toereikend is of dat er toevoegingen moeten komen. Als er nog geen informatiestandaard is, dan wordt deze ontwikkeld (buiten Twiin) op basis van (inter)nationale standaarden.

Gehanteerde bronnen:

- Nationale Visie en Strategie (NVS)[8] en Nationale Strategie gezondheidsinformatiestelsel[9].
- In het Twiin Afsprakenstelsel zijn de basisprincipes en afgeleide principes voor het informatiestelsel voor de zorg meegenomen, zoals beschreven in het Manifest van de DIZRA[10] (Duurzaam Informatiestelsel Zorg Referentie Architectuur). Naar verwachting worden deze basisprincipes in een volgende versie van Twiin vervangen door de principes van het gezondheidsinformatiestelsel, die momenteel in ontwikkeling zijn.
- Trusted Exchange Framework and Common Agreement (TEFCA[11])
- MedMij[12]
- Ziekenhuis Referentie Architectuur[13] (ZiRA)

4.3 | Conceptuele architectuur

De conceptuele architectuur beschrijft welke vereisten een rol spelen bij het Twiin Afsprakenstelsel, wat er van het resultaat wordt verwacht waarvoor de architectuur wordt ontwikkeld. Het ‘wat’ van het afsprakenstelsel. Oftewel het resultaat dat Twiin wil bereiken.

8. https://www.rijksoverheid.nl/documenten/publicaties/2023/03/31/nationale-visie-en-strategie-gezondheidsinformatiestelsel
9. https://www.rijksoverheid.nl/documenten/publicaties/2024/10/31/nationale-strategie
10. https://dizra.gitbook.io/dizra/
11. https://www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf
12. https://afsprakenstelsel.medmij.nl/asverplicht/mmverplicht/
13. https://sites.google.com/site/zirawiki/

Databeschikbaarheid

Het Twiin Afsprakenstelsel is zo ingericht dat het bijdraagt aan databeschikbaarheid. In het Twiin Afsprakenstelsel doelen we met de term databeschikbaarheid op het volgende: data moet situationeel toegankelijk en beschikbaar zijn voor zorgaanbieders voor zover nodig voor het verlenen van zorg. Daarbij moet het mogelijk zijn om gegevens op te vragen, te raadplegen en te gebruiken. Tenminste voor zover de gebruikers er recht op hebben. De privacy en patiëntveiligheid moet geborgd blijven. Dit betekent dat het huidige versnipperde landschap met elkaar verbonden moet worden.

Samenwerking

Om de complexiteit van het zorgveld in goede afspraken te vatten, het draagvlak te vergroten en zo interoperabiliteit op alle lagen te bereiken heeft Twiin als doelstelling om zorgaanbieders, leveranciers en dienstverleners bij de (door)ontwikkeling en de toepassing van het Twiin Afsprakenstelsel te betrekken. Draagvlak en betrokkenheid zijn vereisten voor verbinding.

Implementatie

Het Twiin Afsprakenstelsel bevat afspraken om interoperabiliteit te realiseren en om de verschillende infrastructuren te verbinden. Zorgaanbieders en hun dienstverleners en leveranciers dienen zich aan de afspraken te committeren en te implementeren. Dit houdt in dat de beschreven afspraken ook daadwerkelijk toegepast en/ of uitgevoerd moeten kunnen worden (dus geen ontwikkelingen beschrijft die pas in de toekomst mogelijk zijn).

Betrouwbaar

Er moet vertrouwd kunnen worden op Twiin en op de uitwisseling die door middel van de afspraken in het afsprakenstelsel tot stand komt. Het Twiin Afsprakenstelsel moet een betrouwbare bron zijn voor degenen die er gebruik van maken. De afspraken zijn conform wet- en regelgeving en borgen door middel van privacy by design de veiligheid en betrouwbaarheid. De afspraken in het afsprakenstelsel zijn op een betrouwbare manier tot stand gekomen; er is transparantie over de totstandkoming.

4.4 | Logische architectuur

De logische architectuur beschrijft beknopt welke onderdelen nodig zijn om het resultaat te bereiken dat in de conceptuele architectuur is beschreven. De uitwerking van specificaties en eisen voor de logische architectuur is te vinden in hoofdstuk 10 | Technische kern (see page 164) (voor de generieke aspecten) en in Twiin Implementatiewijzer Zorgtoepassingen (see page 294) (aanvullende specifieke aspecten per zorgtoepassing).

In de visie en conceptuele architectuur is een belangrijk aantal eisen, uitgangspunten en principes geformuleerd (zoals bijvoorbeeld vertrouwen, implementeerbaarheid, standaardisatie en hergebruik). Om hier invulling aan te geven in de uiteindelijke oplossing heeft Twiin voor een aantal logische elementen gekozen:

- Knooppunten
- Communicatiepatronen

- Vertrouwensmodel
- Generieke functies
- Rollen

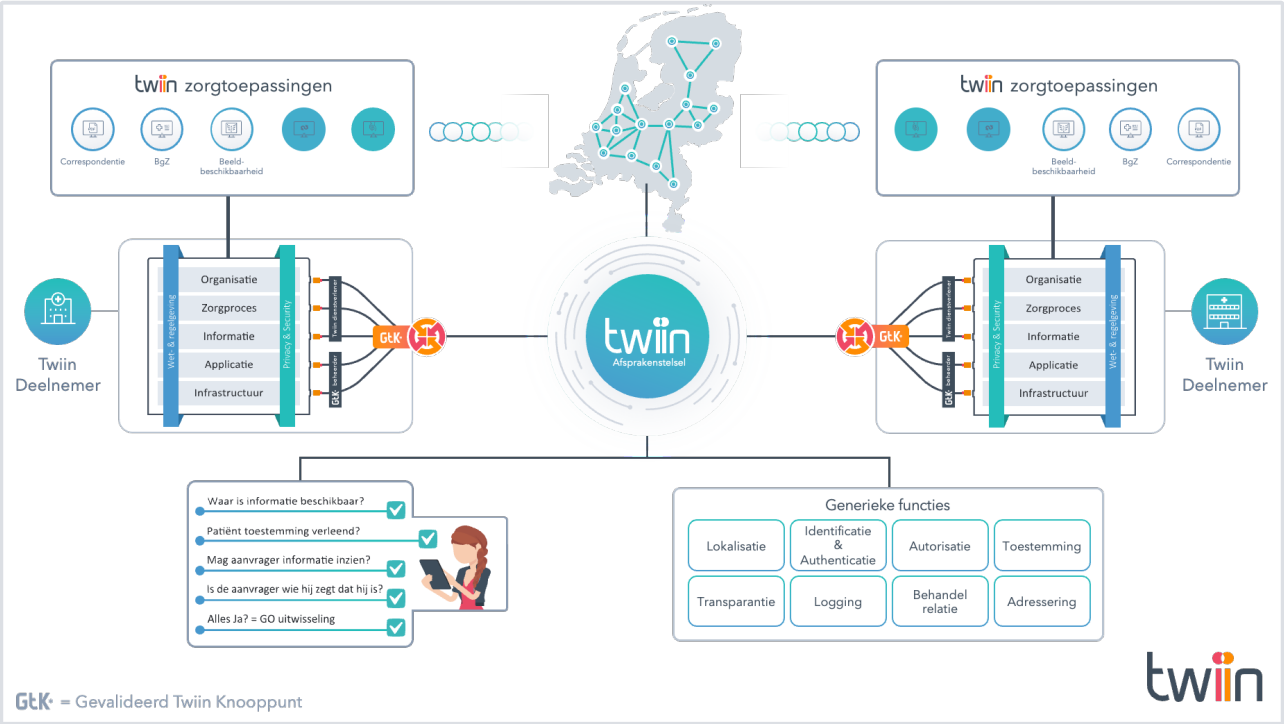
Knooppunten

Door knooppunten (koppelvlakken) te kiezen waarlangs communicatie loopt bestaan er duidelijke elementen in de architectuur die aan bepaalde afspraken voldoen. Knooppunten geven op deze manier invulling aan het verminderen van complexiteit, het gebruik van generieke componenten en standaardisatie. Door landelijk te werken met knooppunten die aan alle vereisten voldoen kan uiteindelijk een landelijk dekkend netwerk worden gevormd.

> De begrippen knooppunt en gemeenschappelijke voorzieningen zijn geïnspireerd op de visie op zorginfrastructuren (Mallie e.a. 2019)[14], maar ook op oplossingen in het buitenland, zoals Carequality (2019)[15] en TEFCA (2019)[16] in de USA of ELGA (2017)[17] in Oostenrijk. Door knooppunten en gemeenschappelijke voorzieningen te implementeren, worden bestaande netwerken, voorzieningen en infrastructuren verbonden en hergebruikt.

Uitwisseling van data gebeurt volgens het Twiin Afsprakenstelsel tussen Gevalideerde Twiin Knooppunten (GtK). Een GtK is een door Twiin gevalideerd koppelvlak dat zorgt voor beschikbaarheid en uitwisseling van gegevens voor één of meer zorgtoepassingen voor één of meerdere zorgaanbieders.

14. https://infoizo.nl/ibieb/presentatie-platform-izo-080319-visie-op-landelijke-samenhang-van-zorginfrastructuren-martijn-mallie-arteria-consulting#:~:text=een%20belangrijke%20voorziening.-,%E2%80%9C,de%20inhoud%20van%20de%20gegevensuitwisseling.%E2%80%9D&text=Afsprakenstelsel%20MedMij%2C%20AORTA%20en%20XDS,informatie%2D%20standaard%20toe%20te%20sturen.&text=Netwerk%2D%20en%20ketenzorg%20worden%20gemeengoed.&text=De%20knooppunten%20en%20gemeenschappelijke%20diensten,(zorgaanbieders%2C%20pati%C3%ABnten%20etc.)
15. https://carequality.org/
16. https://www.healthit.gov/topic/interoperability/policy/trusted-exchange-framework-and-common-agreement-tefca
17. https://www.elga.gv.at/en/about/



Bovenstaande figuur laat zien dat Twiin zich richt op zorgtoepassingen voor de landelijke beschikbaarheid van gezondheidsgegevens. Bestaande regionale, landelijke, categorale zorgnetwerken worden met elkaar in verbinding gebracht via knooppunten door afspraken en gemeenschappelijke voorzieningen. Bij elke uitwisseling, of het beschikbaar stellen van gegevens, zijn controlemechanismen ingebouwd die aansluiten bij wet- en regelgeving.

Communicatiepatronen

Er zijn verschillende communicatiepatronen. In onderdeel 10.1 | Kern Volume 0a - Communicatiepatroon Overview (see page 169) worden de vier communicatiepatronen die van belang zijn voor Twiin verder uitgewerkt:

Communicatiepatroon	Naam van de technische afspraak	Type gegevensuitwisseling	Initiatiefnemer
Gericht verzenden	Push	Verzenden	Verzender
Gericht beschikbaar stellen	Notified Pull	Verzenden	Verzender
Gericht bevragen	Pull	Raadpleegbaar maken / raadplegen	Ontvanger

Ongericht bevragen	Indexed Pull	Raadpleegbaar maken / raadplegen	Ontvanger

> Genoemde communicatiepatronen sluiten aan bij de communicatiepatronen die beschreven zijn in de whitepaper *Communicatiepatronen: de ontwikkeling naar generieke afspraken*[18] versie 1.1 van VWS.

De communicatiepatronen vallen uiteen in twee typen gegevensuitwisselingen. Functioneel wordt dit onderscheid bepaald door de initiator van de communicatie. Het gaat hierbij om verzenden en raadplegen. Als de initiator de houder van de gegevens is, dan wordt gesproken over verzenden. Als de initiator niet de houder van de gegevens is, dan wordt functioneel gesproken over raadplegen.

Dit onderscheid in typen gegevensuitwisselingen is ook een juridisch onderscheid. De wet stelt bijzondere eisen aan een elektronisch uitwisselingssysteem zoals bedoeld in de Wabvpz. Bij het raadpleegbaar maken van gegevens is sprake van een elektronisch uitwisselingssysteem. Dit is verder uitgelegd in het juridische kader (see page 104) bij de tekst over Wabvpz.

Vertrouwensmodel

Bij de uitwisseling van gegevens is betrouwbaarheid en vertrouwen essentieel. Twiin heeft de vertrouwensfuncties die hierbij horen beschreven in het Vertrouwensmodel.

Generieke functies

Om complexiteit te verminderen en tegelijkertijd te standaardiseren is het belangrijk om generieke aspecten te onderkennen. Generieke functies zijn functies die voor meerdere toepassingsgebieden nodig zijn om vindbaarheid, toegankelijkheid, interoperabiliteit of hergebruik van gegevens te kunnen realiseren.

Vaak worden generieke functies (zoals identificatie, authenticatie, autorisatie, lokalisatie, adressering, toestemming en logging) en gemeenschappelijke voorzieningen in één adem genoemd, maar ze zijn niet hetzelfde. De noodzaak om de generieke functies in te vullen is blijvend. De wijze waarop daar invulling aan wordt gegeven door middel van gemeenschappelijke voorzieningen, kan in de loop der tijd wijzigen.

Gemeenschappelijke voorzieningen kunnen invulling geven aan één of meerdere generieke functies. Het Twiin Afsprakenstelsel kan vereisen dat gebruik wordt gemaakt van een gemeenschappelijke voorziening om invulling te geven aan een generieke functie. Voor de keuze om dwingend te verwijzen naar een gemeenschappelijke voorziening geldt een aantal voorwaarden. Een keuze voor een bepaalde gemeenschappelijke voorziening kan ook weer vervallen als niet langer aan de voorwaarden wordt

18. https://www.datavoorgezondheid.nl/site/binaries/site-content/collections/documents/2025/07/14/whitepaper-communicatiepatronen-vws/whitepaper-communicatiepatronen-vws.pdf

voldaan. Het Twiin Afsprakenstelsel verwijst alleen naar gemeenschappelijke voorzieningen die voldoen aan de volgende voorwaarden:

- **Hergebruik**: Meerdere gebruikers vragen om of gebruiken de dienst (eindgebruikers- of uitwisselingssystemen). Het Twiin Afsprakenstelsel sluit in beginsel aan op de keuzes die op landelijk niveau worden gemaakt over de inzet van gemeenschappelijke voorzieningen voor de invulling van een generieke functie.
- De gemeenschappelijke voorziening bevordert de **samenwerking en interoperabiliteit** in de zorg en vermindert redundantie in de keten. Het gaat onder andere om het verlagen van registratie- en beheerlasten en kosten.
- **Standaardisatie**: Gemeenschappelijke voorzieningen maken zoveel mogelijk gebruik van internationale standaarden en, indien noodzakelijk, Nederlandse extensies of beperkingen daarvan.
- **Noodzakelijkheid**: Een gemeenschappelijke voorziening bestaat alleen als deze noodzakelijk is. Als uitwisseling zonder gemeenschappelijke voorziening gerealiseerd kan worden op basis van een open stelsel, heeft dat de voorkeur.
- **Makelaarsfunctie**: De dienst kan een brug- of makelaarsfunctie bieden naar achterliggende gedistribueerde diensten. Een gemeenschappelijke voorziening kan ook een makelaarsfunctie vervullen om verschillende implementaties van de betreffende functie te kunnen bereiken. Via een gemeenschappelijke authenticatiedienst kan bijvoorbeeld gebruik worden gemaakt van verschillende beschikbare authenticatiemiddelen.
- **Agnostisch**: Gemeenschappelijke voorzieningen zijn onafhankelijk van het afsprakenstelsel of de gegevensuitwisseling waarin ze gebruikt worden. De voorzieningen leggen alleen eisen op aan de koppelvlakken.
- **Het proces voor onderhoud en beheer** van de gemeenschappelijke voorziening is duidelijk beschreven en duurzaam geborgd. Ook is er een autorisator aangewezen met een evenwichtige vertegenwoordiging van de belangen van de gebruikers in lijn met NEN 7522.

> ### Statement
>
> Twiin sluit aan op de keuzes die op landelijk niveau worden gemaakt en neemt deze op in het Twiin Afsprakenstelsel.

Rollen

Interoperabiliteit gaat over het verbinden van organisaties. Het Twiin Afsprakenstelsel wil een verbindend afsprakenstelsel zijn, onder andere door partijen te betrekken. Partijen die een rol spelen zijn de zorgaanbieders en hun leveranciers: zij committeren zich aan de afspraken en implementeren deze. Zorgaanbieders staan voor een grote opgave, dit heeft Twiin ertoe gebracht om de rol van dienstverlener te introduceren die de zorgaanbieder kan ondersteunen en ontzorgen. Twiin is tot de volgende rollen gekomen om de samenwerking goed vorm te geven:

- Organisatorische rollen

    - Twiin Deelnemer
    - Twiin Dienstverlener
    - GtK Beheerder
    - GtK Leverancier
- Systeemrol
    - GtK (Gevalideerd Twiin Knooppunt).

Unable to render include or excerpt-include. Could not retrieve page.

Twiin Deelnemer

Organisatie die de Twiin Deelnemersovereenkomst voor het Twiin Afsprakenstelsel heeft getekend. Vooralsnog zijn dit enkel zorgaanbieders zolang niet anders wordt besloten op basis van het reglement.

Twiin Dienstverlener

Een partner die begeleidt bij de implementatie en de ontwikkeling van zorgtoepassingen en die Twiin Deelnemers helpt om te voldoen aan het Twiin Afsprakenstelsel.

De Twiin Dienstverlener faciliteert en ondersteunt zorgaanbieders bij de implementatie. De zorgaanbieder kan kiezen om de taken van de Twiin Dienstverlener en GtK Beheerder zelf in te vullen, maar kan deze ook uitbesteden.

Toelichting
Voor een zorgtoepassing is een regievoerder noodzakelijk. Daarmee doelen we op het faciliteren en ondersteunen van de zorgaanbieders bij de implementatie in de keten. Binnen het Twiin Afsprakenstelsel vervult de Twiin Dienstverlener deze rol. Binnen een samenwerkingsverband kan één van de aangesloten zorgaanbieders deze rol ook zelf invullen.

Voorbeelden van partijen die de rol van Twiin Dienstverlener kunnen vervullen.

- Regionale/categorale samenwerkingsorganisaties
- Zorgaanbieders (voor andere zorgaanbieders en voor de eigen organisatie)
- Landelijke samenwerkingsorganisaties, zoals VZVZ

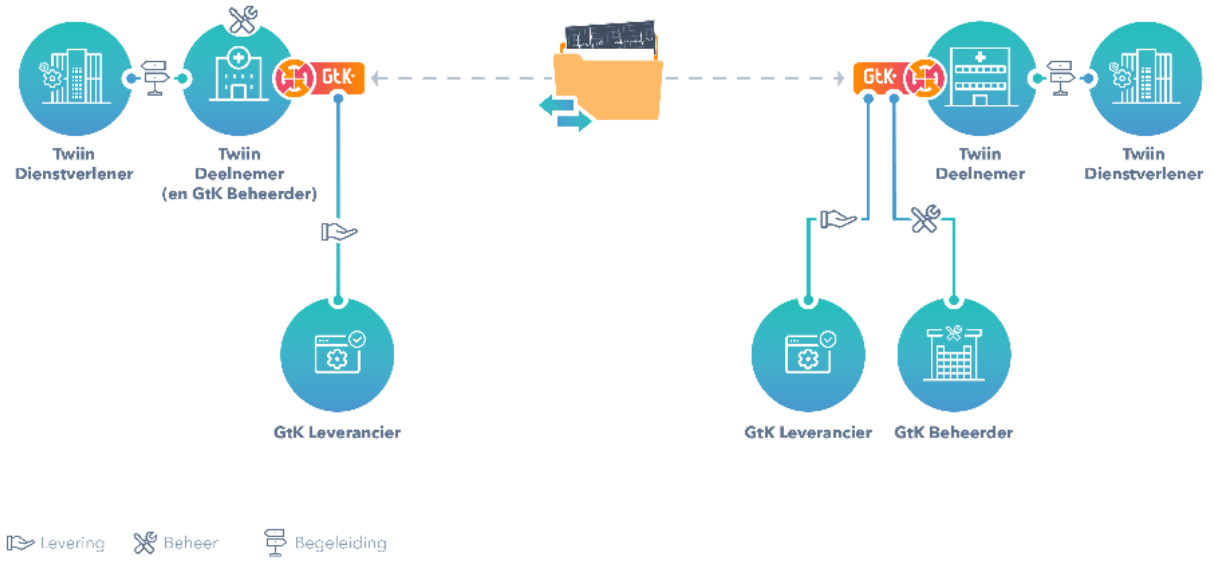
GtK Beheerder

Een organisatie die namens de Twiin Deelnemer invulling geeft aan het technisch beheer van het GtK, zoals omschreven in de Voorwaarden GtK Beheer.

GtK Leverancier

Leverancier van een GtK.

In onderstaande figuur wordt weergegeven hoe de verschillende rollen zich tot elkaar kunnen verhouden.



In bovenstaande figuur worden twee Twiin Deelnemers afgebeeld die gegevens volgens het Twiin Afsprakenstelsel uitwisselen voor een bepaalde zorgtoepassing. Zij maken hiervoor gebruik van verschillende GtK's. De Twiin Deelnemer rechts heeft een GtK Beheerder ingeschakeld voor de onderdelen die het GtK vormen. De Twiin Deelnemer aan de linkerkant is een deelnemer die de rol GtK Beheerder samen met de GtK Leverancier zelf invult. Beide Twiin Deelnemers hebben ook te maken met leverancier(s) voor de onderdelen van de GtK's.

Bovenstaande situatie is een voorbeeld, er kan ook een hybride situatie bestaan: applicaties die door de Twiin Deelnemer zelf worden beheerd en applicaties die door een externe GtK Beheerder worden beheerd die allen gebruikt worden om databeschikbaarheid te realiseren.

Hoe de rollen zich verhouden tot de actoren in het kader van de governance, is uitgewerkt in het hoofdstuk 6 | governance (see page 80).

GtK (Gevalideerd Twiin Knooppunt)

Uitwisseling van data gebeurt volgens het Twiin Afsprakenstelsel tussen Gevalideerde Twiin Knooppunten (GtK). Een GtK is een door Twiin gevalideerde oplossing die zorgt voor beschikbaarheid en uitwisseling van gegevens voor één of meer zorgtoepassingen voor één of meerdere zorgaanbieders.
Een GtK hoeft niet per se uit één uitwisselingssysteem of uit één (aparte) applicatie te bestaan. Een GtK kan gevormd worden door meerdere onderdelen. Het GtK bestaat minimaal uit een koppelvlak op een regionale infrastructuur, een landelijke infrastructuur, een leveranciersnetwerk of een platform – een zorgaanbieder kan ook zelf een GtK hebben.

Voorbeelden van mogelijke GtK's:

- XCA Gateway voor beelduitwisseling
- FHIR Gateway van AORTA
- Nuts-node voor eOverdracht
- FHIR-koppelvlak voor BgZ
- Leverancierspl atformen

Een GtK is een technische component en kan op die manier verschillende rollen aannemen:

- **GtK verzender (sender) / zendend GtK** - van toepassing bij de communicatiepatronen:
  - gericht verzenden / push
  - gericht beschikbaar stellen / notified pull
- **GtK ontvanger (receiver) / ontvangend GtK –** van toepassing bij de communicatiepatronen:
  - gericht verzenden / push
  - gericht beschikbaar stellen / notified pull
- **GtK vrager (requester) / vragend GtK –** van toepassing bij de communicatiepatronen:
  - gericht bevragen / pull
  - gericht beschikbaar stellen / notified pull
  - ongericht bevragen / indexed pull
- **GtK antwoorder (responder) / antwoordend GtK –** van toepassing bij de communicatiepatronen:
  - gericht bevragen / pull
  - gericht beschikbaar stellen / notified pull
  - ongericht bevragen / indexed pull

In de technische kern en de implementatiewijzer van de zorgtoepassingen van Twiin komen deze actoren terug in de communicatiepatronen, transactieschema's en PvE's.

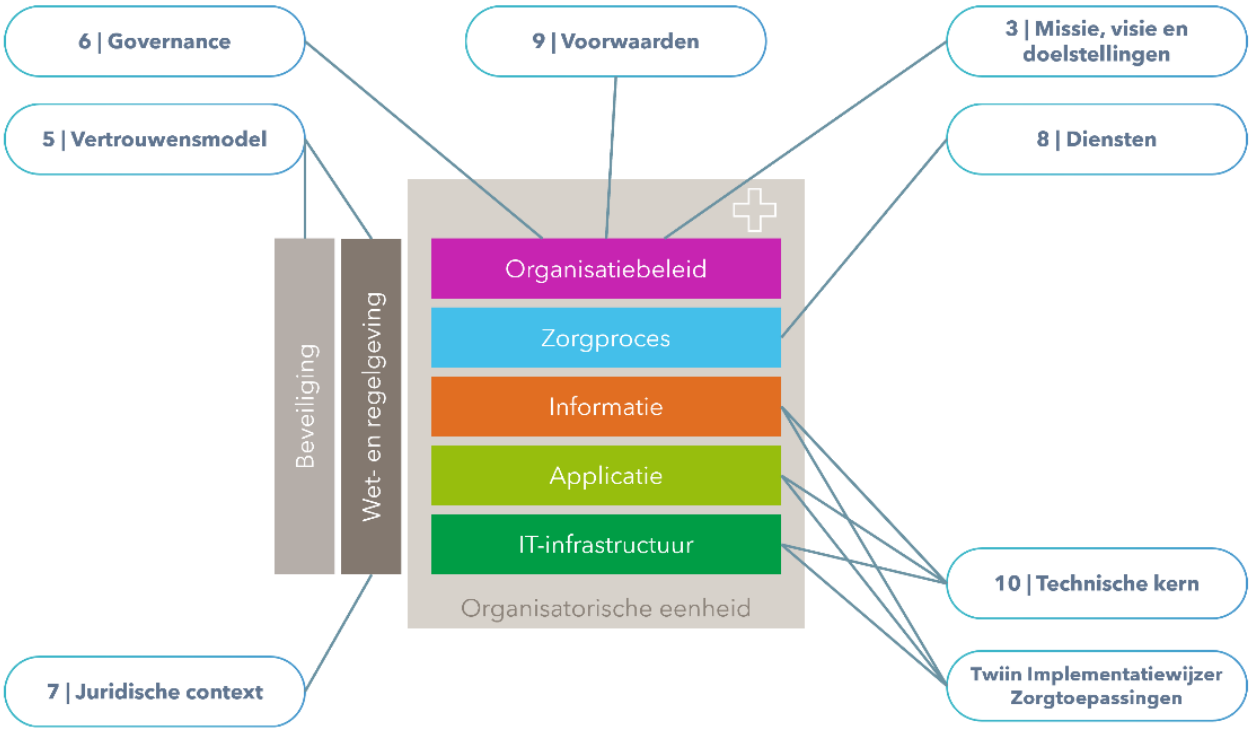
4.5 | Fysieke architectuur

De fysieke architectuur beschrijft de uitvoerbare elementen waarmee de oplossing bereikt kan worden. Twiin maakt zelf geen fysieke oplossingen als het gaat om applicaties of technische infrastructuur - dat is aan de leveranciers van oplossingen. Twiin legt de specificaties vast waaraan de oplossingen moeten voldoen.

Dit onderdeel wordt gebruikt om in te gaan op de producten van Twiin of de ingerichte structuren die bestaan in de samenwerking van de Twiin Organisatie.

Structuur afsprakenstelsel

Twiin sluit aan bij het interoperabiliteitsmodel. In onderstaande weergave is inzichtelijk gemaakt hoe de lagen van het Nictiz-model en de indeling van het afsprakenstelsel samenhangen.



Solution architectuur

Technische kern: generiek

De technische uitwerking van de communicatiepatronen, de transactieschema's en de transacties zijn ondergebracht in het onderdeel 10 | Technische kern (see page 164) van het afsprakenstelsel.

In de technische kern staan de generieke aspecten van de uitgewerkte afspraken en eisen. De solution architectuur is zoveel mogelijk onderverdeeld in herbruikbare bouwblokken. Dit om flexibiliteit te behouden bij het steeds verder groeien van het Twiin Afsprakenstelsel en om de complexiteit zoveel mogelijk te reduceren.

Het hergebruik wordt ook op een andere wijze ingevuld: er wordt verwezen naar standaarden en normen wanneer dat mogelijk is.

Implementatiewijzer: specifiek

In de implementatiewijzer van de zorgtoepassingen staan de specifieke afspraken en eisen die horen bij een bepaalde zorgtoepassing. Vanuit de zorgtoepassingen worden generieke elementen in de technische kern hergebruikt (hier wordt naar verwezen). Het geheel voor de zorgtoepassingen van Twiin bestaat dan uit actoren en communicatiepatronen die uitgewerkt zijn in transactieschema's en PvE's.

Samenwerking

De technische kern bevat de generieke solution architectuur waarin technische afspraken zijn opgenomen. Deze technische afspraken worden geschreven in werkgroepen waarin diverse betrokken partijen samenwerken.

De verschillende rollen hebben in de governance van het Twiin Afsprakenstelsel een plek gekregen: voor alle verantwoordelijkheden en afspraken zie: 6 | Governance (see page 80) en 8 | Diensten en 9 | Voorwaarden .

Release Twiin Afsprakenstelsel

Een release van het Twiin Afsprakenstelsel bestaat uit de afspraken waaraan partijen zich committeren en die ook daadwerkelijk geïmplementeerd kunnen worden. Bij het uitbrengen van releases stemt Twiin af met de aangesloten partijen.

Ondersteuning

Het is niet altijd mogelijk om (direct of op korte termijn) te voldoen aan de gemeenschappelijke afspraken om uit te wisselen. Verschillen moeten dan overbrugd worden. Het Twiin Afsprakenstelsel biedt een aantal 'brug functies':

- Twiin heeft een groeimodel (kies Factsheet Groeimodel)[19] gemaakt dat de Twiin Deelnemers helpt om te gaan voldoen aan het Twiin Afsprakenstelsel en te komen tot validatie.
- De deelnemersovereenkomst met samenwerkingsvoorwaarden. Zolang de Twiin Deelnemer nog niet is gevalideerd, kan de Twiin Deelnemer enkel in beperkt verband op basis van de Samenwerkingsvoorwaarden de zorgtoepassingen van twiin uitwisselen (Samenwerkingsvoorwaarden zoals omschreven in artikel 3 van de Deelnemersovereenkomst (see page 84)).
- Twiin Dienstverlener: om zorgaanbieders te ondersteunen bij het voldoen aan het Twiin Afsprakenstelsel en samenwerkingsvoorwaarden te beheren.

Ontwikkelsupplement

Het Twiin Afsprakenstelsel bevat afspraken die daadwerkelijk geïmplementeerd kunnen worden. Om ook ruimte te geven aan toekomstige ontwikkelingen en alvast afspraken uit te werken die in de toekomst liggen – en deze ook te publiceren – heeft Twiin het Ontwikkelsupplement[20] gerealiseerd. Dit Ontwikkelsupplement volgt zoveel mogelijk de indeling van het Twiin Afsprakenstelsel maar kan – in verschillende niveaus van volwassenheid – incompleet uitgewerkte onderdelen bevatten. Het Ontwikkelsupplement kent geen vaststaand releasebeleid.

19. https://www.twiin.nl/downloads
20. https://ontwikkelsupplement.twiin.nl

5 | Vertrouwensmodel

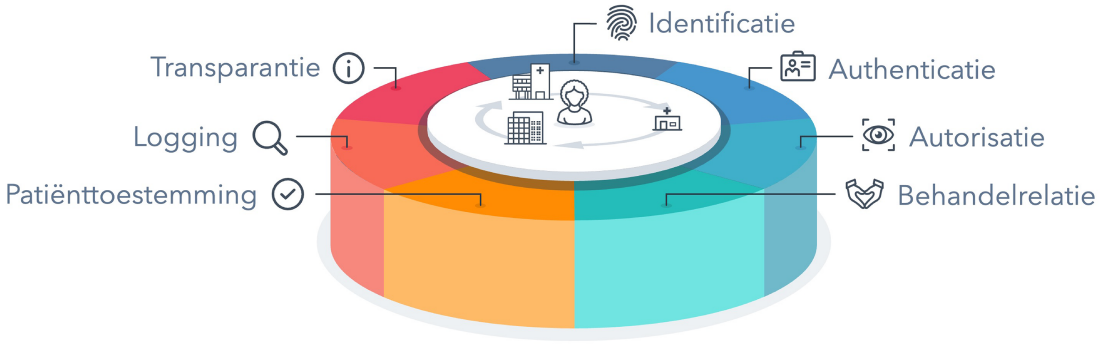
Belang vertrouwensmodel

Het belang van het vertrouwensmodel is meervoudig:

- De cliënt moet erop kunnen vertrouwen dat de zorgverleners en zorgaanbieders de vertrouwelijkheid van zijn dossier adequaat borgen, ook bij de uitwisseling van gezondheidsgegevens.
- Zorgverleners hebben een beroepsgeheim (op basis van de Wet BIG (see page 102) en WGBO (see page 102)). Het beroepsgeheim geldt voor alle informatie die zij in de uitoefening van hun beroep over een cliënt te weten komen. Dus ook het feit dat een cliënt onder behandeling is bij een zorgverlener valt hieronder. Anderen die beroepsmatig kennis krijgen van gezondheidsgegevens van de cliënt zijn gebonden aan een afgeleid beroepsgeheim. Degene op wie de geheimhouding rust, moet erop kunnen vertrouwen dat de juiste maatregelen zijn getroffen om zijn beroepsgeheim te borgen.
- Zorgaanbieders moeten adequate maatregelen treffen om de persoonsgegevens in medische dossiers te beveiligen, ook bij uitwisseling (op basis van de AVG (see page 102)). Zorgaanbieders zijn verplicht om de beveiligingsnormen voor de zorg toe te passen en het vertrouwensmodel geeft invulling aan die normen (op basis van het Besluit elektronische gegevensverwerking door zorgaanbieders, 'Begz (see page 102)'). Ook zijn zorgaanbieders verplicht de juiste randvoorwaarden te organiseren die zorgverleners in staat stellen goede zorg te verlenen (op basis van de Wkkgz (see page 102)). Het gaat hierbij onder andere om de inrichting van de organisatie, de toedeling van verantwoordelijkheden en bevoegdheden en de beschikbaarheid van middelen. In het vertrouwensmodel is dan ook uitgewerkt welke partij waarvoor verantwoordelijk is bij het realiseren van databeschikbaarheid.

Zeven vertrouwensfuncties

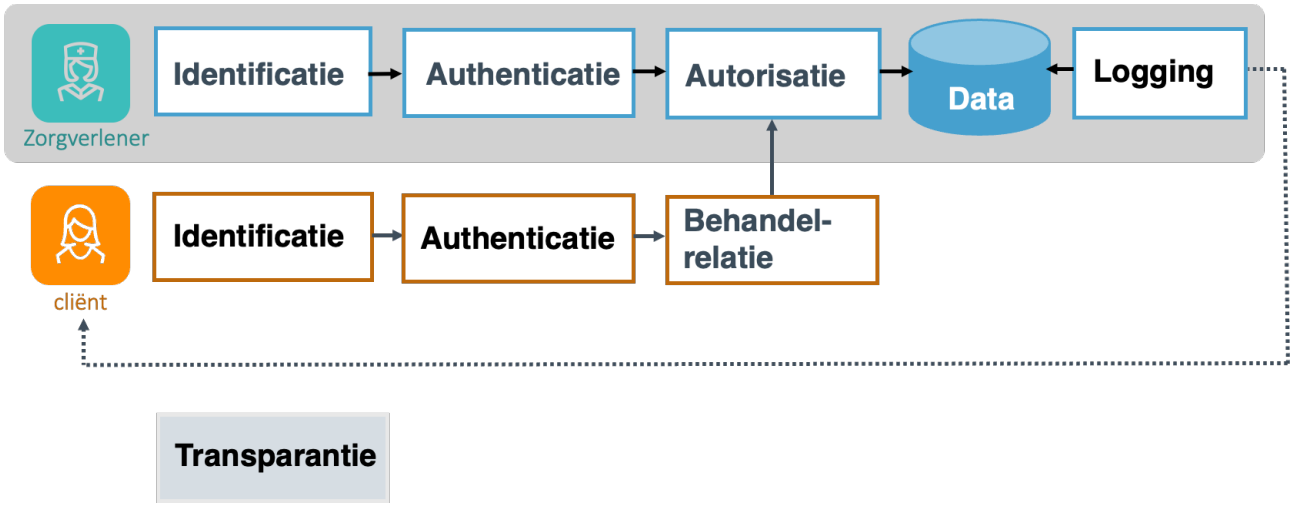
Het vertrouwensmodel bestaat uit zeven vertrouwensfuncties, gevisualiseerd in onderstaande figuur. Bij elke elektronische uitwisseling geldt dat aan deze zeven functies invulling moet zijn gegeven. Deze vertrouwensfuncties hangen met elkaar samen; keuzes ten aanzien van één functie zijn van invloed op keuzes over een andere functie. Daarom zijn deze vertrouwensfuncties in één figuur bijeengebracht. In de onderliggende pagina's is voor elk van de zeven onderdelen beschreven welke afspraken gelden voor iedere vertrouwensfunctie.



Onderlinge samenhang vertrouwensfuncties

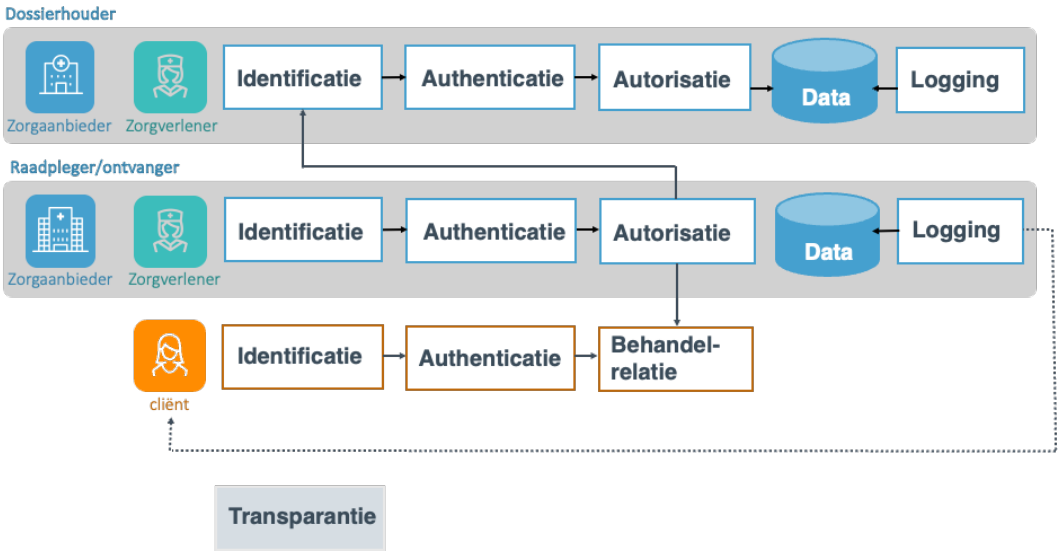
Inrichting vertrouwensfuncties binnen één zorgaanbieder

Hieronder een versimpelde schematische weergave van de samenhang van de vertrouwensfuncties binnen één zorgaanbieder. De basis is de vertrouwensketen in het grijze vlak die iedere zorgaanbieder moet inrichten voor de toegang tot de gegevens in de eigen dossiers. Deze vertrouwensketen is opgebouwd uit de stappen identificatie, authenticatie, autorisatie en logging. Authenticatie is, als verificatie van een beweerde identiteit, afhankelijk van identificatiegegevens die gebruikt worden. Autorisatie gebruikt de identificatiegegevens bij het bepalen welke toegang tot gegevens verleend mag worden. Logging legt vast welke toegang is verleend, waarbij de persoon op verzoek een afschrift hiervan kan krijgen. Omdat het gaat om gegevens over een cliënt, moet ook de identiteit van die cliënt worden vastgesteld en geverifieerd. De toegang tot de gegevens is bij gezondheidsgegevens enkel toegestaan bij een behandelrelatie. Transparantie gaat over het geven van heldere informatie aan de cliënt over de verwerking van zijn gegevens.

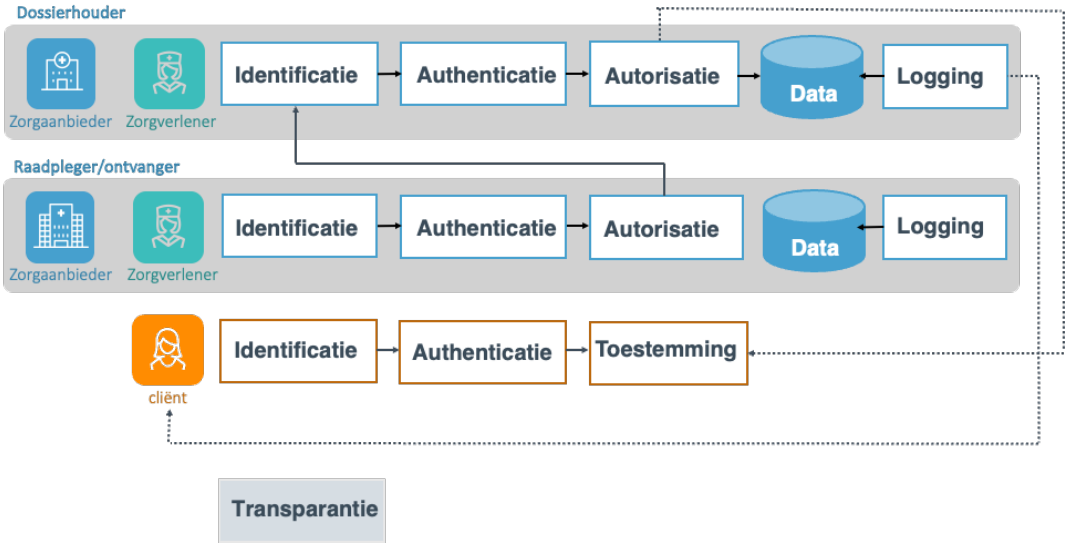


Inrichting vertrouwensfuncties bij uitwisseling tussen zorgaanbieders

Hieronder een versimpelde schematische weergave van de samenhang van de vertrouwensfuncties bij uitwisseling tussen zorgaanbieders. Bij uitwisseling tussen zorgaanbieders, vraagt de raadplegend zorgaanbieder gezondheidsgegevens op, maar enkel als sprake is van een behandelrelatie met een cliënt. Vervolgens moet de dossierhoudend zorgaanbieder de raadplegend/ontvangend zorgaanbieder identificeren en ook de zorgverlener die toegang wenst. De raadplegend zorgaanbieder verstrekt op verzoek de logging aan de cliënt. Dit alles is hieronder weergegeven:



De dossierhoudend zorgaanbieder is verplicht om op verzoek logging te verstrekken aan de cliënt. In veel gevallen is de dossierhoudend zorgaanbieder verplicht om de toestemming van de cliënt te controleren. Het verstrekken van logging door de dossierhouder en controle van de toestemming zijn hieronder weergegeven. De stippellijn duidt hierbij aan dat deze stappen niet in alle gevallen toegepast worden:



Zorgaanbieders moeten de zeven vertrouwensfuncties op eenduidige manier inrichten bij onderlinge uitwisseling van gezondheidsgegevens. Dit om het beroepsgeheim te kunnen borgen bij uitwisseling. Het gaat immers om het verlenen van toegang tot het dossier aan een zorgverlener die werkzaam is bij een andere zorgaanbieder. Ook is een eenduidige inrichting nodig om de persoon goed te kunnen informeren over de verwerking van zijn gegevens. Oftewel om te voldoen aan de vertrouwensfunctie transparantie. De onderlinge relaties tussen de vertrouwensfuncties zijn complexer dan in het bovenstaande schema. Deze relaties hangen ook af van het type gegevensuitwisseling en het communicatiepatroon dat wordt gebruikt.

Samenhang technische kern, voorwaarden en NEN-normen

Verwerkingsverantwoordelijkheid

De afspraken die gelden voor de zeven vertrouwensfuncties zijn uitgewerkt op de zeven onderliggende pagina's van dit hoofdstuk. Op die pagina's is - waar relevant - het verschil aangeduid tussen verzenden en raadpleegbaar maken. Verzenden en raadpleegbaar maken/raadplegen zijn twee verschillende typen gegevensuitwisselingen. Dit verschil is relevant vanwege de wettelijke eisen die gelden voor een elektronisch uitwisselingssysteem zoals bedoeld in de Wabvpz (zie het *Juridische kader* (see page 104)).

De verdeling van de verantwoordelijkheid van de verschillende Twiin Deelnemers die betrokken zijn bij de uitwisseling verschilt ook per type uitwisseling. Per vertrouwensfunctie is die verdeling aangeduid in de schema's in de onderliggende hoofdstukken 5.1 t/m 5.7. Deze verdeling heeft ook betrekking op de verwerkingsverantwoordelijkheid van de Twiin Deelnemers die betrokken zijn bij een uitwisseling, zoals toegelicht in het hoofdstuk Toelichting verwerkingsverantwoordelijkheid (see page 113).

Technische kern en voorwaarden

In de *Technische kern* (see page 164) zijn de afspraken over de zeven vertrouwensfuncties in meer detail uitgewerkt, inclusief specificaties en eisen. Ook wordt hier beschreven hoe de communicatiepatronen invulling geven aan de twee typen gegevensuitwisselingen. Daarnaast zijn er verschillende eisen voor de vertrouwensfuncties vastgelegd in de *Voorwaarden Twiin Deelnemer* (see page 142). In het proces validatie (see page 128) wordt getoetst op deze voorwaarden.

Generieke functies

De zeven onderdelen van het vertrouwensmodel zijn vertrouwensfuncties. Vertrouwensfuncties vormen een subset van de generieke functies. Meer uitleg over generieke functies is te vinden in het hoofdstuk *Architectuur* (see page 46). Vertrouwensfuncties zijn generieke functies die in het bijzonder gericht zijn op het borgen van het vertrouwen. De vertrouwensfuncties corresponderen met de generieke functies waarvoor NEN-normen in ontwikkeling zijn of zijn vastgesteld. Dit is hieronder in het schema aangeduid. Er zijn ook generieke functies die geen vertrouwensfuncties zijn, zoals lokalisatie en adressering. Deze twee generieke functies zijn wel randvoorwaardelijk voor uitwisseling van gezondheidsgegevens.

Normen voor informatiebeveiliging

Voor vertrouwen is informatiebeveiliging van groot belang. De NEN 7510, NEN 7512 en NEN 7513-normen zijn gericht op informatiebeveiliging, waarbij de NEN 7512-norm meer in het bijzonder is bedoeld als 'vertrouwensbasis voor gegevensuitwisseling'. De NEN 7512-norm ziet op meer aspecten dan enkel de vertrouwensfuncties. Het Twiin Afsprakenstelsel kent ook meer voorwaarden voor validatie dan enkel de voorwaarden die zien op de vertrouwensfuncties. Zo zijn o.a. de eisen uit de NEN 7510 en NEN 7512 vertaald naar de voorwaarden waarop getoetst wordt bij validatie. Denk bijvoorbeeld aan eisen ten aanzien van beschikbaarheid. Een ander voorbeeld zijn de voorwaarden die zien op veilig netwerk.

Het Twiin Afsprakenstelsel is daarbij het geheel van afspraken dat nodig is om het vertrouwen te borgen in de uitwisseling van gezondheidsgegevens. Het vormt het kader zoals bedoeld de NEN 7512. Binnen dit kader zijn ook de diensten (see page 119) van belang om het vertrouwen tussen partijen te borgen. Validatie is al genoemd. Daarnaast is ook toetreding (see page 119), ketenregie (see page 136) en handhaving (see page 140) van belang voor het vertrouwen. Deze diensten worden in hoofdstuk 8 (see page 119) beschreven. Naast de diensten heeft Twiin ook een informatiebeveiligingsbeleid (see page 117).

Vertrouwens functies	Specifieke NEN-norm* (naast NEN 7510 en NEN 7512)	Voorwaarden	Verwijzing uitwerking technische kern
Identificatie	NEN 7518	9.1 | 5.7-5.9	10.2.1 | Generieke functie - Identificatie en Authenticatie (see page 180)
Authenticatie	NEN 7518	9.1 | 5.10-5.11	10.2.1 | Generieke functie - Identificatie en Authenticatie (see page 180)
Autorisatie	NEN 7520	9.1 | 5.12	10.2.2 | Generieke functie - Autorisatie (see page 180)

Vertrouwens functies	Specifieke NEN-norm* (naast NEN 7510 en NEN 7512)	Voorwaarden	Verwijzing uitwerking technische kern
Behandelrelatie	n.v.t.	9.1 | 3.1	NVT
Toestemming	NEN 7517	9.1 | 5.13-5.14	10.2.3 | Generieke functie - Toestemming (see page 181)
Logging	NEN 7513	9.1 | 5.19-5.20, 9.3 | 4.3	10.2.4 | Generieke functie - Logging (see page 182)
Transparantie	n.v.t.	9.1 | 2.6	NVT
Generieke functies die randvoorwaardelijk zijn voor uitwisseling van gegevens:			
Adressering	n.v.t.	9.1 | 5.17-5.18, 9.3 | 4.1-4.2	10.2.5 | Generieke functie - Adressering (see page 184)
Lokalisatie	NEN 7519	9.1 | 5.15-5.16	10.2.6 | Generieke functie - Lokalisatie (see page 184)

*** Statement**

Het Twiin Afsprakenstelsel volgt de ontwikkeling van de NEN-normering van de generieke functies en sluit hierop aan. Niet alle landelijke normen en technische afspraken zijn al gereed. Zie het hoofdstuk met het overzicht van de toepasselijke normen (see page 115). Waar dat nodig is om gegevensuitwisseling tot stand te brengen, bevat het Twiin Afsprakenstelsel nu nog een eigen invulling. Als deze normen en afspraken wel beschikbaar zijn, zullen deze worden overgenomen in een volgende versie van het afsprakenstelsel.

Uitwisselingskompas

Het vertrouwensmodel zoals uitgewerkt in het Twiin Afsprakenstelsel correspondeert met de bovenste laag van het Uitwisselingskompas[21] van VZVZ. De onderste laag van het uitwisselingskompas bestaat uit de generieke functies adressering en lokalisatie. Het verschil tussen het Twiin Vertrouwensmodel en het kompas is het volgende: Het kompas is met name een hulpmiddel om het gesprek te faciliteren, terwijl in het Twiin Afsprakenstelsel afspraken zijn vastgelegd over hoe invulling moet worden gegeven aan deze onderdelen.

21. https://www.vzvz.nl/het-uitwisselingskompas

5.1 | Vertrouwen: Identificatie

Identificatie

Identificatie is het geven van kenmerken waarmee de identiteit van een persoon of organisatie eenduidig kan worden vastgesteld. Om zorgverleners, zorgaanbieders en cliënten tussen en over de instellingen heen te kunnen herkennen moeten deze actoren uniek identificeerbaar zijn. Bij uitwisseling van gegevens tussen de zorgverleners én met cliënten, speelt identificatie van cliënten, zorgverleners en zorgaanbieders een belangrijke rol. Dit is namelijk de basis van verdere controles die uitgevoerd moeten worden.

Identificatie van een cliënt

Voor het relateren van gegevens over dezelfde cliënt bij verschillende zorgaanbieders, is het gebruik van het BSN verplicht gesteld (zie het *Juridisch kader* (see page 104), onder Wabvpz).

In sommige situaties is het BSN niet bruikbaar, of is er onzekerheid over de koppeling met de persoon. Pasgeborenen of buitenlanders hebben bijvoorbeeld niet altijd (al) een BSN en de cliënt is niet altijd fysiek aanwezig om de identiteit te verifiëren.

Volgens art. 28 Besluit gebruik BSN in de zorg gebruikt men in bovenstaande uitzonderingssituaties niet het BSN, maar geslachtsnaam, voornamen, geboortedatum, postcode en huisnummer van het woonadres. Er is nog geen landelijke afspraak hoe zorgaanbieders moeten omgaan met een niet aanwezig BSN. Daarom kunnen zorgaanbieders in die situatie voorlopig nog geen gegevens uitwisselen op basis van validatie door Twiin.

Zorgaanbieders

Om zorgaanbieders te kunnen identificeren, vereist de NEN 7512 dat er een afspraak gemaakt moet worden over het gebruik van een eenduidig identificatienummer. Als een cliënt bijvoorbeeld zijn of haar zorgaanbieder toestemming wil geven, dan is het noodzakelijk dat deze eenduidig te identificeren valt. Onwenselijk is dat de ene keer het KvK-nummer (Kamer van Koophandel) gebruikt wordt en dan weer het AGB of het UZI-register abonneenummer (URA). Om zorgaanbieders te identificeren kiest Twiin voor het URA. Dit is een nummer dat alleen aan zorgaanbieders uitgegeven wordt en ook niet-declarerende zorgaanbieders kunnen een URA krijgen. Deze keuze ligt in lijn met de uitgangspunten zoals geformuleerd in het Informatieberaad Zorg. Waarbij van belang is dat zorgaanbieders zich in het Integraal Zorgakkoord (IZA) hebben verbonden aan de oplossingen die door VWS in afstemming met het Informatieberaad Zorg zijn vastgesteld voor de generieke functies.

Zorgverleners

Ook zorgverleners moeten identificeerbaar zijn door de partijen die betrokken zijn bij de gegevensuitwisseling (NEN 7512). Op basis van bijvoorbeeld een medewerkersnummer van een andere organisatie kan niet zelfstandig en/of onafhankelijk de identiteit vastgesteld worden. UZI is momenteel het breedst bruikbare landelijke stelsel om zorgverleners en medewerkers te identificeren. Alternatieven zouden zijn: BIG-register of AGB-register. In de eerste zitten niet alle specialismen en geen medewerkers (indien nodig), in de tweede zitten alleen maar declarerende zorgverleners. Het UZI-

register dekt bredere specialismen dan het BIG-register en ook niet-declarerende zorgverleners (zoals in jeugdgezondheidszorg) staan hierin. De keuze voor het UZI-stelsel ligt in lijn met de uitgangspunten zoals geformuleerd in het Informatieberaad. De opvolging van het UZI-nummer wordt het DEZI-nummer (Dé ZorgIdentiteit). Waar bij het nu zo is dat om een UZI-nummer te verkrijgen er ook een identificatiemiddel (de UZI-pas) afgenomen dient te worden. In het DEZI-stelsel wordt deze koppeling losgelaten.

Ontwikkelingen

Er is een norm in ontwikkeling, NEN 7518, over identificatie en authenticatie. Daarnaast is er een Wetsvoorstel identificatie en authenticatie in de zorg (Wet Diaz) in behandeling. Twiin volgt de ontwikkelingen en zodra passende identificatiemiddelen beschikbaar komen, zullen die een plek krijgen in het Twiin Afsprakenstelsel.

Vereiste	Wie is (verwerkings)verantwoordelijk Dossierhouder of dossierraadpleger/-ontvanger	Invulling Twiin	Toelichting
Cliënten worden geïdentificeerd met een landelijk uniek nummer: het BSN	Dossierhouder en dossierraadpleger/-ontvanger dienen cliënten op dezelfde manier te identificeren.	BSN	Er is nog geen landelijke afspraak voor de implementatie voor situaties waarin een BSN ontbreekt. Het Twiin Afsprakenstelsel gaat daarom vooralsnog uit van uitwisseling op basis van BSN. Zonder BSN kan voorlopig geen uitwisseling plaatsvinden op basis van validatie door Twiin.

Vereiste	Wie is (verwerkings)verantwoordelijk Dossierhouder of dossierraadpleger/-ontvanger	Invulling Twiin	Toelichting
Zorgaanbieders worden geïdentificeerd met een landelijk uniek nummer	Dossierhouder en dossierraadpleger/-ontvanger dienen elkaar te kunnen identificeren.	URA	Het URA wordt naast het AGB-nummer gebruikt als codestelsel in de zib zorgaanbieder. De uitgevers van deze nummers controleren of de organisatie aan wie het nummer wordt toegekend echt zorg levert, maar in het ABG-register zitten alleen declarerende zorgaanbieders. Het URA is daarmee het breedst toepasbare landelijke stelsel om zorgaanbieders te identificeren. Gebruik van het URA is ook in lijn met besluiten die in het verleden in het informatieberaad zijn gemaakt. Het URA is verplicht, en aanvullend op het URA mogen ook andere identificatienummers gebruikt worden.

Vereiste	Wie is (verwerkings)verantwoordelijk Dossierhouder of dossierraadpleger/-ontvanger	Invulling Twiin	Toelichting
Zorgverleners worden geïdentificeerd met een landelijk uniek nummer	*Bij raadpleegbaar maken*:* De dossierraadpleger dient het landelijke unieke nummer te gebruiken, zodat de communicatiepartij(en) op basis hiervan verdere controles kunnen uitvoeren. De dossierhouder dient de raadplegende (verantwoordelijke) zorgverlener te kunnen identificeren. *Bij verzenden*:* De dossierhouder dient de verzendende zorgverlener te identificeren en het landelijke unieke nummer mee te sturen naar dossierontvanger.	UZI of een ander uniek tot één persoon te herleiden nummer op het juiste betrouwbaarheidsniveau.	Dit is alleen van toepassing op de dossierraadpleger. Deze dient het landelijke unieke nummer te gebruiken, zodat de communicatiepartij(en) op basis hiervan verdere controles kunnen uitvoeren. De verwachting is dat er in de toekomst meerdere eisen gesteld zullen worden aan de uitgifte van unieke persoonsnummers (in de NEN 7518). Dit zal worden ingevuld door het DEZI-register. Twiin stelt nu alleen de eis dat het nummer uniek is en moet blijven. Na bijvoorbeeld uitdiensttreding mag het nummer niet opnieuw gebruikt worden voor een ander individu.

* Verzenden en raadpleegbaar maken verwijzen naar de twee typen gegevensuitwisselingen. De communicatiepatronen (see page 169) zoals uitgewerkt in de technische kern kunnen worden onderverdeeld in deze twee typen.

5.2 | Vertrouwen: Authenticatie

Authenticatie

Authenticatie betreft de verificatie van een bepaalde bewering. In het kader van authenticatie als vertrouwensfunctie is met authenticatie nu bedoeld de verificatie van een beweerde identiteit. Met identificatiemiddelen kan een persoon of organisatie duidelijk maken aan een ander wie hij is en dat hij het echt is. Het is gericht op het creëren van gewaarborgd vertrouwen bij een ander.

Na het elektronisch identificeren volgt een bevestiging van de echtheid van een aan een ander opgegeven of kenbaar gemaakte identiteit. De bevestiging die de vertrouwende partij ontvangt, is veelal afkomstig van een derde partij die de identiteit op echtheid heeft gecontroleerd en vastgelegd. Authenticatie is het proces dat bevestiging mogelijk maakt.

Verantwoordelijkheden

Voor het veilig delen van medische gegevens via een uitwisselingsinfrastructuur moeten zorgaanbieders en ook zorgverleners zich authenticeren. Daarnaast is het belangrijk het toegangsbeleid tot medische gegevens in te richten en te beheren:

- De zorgaanbieder moet zorgdragen voor passende beveiliging en bescherming van de persoonsgegevens die hij verwerkt.
- De zorgaanbieder moet zorgen dat de digitale toepassing die toegang geeft tot persoonsgegevens op passende wijze beveiligd is en een voldoende betrouwbaarheidsniveau van authenticatie kent.

Bij uitwisseling tussen zorgaanbieders is de brondossierhouder voor bovenstaande zaken verantwoordelijk. De geheimhoudingsplicht rust op de dossierhouder. Daarom is het van belang dat deze met grote zekerheid weet wie hij toestaat gegevens te verwerken. Daarnaast vereist de wet dat het verwerken van persoonsgegevens goed beveiligd plaatsvindt. Authenticatie op het juiste betrouwbaarheidsniveau is daarmee een eis van passende beveiliging. Als het gaat om gegevens waarop het medisch beroepsgeheim van de zorgverlener rust, verlangt de Autoriteit Persoonsgegevens (AP) het 'hoogste' betrouwbaarheidsniveau (eIDAS (see page 102) niveau hoog, in lijn met de uitvoeringsverordening (EU) 2015/1502).

Betrouwbaarheid

De betrouwbaarheid van het identificatiemiddel wordt onder meer bepaald door:

- de koppeling tussen persoonsidentificatiegegevens met de persoon
- het uitgifteproces van een elektronisch identificatiemiddel
- het beheer van het middel
- de gebruikte techniek
- en de inrichting van het authenticatieproces.

Hoe veiliger het authenticatiemechanisme, hoe hoger het betrouwbaarheidsniveau van de authenticatie.

Authenticeren zorgaanbieders

Voor het authenticeren van zorgaanbieders (en hun systemen) is geen concrete technische invulling van de norm van een hoog betrouwbaarheidsniveau die volgt uit wet- en regelgeving. Voor organisaties is nu het systeem eHerkenning ingericht. Dit systeem heeft het hoogste betrouwbaarheidsniveau op basis

van multi-factorauthenticatie. Deze vorm van authenticatie kan echter niet autonoom worden uitgevoerd voor een systeem, omdat voor authenticatie met een tweede factor is altijd een persoon nodig is. Dit maakt het onwerkbaar bij gegevensuitwisseling, met name bij de organisatie die informatie ontvangt en de organisatie die geraadpleegd wordt. Het is kortom niet mogelijk om zorgaanbieders te identificeren op basis van eIDAS hoog betrouwbaarheidsniveau.

Ontwikkelingen

Er zijn verschillende nieuwe technologische ontwikkelingen die betrouwbaar zijn en toegepast zouden kunnen worden (al voldoen deze niet aan eIDAS hoog betrouwbaarheidsniveau, in de zin dat systemen niet autonoom kunnen deelnemen aan een gegevensuitwisseling), zoals PKIo-middelen (eHerkenning, UZI-servercertificaten) of verifiable credentials. Ook hier geldt dat de betrouwbaarheid van het identificatiemiddel voor organisaties/systemen wordt bepaald door onder meer de koppeling tussen identificatiegegevens met de organisatie, het uitgifteproces van een elektronisch identificatiemiddel, het beheer van het middel, de gebruikte techniek en de inrichting van het authenticatieproces. Hoe veiliger het authenticatiemechanisme is, hoe hoger het betrouwbaarheidsniveau van de authenticatie.

Er is een norm in ontwikkeling, NEN 7518, over identificatie en authenticatie. Daarnaast is er een Wetsvoorstel identificatie en authenticatie in de zorg (Wet Diaz) in behandeling. Twiin volgt de ontwikkelingen en zodra passende identificatiemiddelen beschikbaar komen, zullen die een plek krijgen in het Twiin Afsprakenstelsel.

Vereiste	Wie is (verwerkings)verantwoordelijk Dossierhouder of dossierraadpleger/-ontvanger	Invulling Twiin	Toelichting
Zorgaanbieders moeten elkaars identiteit met zekerheid kunnen vaststellen.	Beide	Identiteit van de zorgaanbieder: URA	De communicerende zorgaanbieders dienen als identificatie het UZI-register Abonneenummer (URA) gebruiken. De authenticatie van deze identiteit kan nog niet (altijd) op een hoog niveau plaatsvinden, slechts het op Twiin aangesloten GtK kan geauthenticeerd worden op basis van een PKIo-servercertificaat.

Vereiste	Wie is (verwerkings)verantwoordelijk Dossierhouder of dossierraadpleger/–ontvanger	Invulling Twiin	Toelichting
Zorgaanbieders moeten de voor de uitwisseling verantwoordelijke zorgverlener met zekerheid kunnen identificeren.	*Bij raadpleegbaar maken*:* De raadplegende zorgaanbieder moet zijn eigen gebruiker identificeren en authenticeren (NEN 7510 (see page 102)). De dossierhouder moet de identiteit kunnen controleren (d.m.v. een cryptografisch bewijs als een elektronische handtekening, volgens NEN 7512 (see page 102)). *Bij verzenden*:* De verzendende partij moet zijn eigen gebruiker identificeren en authenticeren (NEN 7510). De dossierontvanger moet de identiteit kunnen controleren (d.m.v. een cryptografisch bewijs als een elektronische handtekening, volgens NEN 7512).	*Bij raadpleegbaar maken:* De dossierraadpleger dient zijn eigen gebruikers te authenticeren op eIDAS hoog betrouwbaarheidsniveau. De authenticatie van de gebruikers door het Twiin–netwerk heen is nog niet mogelijk. Door het nog ontbreken van landelijke afspraken over cryptografisch bewijs hiervan/ ondertekening wordt dit door Twiin nog niet vereist. De dossierhouder kan de externe gebruiker daarmee wel identificeren maar niet met zekerheid (authenticeren). *Bij verzenden:* De dossierhouder dient zijn eigen gebruikers te authenticeren op eIDAS hoog betrouwbaarheidsniveau.	NEN 7512:2022 bepaalt het volgende: “Authenticatie van gebruikers van uit te wisselen persoonlijke gezondheidsinformatie moet in overeenstemming met eIDAS zijn, waarbij het betrouwbaarheidsniveau ‘hoog’ moet worden gebruikt.” Dit betekent dat de initiërende gebruiker geauthenticeerd moet worden. Ondertekening van het uitgewisselde is ook verplicht (NEN 7512:2022): “Ondertekening bij uitwisseling dient twee doelen. Ten eerste de toegenomen zekerheid omtrent de integriteit van de uitgewisselde gegevens en ten tweede de zekerheid omtrent de afzender. Immers, veel instellingen hebben grote hoeveelheden medewerkers en voorkomen behoort te worden dat een niet daartoe geautoriseerde medewerker de indruk kan wekken dat een onjuiste uitwisseling eigenlijk een goede uitwisseling is.” Ondertekening van gegevens is bedoeld voor de ontvanger. De ontvanger is op basis van NEN 7512:2022 gehouden om de ondertekening te controleren, dus bij raadplegen de dossierhouder en bij verzenden de dossierontvanger. De risicoklasse van de uitwisseling bepaalt welk betrouwbaarheidsniveau vereist is voor de handtekening.

Vereiste	Wie is (verwerkings)verantwoordelijk Dossierhouder of dossierraadpleger/–ontvanger	Invulling Twiin	Toelichting
		De authenticatie van de gebruikers door het Twiin–netwerk heen is nog niet mogelijk. Door het nog ontbreken van landelijke afspraken over cryptografisch bewijs hiervan / ondertekening wordt dit door Twiin nog niet vereist. Op welke manier en met welk betrouwbaarheidsniveau deze ondertekening moet plaats vinden hangt ook af van de NEN 7512 risicoklasse waar de betreffende gegevensuitwisseling onder valt. De dossierontvanger kan de externe gebruiker daarmee wel identificeren maar niet met zekerheid (authenticeren).	

* Verzenden en raadpleegbaar maken verwijzen naar de twee typen gegevensuitwisselingen. De communicatiepatronen (see page 169) zoals uitgewerkt in de technische kern kunnen worden onderverdeeld in deze twee typen.

5.3 | Vertrouwen: Autorisatie

Autorisatie

Autorisatie bepaalt of een zorgverlener informatie mag raadplegen op basis van zijn rol in het zorgproces. Hierbij moet de te raadplegen informatie proportioneel zijn. Dat betekent dat de inhoud en omvang van de informatie moet passen bij het doel waarvoor en de context waarin hij de informatie wil gebruiken. Het betreft hier alleen de autorisatie voor het raadplegen van informatie van buiten de eigen instelling.

Beroepsgeheim en toestemming

Op de zorgverleners rust het beroepsgeheim. Zorgverleners mogen alleen onder bepaalde voorwaarden hun beroepsgeheim doorbreken (zie ook onderdeel *Toestemming* van het vertrouwensmodel).

Proportionaliteit

Ook als een cliënt toestemming heeft gegeven, blijft de zorgverlener en zorgaanbieder verplicht om ervoor te zorgen dat niet meer gegevens worden gedeeld dan noodzakelijk. Als een zorgverlener meer gegevens deelt dan noodzakelijk, is dat een schending van het beroepsgeheim. Zorgverleners moeten kortom zorg dragen voor proportionaliteit.

De dossierhouder kan zorg dragen voor proportionaliteit, als de dossierhouder kan controleren welke zorgverlener welk dossier raadpleegt voor welk doel. Dit kan door in autorisatierichtlijnen en informatiestandaarden vast te leggen welke informatie nodig is. De dossierhouder moet vervolgens de toepassing van deze autorisatierichtlijnen en informatiestandaarden toepassen.[1]

Autorisatie en uitwisseling

Communicerende partijen en kaderstellende partijen moeten autorisatiebeleid vaststellen om gegevensuitwisseling tot stand te brengen (NEN 7512:2022, paragraaf 6.1.1). De Twiin Organisatie geeft hier als kaderstellende partij invulling aan met dit hoofdstuk 5.3. De Twiin Deelnemers geven hier invulling aan door het tekenen van de Twiin Deelnemersovereenkomst. Overigens bepaalt ook de *Gedragslijn toegangsbeveiliging digitale patiëntdossiers* dat het maken van afspraken over autorisatie verplicht is. In deze gedragslijn staat specifiek: "De organisatie moet alle partijen identificeren en documenteren waarmee cliëntgegevens worden uitgewisseld, en met deze partijen moeten contractuele afspraken over toegang en rechten worden gemaakt, alvorens cliëntgegevens uit te wisselen."[2]

De verantwoordelijkheid om specifieke afspraken te maken rust hier op de zorgaanbieder als instelling en niet op de zorgverleners. Overigens blijven zorgverleners wel tuchtrechtelijk aansprakelijk. Het centraal tuchtcollege heeft bepaald dat zorgverleners een regiebehandelaar moeten aanwijzen als de aard en/of complexiteit van de behandeling dat nodig maakt, bijvoorbeeld bij zorg die door zorgverleners van verschillende instellingen wordt verleend. Die regiebehandelaar moet er onder andere op toezien dat er een adequate informatie-uitwisseling is tussen de bij de behandeling van de cliënt betrokken zorgverleners.[3]

In de NEN 7513:2024 (paragraaf 8.5.2) is omschreven dat zorgaanbieders als uitwerking van wetgeving autorisatieprotocollen opstellen waarin de reguliere toegang tot bepaalde zorggegevens wordt gekoppeld aan een rol in het zorgproces. Deze werkwijze komt overeen met besluiten die zijn genomen binnen het Informatieberaad Zorg. Waarbij van belang is dat zorgaanbieders zich in het Integraal Zorgakkoord (IZA) hebben verbonden aan de oplossingen die door VWS in afstemming met het Informatieberaad Zorg zijn vastgesteld voor de generieke functies.

Ontwikkelingen

NEN is gestart met de ontwikkeling van een norm over autorisatie (NEN 7520). Twiin volgt de ontwikkelingen en zal aansluiten bij de uitkomsten.

Vereiste	Wie is (verwerkings)verantwoordelijk Dossierhouder of dossierraadpleger/-ontvanger	Invulling Twiin	Toelichting
De bron is verplicht om te zorgen dat niet meer gegevens worden geraadpleegd/vrijgegeven dan noodzakelijk en volgt de autorisatieafspraken zoals die voor de betreffende toepassing zijn afgesproken.	*Bij verzenden*:* Dossierhouder *Bij raadpleegbaar maken*:* Dossierhouder	Voor iedere gegevensuitwisseling zijn er afspraken gemaakt over wie welke gegevens (waarom) uitwisselen. Als deze autorisatieafspraken er niet op landelijk niveau zijn (tussen de betrokken zorgkoepels), zal Twiin (tijdelijke) afspraken maken met de Twiin Deelnemers.	Twiin volgt de ontwikkeling van de landelijke afspraken over autorisatie in de NEN 7520 en zal daarop aansluiten.

* Verzenden en raadpleegbaar maken verwijzen naar de twee typen gegevensuitwisselingen. De communicatiepatronen (see page 169) zoals uitgewerkt in de technische kern kunnen worden onderverdeeld in deze twee typen.

Voetnoten

1. Er is nog maar een beperkt aantal autorisatierichtlijnen beschikbaar. Het LSP kent een Medisch Autorisatie Protocol (MAP). Een ander voorbeeld is een autorisatierichtlijn voor medicatieveiligheid (https://www.aorta-lsp.nl/over-aorta-lsp/autorisatierichtlijnen/autorisatierichtlijn-medicatieveiligheid). In het kader van radiologisch onderzoek is binnen Twiin een concept autorisatierichtlijn opgesteld.

2. Gedragslijn toegangsbeveiliging digitale patiëntdossiers 2.0, d.d. 4 juli 2022 Te downloaden via: https://www.nvz-ziekenhuizen.nl/sites/default/files/2023-11/gedragslijn_toegangsbeveiliging_digitale_patientdossiers_nederlandse_vereniging.pdf
3. Centraal Tuchtcollege, 29 januari 2021 (ECLI:NL:TGZCTG:2021:36) https://tuchtrecht.overheid.nl/zoeken/resultaat/uitspraak/2021/ECLI_NL_TGZCTG_2021_36 .

5.4 | Vertrouwen: Behandelrelatie

Behandelrelatie

De verantwoordelijke gebruiker mag alleen toegang krijgen tot de cliëntgegevens, als er een (actieve) behandelrelatie is tussen de cliënt en deze gebruiker én als de zorgaanbieder een actieve behandelingsovereenkomst heeft met de cliënt.

Reikwijdte behandelingsovereenkomst en behandelrelatie

De reikwijdte van de behandelingsovereenkomst is tamelijk ruim. Er is sprake van een behandelingsovereenkomst als een zorgaanbieder zich beroepsmatig verbindt tot het 'verrichten van handelingen op het gebied van de geneeskunst'. Het kan hierbij gaan om alle verrichtingen – waaronder onderzoek en het geven van raad – met het doel om een cliënt 'van een ziekte te genezen, hem voor het ontstaan van een ziekte te behoeden of zijn gezondheidstoestand te beoordelen, dan wel verloskundige bijstand te verlenen'.

In sommige gevallen, zoals bij een eenmanspraktijk van een huisarts, zijn zorgaanbieder en zorgverlener dezelfde persoon. In de meeste gevallen is de zorgaanbieder echter een rechtspersoon, bijvoorbeeld een ziekenhuis, en is de zorgverlener de behandeld arts, bijvoorbeeld een specialist.

Zorgverleners zijn gehouden aan het beroepsgeheim en mogen anderen dan de cliënt geen inlichtingen over de cliënt verstrekken. Ze mogen anderen dan de cliënt ook geen inzage in of afschrift van de gegevens uit het dossier bieden, zonder toestemming van de cliënt. Een uitzondering geldt voor degenen die:

- rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst;
- optreden als vervanger van degene die een behandelingsovereenkomst heeft met de cliënt.

In beide gevallen geldt dat de informatieverstrekking noodzakelijk moet zijn voor het verrichten van de betrokken werkzaamheden.

Verder geldt een uitzondering voor situaties waarin een wettelijk vertegenwoordiger toestemming moet geven voor een behandeling.

Verzenden van gegevens

Bij het verzenden van gegevens verstuurt de dossierhouder zelf actief cliëntgegevens naar een bekende ontvanger. Zodoende bepaalt de dossierhouder zelf welke andere zorgaanbieder deze gegevens ontvangt. Bij de dossierhouder moet bekend zijn of deze zorgaanbieder een geneeskundige

behandelingsovereenkomst met de betrokken cliënt heeft of – bij een verwijzing – krijgt. De ontvangende zorgaanbieder (dossierontvanger) zal daarentegen moeten borgen dat de ontvangen gegevens alleen beschikbaar worden gesteld aan een zorgverlener met een behandelrelatie.

Gericht bevragen bij raadplegen van gegevens

Bij het raadplegen van gegevens is van belang dat de dossierraadpleger alleen gegevens opvraagt bij zorgaanbieders waar de cliënt al bekend is. Het beroepsgeheim staat eraan in de weg dat de raadpleger gegevens opvraagt bij alle zorgaanbieders die bereikbaar zijn via een elektronisch uitwisselingssysteem. Op die manier zou de dossierraadpleger aan zorgaanbieders die de cliënt niet kennen, bekend maken dat hij een behandelingsovereenkomst heeft met de cliënt. Dat is onwenselijk. Het bestaan van de geneeskundige behandelingsovereenkomst valt immers onder het beroepsgeheim. De dossierraadpleger is zodoende gehouden om alleen gericht gegevens op te vragen om zijn eigen beroepsgeheim ten aanzien van het bestaan van de geneeskundige behandelingsovereenkomst te borgen. Een lokalisatievoorziening is hiervoor een geschikte oplossing. De lokalisatievoorziening zorgt ervoor dat alleen gegevens worden opgevraagd bij zorgaanbieders waar de cliënt al bekend is.

Behandelingsovereenkomst zorgaanbieder bij raadplegen van gegevens

Bij het raadplegen van gegevens is het in beginsel de verantwoordelijkheid van een dossierhouder om te controleren of er sprake is van een behandelingsovereenkomst met de cliënt. De dossierhouder kan dit echter niet goed zelf controleren. De dossierhouder is vaak niet betrokken bij een opvolgend zorgtraject. Wanneer de huisarts de cliënt bijvoorbeeld doorverwijst naar het ziekenhuis, weet de huisarts niet altijd welk ziekenhuis de cliënt kiest. Zoals hierboven aangeduid zijn er geen middelen om zekerheid te bieden aan de bron over het bestaan van een behandelingsovereenkomst. Wanneer gegevens worden geraadpleegd moet de dossierhouder er daarom op vertrouwen dat de dossierraadpleger een behandelingsovereenkomst met de cliënt heeft. Wenselijk is om aanvullend op de afspraak over controle van de logging te zorgen voor een notificatie van de raadpleging naar de cliënt. Twiin geeft hier nog geen invulling aan.

Behandelrelatie zorgverlener bij raadplegen van gegevens

Welke zorgverleners de cliënt precies gaan behandelen, is vooraf niet altijd te zeggen. Hoofdbehandelaars kunnen bijvoorbeeld vervangen worden bij afwezigheid en veel zorgverleners werken in shifts en worden flexibel ingezet. Welke zorgverlener precies een behandelrelatie heeft met de cliënt, is soms voor een raadplegende instelling al lastig te bepalen. In dit vertrouwensmodel maken we daarom de afspraak dat de raadplegende zorgaanbieder controleert of er een behandelrelatie is met de raadplegende zorgverlener. De dossierhouder moet erop vertrouwen dat dit op de juiste manier gebeurt. Aanvullend is wenselijk om afspraken te maken over de controle van de behandelrelatie door middel van feitelijke omstandigheden. Een voorbeeld hiervan is een situatie waarbij een zorgverlener op de afdeling werkt waar de cliënt wordt behandeld en op dat moment dienst heeft.

Vereiste	Wie is (verwerkings)verantwoordelijk Dossierhouder of dossierraadpleger/-ontvanger	Invulling Twiin	Toelichting
Zorgaanbieders moeten zorgen dat enkel zorgaanbieders met een behandelingsovereenkomst en zorgverleners met een behandelrelatie het betrokken dossier kunnen raadplegen.	*Bij verzenden*:* Dossierontvanger *Bij raadpleegbaar maken*:* Dossierraadpleger	De dossierraadpleger en -ontvanger moeten beide een autorisatiestructuur hebben ingericht en zorgdragen voor logging en adequate controle van de logging. Twiin geef nog geen invulling aan controle van de behandelrelatie door middel van de techniek.	Adequate logging betekent dat dossierhouders achteraf de behandelingsovereenkomst en behandelrelatie moeten kunnen controleren. De inrichting van de logging moet passen bij de complexiteit van het systeem. Waar nodig moeten zorgaanbieders aanvullende logging en controle van logging inrichten. Er zijn nog geen oplossingsrichtingen voor controle voor de behandelrelatie op basis van techniek. Met de EHDS zal er een inrichting moeten komen voor het versturen van notificaties van raadplegingen naar de cliënt.

* Verzenden en raadpleegbaar maken verwijzen naar de twee typen gegevensuitwisselingen. De communicatiepatronen (see page 169) zoals uitgewerkt in de technische kern kunnen worden onderverdeeld in deze twee typen.

5.5 | Vertrouwen: Toestemming

Toestemming

De dossierhouder moet controleren of de cliënt afdoende toestemming heeft gegeven voordat hij toegang verleent tot diens cliëntgegevens.

Veronderstelde toestemming
Veronderstelde toestemming is toegestaan bij het verzenden van gegevens in het kader van een verwijzing en daarnaast in een aantal andere situaties zoals in een noodsituatie. Wel is vereist dat de cliënt vooraf kennis heeft kunnen nemen van de mogelijkheid dat zijn toestemming in bepaalde situaties mag worden verondersteld (tenzij dit niet mogelijk is, bijvoorbeeld in noodsituaties) én dat de cliënt daartegen geen bezwaar heeft gemaakt. Het is de verantwoordelijkheid van de dossierhouder om te bepalen of veronderstelde toestemming toereikend is en om te controleren of de cliënt geen bezwaar heeft gemaakt, voordat gegevens verzonden worden.

Uitdrukkelijke toestemming

Uitdrukkelijke toestemming is vereist voorafgaand aan het raadpleegbaar maken van gegevens door middel van een elektronisch uitwisselingssysteem zoals bedoeld in de Wabvpz. Kortom, uitdrukkelijke toestemming is nodig als van tevoren nog niet bepaald kan worden welke gegevens, wanneer en door wie geraadpleegd kunnen worden via zo'n systeem. Uitdrukkelijke toestemming betekent toestemming die vrijelijk is gegeven, ondubbelzinnig, specifiek en geïnformeerd is. Bij gebruik van een elektronisch uitwisselingssysteem zoals bedoeld in de Wabvpz, geldt dat niet alleen toestemming moet worden gevraagd voor het gebruik van deze infrastructuur, maar ook voor wat en voor wie de gegevens beschikbaar worden gesteld. Het is de verantwoordelijkheid van de dossierhouder om te controleren of de cliënt uitdrukkelijke toestemming heeft gegeven, voordat gegevens beschikbaar worden gemaakt voor raadplegen via een elektronisch uitwisselingssysteem. De dossierhouder moet ook voor iedere bevraging van het dossier controleren of de toestemming toereikend is.

Verantwoordelijkheid

De verantwoordelijke zorgaanbieder kan de toepassing van het autorisatieprotocol of controle op de cliënttoestemming/het bezwaar elders beleggen. Het gebruikte uitwisselingssysteem kan dit bijvoorbeeld namens de verantwoordelijke zorgaanbieder doen.

Ontwikkelingen

Er is een norm in ontwikkeling, NEN 7517, over toestemming. Twiin volgt de ontwikkelingen en sluit daarop aan.

Vereiste	Wie is (verwerkings)verantwoordelijk Dossierhouder of dossierraadpleger/-ontvanger	Invulling Twiin	Toelichting
De dossierhouder is verantwoordelijk voor de controle van de toestemming van de cliënt. *Bij verzenden*:* Veronderstelde toestemming is toegestaan als het gaat om de use case verwijzen en verder in een beperkt aantal situaties zoals in een noodsituatie. Bij opvragen dossier is WGBO-toestemming vereist. *Bij raadpleegbaar maken*:* Voorafgaande uitdrukkelijke toestemming is vereist.	Dossierhouder	Gebruik van Mitz bij raadpleegbaar maken	Twiin onderschrijft de wens van menig cliënt dat deze de toestemming voor de uitwisseling van gegevens via één kanaal kan regelen en dit niet per zorgaanbieder hoeft te doen. Deze mogelijkheid biedt Mitz. De cliënt kan binnen Mitz zijn eigen toestemmingskeuzes vastleggen. Daarnaast kan de zorgverlener namens de cliënt toestemmingskeuzes vastleggen in Mitz.

* Verzenden en raadpleegbaar maken verwijzen naar de twee typen gegevensuitwisselingen. De communicatiepatronen (see page 169) zoals uitgewerkt in de technische kern kunnen worden onderverdeeld in deze twee typen.

5.6 | Vertrouwen: Logging

Logging

Logging vindt zowel plaats bij de raadplegende/ontvangende partij als de dossierhouder. Hiermee wordt voldaan aan de NEN 7513. Daarnaast biedt het de dossierhouder inzage in wie cliëntgegevens heeft uitgewisseld en onder welke autorisatie dit is gedaan.

Gestandaardiseerde logging
Uit zowel artikel 15e Wabvpz (see page 102) als NEN 7510 (see page 102), NEN 7512 (see page 102) en met name NEN 7513 (see page 102) volgt dat zorgaanbieders cliënten inzage moeten kunnen geven in wie toegang

heeft gehad tot het cliëntdossier. Uit NEN 7513 volgt verder dat loggegevens uit de verschillende bronnen gecombineerd moeten kunnen worden in een overzicht. Gestandaardiseerde logging is een voorwaarde om dat mogelijk te maken. Bij informatiedomein overschrijdende (buiten de zorgaanbieder) of landelijke communicatie, moet logging uit verschillende bronnen vergelijkbaar zijn. Hiervoor moet een exportfaciliteit aanwezig zijn. Hierbij moet syntax en semantiek van de export vastliggen volgens de eisen in de NEN-norm. Telkens wanneer cliëntgegevens worden uitgewisseld, dienen loggegevens bijgehouden te worden.

Cliëntinzage

Cliënten hebben het recht de bijgehouden loggegevens van hun dossier in te zien. Zij kunnen zo monitoren wie wanneer hun gegevens heeft geraadpleegd. De naam van de betreffende verantwoordelijke dossierraadpleger moet worden getoond. Uitzonderingen zijn alleen toegestaan als het privacybelang van de zorgverlener zwaarder weegt dan het recht op inzage in de logging op persoonsnaam.

Vereiste	Wie is (verwerkings)verantwoordelijk Dossierhouder of dossierraadpleger/-ontvanger	Invulling Twiin	Toelichting
De communicerende partijen moeten voorzieningen in stand houden waarmee inzage in de loggingbestanden tot op gebruikersniveau voor de betrokken cliënten mogelijk is.	Dossierhouder en dossierraadpleger/-ontvanger	Twiin Deelnemers binden zich via de Voorwaarden Twiin Deelnemer (see page 142) aan het geven van inzage aan cliënten	Met de EHDS zal er een inrichting moeten komen voor het versturen van notificaties van raadplegingen naar de cliënt.
De communicerende partijen moeten afspraken maken over de interne inzage in en systematische controle van logging.	Dossierhouder en dossierraadpleger/-ontvanger	Twiin Deelnemers binden zich via de Voorwaarden Twiin Deelnemer aan het uitvoeren van de logging.	Eisen aan de inzage en systematische controle van de logging zullen nog worden opgenomen in het Twiin Afsprakenstelsel.

Vereiste	Wie is (verwerkings)verantwoordelijk Dossierhouder of dossierraadpleger/-ontvanger	Invulling Twiin	Toelichting
De communicerende partijen moeten afspraken maken over de wederzijdse inzage in de loggingbestanden en de termijn waarop deze mogelijk wordt gemaakt. In geval van (mogelijke) incidenten die onderzocht moeten worden is eventueel toegang tot de logging van de communicatiepartij nodig.	Dossierhouder en dossierraadpleger/-ontvanger	Twiin Deelnemers binden zich via de Voorwaarden Twiin Deelnemer aan het uitvoeren van de logging.	Zie hierover nr. 2.6 Voorwaarden Twiin Deelnemer (see page 142) en tevens het proces Incidentmelding (see page 137).

5.7 | Vertrouwen: Transparantie

ⓘ Transparantie

Communicerende partijen moeten transparant zijn in welke gegevens ze op welke manier uitwisselen.

Privacy statement

Artikel 12 van de AVG (see page 102) verplicht de zorgaanbieder als verwerkingsverantwoordelijke tot transparante verwerking van persoonsgegevens. De zorgaanbieder moet aan de cliënt beknopte, transparante, begrijpelijke informatie verstrekken in een gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal. Gebruikelijk is om deze informatie op te nemen in een privacyverklaring.

Het gaat hierbij onder meer om:

- de identiteit en de contactgegevens van de verwerkingsverantwoordelijke
- de verwerkingsdoeleinden
- de betrokken categorieën van persoonsgegevens
- de ontvangers, of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt
- alle beschikbare informatie over de bron van die gegevens, wanneer de persoonsgegevens niet bij de betrokkene worden verzameld

Ook moet de verwerkingsverantwoordelijke de betrokkene wijzen op zijn rechten om te verzoeken om rectificatie, beperking van de verwerking, het maken van bezwaar tegen de verwerking of het wissen van persoonsgegevens (Artikel 13 en 14 AVG).

Elektronisch uitwisselingssysteem

Op basis van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz (see page 102)) gelden aanvullende eisen ten aanzien van transparantie bij gebruik van een elektronisch uitwisselingssysteem zoals bedoeld in die wet. Artikel 15c Wabvpz verplicht de zorgaanbieder de cliënt te informeren over zijn rechten bij elektronische gegevensuitwisseling, de wijze waarop hij zijn rechten kan uitoefenen en over de werking van het elektronisch uitwisselingssysteem dat voor de gegevensuitwisseling in het kader van Twiin wordt gebruikt. Wanneer nieuwe categorieën van zorgaanbieders aansluiten bij Twiin, of de werking van Twiin substantieel wordt gewijzigd, informeert de zorgaanbieder de cliënt over deze wijziging, alsmede over de mogelijkheid om de gegeven toestemming aan te passen of in te trekken.

Cliëntinzage

Onderdeel van transparantie is ook dat cliënten het recht hebben de bijgehouden loggegevens van hun dossier in te zien. Dit aspect van transparantie is uitgewerkt in het hoofdstuk logging.

Vereiste	Wie is (verwerkings)verantwoordelijk Dossierhouder of dossierraadpleger/-ontvanger	Invulling Twiin	Toelichting
Zorgaanbieders moeten de cliënt op begrijpelijke wijze informeren over uitwisseling van gegevens en de uitoefening van zijn rechten.	Dossierhouder en dossierraadpleger/-ontvanger	De dossierraadpleger en -ontvanger moeten beide de cliënt in de privacyverklaring goed informeren over uitwisseling en over zijn AVG-rechten en tevens moeten zij zorgdragen voor een procedure waarmee cliënten de logging kunnen opvragen.	Niet van toepassing

6 | Governance

Inleiding

Onder governance verstaan we de inrichting van de rollen, taken, verantwoordelijkheden en spelregels die nodig zijn voor het beheer en de doorontwikkeling van het Twiin Afsprakenstelsel. In het Twiin Afsprakenstelsel is vastgelegd hoe de inspraak en de besluitvorming wordt georganiseerd, wie de betrokken partijen zijn en wie zij vertegenwoordigen. De governance van Twiin bepaalt ook hoe partijen waarborgen dat alle deelnemende organisaties voldoen en blijven voldoen aan de afspraken. Daaronder valt onder andere het maken van contractuele afspraken en de toetsing van de Twiin Voorwaarden. Een goede inrichting van de governance draagt bij aan het vertrouwen in het Twiin Afsprakenstelsel.

Op deze pagina volgt een overzicht van de rollen in het Twiin Afsprakenstelsel. Daarna wordt uitgelegd hoe de Twiin Deelnemer (de zorgaanbieder) zich verbindt aan het Twiin Afsprakenstelsel door de Deelnemersovereenkomst te tekenen. Vervolgens volgt een uitleg over de verklaringen die de GtK Leverancier, GtK Beheerder en Twiin Dienstverlener ondertekenen en waarmee zij zich verbinden aan het Twiin Afsprakenstelsel. Dan wordt uitgelegd hoe validatie is ingericht. Tot slot volgt uitleg over de wijze waarop partijen inspraak hebben bij de doorontwikkeling van het Twiin Afsprakenstelsel.

Rollen en actoren

Het Twiin Afsprakenstelsel gaat uit van de volgende rollen en actoren:

Rol: De Twiin Deelnemer wisselt binnen de kaders van het Twiin Afsprakenstelsel gegevens uit met andere Twiin Deelnemers.

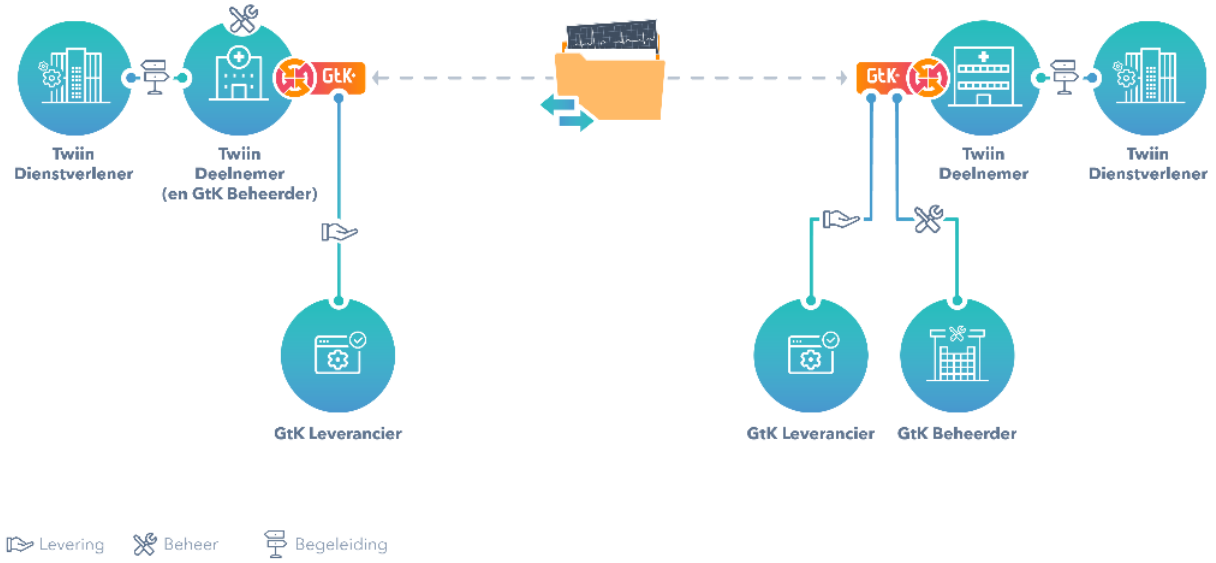
Rol: De Twiin Dienstverlener biedt diensten aan één of meer Twiin Deelnemers. Dit omvat onder andere het begeleiden bij de implementatie, beheer en ontwikkeling van één of meer zorgtoepassingen binnen een regio en/of binnen een categoraal netwerk en ondersteuning bij het voldoen aan het Twiin Afsprakenstelsel.

Rol: De GtK Beheerder voert beheertaken uit ten aanzien van een GtK, waaronder het inrichten van een servicedesk.

Rol: De GtK Leverancier is de leverancier van een GtK.

Actor: Het Twiin Bestuur is het organisatieonderdeel van de Twiin Organisatie dat eindverantwoordelijk is voor het beheer en de doorontwikkeling van het Twiin Afsprakenstelsel. Vooralsnog is dit de stuurgroep van het programma Twiin. In het licht van de keuze voor Twiin als Landelijk Vertrouwensstelsel heeft VWS opdracht gegeven voor een verkenning naar de positie en het eigenaarschap van het Twiin Afsprakenstelsel voor de komende 3 á 4 jaar. Vooruitlopend op definitieve besluitvorming over de positie van het Twiin Afsprakenstelsel in stelselregie heeft VZVZ aangegeven bereid te zijn om als Twiin Beheerorganisatie op te treden. In de stuurgroep V&V (inmiddels DTO) van 29 juni 2023 is afgesproken dat VZVZ voorlopig een aantal operationele beheertaken oppakt. De beheerstaken blijven initieel beperkt tot contractbeheer (ondertekenen van de deelnemersovereenkomsten) en worden gefaseerd uitgebreid al naar gelang het tempo waarin de opschaling van de implementatie plaatsvindt.

De partijen die zijn aangesloten (see page 119) bij het Twiin Afsprakenstelsel in één of meer van de vier rollen vormen samen met de Twiin Organisatie het Twiin Samenwerkingsverband.



Bovenstaand figuur laat zien hoe de rollen zich tot elkaar verhouden. Centraal staan de Twiin Deelnemers die gegevens uitwisselen door middel van een GtK. De figuur toont dat de Twiin Dienstverlener naast de Twiin Deelnemer staat om te begeleiden bij de implementatie van één of meer zorgtoepassingen. Verder laat de figuur zien dat er ruimte is voor verschillen in de wijze waarop partijen samenwerken. De GtK Leverancier kan ook het beheer op zich nemen, terwijl het ook mogelijk is dat er een afzonderlijke partij is die het beheer op zich neemt. Deze krijgt dan de rol van GtK Beheerder.

Deelnemersovereenkomst

Inspanningsverplichting

De Twiin Deelnemer (de zorgaanbieder) sluit de Deelnemersovereenkomst met de Twiin Organisatie. Een Twiin Deelnemer kan eventueel een Twiin Dienstverlener machtigen om dit namens hem te doen. Na toetreding kan de Twiin Deelnemer uitwisselen volgens het éénhandtekeningprincipe met andere Twiin Deelnemers die voldoen aan dezelfde Samenwerkingsvoorwaarden. De voorwaarden die gelden vanaf ondertekening en de voorwaarden die gelden vanaf validatie zijn opgenomen in de 9.1 | Voorwaarden Twiin Deelnemer (see page 142). De Twiin Dienstverlener houdt bij welke andere Twiin Deelnemers voldoen aan dezelfde Samenwerkingsvoorwaarden. Door het tekenen van de Deelnemersovereenkomst is de Twiin Deelnemer gehouden om toe te werken naar validatie voor één of meerdere zorgtoepassingen (inspanningsverplichting). Vanaf validatie moet de Twiin Deelnemer voldoen aan alle Twiin voorwaarden en kan de Twiin Deelnemer landelijk gegevens uitwisselen.

Eénhandtekeningprincipe

De governance is zo ingericht dat gaandeweg meer deelnemers kunnen aansluiten. Deze opzet betekent dat deelnemende partijen éénmaal een Deelnemersovereenkomst ondertekenen en daarmee ook akkoord gaan met toetreding van nieuwe leden en nieuwe versies van het Twiin Afsprakenstelsel. Zo voorkomen we dat het toetreden van nieuwe Twiin Deelnemers en de release van nieuwe versies van het Twiin Afsprakenstelsel leiden tot het steeds opnieuw tekenen van overeenkomsten met nieuwe deelnemers. Bovendien is de governance zo ingericht dat Twiin Deelnemers ruimte hebben om toe te groeien naar validatie.

Voorwaarden

De Twiin Deelnemer zorgt ervoor dat per zorgtoepassing één Twiin Dienstverlener is aangewezen die de 9.2 | Voorwaarden Twiin Dienstverlener (see page 151) vervult, waaronder het beheer van de Samenwerkingsvoorwaarden voor Twiin Deelnemer. De Twiin Deelnemer zorgt dat de Twiin Organisatie beschikt over de contactgegevens van de door haar ingeschakelde Twiin Dienstverlener(s) en stelt de Twiin Organisatie op de hoogte als sprake is van een wisseling.

De Twiin Deelnemer zorgt ervoor dat de Voorwaarden Twiin Dienstverlener zijn belegd. Datzelfde geldt voor de 9.3 | Voorwaarden GtK Beheer (see page 155). Als de Twiin Deelnemer een externe partij inschakelt voor GtK beheer, maakt de Twiin Deelnemer zelf passende afspraken met deze partij.

In veel gevallen zal de Twiin Deelnemer zelf al afspraken gemaakt hebben met externe partijen die de rol vervullen van Twiin Dienstverlener en/of GtK Beheerder. Zo niet, dan kan de deelnemer gebruikmaken van de modelovereenkomsten die Twiin beschikbaar stelt. De Twiin Deelnemer kan de modelovereenkomsten ook gebruiken om bestaande afspraken te toetsen. Het gaat om de een model dienstverleningsovereenkomst en model beheerovereenkomst. Deze modelovereenkomsten zijn op te vragen via info@twiin.nl[22].

Verklaringen

Verklaring Twiin Dienstverlener

De Twiin Dienstverlener ondertekent de 9.2 | Voorwaarden Twiin Dienstverlener (see page 151). Daarin verklaart deze partij dat hij de taken en verantwoordelijkheden op zich neemt zoals die in het Twiin Afsprakenstelsel voor deze rol staan beschreven. De Twiin Organisatie onderschrijft met het accepteren van de verklaring dat de diensten die de Twiin Dienstverlener aanbiedt, passend zijn om invulling te geven aan zijn rol zoals omschreven in het Twiin Afsprakenstelsel.

De Twiin Deelnemer kan ook de rol van Twiin Dienstverlener vervullen voor zichzelf en voor andere Twiin Deelnemers.

Het proces voor het tekenen van een Verklaring Twiin Dienstverlener is beschreven op de pagina 8.1.2 | Aansluiten Twiin Dienstverlener (see page 121).

Verklaring GtK Beheerder

De Twiin Deelnemer kan besluiten om de taken en verantwoordelijkheden van de GtK Beheerder geheel of ten dele zelf uit te voeren. De Twiin Deelnemer kan ook besluiten om een aparte GtK Beheerder in te schakelen. Als de GtK Beheerder een rol krijgt en betrokken wil worden bij de doorontwikkeling van het Twiin Afsprakenstelsel op basis van het 6.6 | Reglement (see page 98), is vereist dat GtK Beheerder de 6.3 |

22. mailto:info@twiin.nl

Verklaring GtK Beheerder (see page 94) tekent. Daarin verklaart de GtK Beheerder dat hij de taken en verantwoordelijkheden op zich neemt zoals die in het Twiin Afsprakenstelsel voor zijn rol staan beschreven. De Twiin Organisatie onderschrijft met het accepteren van de verklaring dat de diensten die de GtK Beheerder aanbiedt, passend zijn om invulling te geven aan zijn rol zoals omschreven in het Twiin Afsprakenstelsel.

Het proces voor het tekenen van een Verklaring GtK Beheer is beschreven in onderdeel 8.1.3 | Aansluiten GtK Beheerder (see page 124).

Verklaring GtK Leverancier

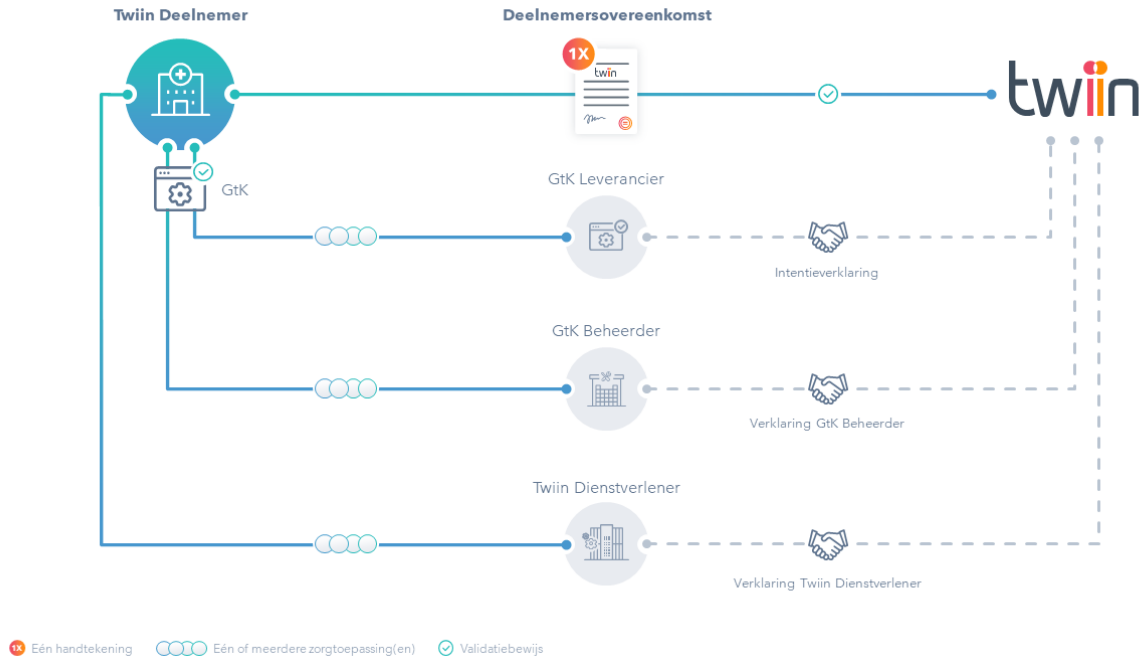
Een leverancier die een applicatie of functionaliteit wil laten valideren als GtK, tekent eerst een 6.4 | Verklaring GtK Leverancier (see page 95) waarin is bepaald dat de leverancier zich inspant om zo goed mogelijk te voldoen aan het Twiin Afsprakenstelsel.

Het proces voor het tekenen van een Verklaring GtK Leverancier is beschreven in onderdeel 8.1.4 | Aansluiten GtK Leverancier (see page 126).

Validatie

Validatie is de manier waarop geborgd wordt dat het GtK en de Twiin Deelnemer voldoen aan alle voorwaarden.

1. **Validatie Twiin Deelnemer**: Als het proces 8.2.1 | Validatie Twiin Deelnemer (see page 128) met goed gevolg is doorlopen voor één of meer zorgtoepassingen, voldoet de Twiin Deelnemer voor die zorgtoepassing(en) aan alle voorwaarden van het Twiin Afsprakenstelsel voor het landelijk beschikbaar stellen en uitwisselen van gegevens. De Twiin Deelnemer verkrijgt een bewijs van validatie. De Twiin Dienstverlener ondersteunt de Twiin Deelnemer bij het doorlopen van de stappen die nodig zijn om te komen tot validatie. De Twiin Deelnemer maakt gebruik van een GtK en doorloopt zelf ook het validatieproces.
2. **Validatie GtK**: Als het proces 8.2.2 | Validatie GtK (see page 132) met goed gevolg is doorlopen, voldoet de applicatie aan alle eisen om te kunnen gebruiken voor uitwisseling op basis van het Twiin Afsprakenstelsel.



Bovenstaand figuur laat zien hoe de verschillende rollen zich tot elkaar verhouden bij het tekenen van de Deelnemersovereenkomst, de verklaringen en de validatie.

Releasebeleid en reglement

Het 6.5 | Releasebeleid (see page 97) bepaalt hoe vaak wijzigingen door middel van een nieuwe release kunnen worden doorgevoerd en welke versies geldig zijn. Het 6.6 | Reglement (see page 98)beschrijft hoe de relevante stakeholders worden betrokken bij de ontwikkeling van het Twiin Afsprakenstelsel en hoe de besluitvorming verloopt ten aanzien van het vaststellen van nieuwe releases. In het reglement is vastgelegd hoe partijen worden gerepresenteerd en kunnen meebeslissen over wijzigingen. De Twiin Organisatie zorgt als beheerder van het Twiin Afsprakenstelsel dat de vertegenwoordiging helder is en dat de besluitvorming transparant en open toegankelijk is voor de Twiin Deelnemers, Twiin Dienstverleners, GtK Beheerders en GtK Leveranciers.

6.1 | Deelnemersovereenkomst

Twiin Deelnemersovereenkomst

Partijen:

1. [Naam Twiin Organisatie], gevestigd aan de [straat] te [postcode] [plaatsnaam], rechtsgeldig vertegenwoordigd door […] (hierna te noemen "**Twiin Organisatie**");

en

2. [Zorgaanbieder], gevestigd te […], rechtsgeldig vertegenwoordigd door […] (hierna te noemen "**[Deelnemer]**");

hierna afzonderlijk te noemen 'Partij' en gezamenlijk te noemen 'Partijen'.

Overwegingen:

A. Deelnemer wil toetreden tot het Twiin Afsprakenstelsel, een landelijk afsprakenstelsel op basis waarvan verschillende organisaties veilig en betrouwbaar gegevens kunnen uitwisselen over bestaande zorgnetwerken, platformen en voorzieningen heen. Het gaat hierbij om databeschikbaarheid door middel van raadplegen en door middel van verzenden.

B. Deelnemer erkent de Twiin doelstellingen, de Twiin principes en het juridische kader van het Twiin Afsprakenstelsel en is bereid daarnaar te handelen;

C. Na toetreding kan Deelnemer onder regie van de Twiin Dienstverlener uitwisselen volgens het éénhandtekeningprincipe met andere Twiin Deelnemers die voldoen aan dezelfde Samenwerkingsvoorwaarden, zoals hieronder gedefinieerd. Het éénhandtekeningprincipe betekent dat de Deelnemer éénmalig deze overeenkomst tekent en daarmee partij wordt bij het Twiin Afsprakenstelsel samen met alle andere Twiin Deelnemers;

D. Deelnemer erkent dat voor landelijke uitwisseling met alle Twiin Deelnemers de Samenwerkingsvoorwaarden niet afdoende zijn en deelnemer verbindt zich onder regie van de Twiin Dienstverlener zo snel mogelijk te komen tot naleving van de Twiin Voorwaarden;

E. Deelnemer heeft de intentie om zich te laten valideren volgens het Proces Validatie, zoals hieronder gedefinieerd. Voor zover er nog geen implementatiehandleiding is voor de specifieke zorgtoepassing waar Deelnemer gebruik van wil maken, is Deelnemer bereid mee te helpen bij het ontwikkelen daarvan;

F. Na validatie kan Deelnemer komen tot landelijke uitwisseling op basis van het Twiin Afsprakenstelsel met alle aangesloten organisaties en heeft Deelnemer zekerheid dat deze voldoen aan het Twiin Afsprakenstelsel;

G. De Twiin Organisatie beheert het Twiin Afsprakenstelsel en faciliteert de verdere ontwikkeling daarvan en sluit daarbij voor de verschillende zorgtoepassingen aan op de uitwerking van de onder de Wegiz aangewezen gegevensuitwisselingen.

Komen hierbij overeen:

1. *Definities en hiërarchie overeenkomst*

a. De volgende begrippen hebben voor het doel van deze overeenkomst de volgende betekenis:

i. Bewijs van Validatie: het bewijs dat aan Deelnemer wordt verstrekt van het succesvol doorlopen van het Proces Validatie;

ii. Deelnemer: de Partij die is toegetreden tot het Twiin Afsprakenstelsel;

iii. GtK: een applicatie of een koppelvlak met functionaliteit voor gegevensuitwisseling;

iv. GtK Beheerder: een organisatie die verantwoordelijk is voor het technisch beheer over het GtK welke rol (geheel of ten dele) namens de Deelnemer door een derde partij uitgevoerd kan worden en ook door Deelnemer zelf;

v. Overeenkomst: de onderhavige overeenkomst;

vi. Proces Validatie: het proces zoals Twiin Deelnemers dat doorlopen om vast te stellen of zij voldoen aan de Twiin Voorwaarden die gelden voor landelijke uitwisseling zoals opgenomen in de vigerende versie van het Twiin Afsprakenstelsel;

vii. Reglement: het reglement waarin is vastgelegd hoe de vertegenwoordiging van de Twiin Deelnemers is geregeld voor de besluitvormingsprocedure over nieuwe releases;

viii. Samenwerkingsvoorwaarden: de voorwaarden die beschrijven in hoeverre sprake is van een afwijking van de Twiin Voorwaarden en die worden opgenomen in een bijlage bij deze overeenkomst;

ix. Twiin Afsprakenstelsel: set van afspraken, procedures en regels op het gebied van organisatie, besturing, toezicht, beheer, architectuur, toepassingen en techniek op basis waarvan Twiin Deelnemers landelijk gegevens uit kunnen wisselen waarbij dit stelsel releasematig wordt ontwikkeld en waarvan de vigerende versie gepubliceerd is op de website www.twiin.nl[23];

x. Twiin Dienstverlener: een implementatie- en kennispartner die begeleidt bij de implementatie, beheer en ontwikkeling van zorgtoepassingen en die één of meer Twiin Deelnemer(s) ondersteunt om te voldoen aan het Twiin Afsprakenstelsel;

xi. Twiin Deelnemer: organisatie die is toegetreden tot het Twiin Afsprakenstelsel;

xii. Twiin Voorwaarden: de voorwaarden voor Twiin Deelnemers die deel uitmaken van de vigerende versie van de het Twiin Afsprakenstelsel;

xii. Vertrouwelijke Informatie: informatie die in het kader van deze overeenkomst door Deelnemer en de Twiin Organisatie wordt uitgewisseld waaronder in het kader van toetreding en validatie en die als vertrouwelijk is gemarkeerd of waarvan het vertrouwelijke karakter aan de ontvangende Partij genoegzaam bekend was;

xiv. Zorgtoepassing: de oplossing voor gegevensbeschikbaarheid ter ondersteuning van een specifiek zorgproces.

b. De bijlagen vormen een onlosmakelijk deel van deze overeenkomst.

23. http://www.twiin.nl/

2. *Beheer Twiin Afsprakenstelsel*

a. Deelnemer is ermee bekend en verklaart zich ermee akkoord dat de Twiin Voorwaarden van tijd tot tijd eenzijdig gewijzigd kunnen worden in het kader van het releasematig beheer van het Twiin Afsprakenstelsel waaronder ook wijzigingen:

i. op basis van besluitvorming conform het Reglement;

ii. voor zover noodzakelijk door wijziging van wet- en regelgeving;

iii. voor zover noodzakelijk om te blijven voldoen aan de actuele beveiligingsstandaarden.

b. Wijzigingen in het Twiin Afsprakenstelsel treden steeds in werking op de wijze als beschreven in het Twiin Afsprakenstelsel. In geval van wijzigingen in de Twiin Voorwaarden is Deelnemer verplicht binnen daarvoor vastgestelde termijnen alle stappen te zetten en alle aanpassingen door te voeren die nodig zijn om te blijven voldoen aan de Twiin Voorwaarden.

3. *Rechten en verplichtingen Deelnemer zonder validatie*

a. Deelnemer gaat deze overeenkomst aan met het doel om met andere Twiin Deelnemers gegevens van cliënten elektronisch uit te wisselen. Deelnemer is bereid om gegevens uit te wisselen met andere Twiin Deelnemers die dezelfde Samenwerkingsvoorwaarden onderschrijven.

b. Deelnemer voldoet en blijft voldoen aan alle Twiin Voorwaarden waarvan geen afwijking mogelijk is. Hiermee draagt Deelnemer zorg voor de minimale randvoorwaarden voor uitwisseling van medische gegevens.

c. Deelnemer erkent dat de Samenwerkingsvoorwaarden niet afdoende zijn voor landelijke uitwisseling van gegevens met alle Twiin Deelnemers. Deelnemer bepaalt in afstemming met de Twiin Dienstverlener met welke Twiin Deelnemers hij uitwisselt op basis van de Samenwerkingsvoorwaarden.

d. Deelnemer spant zich ervoor in dat de Samenwerkingsvoorwaarden zo min mogelijk afwijken van de Twiin Voorwaarden en laat zich hierbij adviseren en bijstaan door de Twiin Dienstverlener.

e. Deelnemer zorgt ervoor dat hij zo snel mogelijk voldoet aan alle Twiin Voorwaarden ten einde het Proces Validatie voor minstens één zorgtoepassing met succes af te ronden. Deelnemer spant zich in om alle stappen te zetten die daarvoor nodig zijn. Deelnemer volgt hierbij het groeimodel dat de Twiin Organisatie hiervoor heeft ontwikkeld en laat zich hierbij ondersteunen door de Twiin Dienstverlener.

4. *Rechten en verplichtingen Deelnemer met Validatie*

a. Zodra Deelnemer gevalideerd is voor een bepaalde zorgtoepassing, is Deelnemer verplicht voor die zorgtoepassing:

i. Aantoonbaar te voldoen aan het Twiin Afsprakenstelsel, waaronder de Twiin Voorwaarden, ook in het geval een voorwaarde niet in de vorm van een verplichting is omschreven;

ii. Zich te conformeren aan de operationele processen (see page 119) en het beleid van het Twiin Afsprakenstelsel, alsmede de voor de Deelnemer relevante architectuur (see page 37) en technische specificaties (see page 164); en

iii. Zijn werkprocessen zodanig in te richten dat die in overeenstemming zijn met alle processen en regelingen zoals die zijn beschreven in het Twiin Afsprakenstelsel;

iv. Kennis te nemen van de wijzigingen en daarbij behorende release notes van het Twiin Afsprakenstelsel, zodat de Deelnemer steeds van de meeste recente versie van het Twiin Afsprakenstelsel op de hoogte is.

b. Deelnemer maakt na validatie voor de betrokken zorgtoepassing enkel gebruik van een GtK die aantoonbaar voldoet aan de eisen van het Twiin Afsprakenstelsel. Het GtK voldoet aantoonbaar aan de eisen van het Twiin Afsprakenstelsel als deze is gevalideerd op basis van het Twiin Afsprakenstelsel.

c. Deelnemer is gehouden om zich periodiek opnieuw te laten toetsen op naleving van de Twiin Voorwaarden, conform de termijnen zoals beschreven in het Proces Validatie. Deelnemer verstrekt aan de Twiin Organisatie alle relevante informatie voor het verkrijgen, behouden en periodiek hernieuwen van het Bewijs van Validatie.

d. Aan het Bewijs van Validatie kan Deelnemer niet de verwachting ontlenen dat de Deelnemer voldoet aan de voorwaarden van de overeenkomst. Het blijft te allen tijde de verantwoordelijkheid van de Deelnemer om volledig te voldoen aan alle voorwaarden van de overeenkomst, waaronder mede begrepen de afspraken uit het Twiin Afsprakenstelsel.

5. *GtK-beheer*

a. Deelnemer zal de benodigde verbindingen tot stand brengen tussen de eigen zorginformatiesystemen en het GtK en tussen het eigen GtK en die van andere Twiin Deelnemers.

b. Deelnemer is ervoor verantwoordelijk dat het beheer van het GtK adequaat wordt uitgevoerd en dat de voorwaarden van GtK-beheer worden vervuld. Deelnemer kan deze verplichtingen nakomen door een GtK Beheerder in te schakelen.

c. Als een derde partij in opdracht van Deelnemer persoonsgegevens verwerkt in het kader van deze overeenkomst, sluit Deelnemer een verwerkersovereenkomst met deze derde partij.

6. *Beheer Samenwerkingsvoorwaarden en rol Twiin Dienstverlener*

a. Deelnemer zorgt ervoor dat er per zorgtoepassing één Twiin Dienstverlener is aangewezen die de voorwaarden van de Twiin Dienstverlener vervult, waaronder het beheer van de Samenwerkingsvoorwaarden voor Deelnemer. Deelnemer zorgt dat de Twiin Organisatie beschikt over de contactgegevens van de door hem ingeschakelde Twiin Dienstverlener(s) en stelt de Twiin Organisatie op de hoogte als sprake is van een verandering.

b. In opdracht van de Deelnemer houdt de Twiin Dienstverlener het overzicht bij van de Twiin Deelnemers waarmee Deelnemer uitwisselt op basis van de Samenwerkingsvoorwaarden.

c. De Deelnemer beslist zelf om de Twiin Dienstverlener eventueel een mandaat te geven om besluiten te nemen over de vraag met welke andere Twiin Deelnemers de Deelnemer uitwisselt.

d. De Twiin Dienstverlener geeft advies en doet voorstellen over (het tijdspad voor) de tussenstappen en het tijdspad om afwijkingen zoals omschreven in de Samenwerkingsvoorwaarden zo snel mogelijk te laten vervallen om te zorgen dat deelnemer zo snel mogelijk voldoet aan alle Twiin Voorwaarden.

e. De Deelnemer kan ook zelf de rol van Twiin Dienstverlener vervullen voor zichzelf en voor andere Twiin Deelnemers. In dat geval, is de Deelnemer zelf gehouden om de voorwaarden van die rol te vervullen.

7. *Taken en verantwoordelijkheden Twiin Organisatie*

a. De Twiin Organisatie is verplicht om het Twiin Afsprakenstelsel te onderhouden, waaronder ook is begrepen het zorgen voor periodieke herziening in lijn met ontwikkelingen in wet- en regelgeving, beveiligings-, kwaliteits- en informatiestandaarden.

b. De Twiin Organisatie zorgt ervoor dat Twiin Deelnemers zich kunnen laten vertegenwoordigen bij de besluitvorming over wijzigingen in het Twiin Afsprakenstelsel. De Twiin Organisatie zorgt ervoor dat de vertegenwoordiging van deze groepen adequaat is en de besluitvormingsprocedure transparant, zoals omschreven in het Reglement. De Twiin Organisatie zorgt ervoor dat Twiin Dienstverleners en GtK Beheerders in de rol van expert een inhoudelijke bijdrage kunnen leveren.

c. De Twiin Organisatie faciliteert het Proces Validatie dat Twiin Deelnemers doorlopen. Als Deelnemer voldoet aan de Twiin Voorwaarden verstrekt de Twiin Organisatie aan Deelnemer een Bewijs van Validatie.

d. De Twiin Organisatie heeft het recht om te controleren op de naleving van de Twiin Voorwaarden door Deelnemer conform het Twiin Afsprakenstelsel, zowel periodiek als bij signalen van niet-naleving.

e. Indien Deelnemer aantoonbaar niet voldoet aan het Twiin Afsprakenstelsel en/of de overige verplichtingen uit de overeenkomst, heeft de Twiin Organisatie het recht om het Bewijs van Validatie van de Deelnemer per direct in te trekken tot het moment dat Deelnemer naar het oordeel van de Twiin Organisatie heeft aangetoond dat hij zijn verplichtingen wel nakomt.

f. De Twiin Organisatie spant zich in om steeds voordat hij gebruikmaakt van de bevoegdheden als beschreven in artikel 7.e in overleg te treden met de Deelnemer, tenzij de aard of de spoedeisendheid van de tekortkoming dat naar het oordeel van de Twiin Organisatie niet toelaten.

g. Indien de Twiin Organisatie gebruik maakt van het recht als bedoeld in artikel 7.e van de overeenkomst meldt hij dit onverwijld aan de Deelnemer.

8. *Toetreding nieuwe leden Twiin Afsprakenstelsel*

a. Deelnemer gaat akkoord met toetreding van andere partijen tot het Twiin Afsprakenstelsel.

b. Het staat Deelnemer vrij individueel afspraken te maken met andere organisaties en samenwerkingsverbanden over elektronische gegevensuitwisseling mits dat geen nadelig effect heeft op de afspraken zoals geregeld in deze overeenkomst.

9. *Intellectuele eigendomsrechten, publicatie, geheimhouding*

a. Deelnemer verkrijgt een licentie op het gebruik van het Twiin Afsprakenstelsel inclusief alle onderliggende modellen, begeleidende documenten en hulpmiddelen op basis van de Creative Commons licentievoorwaarden getiteld 'Naamsvermelding-GelijkDelen 4.0 Internationaal'. De volledige licentievoorwaarden zijn beschikbaar via: http://creativecommons.org/licenses/by-sa/4.0/ .

b. De Twiin Organisatie heeft het recht om het bestaan van deze overeenkomst, de naam en het logo van Deelnemer in haar communicatiemiddelen te vermelden waaronder op de website voor zover nodig voor de doelstellingen van het Twiin Afsprakenstelsel. Deelnemer heeft enkel het recht om het logo van de Twiin Organisatie te gebruiken om kenbaar te maken dat Deelnemer is toegetreden of gevalideerd conform de publicatierichtlijnen van de Twiin Organisatie en voor overige doeleinden enkel na voorafgaande schriftelijke goedkeuring.

c. Partijen erkennen het gerechtvaardigde en grote belang bij bescherming van Vertrouwelijke Informatie en Partijen verplichten zich tot strikte geheimhouding hiervan, tenzij een wettelijke plicht of een rechterlijke uitspraak openbaarmaking van deze gegevens gebiedt. Partijen dragen ervoor zorg dat zij deze geheimhoudingsplicht mede opleggen aan hun medewerkers en aan hun eventuele opdrachtnemers.

d. Deze geheimhouding duurt tot vijf (5) jaar na de beëindiging van deze overeenkomst.

10. *Kosten en aansprakelijkheid*

a. Partijen dragen ieder de eigen kosten, zowel van ICT-voorzieningen als voor inzet van medewerkers als overige met de samenwerking samenhangende kosten. Iedere Partij is verantwoordelijk en aansprakelijk voor het eigen handelen en draagt ieder voor zich zorg voor afdoende dekking van de aansprakelijkheid.

b. Iedere contractuele en buiten-contractuele aansprakelijkheid van de Twiin Organisatie is beperkt tot een bedrag van €10.000,-- per gebeurtenis of reeks van samenhangende gebeurtenissen. De Twiin Organisatie is uitsluitend aansprakelijk voor directe schade, dat wil zeggen schade die in een direct en onlosmakelijk verband staat met de schadeveroorzakende gebeurtenis. Iedere aansprakelijkheid van de Twiin Organisatie voor indirecte schade is uitgesloten. Met indirecte schade wordt gedoeld op gederfde winst, gemiste besparingen, verminderde goodwill, schade door bedrijfsstagnatie en schade als gevolg van aanspraken van een cliënt.

c. De beperking en uitsluitingen van aansprakelijkheid in dit artikel gelden tenzij er sprake is van opzet of grove schuld van de Twiin Organisatie, personeel van de Twiin Organisatie dan wel voor zover enige beperking of uitsluiting rechtens niet is toegestaan.

d. Partijen stellen elkaar op de hoogte in geval van onderzoek en/of handhaving door een toezichthouder in verband met deze overeenkomst. Als de medewerking van een andere Partij

nodig is in geval van een onderzoek en/of handhaving verplicht deze Partij zich om al het redelijke te doen wat binnen de kaders van deze overeenkomst verwacht mag worden.

11. *Aanvang, duur, beëindiging en gevolgen van beëindiging*

a. De overeenkomst gaat in op het tijdstip van ondertekenen en geldt voor een periode die eindigt op één januari van eerstvolgende kalenderjaar. Na verloop van de eerste termijn wordt de overeenkomst telkens met een termijn van twee jaar verlengd.

b. Deelnemer heeft het recht om deze overeenkomst op elk moment schriftelijk op te zeggen met een opzegtermijn van minimaal zes (6) maanden. De Twiin Organisatie heeft het recht om deze overeenkomst op te zeggen met een opzegtermijn van minimaal twaalf (12) maanden als sprake is van zwaarwegende omstandigheden die verhinderen dat zij aan haar verplichtingen kan voldoen, zoals wijzigingen van wet- en regelgeving die de nakoming van de overeenkomst verhinderen. Op verzoek werkt de Twiin Organisatie in voorkomend geval mee aan een overdracht van haar taken en verplichtingen aan een opvolgende partij en spant zich in om deze overdracht te bewerkstelligen.

c. Ieder der Partijen is gerechtigd de overeenkomst door middel van een aangetekend schrijven zonder rechterlijke tussenkomst te ontbinden als de andere Partij, ook na een deugdelijke schriftelijke ingebrekestelling, stellende een redelijke termijn, toerekenbaar tekort blijft komen in de nakoming van wezenlijke verplichtingen op grond van de overeenkomst, waaronder is begrepen niet naleving van artikel 2.b van deze overeenkomst.

d. De overeenkomst kan door elk der Partijen met onmiddellijke ingang worden beëindigd jegens de andere Partij, zonder dat een nadere opzegging, ingebrekestelling of rechterlijke uitspraak is vereist, indien deze andere Partij in staat van faillissement wordt gesteld, surseance van betaling wordt verleend, of als zodanig beslag op het geheel of een gedeelte van zijn vermogen wordt gelegd dat nakoming van de verplichtingen uit de overeenkomst in redelijkheid niet te verwachten is, zijn rechtspersoonlijkheid verliest, wordt ontbonden of wordt geliquideerd. Geen der Partijen zal wegens beëindiging op grond van dit artikellid tot enige schadevergoeding zijn gehouden.

e. Deelnemer is ook na beëindiging gehouden aan de bewaarplicht van de uitgewisselde informatie en de logging gedurende de wettelijke bewaartermijnen.

12. *Overdracht, meldingsplicht en toepasselijk recht*

a. De Twiin Organisatie is gerechtigd haar rechten en verplichtingen uit deze overeenkomst geheel of gedeeltelijk over te dragen. De Twiin Organisatie is tevens gerechtigd deze overeenkomst door een derde partij over te laten nemen in het kader van de inrichting van stelselregie door VWS en Deelnemer verklaart hierbij reeds nu voor alsdan aan een eventuele overdracht van de overeenkomst mee te werken.

b. Deelnemer stelt Twiin Organisatie op de hoogte van een fusie, overname, splitsing en/of wijziging in haar statutaire naam en van alle overige wijzigingen die gevolgen hebben voor de toepasselijkheid van het Bewijs van Validatie. Deelnemer stuurt de notificatie zo snel mogelijk maar uiterlijk binnen twee weken na afronding.

c. Op deze overeenkomst is uitsluitend Nederlands recht van toepassing.

[ondertekening volgt op een nieuwe pagina]

Ondertekeningblad

Aldus opgemaakt en voor akkoord getekend, namens:

[Statutaire naam Twiin Organisatie]

Te [plaats]
[datum ondertekening]
[handtekening]
[naam ondertekenaar]
[functie, b.v. Lid Raad van Bestuur]

[Statutaire naam Deelnemer]

Te [plaats]
[datum ondertekening]
[handtekening]
[naam ondertekenaar] *[functie, b.v. Lid Raad van Bestuur]*

Bijlage – Samenwerkingsvoorwaarden – in te vullen per zorgtoepassing

Toelichting:

Per Zorgtoepassing worden bijlagen bij deze Overeenkomst ingevuld. Deze bijlagen bestaan uit de Twiin Voorwaarden met daarin de Samenwerkingsvoorwaarden.

De Twiin Dienstverlener beheert de Samenwerkingsvoorwaarden voor Deelnemer en houdt bij met welke andere Twiin Deelnemers de Deelnemer uitwisselt op basis van de Samenwerkingsvoorwaarden.

Zodra de Twiin Deelnemer de Twiin Deelnemersovereenkomst heeft ondertekend, is Deelnemer gebonden aan de Twiin Voorwaarden. De Twiin Voorwaarden geven tot aan validatie ruimte om op een aantal onderdelen te kiezen voor een eigen invulling. Die eigen invulling legt Deelnemer vast in de Samenwerkingsvoorwaarden. De Twiin Dienstverlener beheert de Samenwerkingsvoorwaarden voor Deelnemer.

6.2 | Verklaring Twiin Dienstverlener

De Twiin Dienstverlener

De Twiin Dienstverlener is een belangrijke partner van Twiin en omarmt het Twiin Afsprakenstelsel bij realisatie en optimalisatie van het beschikbaar stellen en delen van gezondheidsgegevens van Twiin Deelnemers.

De Twiin Dienstverlener ondersteunt Twiin in verbetering van het Twiin Afsprakenstelsel, bijvoorbeeld door het inbrengen van ervaringen uit de praktijk.

Ondertekening

Met deze ondertekening, verklaart de Twiin Dienstverlener:

- het belang van verbindende (inter)nationale afspraken voor gegevensuitwisseling te onderschrijven, zoals vastgelegd in het Twiin Afsprakenstelsel;
- actief met haar zorgaanbieders en Twiin samen te willen werken aan concrete toepassing van (groeipaden naar) het Twiin Afsprakenstelsel bij het beschikbaar stellen en delen van gezondheidsgegevens;
- de taken en verantwoordelijkheden op zich te nemen zoals die in het afsprakenstelsel staan beschreven in de 9.2 | Voorwaarden Twiin Dienstverlener (see page 151) samen met de Twiin Casemanager zijn doorgenomen en akkoord bevonden; en
- akkoord te gaan met de vermelding van haar organisatie en logo in het overzicht van Twiin Dienstverleners op de social media van Twiin.

Met deze ondertekening, verklaart Twiin:

- dat de Twiin Dienstverlener met het type diensten dat hij aanbiedt invulling kan geven aan de rol van Twiin Dienstverlener zoals omschreven in het Twiin Afsprakenstelsel; en
- akkoord te gaan met het gebruik van de term Twiin Dienstverlener in online en offline communicatie door Twiin Dienstverlener.

Statutaire naam:	**Twiin Organisatie**
Naam:	Naam:
Functie:	Functie:
Datum, plaats:	Datum, plaats:
Handtekening:	Handtekening:

6.3 | Verklaring GtK Beheerder

De GtK Beheerder

De GtK Beheerder is een belangrijke partner van Twiin en omarmt het Twiin Afsprakenstelsel bij het beheer van zorgtoepassingen voor het beschikbaar stellen en delen van gezondheidsgegevens van Twiin Deelnemers.

De GtK Beheerder ondersteunt Twiin in verbetering van het Twiin Afsprakenstelsel, bijvoorbeeld door het inbrengen van ervaringen uit de praktijk.

Ondertekening

Met deze ondertekening, verklaart de GtK Beheerder:

- Het belang van verbindende (inter)nationale afspraken voor gegevensuitwisseling te onderschrijven, zoals vastgelegd in het Twiin Afsprakenstelsel;
- actief mee te willen werken aan veilige en betrouwbaar beschikbaar stellen en delen van gezondheidsgegevens conform het Twiin Afsprakenstelsel;
- de taken en verantwoordelijkheden op zich te nemen zoals die staan beschreven in de 9.3 | Voorwaarden GtK Beheer (see page 155) en samen met de Twiin Casemanager zijn doorgenomen en akkoord bevonden; en
- akkoord te gaan met de vermelding van haar organisatie en logo in het overzicht van GtK Beheerders op de social media van Twiin.

Met deze ondertekening, verklaart Twiin:

- dat de GtK Beheerder met het type diensten dat hij aanbiedt invulling kan geven aan de rol van GtK Beheerder zoals omschreven in het Twiin Afsprakenstelsel; en
- akkoord te gaan met het gebruik van de term GtK Beheerder in online en offline communicatie door GtK Beheerder.

Statutaire naam:	**Twiin Organisatie**
Naam:	Naam:
Functie:	Functie:
Datum, plaats:	Datum, plaats:
Handtekening:	Handtekening:

6.4 | Verklaring GtK Leverancier

Ondergetekenden

1. [Naam Twiin Organisatie], gevestigd aan de [straat] te [postcode] [plaatsnaam], rechtsgeldig vertegenwoordigd door […] (hierna te noemen "**Twiin Organisatie**");

en

2. [statutaire naam leverancier], statutair gevestigd te _____ en kantoor houdende te _____ aan de _____ met KvK nr. _____, te deze rechtsgeldig vertegenwoordigd door de [heer/mevrouw X], functie _____, die deze overeenkomst namens haar ondertekent (hierna te noemen "**Leverancier**").

Overwegingen

A. De Leverancier omarmt het Twiin Afsprakenstelsel en is van plan om zijn applicatie te laten valideren voor één of meer zorgtoepassingen.

B. De Twiin Organisatie beheert het Twiin Afsprakenstelsel en zorgt ervoor dat partijen ruimte hebben om deel te nemen aan de doorontwikkeling zoals vastgelegd in het reglement (see page 98).

Verplichtingen

1. Met deze ondertekening, verklaart de Leverancier:

   a. Het Twiin Afsprakenstelsel te erkennen als landelijk afsprakenstelsel om te zorgen voor gegevensuitwisseling in de zorg;

   b. zich in te spannen bij het actief meewerken aan veilige en betrouwbare gegevensuitwisseling conform het Twiin afsprakenstelsel

   c. zich te goeder trouw in te zullen spannen om zijn applicatie te laten valideren op basis van het Twiin Afsprakenstelsel als GtK; en

   d. akkoord te gaan met de vermelding van zijn organisatie en logo in het overzicht van GtK Leveranciers op de website en social media van Twiin.

2. Met deze ondertekening, verklaart de Twiin Organisatie:

   a. Dat de Leverancier deel kan nemen aan de Overlegtafel GtK zoals omschreven in het Reglement; en

   b. akkoord te gaan met het gebruik van de term GtK Leverancier door Leverancier in online en offline communicatie.

3. Op de onderhavige verklaring zijn geen algemene of bijzondere leverings- of betalingsvoorwaarden of enige andere of bijzondere voorwaarden van welke partij dan ook van toepassing.

4. Op deze verklaring is Nederlands recht van toepassing. Alle geschillen welke tussen partijen mochten ontstaan, naar aanleiding van de onderhavige overeenkomst dan wel van nadere overeenkomsten die daarvan het gevolg mochten zijn of uit enige andere bestaande of toekomstige rechtsbetrekking zoals bijvoorbeeld zij het niet uitsluitend ter zake van onrechtmatige daad, onverschuldigde betaling en ongegronde verrijking, zullen worden beslecht door de rechtbank te Utrecht, zulks behoudens voor zover dwingende competentieregels aan deze keuze in de weg zouden staan.

Ondertekening

Statutaire naam Leverancier:	**Twiin Organisatie**
Naam:	Naam:
Functie:	Functie:
Datum, plaats:	Datum, plaats:
Handtekening:	Handtekening:

6.5 | Releasebeleid

Het Twiin Afsprakenstelsel ontwikkelt zich voortdurend. Ontwikkelingen binnen en rondom Twiin Afsprakenstelsel kunnen aanleiding geven om afspraken uit het stelsel te wijzigen. De Twiin Organisatie spant zich ervoor in om te borgen dat wijzigingen in wet- en regelgeving en normen zo goed mogelijk worden verwerkt in het Twiin Afsprakenstelsel door middel van het uitbrengen van nieuwe releases. De Twiin Organisatie spant zich ervoor in om waar mogelijk inbreng te leveren bij landelijke ontwikkelingen die impact hebben op het Twiin Afsprakenstelsel.

Releasecriteria

Releases voor het afsprakenstelsel worden als volgt aangeduid:

1. **Major:** Wijzigingen die invloed hebben op de functionaliteit en niet backwards compatible zijn.
2. **Minor:** Wijzigingen die invloed hebben op de functionaliteit en backwards compatible zijn.
3. **Patch**: Wijzigingen die geen invloed hebben op de functionaliteit en backwards compatible zijn.

Releasefrequentie

- De Twiin Organisatie publiceert maximaal tweemaal (2) per jaar een nieuwe release met impact voor de Deelnemers (major of minor release) volgens een vooraf aangekondigde planning.
- De Twiin Organisatie kan op ieder moment patch releases uitbrengen als dat nodig is, zoals voor het herstellen van fouten.

Geldigheid

De actuele en de voorlaatste release zijn geldig (ook wel n-1 genoemd). Dit betekent dat Twiin Deelnemers, GtK's en GtK Beheerders maximaal één (1) jaar de tijd hebben om de nieuwe release te implementeren.

Versiebeheer

De Twiin Organisatie hanteert de Semantic Versioning-specificatie voor het versiebeheer, zie https://semver.org. Dit betekent dat het versienummer wordt weergegeven door 3 nummers die met een punt zijn gescheiden (x.y.z waarbij x de majorrelease is, y de minor en z de patch).

Status en post-fix

- De status van iedere versie van het Twiin Afsprakenstelsel volgt uit de post-fix:
  - **Zonder toevoeging:** Een versie met de status normatief
  - **Uitgefaseerd**: Een versie die inmiddels niet meer normatief is. Deze is vervangen door een nieuwe versie met normatieve status
- De status van een implementatiewijzer volgt uit status van de versie van het Twiin Afsprakenstelsel waarin deze implementatiewijzer is gepubliceerd. In aanvulling kan aan een implementatiewijzer nog de volgende status worden toegekend:
  - **Trial**: Een versie voor beproeving in een pilot, waarmee wordt bedoeld een beproeving in een productieomgeving met echte cliëntgegevens

- De onderdelen in het ontwikkelsupplement kunnen de volgende status hebben:
  - **Informative:** Een eerste uitwerking en/of het resultaat van een fit-gap analyse
  - **Draft**: Een versie op basis waarvan een verkenning kan worden uitgevoerd
  - **Candidate:** Een versie op basis waarvan een Proof of Concept (“PoC”) kan worden uitgevoerd, waarmee wordt bedoeld een beproeving in een testomgeving met gefingeerde cliëntgegevens

Afhankelijkheid Release Twiin Afsprakenstelsel en de Twiin Zorgtoepassingen

- Het Twiin Afsprakenstelsel en de Twiin Zorgtoepassingen opgenomen in het Twiin Afsprakenstelsel hebben dezelfde versienummers, aangezien de zorgtoepassingen afhankelijk zijn van het generieke deel van het afsprakenstelsel.
- Bij verhoging van een release van het Twiin Afsprakenstelsel zal de zorgtoepassing ook een nieuw releasenummer krijgen.

Besluitvorming

Het Twiin Bestuur besluit over het vaststellen van een nieuwe release en over de ‘Release roadmap’ met de onderwerpen voor een eerstvolgende release. De Twiin Deelnemers, Twiin Dienstverleners, GtK Beheerders en GtK Leveranciers zijn vertegenwoordigd bij deze besluitvorming zoals vastgelegd in het reglement (see page 98).

6.6 | Reglement

Artikel 1. Definities

In dit Reglement hebben begrippen de betekenis die daaraan is toegekend in de lijst met begrippen van het Twiin Afsprakenstelsel. In dit Reglement worden daarnaast een aantal andere begrippen gebruikt, telkens aangeduid met een hoofdletter, met de volgende betekenis:

- Overlegtafel: duidt op de Overlegtafel Twiin Deelnemers & Twiin Dienstverleners en/of de Overlegtafel GtK's.
- Overlegtafel Twiin Deelnemers & Twiin Dienstverleners: de overlegtafel zoals uitgewerkt in artikel 3 van dit Reglement.
- Overlegtafel GtK's: de overlegtafel zoals uitgewerkt in artikel 4 van dit Reglement.

Artikel 2. Achtergrond en doel

In het Reglement is uitgewerkt hoe de vertegenwoordiging van Twiin Deelnemer, Twiin Dienstverlener, GtK Beheerder en GtK Leverancier is geregeld bij de advisering over de verdere ontwikkeling van het Twiin Afsprakenstelsel, waaronder bij het vaststellen van nieuwe releases van het Twiin Afsprakenstelsel. Besluitvorming over de doorontwikkeling van het Twiin Afsprakenstelsel vindt plaats in overeenstemming met het releasebeleid (see page 97) en het juridisch kader (see page 104). Zoals uitgelegd in de 3 | Missie, visie en doelstellingen (see page 35), volgt de Twiin Organisatie de stragegische besluiten die worden genomen op basis van de Nationale Strategie voor het Gezondheidsinformatiestelsel. De overlegtafels zijn bedoeld om te adviseren over uitvoeringsvragen die spelen binnen deze kaders.

Artikel 3. Overlegtafel Twiin Deelnemers & Twiin Dienstverleners

De Overlegtafel Twiin Deelnemers & Twiin Dienstverleners bestaat uit vertegenwoordigers van de Twiin Deelnemers en Twiin Dienstverleners (hierna te noemen "Lid"). Elk Lid wordt geacht naar behoren gemachtigd te zijn om te beraadslagen en te adviseren over de onderwerpen die op de agenda staan van het overleg en daarover ook geïnformeerd te zijn.

Artikel 4. Overlegtafel GtK's

De Overlegtafel GtK's bestaat uit vertegenwoordigers van GtK Leveranciers en GtK Beheerders (hierna te noemen "Lid"). Elk Lid wordt geacht naar behoren gemachtigd te zijn om te beraadslagen en te adviseren over de onderwerpen die op de agenda staan van het overleg en ter zake kundig te zijn.

Artikel 5. Vergaderingen

a. Voor iedere overlegtafel zorgt Twiin voor een onafhankelijk voorzitter.

b. Iedere overlegtafel vergadert minimaal één keer per geplande release of zo veel vaker als de voorzitter dit nodig acht. Ieder lid van een overlegtafel kan hiertoe een verzoek indienen. De voorzitter stelt de agenda vast. De agenda wordt uiterlijk een week van tevoren gedeeld met alle leden. Minimaal éénmaal per jaar wordt besproken het vaststellen van de nieuwe release en de release roadmap.

c. De notulen, inclusief besluitenlijst worden gedeeld binnen twee weken na afloop van de vergadering.

d. Iedere overlegtafel wordt ondersteund door een secretaris, welke wordt geleverd door de Twiin Organisatie.

e. De Twiin Organisatie kan besluiten om de beide overlegtafels gezamenlijk bijeen te laten komen.

Artikel 6. Taken

Iedere overlegtafel heeft de volgende taken:

- Adviseren van het Twiin Bestuur over doorontwikkeling van het Twiin Afsprakenstelsel binnen het juridische kader en de strategische besluiten die worden genomen op basis van de Nationale Strategie voor het Gezondheidsinformatiestelsel.
- Adviseren van het Twiin Bestuur over de wijze of timing van de implementatie van een nieuwe release van het Twiin Afsprakenstelsel.

De Twiin Organisatie zorgt voor consultatie van Twiin Deelnemers, Twiin Dienstverleners, GtK Leveranciers en GtK Beheerders door middel van onder andere expertgroepen.

Artikel 7. Adviezen

a. De adviezen zoals benoemd in artikel 6 van de beide overlegtafels kunnen zien op het vaststellen van een nieuwe major of minor release en op de onderwerpen voor een eerstvolgende release, de release roadmap. De overlegtafels worden voorafgaand aan publicatie geïnformeerd over het uitbrengen van een patch release. Het Twiin Bestuur geeft binnen dertig dagen een reactie op de gegeven adviezen. Op verzoek van een overlegtafel licht het Twiin Bestuur deze reactie mondeling toe aan de overlegtafel.

b. In geval na mondelinge toelichting een overlegtafel en het Twiin Bestuur van inzicht verschillen, roept de Twiin Organisatie beide overlegtafels gezamenlijk bijeen om een oplossing te zoeken naar een manier om recht te doen aan het advies. Zo nodig neemt het Twiin Bestuur een beslissing die zo goed mogelijk recht doet aan de belangen van beide tafels.

c. De Overlegtafel Twiin Deelnemers & Twiin Dienstverleners heeft instemmingsrecht als het gaat om een besluit om het Twiin Afsprakenstelsel zo aan te passen dat andere deelnemers dan zorgaanbieders zoals bedoeld in de Wet kwaliteit klachten en geschillen in de zorg toe kunnen treden tot het Twiin Afsprakenstelsel. Besluitvorming verloopt conform artikel 8a.

Artikel 8. Wijze van besluitvorming

a. Adviezen worden op basis van consensus vastgesteld. Wanneer dit niet mogelijk blijkt, worden reguliere adviezen vastgesteld met meerderheid van stemmen.

b. Een lid van een overlegtafel kan zich tijdens een vergadering laten vertegenwoordigen door een van de andere lid van de desbetreffende overlegtafel, waarbij een Twiin Deelnemer zich in zo'n geval laat vertegenwoordigen door zijn Twiin Dienstverlener. Dit dient voorafgaand aan de vergadering per mail aan de secretaris te worden medegedeeld door middel van het machtigingsformulier.

Artikel 9. Wijziging en aanvulling Reglement

a. De beide overlegtafels evalueren jaarlijks de samenwerking en de overlegstructuur van de overlegtafel. Wijzigingen van dit Reglement zijn mogelijk conform het releasebeleid.

b. Een overlegtafel kan in een huishoudelijk reglement aanvullende bepalingen vaststellen welke alleen gelden voor die overlegtafel. Bij tegenstrijdigheid met de algemene bepalingen in dit Reglement, prevaleren de algemene bepalingen.

7 | Juridische context

Het Twiin Afsprakenstelsel bevat afspraken over het landelijk beschikbaar stellen en uitwisselen van gezondheidsgegevens. Het Twiin Afsprakenstelsel is in lijn met de toepasselijke wet- en regelgeving en normen. Het Twiin Afsprakenstelsel wordt aangepast als dat nodig is gelet op de ontwikkeling van wet- en regelgeving en/of toepasselijke normen.

Op basis van het Twiin Afsprakenstelsel kunnen Twiin Deelnemers gegevens uitwisselen via een GtK. Welke partij welke rol heeft binnen het Twiin Afsprakenstelsel is omschreven in de governance (see page 80). Wat er van deze partijen wordt verwacht en welke eisen worden gesteld, moet passen binnen het juridisch kader. Op de pagina 7.1 | Juridisch kader (see page 104) is een overzicht opgenomen van de toepasselijke wet- en regelgeving met een samenvatting per onderdeel van de inhoud. Tevens is per onderdeel aangeduid op welke manier het Twiin Afsprakenstelsel invulling geeft aan deze wet- en regelgeving. Ook moeten partijen voldoen aan de toepasselijke normen. Op de pagina 7.3 | Toepasselijke normen (see page 115) is tevens per norm een samenvatting gegeven van de inhoud van de norm. Op de pagina 7.2 | Toelichting verwerkingsverantwoordelijkheid (see page 113) is uitgewerkt welke partij op basis van de AVG verwerkingsverantwoordelijk is voor de verschillende verwerkingen op basis van het Twiin Afsprakenstelsel.

Overzicht wet- en regelgeving

De wet- en regelgeving die van toepassing is op gegevensuitwisseling in de zorg is voortdurend in beweging. Tabel 2.1 is een overzicht van de relevante wet- en regelgeving voor het Twiin Afsprakenstelsel (geldend op 12 september 2025). Dit overzicht zal worden uitgebreid met het wetsvoorstel identificatie en authenticatie in de zorg (Wet Diaz), zodra deze is vastgesteld. Dit geldt ook voor de NIS-2 richtlijn zodra deze in een geldende Nederlandse wet is omgezet.

Naam en vindplaats	Afkorting
Wet op de geneeskundige behandelingsovereenkomst https://wetten.overheid.nl/BWBR0005290/2025-07-18#Boek7_Titeldeel7_Afdeling5	WGBO
Wet op de beroepen in de individuele gezondheidszorg https://wetten.overheid.nl/BWBR0006251/2025-07-05	Wet BIG
Wet kwaliteit, klachten en geschillen zorg *De wet vervangt de wetten Kwaliteitswet Zorginstellingen en de Wet klachtrecht cliënten zorgsector.* https://wetten.overheid.nl/BWBR0037173/2025-07-05	Wkkgz

Algemene verordening gegevensbescherming *Deze Europese verordening vervangt sinds 25 mei 2018 de Richtlijn bescherming persoonsgegevens en de Wet bescherming persoonsgegevens (Wbp).* https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A02016R0679-20160504	AVG
Uitvoeringswet Algemene verordening gegevensbescherming https://wetten.overheid.nl/BWBR0040940/2021-07-01	UAVG
Verordening betreffende de Europese ruimte voor gezondheidsgegevens Deze verordening ziet op de inrichting van een Europese ruimte voor gezondheidsgegevens en wijzigt de eerdere Richtlijn 2011/24/EU en Verordening (EU) 2024/2847. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202500327	EHDS
Verordening betreffende elektronische identificatie en vertrouwensdiensten Deze verordening wijzigt verordening (EU) nr. 910/2014. https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32024R1183	eIDAS
Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg *Deze wet heette tot 1 juli 2017 de Wbsn-z (Wet gebruik Burgerservicenummer in de zorg).* ***De Wet Cliëntenrechten is opgenomen in hoofdstuk 3a van de Wabvpz.*** https://wetten.overheid.nl/BWBR0023864/2025-07-05	Wabvpz
Besluit elektronische gegevensverwerking door zorgaanbieders https://wetten.overheid.nl/BWBR0040238/2020-10-01	Begz
Wet elektronische gegevensuitwisseling in de zorg https://wetten.overheid.nl/BWBR0048095/2025-07-05	Wegiz

Besluit elektronische gegevensuitwisseling in de zorg https://wetten.overheid.nl/BWBR0040238/2020-10-01	Begiz

7.1 | Juridisch kader

In dit hoofdstuk staat een overzicht van de wet- en regelgeving en de normen die van toepassing zijn op het beschikbaar stellen en uitwisselen van gezondheidsgegevens. Per onderdeel is een samenvatting opgenomen van de inhoud. Tevens is aangeduid per onderdeel op welke manier het Twiin Afsprakenstelsel invulling geeft aan de wet- en regelgeving en de normen.

Inhoud

Wet op de geneeskundige behandelingsovereenkomst (WGBO)

Cliëntenrechten

De WGBO bevat onder andere het recht van de cliënt:

- op inzage in en afschrift van het eigen dossier
- een verklaring aan het dossier toe te voegen
- gegevens uit het dossier te laten vernietigen

Daarnaast bevat de WGBO regels over de vertegenwoordiging van de cliënt.

Professionele standaard, dossierplicht en beroepsgeheim

Deze wet verplicht de zorgverlener onder andere:

- zich te houden aan de professionele standaard en de kwaliteitsstandaarden
- te voldoen aan de informatieplicht richting de cliënt
- te voldoen aan de dossierplicht

De zorgverlener is op basis van deze wet gebonden aan het medische beroepsgeheim. Hij mag dus niet zonder toestemming van de cliënt aan anderen dan de cliënt inlichtingen over de cliënt dan wel inzage in of afschrift van de gegevens uit het dossier verstrekken. Degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst, of de vervanger van de zorgverlener, mogen de gegevens van de cliënt wél inzien zonder toestemming van de cliënt, mits noodzakelijk voor het uitvoeren van hun werkzaamheden. Verder geldt een uitzondering voor situaties waarin een wettelijk vertegenwoordiger toestemming moet geven voor een behandeling.

Toepassing op het Twiin Afsprakenstelsel

De WGBO bepaalt dat de vertrouwelijkheid van het dossier geborgd moet worden, maar bepaalt niet precies welke waarborgen daarvoor nodig zijn bij uitwisseling. Het Twiin Afsprakenstelsel bevat hiervoor een nadere uitwerking in het vertrouwensmodel (see page 56).

Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)

Beroepsgeheim beroepsbeoefenaren

De Wet BIG heeft als doel om de kwaliteit van de beroepsuitoefening te bevorderen en te bewaken en de cliënt te beschermen tegen ondeskundig en onzorgvuldig handelen door beroepsbeoefenaren. Deze term wordt hieronder toegelicht. Daarnaast legt de Wet BIG aan de beroepsbeoefenaren het beroepsgeheim op. Dit beroepsgeheim geldt ten opzichte van alles wat hen bij de uitoefening van hun beroep wordt toevertrouwd of waarvan zij kennis krijgen en waarvan zij het vertrouwelijke karakter moeten begrijpen.

De Wet BIG bevat een systeem van titelbescherming voor een beperkt aantal beroepsgroepen. Wie een wettelijk geregeld beroep uitoefent, mag een publiekrechtelijk beschermde beroeps- of opleidingstitel voeren. Om te worden aangemerkt als een beroepsbeoefenaar in de zin van de Wet BIG moet worden voldaan aan een aantal wettelijke eisen. De belangrijkste daarvan hebben betrekking op de opleiding.

Door een beschermde titel te voeren is voor derden duidelijk op welk gebied een bepaalde beroepsbeoefenaar deskundig is. Een beroep kan op twee manieren wettelijk worden geregeld: Er is een ‘zware’ regeling bij wet (artikel 3 Wet BIG) en een ‘lichte’ regeling bij algemene maatregel van bestuur (artikel 34 Wet BIG). Bij wet worden acht beroepen geregeld, te weten: arts, tandarts, apotheker, gezondheidszorgpsycholoog, psychotherapeut, fysiotherapeut, verloskundige en verpleegkundige.

Tuchtrecht

Ook voorziet de Wet BIG in tuchtrechtspraak. Dit is een bijzondere vorm van rechtspraak die erop gericht is de kwaliteit van de beroepsuitoefening te bevorderen en bewaken. Beroepen genoemd in artikel 3 Wet BIG vallen onder het tuchtrecht. Artikel 34 Wet BIG-beroepen vallen niet onder het tuchtrecht.

Registers

Voor de beroepen genoemd in artikel 3 Wet BIG heeft de rijksoverheid een register ingesteld. Het gaat hier om een zogeheten constitutieve registratie. Die komt erop neer dat alleen geregistreerde personen de beroepstitel mogen voeren. Ook derden kunnen op verzoek informatie krijgen uit het register. Zij kunnen dus nagaan of een beroepsbeoefenaar met recht een beschermde beroepstitel voert en of er mogelijk sprake is van beperkende voorwaarden op het punt van de beroepsuitoefening.

De ‘lichte’ regeling bij algemene maatregel van bestuur is voornamelijk bedoeld voor de paramedische beroepen. Voorbeelden zijn: de diëtist, de logopedist en de mondhygiënist. In de algemene maatregel van bestuur wordt het deskundigheidsgebied omschreven en de opleiding geregeld. Wie aan de gestelde eisen voldoet heeft het recht een opleidingstitel te voeren. De overheid houdt voor deze beroepsgroepen geen register bij. In de praktijk worden dergelijke registers veelal wel bijgehouden door de beroepsgroepen.

Toepassing op het Twiin Afsprakenstelsel

Ook de Wet BIG bepaalt dat de beroepsbeoefenaren gehouden zijn aan het beroepsgeheim zonder dat de wet regelt hoe het beroepsgeheim geborgd moet worden bij uitwisseling. Het Twiin Afsprakenstelsel

bevat hiervoor een nadere uitwerking in het vertrouwensmodel. Een belangrijk onderdeel van dit vertrouwensmodel is een betrouwbare identificatie van de zorgverleners die betrokken zijn bij de uitwisseling van gegevens.

Het systeem van titelbescherming in de Wet BIG is voor de landelijke infrastructuur van belang vanwege de bijbehorende registers. De uitgifte van UZI-identificatiemiddelen maakt gebruik van deze registers. In het vertrouwensmodel is gekozen voor de UZI-identificatiemiddelen.

Wet kwaliteit, klachten en geschillen in de zorg (Wkkgz)

Goede zorg, definitie zorgaanbieder en klachtrecht

De Wkkgz legt vast wat goede zorg precies inhoudt. Ook bevat deze wet een definitie van een zorgaanbieder. Volgens deze wet moet de zorgaanbieder als instelling zorgen voor 'zodanige toedeling van verantwoordelijkheden, bevoegdheden alsmede afstemmings- en verantwoordingsplichten, dat een en ander redelijkerwijs moet leiden tot het verlenen van goede zorg.' De Wkkgz bepaalt dat zorgaanbieders een interne werkwijze moeten hebben, waarmee medewerkers incidenten veilig kunnen melden.

Ook bepaalt de Wkkgz wat er moet gebeuren als cliënten een klacht hebben over de zorg. Op basis van de Wkkgz kunnen cliënten terecht bij de klachtenfunctionaris van de zorgaanbieder. Daarnaast biedt de wet ook een laagdrempelig alternatief: de onafhankelijke geschilleninstantie. Die doet een uitspraak waaraan beide partijen zich moeten houden. De geschilleninstantie kan ook een schadevergoeding toekennen tot EUR 25.000,-.

Toepassing op het Twiin Afsprakenstelsel

Vooralsnog kunnen alleen zorgaanbieders zoals bedoeld in de Wkkgz de Deelnemersovereenkomst (see page 84) tekenen, totdat anders wordt besloten conform de besluitvormingsprocedure die in het reglement (see page 98) is omschreven. Uit de Wkkgz volgt dat de zorgaanbieder verantwoordelijk is om de juiste randvoorwaarden in te richten die zorgverleners in staat stellen goede zorg te verlenen. Het gaat hierbij onder andere om de inrichting van de organisatie, de toedeling van verantwoordelijkheden en bevoegdheden en de beschikbaarheid van middelen. Gelet hierop, sluit de zorgaanbieder de Deelnemersovereenkomst en zorgt voor adequate contractuele afspraken met de Twiin Dienstverlener, de GtK Leverancier en met de eventuele GtK Beheerder zoals uitgewerkt in de governance (see page 80).

Algemene verordening gegevensbescherming (AVG)

Persoonsgegevens

De AVG is een Europese wet die rechtstreekse werking heeft in de hele Europese Unie. De AVG regelt onder welke voorwaarden persoonsgegevens verwerkt mogen worden binnen de EU.

Persoonsgegevens zijn alle gegevens die zien op een geïdentificeerde of identificeerbare natuurlijke persoon. Deze wordt in de AVG de 'betrokkene' genoemd. Onder ‘verwerking van gegevens’ valt onder andere: verzamelen, vastleggen, ordenen, bewaren, bewerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van

terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van gegevens.

Grondslag en doel

De AVG bepaalt dat dit slechts is toegestaan als sprake is van een rechtmatige grondslag. De AVG noemt zes grondslagen voor verwerking, waaronder toestemming van de betrokkene en uitvoeren van een overeenkomst. Bovendien mogen persoonsgegevens op basis van het proportionaliteitsbeginsel enkel worden verwerkt voor zover dat nodig is voor welbepaalde doeleinden.

Daarbij geldt een verbod om bijzondere categorieën van persoonsgegevens te verwerken, waaronder gegevens over gezondheid, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Op dit verbod is een beperkt aantal uitzonderingen van toepassing. Eén van die uitzonderingen is dat de verwerking noodzakelijk is voor het verstrekken van gezondheidszorg. Een andere uitzondering is uitdrukkelijke toestemming.

Rechten van betrokkenen

Betrokkenen hebben verschillende rechten op basis van de AVG, waaronder het recht op transparantie, informatie en toegang tot persoonsgegevens, rectificatie en wissing van gegevens en het recht van bezwaar.

Verwerkingsverantwoordelijke en verwerker

De verwerkingsverantwoordelijke bepaalt het doel van en de middelen voor de verwerking van de persoonsgegevens en is daarmee verantwoordelijk voor de verwerking. Dat brengt een aantal verplichtingen met zich mee. Zo is de verwerkingsverantwoordelijke verplicht om betrokkenen goed te informeren over de verwerking van hun gegevens en over hun privacyrechten op basis van de AVG, waaronder het recht op inzage, rectificatie, vergetelheid, beperking, dataportabiliteit en bezwaar. Uit deze rechten volgt dat de verwerkingsverantwoordelijke inzichtelijk moet hebben welke persoonsgegevens hij verwerkt, waar deze zich bevinden en hoe deze definitief verwijderd kunnen worden. De verwerkingsverantwoordelijke is ook verplicht om passende technische en organisatorische maatregelen te nemen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. De verwerker verwerkt persoonsgegevens enkel ten behoeve van de verwerkingsverantwoordelijke en onder de voorwaarden zoals vastgelegd in een verwerkersovereenkomst.

Verwerkersovereenkomst

De AVG verplicht de verwerkingsverantwoordelijke een verwerkersovereenkomst te sluiten met iedere verwerker. De AVG bepaalt ook dat de verwerkersovereenkomst aan een aantal eisen moet voldoen. In die overeenkomst moet onder andere worden bepaald wat de aard en het doel zijn van de verwerking, de duur van de verwerking en het soort persoonsgegevens en de categorieën van betrokkenen. Een verwerker is niet zelfstandig verantwoordelijk voor de verwerking van de persoonsgegevens, maar heeft wel een aantal afgeleide verplichtingen voor onder meer beveiliging en geheimhouding van de gegevens. De verwerkersovereenkomst moet er onder andere voor zorgen dat verwerker voldoende

waarborgen biedt ten aanzien van de technische- en organisatorische beveiligingsmaatregelen met betrekking tot de verwerking van de aan hem ter beschikking gestelde persoonsgegevens. De Brancheorganisaties Zorg hebben een model verwerkersovereenkomst opgesteld die voldoet aan de eisen van de AVG, te vinden via: https://www.brancheorganisatieszorg.nl/nieuws_list/modelverwerkersovereenkomst-voor-de-zorgsector/

Data protection impact assessment (DPIA)

De AVG verplicht om een data protection impact assessment (DPIA) uit te voeren als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de mensen van wie de organisatie gegevens verwerkt. Een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen, om daarna maatregelen te kunnen nemen om de risico's te verkleinen.

Zie voor actuele informatie https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia?qa=PIA

Toepassing op het Twiin Afsprakenstelsel

Iedere Twiin Deelnemer is zelfstandig verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens in de eigen zorginformatiesystemen waaronder het GtK. Daaruit volgen een aantal verplichtingen zoals verder uitgewerkt in het hoofdstuk 7.2 | Toelichting verwerkingsverantwoordelijkheid (see page 113).

Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)

Verwerkingsverbod en BSN

De UAVG geeft nadere invulling aan de AVG binnen Nederland. Daar waar de AVG ruimte laat voor nationale regelingen of soms opdraagt tot het treffen van een regeling, komt de UAVG in beeld. De UAVG bepaalt dat de uitzondering op het verwerkingsverbod van gezondheidsgegevens voor het verstrekken van gezondheidszorg enkel geldt voor hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening en enkel voor zover de verwerking noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene dan wel het beheer van de betreffende instelling of beroepspraktijk (artikel 30 lid 3 UAVG).

De Uitvoeringswet AVG regelt dat het BSN alleen mag worden gebruikt bij de verwerking van persoonsgegevens ter uitvoering van de desbetreffende wet dan wel voor doeleinden bij de wet bepaald (art 46 UAVG).

In de UAVG is uitgewerkt dat minderjarigen vanaf 16 jaar zelfstandig beslissen over de verwerking van hun persoonsgegevens (artikel 5 UAVG).

Toepassing op het Twiin Afsprakenstelsel

De Twiin Deelnemers zijn vooralsnog enkel zorgaanbieders. De gegevens worden uitgewisseld voor het doel van het verlenen van zorg, zodat de uitzonderingsgrond op het verwerkingsverbod op hen van

toepassing is. Zorgaanbieders beschikken over een wettelijke grondslag om het BSN van cliënten te verwerken (de Wabvpz).

Verordening betreffende de Europese ruimte voor gezondheidsgegevens (EHDS)

Op 26 maart 2025 is de verordening voor een European Health Data Space (EHDS) in werking getreden. De EHDS is gericht is op drie hoofddoelen. Het eerste doel is om personen meer zeggenschap te geven over hun gezondheidsgegevens. Het tweede doel is om een eengemaakte markt te bevorderen voor systemen voor elektronische cliëntendossiers. Het derde doel is zorgen voor een consistent, betrouwbaar en efficiënt systeem voor het hergebruik van gezondheidsgegevens voor onderzoek, innovatie, beleidsvorming en regelgeving (secundair gebruik).

De EHDS is een verordening. Dat wil zeggen dat deze wet rechtstreeks van toepassing is in Nederland. Het is niet nodig en het is ook niet de bedoeling dat deze verordening wordt omgezet in Nederlandse wetgeving. Wel is het nodig dat nationale wetgeving in lijn wordt gebracht met de EHDS en wetgeving die hetzelfde onderwerp regelt zal door de EHDS en/of de uitvoeringswet EHDS moeten worden vervangen. Aanpassingen zullen nodig zijn aan de Wegiz en aan de Wabvpz. Welke aanpassingen dat precies zijn, zal nog moeten blijken. Nederland moet zich hierbij houden aan de implementatietermijnen. Voor standaardisatie zijn de belangrijkste implementatietermijnen 26 maart 2029 en 26 maart 2031. Twiin volgt de ontwikkelingen om te bepalen op welke manier de EHDS de toegepast moet worden in het Twiin Afsprakenstelsel.

Verordening betreffende elektronische identificatie en vertrouwensdiensten (eIDAS)

Betrouwbaarheidsniveaus

De verordening betreffende elektronische identificatie en vertrouwensdiensten maakt wederzijdse erkenning van nationale inlogmiddelen mogelijk. De NEN 7510 verwijst naar deze wet voor de betrouwbaarheidsniveaus voor authenticatiemiddelen.

Toepassing op het Twiin Afsprakenstelsel

De betrouwbaarheid van de authenticatie (see page 65) moet voldoen aan eIDAS.

Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)

Elektronisch uitwisselingssysteem

De Wabvpz regelt de voorwaarden voor het gebruik van een elektronisch uitwisselingssysteem. Dit is een systeem waarmee zorgaanbieders op elektronische wijze, dossiers, gedeelten van dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar kunnen maken.

Rechten van de cliënt

De belangrijkste rechten van de cliënt die in de Wabvpz geregeld worden, zijn:

- het recht op (kosteloos) elektronische inzage in zijn dossier
- het recht op een (kosteloos) elektronisch afschrift van zijn dossier
- sinds juli 2020: het recht op een (kosteloos) elektronisch overzicht wie en op welke datum bepaalde informatie in een elektronisch uitwisselingssysteem beschikbaar heeft gesteld, en wie en op welke datum informatie heeft ingezien of opgevraagd

De Wabvpz doet geen afbreuk aan de privacy-rechten van betrokkenen op basis van de AVG.

Plichten van de zorgaanbieder

De belangrijkste plichten van een zorgaanbieder bij (elektronische) gegevensuitwisseling zijn:

- de plicht de cliënt te informeren over zijn rechten bij elektronische gegevensuitwisseling, de wijze waarop hij zijn rechten kan uitoefenen, de werking van het elektronisch uitwisselingssysteem en welke zorgaanbieders zijn aangesloten op het systeem
- de plicht om de cliënt uitdrukkelijke toestemming te vragen voor het beschikbaar stellen van de cliëntgegevens via een elektronisch uitwisselingssysteem
- de plicht om de cliënt te informeren als nieuwe categorieën zorgverleners aansluiten bij het elektronisch uitwisselingssysteem

Het gebruik van het BSN

De Wabvpz bevat verplichtingen over het gebruik van het BSN. Om cliënten in de zorg op een betrouwbare manier te kunnen identificeren, moeten zorgaanbieders, indicatieorganen en zorgverzekeraars het BSN verplicht gebruiken in hun administratie en bij de onderlinge communicatie over cliënten. Om geen twijfel te laten bestaan over de correctheid van het BSN worden er twee acties uitgevoerd:

- **BSN-verificatie**
  Hierbij verifieert de zorgaanbieder dat bepaalde persoonskenmerken, waaronder naam, geslacht en geboortedatum, bij een BSN horen. Als persoonskenmerken en BSN bij elkaar horen, spreken we van een ‘geverifieerd BSN’. Voor de verificatie gebruikt de zorgaanbieder de interfaces van de SBV-Z (Sectorale Berichtenvoorziening in de Zorg) die zorgen voor de ontsluiting van het BSN-register en het Registratie Niet-ingezetenen.
- **BSN-validatie**
  Zodra de nieuwe cliënt voor het eerst in de zorginstelling komt, wordt aan de hand van een geldig Wettig Identiteits Document (WID: paspoort, rijbewijs, ID-kaart) gecontroleerd of de persoon voor de balie inderdaad degene is die is of wordt ingeschreven in het EPD. Hierdoor is vanaf dat moment sprake van een ‘gevalideerd BSN’.
  Het is ook mogelijk de geldigheid van het identiteitsbewijs elektronisch te laten controleren met behulp van een (tweede) koppeling met het SVB-Z voor de WID-controle. Dit kan men bijvoorbeeld doen als er twijfel is over de geldigheid van het identiteitsbewijs. Om een BSN te

valideren is deze controlestap echter niet vereist en niet alle zorgaanbieders hebben de koppeling in gebruik. Het kan voorkomen dat het BSN van een cliënt wel bekend is binnen het EPD, maar dat deze nog niet is gevalideerd. Bijvoorbeeld als een cliënt zich nog niet heeft geïdentificeerd met een identiteitsbewijs.

Het gebruik BSN in de praktijk

Voor gebruik van het BSN bij uitwisseling van gegevens tussen verschillende zorgaanbieders moeten zorgaanbieders aan de volgende regels voldoen:

- Voordat de zorgverlener/zorgaanbieder gegevens van een cliënt mag delen met een andere zorgaanbieder, moet de brondossierhouder een gevalideerd BSN van de cliënt hebben. Dat wil dus zeggen dat de cliënt fysiek in de zorginstelling is geweest en dat de identiteit van de cliënt is vastgesteld aan de hand van een wettig identiteitsdocument. NB: dit staat los van het feit dat de cliënt daarnaast toestemming moet hebben gegeven voor het delen van zijn gegevens.
- Voor het raadplegen van gedeelde cliëntgegevens van een andere zorgaanbieder is het voldoende dat de cliënt in de eigen organisatie bekend is met een geverifieerd BSN. De cliënt hoeft hiervoor dus nog niet fysiek aanwezig geweest te zijn.

In sommige gevallen, zoals bij een spoedverwijzing of een intercollegiaal consult, kan het voorkomen dat de cliënt nog niet bekend is bij de zorgaanbieder die gegevens raadpleegt. Uitgangspunt is in deze gevallen dat men erop kan vertrouwen dat de zorgaanbieder die de medische gegevens heeft vastgelegd en aangemeld voor delen buiten de organisatie, het BSN heeft geverifieerd. Het proces van validatie van het BSN in de raadplegende zorginstelling blijft bestaan. De eerste keer dat een cliënt daar fysiek aanwezig is, geldt de reguliere validatieprocedure.

Toepassing op het Twiin Afsprakenstelsel

In de technische kern zijn twee typen gegevensuitwisseling uitgewerkt: verzenden en raadpleegbaar maken. Bij het tweede type (raadpleegbaar maken) is sprake van een elektronisch uitwisselingssysteem zoals bedoeld in de Wabvpz.

In het vertrouwensmodel (see page 56) is uitgewerkt per onderdeel welke eisen gelden bij de twee typen gegevensuitwisseling (verzenden en raadpleegbaar maken).

In het onderdeel van het vertrouwensmodel is vastgelegd hoe Twiin Deelnemers de uitdrukkelijke toestemming van de cliënt registreren zoals vereist in de Wabvpz. In het onderdeel transparantie (see page 78) van het vertrouwensmodel is nadere invulling gegeven aan de wijze waarop Twiin Deelnemers de cliënt informeren zoals vereist in de Wabvpz.

Het onderdeel van het vertrouwensmodel legt vast dat Twiin Deelnemers verplicht zijn de cliënt met BSN te identificeren.

Besluit elektronische gegevensverwerking door zorgaanbieders (Begz)

Naleving NEN-normen

Dit besluit van 10 november 2017, beschrijft nadere regels over functionele, technische en organisatorische maatregelen bij elektronische gegevensverwerking door en tussen zorgaanbieders. Het Begz bepaalt onder andere dat een zorgaanbieder moet zorgen voor een veilig en zorgvuldig gebruik van het zorginformatiesysteem en van het elektronisch uitwisselingssysteem waarop hij is aangesloten, conform NEN 7510 en NEN 7512 en dat de logging voldoet aan NEN 7513. Overigens is het Begz niet de enige wet die naleving van een NEN-norm vereist. De Regeling gebruik burgerservicenummer in de zorg verplicht dat gegevensverwerking van het BSN voldoet aan NEN 7510.

Het Begz verplicht de verantwoordelijke voor een elektronisch uitwisselingssysteem om te werken met een zorgserviceprovider die is geautoriseerd volgens in NEN 7512 vastgestelde criteria. Een zorgserviceprovider is een netwerkleverancier van een beveiligde netwerkverbinding tussen een zorginformatiesysteem en een elektronisch uitwisselingssysteem.

Ook verplicht het Begz de rechtspersoon die een elektronisch uitwisselingssysteem beheert en in stand houdt, eens in de vijf jaar door middel van een audit te laten vaststellen dat het systeem voldoet aan NEN 7510 en NEN 7512 en daarnaast om te borgen dat de logging van het systeem voldoet aan NEN 7513. Op basis van artikel 5 Begz is vastgesteld (Staatscourant 2019, 38007)[24] dat de logging ten minste 5 jaar bewaard vanaf het moment dat de logregel wordt geschreven.

Toepassing op het Twiin Afsprakenstelsel

De Voorwaarden Twiin Deelnemer (see page 142) verplichten de Twiin Deelnemer aantoonbaar te zorgen voor een veilig en zorgvuldig gebruik van het eigen zorginformatiesysteem en een veilig en zorgvuldig gebruik van het uitwisselingssysteem, overeenkomstig het bepaalde in NEN 7510 en NEN 7512 en NEN 7513.

Wet elektronische gegevensuitwisseling in de zorg (Wegiz)

Verplichte digitale gegevensuitwisseling

De Wegiz is opgezet als een kaderwet. De onderliggende AMvB's bepalen welke gegevensuitwisseling verplicht digitaal moeten verlopen en aan welke eisen de uitwisseling moet voldoen. De minister legt in een meerjarenagenda een lijst vast met gegevensuitwisselingen die aangewezen kunnen worden.

De Wegiz is primair gericht op het uitwisselen van cliëntgegevens tussen zorgaanbieders. Voor aangewezen gegevensuitwisselingen kan een AMvB bepalen dat uitwisseling met een persoonlijke gezondheidsomgeving (PGO) ook verplicht is.

Er zijn twee sporen mogelijk. De AMvB kan enkel verplichten tot elektronische uitwisseling. Dat wordt 'spoor 1' genoemd. De wet kan ook verplichten tot interoperabele uitwisseling. Dat wordt 'spoor 2'

24. https://zoek.officielebekendmakingen.nl/stcrt-2019-38007.html

genoemd. Bij spoor 2 liggen de eisen ten aanzien van taal en techniek vast in een NEN-norm. Bij spoor 2 zijn leveranciers verplicht om te zorgen voor certificering.

Toepassing op het Twiin Afsprakenstelsel

Het Twiin Afsprakenstelsel sluit zo goed mogelijk aan op de meerjarenagenda van de Wegiz bij de ontwikkeling van de verschillende zorgtoepassingen. De zorgtoepassingen zelf sluiten aan bij de relevante NEN-normen en bijbehorende kwaliteits- en informatiestandaarden.

Besluit elektronische gegevensuitwisseling in de zorg (Begiz)

Verplichte digitale uitwisseling recept

Het besluit is de eerste AMvB op basis van de Wegiz waarin is bepaald dat een gegevensuitwisseling verplicht digitaal moet verlopen. Specifiek ziet het besluit op de uitwisseling van een recept door een huisarts aan een terhandsteller. In dit geval gaat het om een spoor 1 aanwijzing.

Toepassing op het Twiin Afsprakenstelsel

Het Twiin Afsprakenstelsel sluit zo goed mogelijk aan op de meerjarenagenda van de Wegiz bij de planning voor de ontwikkeling van de verschillende zorgtoepassingen.

7.2 | Toelichting verwerkingsverantwoordelijkheid

Twiin Deelnemer als verwerkingsverantwoordelijke

Iedere zorgaanbieder is als Twiin Deelnemer zelfstandig verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens in de eigen zorginformatiesystemen, waaronder het GtK.

Het Twiin Afsprakenstelsel helpt Twiin Deelnemers door vast te leggen waar de verantwoordelijkheid van de één begint en waar die eindigt. Heldere afspraken en documentatie op dit punt is met name van belang bij gebruik van een elektronisch uitwisselingssysteem. Zo'n systeem maakt immers mogelijk dat een zorgverlener werkzaam bij een dossierraadpleger gegevens kan raadplegen in het dossier van een dossierhouder. Maar ook bij het verzenden van gezondheidsgegevens is van belang dat de verantwoordelijkheidsverdeling duidelijk is. De toedeling van de verantwoordelijkheid bij uitwisseling is vastgelegd in het schema bij iedere vertrouwensfunctie van het vertrouwensmodel. Zie de schema's in hoofdstuk 5.1 t/m 5.7. In die schema's is onderscheid gemaakt tussen de verantwoordelijkheid voor de twee typen gegevensuitwisselingen: raadplegen en verzenden.

GtK Leverancier en GtK Beheerder als verwerker

Als de Twiin Deelnemer een GtK Beheerder heeft ingeschakeld, is deze partij verwerker in opdracht van de Twiin Deelnemer. De GtK Beheerder is verwerker in opdracht van de Twiin Deelnemer voor het uitvoeren van beheer, leveren van support en de monitoring. Als er naast de GtK Beheerder een

leverancier bepaalde diensten levert, zoals technisch beheer, is ook deze partij (sub)verwerker. Dat kan zijn in opdracht van Twiin Deelnemer als verwerker of in opdracht van de GtK Beheerder als (sub)verwerker. Als de GtK Leverancier dit soort diensten levert, is deze partij dan ook verwerker of subverwerker van de Twiin Deelnemer.

Verplichtingen Twiin Deelnemer als verwerkingsverantwoordelijke

Iedere Twiin Deelnemer heeft als verwerkingsverantwoordelijke de volgende verplichtingen:

- De Twiin Deelnemer is als verwerkingsverantwoordelijke het aanspreekpunt bij verzoeken van betrokkenen op basis van hun AVG-privacyrechten zoals uitgewerkt in de Voorwaarden Twiin Deelnemer (see page 142), nr. 2.6. Die voorwaarde verplicht de Twiin Deelnemer om te zorgen voor adequaat proces waarmee de cliënt te allen tijde zijn wettelijke rechten ter bescherming van zijn persoonsgegevens kan uitoefenen. Het proces incidentmelding (see page 137) beschrijft hoe Twiin Deelnemers elkaar zo nodig kunnen contacten over dit soort verzoeken.
- De Twiin Deelnemer moet voldoen aan de toepasselijke beveiligingsnormen, waaronder met name NEN 7510, NEN 7512 en NEN 7513. Het vertrouwensmodel (see page 56) legt op een aantal onderdelen vast op welke wijze zorgaanbieders invulling geven aan deze normen. Tevens is het onderdeel transparantie (see page 78) van het vertrouwensmodel een invulling van het recht van de betrokkene op transparantie. Het onderdeel toestemming (see page 74) van het vertrouwensmodel is een invulling van de AVG-grondslag toestemming.
- De Twiin Deelnemer is ervoor verantwoordelijk dat zijn eigen GtK voldoen aan de toepasselijke beveiligingsnormen, waaronder met name NEN 7510, NEN 7512 en NEN 7513. Met het proces Validatie GtK (see page 132) toetst de Twiin Organisatie de naleving van deze normen. Verder is in de dienst risicoanalyse (see page 138) is vastgelegd dat periodiek in overleg met de Twiin Deelnemers de risicoanalyse wordt bijgesteld wat ertoe kan leiden dat ook het informatiebeveiligingsbeleid (see page 117) wordt aangescherpt.
- Deelnemer is verplicht om een (sub)verwerkersovereenkomst te (laten) sluiten met alle (sub)verwerkers zoals uitgewerkt in de Voorwaarden Twiin Deelnemer
- De Twiin Deelnemer is gehouden om zo nodig zelf een gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren als het gaat om verwerkingsactiviteit met een hoog privacyrisico zoals ook vastgesteld in de Voorwaarden Twiin Deelnemer.

Buiten scope

De Twiin Dienstverlener verwerkt geen persoonsgegevens in het kader van het Twiin Afsprakenstelsel.

Ook de Twiin Organisatie verwerkt geen persoonsgegevens in het kader van het Twiin Afsprakenstelsel.

Het Twiin Afsprakenstelsel schrijft in een aantal gevallen het gebruik van gemeenschappelijke voorzieningen voor. De gemeenschappelijke voorzieningen zijn zelf niet in het Twiin Afsprakenstelsel beschreven en deze worden ook niet door de Twiin Organisatie ontwikkeld en/of beheerd. De Twiin Organisatie heeft zodoende geen rol van eigenaar, verwerkingsverantwoordelijke of (sub)verwerker ten aanzien van deze gemeenschappelijke voorzieningen.

7.3 | Toepasselijke normen

In dit hoofdstuk staat een overzicht van de NEN-normen die van toepassing zijn op het beschikbaar stellen en uitwisselen van gezondheidsgegevens. Per onderdeel is een samenvatting opgenomen van de inhoud. Tevens is aangeduid per norm op welke manier het Twiin Afsprakenstelsel invulling geeft aan de norm.

Normenkader informatiebeveiliging

Om veilig met elektronische medische gegevens om te gaan, heeft het Nederlands Normalisatie-instituut (NEN) een aantal normen ontwikkeld. De eerste norm die is ontwikkeld is de NEN 7510, de norm voor informatiebeveiliging in de zorg. Deze norm is gebaseerd op de Code voor Informatiebeveiliging, de ISO-27000-serie. De reden om deze NEN-norm op te stellen is dat er zorgspecifieke aandachtspunten zijn, met name het belang van de vertrouwelijkheid en integriteit van persoonlijke gezondheidsinformatie. De NEN 7510 is voor de zorg aangevuld met NEN 7512 vertrouwensbasis voor gegevensuitwisseling en de NEN 7513 logging. Zorgaanbieders zijn verplicht om NEN 7510 toe te passen bij de verwerking van BSN en alle drie de normen bij gebruik van een elektronisch uitwisselingssysteem.

NEN 7510, informatiebeveiliging in de zorg (NEN 7510-1&2:2017+A1:2020)

De NEN 7510 bestaat uit twee onderdelen. NEN 7510-1 beschrijft de eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging.
NEN 7510-2 voorziet in richtlijnen voor zorginstellingen en andere beheerders van persoonlijke gezondheidsinformatie over hoe het beste de beschikbaarheid, integriteit en vertrouwelijkheid van dergelijke informatie kan beschermen.

NEN 7512, vertrouwensbasis voor gegevensuitwisseling (NEN 7512:2022)

In de NEN 7512 is een methodiek uitgewerkt voor het classificeren van risico's en het vaststellen van beheersmaatregelen bij de uitwisseling van gegevens. Deze norm bepaalt dat authenticatie van gebruikers van uit te wisselen persoonlijke gezondheidsinformatie in overeenstemming met eIDAS moet zijn, waarbij het betrouwbaarheidsniveau 'hoog' moet worden gebruikt.

De norm verplicht ook ondertekening van het uitgewisselde met een elektronische handtekening op het juiste eIDAS betrouwbaarheidsniveau. In de norm staat hierover het volgende: "Ondertekening bij uitwisseling dient twee doelen. Ten eerste de toegenomen zekerheid omtrent de integriteit van de uitgewisselde gegevens en ten tweede de zekerheid omtrent de afzender. Immers, veel instellingen hebben grote hoeveelheden medewerkers en voorkomen behoort te worden dat een niet daartoe geautoriseerde medewerker de indruk kan wekken dat een onjuiste uitwisseling eigenlijk een goede uitwisseling is."

NEN 7513, logging (NEN 7513:2018)

Deze norm bepaalt:

- welke gegevens in de logging aanwezig moeten zijn

- welke gebeurtenissen moeten worden gelogd
- welke gegevens van die gebeurtenissen moeten worden vastgelegd
- aan welke kwaliteitseisen het loggen en de logbestanden moeten voldoen

Verder biedt de norm houvast aan zorginstellingen en andere beheerders van persoonlijke gezondheidsinformatie over het verstrekken van informatie over wie toegang heeft gehad tot haar of zijn elektronisch cliëntdossier.

Toepassing op het Twiin Afsprakenstelsel

De Voorwaarden Twiin Deelnemer (see page 142) verplichten de Twiin Deelnemer aantoonbaar te zorgen voor een veilig en zorgvuldig gebruik van het eigen zorginformatiesysteem en een veilig en zorgvuldig gebruik van het uitwisselingssysteem, overeenkomstig het bepaalde in NEN 7510, NEN 7512 en NEN 7513. De normen zijn toegepast in het vertrouwensmodel (see page 56) en dan met name in de onderdelen authenticatie (see page 65), autorisatie (see page 70) en logging (see page 76) en ook in de uitwerking van die functies in de technische kern (see page 164).

Generieke functies

De normen voor generieke functies zijn nog in ontwikkeling. Het gaat om toestemming (NEN 7517), identificatie en authenticatie (NEN 7518), lokalisatie (NEN 7519) en autorisatie (NEN 7520).

Toepassing op het Twiin Afsprakenstelsel

Twiin volgt de ontwikkeling van de NEN-normering van generieke functies. Als één of meer van deze normen zijn vastgesteld, zullen de relevante onderdelen van het vertrouwensmodel zo nodig worden aangepast.

Specifieke gegevensuitwisselingen

NEN 7503, Voorschrijven en ter handstellen medicatie (NEN 7503:2022)

NEN 7503 specificeert de use cases voor het voorschrijven en het ter hand stellen van medicatie en de daarvoor benodigde verwerking en uitwisseling van medicatiegegevens. NEN 7503 formuleert eisen voor zorgaanbieders om hiervoor de gecertificeerde informatiesystemen zorgvuldig in te zetten en te beheren. NEN 7503 specificeert daarnaast de eisen waaraan informatiesystemen en de elektronische berichtuitwisseling tussen voorschrijvers van medicatievoorschriften en verstrekkers van geneesmiddelen moeten voldoen.

Toepassing op het Twiin Afsprakenstelsel

Twiin wil in de toekomst ook voor deze gegevensuitwisselingen een implementatiewijzer opstellen.

NEN 7540, Basisgegevensset Zorg (NEN 7540:2024)

NEN 7540 specifieert twee use cases voor de uitwisseling van de BgZ tussen instellingen voor medisch specialistische zorg. De twee use cases zijn: uitwisseling BgZ bij verwijzing of overdracht en opvraging BgZ bij eerdere behandelaar. NEN 7540 formuleert eisen voor zorgaanbieders om hiervoor de

gecertificeerde zorginformatiesystemen en elektronische uitwisselingssystemen zorgvuldig in te zetten en te beheren.

Toepassing op het Twiin Afsprakenstelsel

Twiin heeft een implementatiewijzer opgesteld voor de Basisgegevensset Zorg (see page 294).

NEN 7541, Beeldbeschikbaarheid

De norm voor beeldbeschikbaarheid is nog in ontwikkeling. Twiin volgt de ontwikkeling van de NEN-normering en zal de implementatiewijzer Beeldbeschikbaarheid (see page 414) aanpassen waar nodig om in lijn te blijven met deze norm. Ook draagt de Twiin Organisatie bij aan de ontwikkeling van deze norm met kennis en expertise.

Toepassing op het Twiin Afsprakenstelsel

Twiin heeft een implementatiewijzer opgesteld voor Beeldbeschikbaarheid (see page 414).

NEN 7542, Medicatiegegevens, NEN 7545, eOVerdracht, NEN 7546, Acute zorg

Deze normen zijn in ontwikkeling.

Toepassing op het Twiin Afsprakenstelsel

Twiin wil in de toekomst ook voor deze gegevensuitwisselingen een implementatiewijzer opstellen.

7.4 | Informatiebeveiligingsbeleid

Aangezien gezondheidsgegevens van personen privacygevoelige gegevens zijn, is informatiebeveiliging van groot belang voor uitwisseling op basis van het Twiin Afsprakenstelsel. Privacy en Security by Design zijn dan ook onderdeel van de Twiin Principes (see page 38). De informatieveiligheid is, in aanvulling op de wet- en regelgeving die per definitie van toepassing is op de Twiin Deelnemers, GtK Beheerders en GtK Leveranciers, op drie manieren geborgd in het stelsel:

- Door de gegevensuitwisseling tussen GtK's in hoge mate van detail te beschrijven en belangrijke maatregelen op het gebied van privacy en informatiebeveiliging hierin op te nemen (zie de technische kern).
- Door strenge eisen te stellen aan de privacy en informatiebeveiliging van Twiin Deelnemers, GtK Beheerders en GtK Leveranciers (zie de voorwaarden (see page 142)).
- Door onder verantwoordelijkheid van de Twiin Organisatie aanvullende procedures in te richten, waaronder het proces Incidentmelding (see page 137), het proces Risicoanalyse (see page 138) en het proces Handhaving (see page 140).

De Twiin Organisatie voert de regie over het in kaart brengen van privacy- en informatiebeveiligingsrisico's die individuele deelnemers overstijgen (stelselrisico's) en doet voorstellen voor maatregelen. Hiervoor voert de Twiin Organisatie periodiek een risicoanalyse uit. Op basis van deze risicoanalyse worden zo nodig maatregelen heroverwogen en eventueel aanvullende informatiebeveiligingsmaatregelen gedefinieerd. Dit kan resulteren in bijstelling van de technische kern, de voorwaarden (see page 142) en afspraken over incidentmelding (see page 137) en risicoanalyse (see page

138). De Twiin Organisatie laat (nieuwe) afspraken zoveel mogelijk aansluiten bij eisen van andere stelsels en hergebruiken bestaande certificeringen. Dit om te zorgen voor een goede samenhang van de afspraken wat er ook aan bijdraagt dat de implementatie-, financiële en administratieve lasten zo beperkt mogelijk blijven.

Samen met de Twiin Deelnemers en hun eventuele GtK Beheerders zorgt de Twiin Organisatie ook op een andere manier voor de privacy en informatiebeveiliging van het stelsel. Elke Twiin Deelnemer wijst een verantwoordelijke aan voor privacy en informatiebeveiliging. Twiin Deelnemer kan de rol van contactpersoon voor deze taak ook beleggen bij zijn GtK Beheerder. De contactgegevens worden vermeld in het Twiin Serviceportaal, conform de dienst Ketenregie (see page 136). De Twiin Deelnemer blijft altijd de verwerkingsverantwoordelijke.

Tussen deze verantwoordelijken is zo nodig overleg. Ook is er een proces incidentmelding, zodat duidelijk is wat er van de verschillende partijen wordt verwacht bij incidenten. Twiin Deelnemers (dan wel hun GtK Beheerders) zijn verantwoordelijk voor het doorgeven van de juiste contactpersoon en informeren de Twiin Organisatie bij wijzigingen.

Ten slotte zorgt de Twiin Organisatie voor afstemming over informatiebeveiliging met bestaande partijen en ontwikkelingen in de zorg, en volgt zij de belangrijkste internationale ontwikkelingen.

8 | Diensten

Twiin biedt diensten aan voor Aansluiten, Valideren, Ketenregie, Risicoanalyse en Handhaving. De processen die bij deze diensten horen zijn per dienst uitgewerkt. De onderliggende procedures, handleidingen en overige relevante documentatie zijn in meer detail te raadplegen via Twiin.nl.

Uitgangspunten

Processen worden onder begeleiding van een Twiin Dienstverlener of een Twiin Casemanager doorlopen.

Diensten zoals uitgewerkt in dit hoofdstuk 8 zijn ingericht op basis van de volgende uitgangspunten:

- Alleen neutrale en onafhankelijke organisaties kunnen/mogen de diensten van Twiin aanbieden. Zakelijke belangen mogen geen invloed hebben op de dienstverlening van Twiin.
- De dienstverlening wordt waar mogelijk uitgevoerd door bestaande organisaties die soortgelijke diensten aanbieden voor andere afsprakenstelsels.
- De dienstverlening wordt zo dicht mogelijk bij de bron uitgevoerd: lokaal dan wel regionaal. Hierdoor ontstaan efficiënt ingerichte beheerprocessen en dienstverlening. Regie vindt plaats op landelijk niveau.

Onderliggende pagina's

- 8.1 | Aansluiten (see page 119)
- 8.2 | Valideren (see page 128)
- 8.3 | Ketenregie (see page 136)
- 8.4 | Risicoanalyse (see page 138)
- 8.5 | Handhaving (see page 140)

8.1 | Aansluiten

In dit hoofdstuk is omschreven hoe de verschillende partijen aansluiten bij het Twiin Afsprakenstelsel. Per rol is omschreven hoe partijen zich verbinden aan het afsprakenstelsel. Na het doorlopen van de bijbehorende processen zijn de rollen, taken en verantwoordelijkheden voor betrokken partijen duidelijk en goed belegd.

- 8.1.1 | Aansluiten Twiin Deelnemer (see page 120)
- 8.1.2 | Aansluiten Twiin Dienstverlener (see page 121)
- 8.1.3 | Aansluiten GtK Beheerder (see page 124)
- 8.1.4 | Aansluiten GtK Leverancier (see page 126)

8.1.1 | Aansluiten Twiin Deelnemer

Omschrijving van de dienst

Wanneer een zorgaanbieder kenbaar maakt deel te willen nemen aan Twiin, dan kan dit door aan te sluiten bij het afsprakenstelsel. De dienst Aansluiten heeft als doel de aspirant Twiin Deelnemer te begeleiden bij het aansluitproces.

Doelstelling

De doelstelling van het proces Aansluiten Twiin Deelnemer is dat een zorgaanbieder die de rol Twiin Deelnemer zou willen invullen op de hoogte wordt gebracht van de stappen die doorlopen moeten worden om te komen tot ondertekening van de Deelnemersovereenkomst. De taken en verantwoordelijkheden van de Twiin Deelnemer volgen uit de Voorwaarden Twiin Deelnemer. De aspirant Twiin Deelnemer geeft aan welke Twiin Dienstverlener is ingeschakeld. De Twiin Deelnemer kan er ook voor kiezen zelf de taken en verantwoordelijkheden van de Twiin Dienstverlener op zich te nemen. Na de vaststelling door de aspirant Twiin Deelnemer dat de eigen organisatie voldoet aan de voorwaarden tekenen de aspirant Twiin Deelnemer en de Twiin organisatie de Deelnemersovereenkomst. De Twiin Organisatie publiceert een actuele lijst met Twiin Deelnemers zodat het voor aangesloten partijen duidelijk is welke zorgaanbieders willen uitwisselen op basis van het Twiin Afsprakenstelsel.

Toegevoegde waarde

Door de Deelnemersovereenkomst te ondertekenen geeft de Twiin Deelnemer aan toe te gaan werken naar validatie voor één of meer zorgtoepassingen.

Verantwoordelijkheden

De Twiin Deelnemer is ervoor verantwoordelijk kennis te nemen van de taken en verantwoordelijkheden. De Twiin Deelnemer houdt zich vanaf ondertekening van de Deelnemersovereenkomst aan de Samenwerkingsvoorwaarden en werkt toe naar validatie voor een of meer zorgtoepassingen.

Toelichting processtappen aansluiten Deelnemer

1. Aansluiten	
Input	Intentie van een zorgaanbieder om aan te sluiten bij Twiin en KvK-inschrijving
Activiteit	Een aspirant Twiin Deelnemer vult het aansluitformulier in op Twiin.nl.
Output	Ingevuld aansluitformulier

0. Aansluiten	
Wie?	• Twiin Deelnemer

2. Tekenen Deelnemersovereenkomst	
Input	Zelfbeoordeling voorwaarden Twiin Deelnemer
Activiteit	Na ontvangst van het aansluitformulier wordt de Deelnemersovereenkomst opgesteld en getekend door de Twiin Organisatie en voor ondertekening aan de aspirant Twiin Deelnemer gestuurd. De Twiin Deelnemer ondertekent de Deelnemersovereenkomst en stuurt deze terug aan de Twiin Organisatie.
Output	Getekende Deelnemersoverkomst
Wie?	• Twiin Organisatie • Twiin Deelnemer

3. Publiceren	
Input	Deelnemersovereekomst
Activiteit	De Twiin Organisatie publiceert een actuele lijst met de nieuwe Twiin Deelnemer.
Output	Actuele lijst Twiin Deelnemers
Wie?	• Twiin Organisatie

8.1.2 | Aansluiten Twiin Dienstverlener

Omschrijving van de dienst

Wanneer een organisatie kenbaar maakt als Dienstverlener deel te willen nemen aan Twiin, dan kan dit door aan te sluiten bij het afsprakenstelsel. De dienst Aansluiten heeft als doel de aspirant Twiin Dienstverlener te begeleiden bij het aansluitproces.

Doelstelling

De doelstelling van de dienst Aansluiten Twiin Dienstverlener is dat een partij die de rol Twiin Dienstverlener zou willen invullen op de hoogte wordt gebracht van de stappen die doorlopen moeten worden om te komen tot het tekenen van de Verklaring Twiin Dienstverlener. De taken en verantwoordelijkheden volgen uit de Voorwaarden Twiin Dienstverlener. (see page 151) Na de vaststelling dat de aspirant Twiin Dienstverlener voldoet aan de voorwaarden tekenen de aspirant Twiin Dienstverlener en de Twiin Organisatie de Verklaring Twiin Dienstverlener. De Twiin Organisatie publiceert een actuele lijst met Twiin Dienstverleners zodat het voor een Twiin Deelnemer makkelijker is om een Twiin Dienstverlener te vinden.

Toegevoegde waarde

Door de verklaring te ondertekenen geeft de Twiin Dienstverlener aan te voldoen aan de eisen van het Twiin Afsprakenstelsel voor één of meer zorgtoepassingen. Door het afgeven van een Verklaring Twiin Dienstverlener is het voor de Twiin Deelnemers duidelijk welke partijen ze kunnen benaderen voor ondersteuning bij hun deelname aan Twiin.

Verantwoordelijkheden

- De Twiin Dienstverlener is ervoor verantwoordelijk kennis te nemen van de taken en verantwoordelijkheden en invulling hiervan af te stemmen met de Twiin Deelnemers die met de Twiin Dienstverlener een Dienstverlenersovereenkomst willen sluiten.
- De Twiin Organisatie is verantwoordelijk voor het doorlopen van de taken en verantwoordelijkheden en geeft indien nodig toelichting. Na het doorlopen van de taken en verantwoordelijkheden ondertekent de Twiin Dienstverlener de Verklaring Dienstverlener. De Twiin Organisatie ondertekent deze verklaring ook.

Toelichting processtappen Aansluiten Twiin Dienstverlener

1. Aanmelden

Input	Intentie van een organisatie om aan te sluiten als Twiin Dienstverlener
Activiteit	Een aspirant Twiin Dienstverlener meldt zich bij de Twiin Organisatie.
Output	Informatie over de aspirant Twiin Dienstverlener
Wie?	• Twiin Casemanager • Twiin Dienstverlener

2. Intake	
Input	Lijst van Voorwaarden Twiin Dienstverlener
Activiteit	Een Twiin Casemanager doorloopt samen met de Twiin Dienstverlener de lijst van taken en verantwoordelijkheden en legt vast welke taken en verantwoordelijkheden worden ondersteund.
Output	Ingevuld intakeformulier van taken en verantwoordelijkheden
Wie?	• Twiin Casemanager • Twiin Dienstverlener

3. Tekenen verklaring	
Input	Intakeformulier
Activiteit	Op basis van de ondersteunde taken en verantwoordelijkheden bepaalt de aspirant Twiin Dienstverlener samen met de Twiin Organisatie of deze organisatie deze rol kan vervullen. Indien de Twiin Organisatie en de aspirant Twiin Dienstverlener samen tot het oordeel komen dat de aspirant Twiin Dienstverlener deze rol kan vervullen tekenen zij de Verklaring Twiin Dienstverlener.
Output	Verklaring Twiin Dienstverlener
Wie?	• Twiin Organisatie • Twiin Dienstverlener

4. Publiceren	
Input	Verklaring Twiin Dienstverlener
Activiteit	De Twiin Organisatie publiceert een actuele lijst met de nieuwe Twiin Dienstverlener.
Output	Actuele lijst Twiin Dienstverleners
Wie?	• Twiin Organisatie

8.1.3 | Aansluiten GtK Beheerder

Omschrijving van de dienst

Wanneer een organisatie kenbaar maakt als GtK Beheerder deel te willen nemen aan Twiin, dan kan dit door aan te sluiten bij het afsprakenstelsel. De dienst Aansluiten heeft als doel de aspirant GtK Beheerder te begeleiden bij het aansluitproces.

Doelstelling

Het doel van het proces Aansluiten GtK Beheerder is dat een partij die de rol van GtK Beheerder zou willen vervullen op de hoogte wordt gebracht van de stappen die doorlopen moeten worden om te komen tot het verkrijgen van de Verklaring GtK Beheerder. De taken en verantwoordelijkheden volgen uit de Voorwaarden GtK Beheer (see page 155). De Twiin Organisatie publiceert een actuele lijst met GtK Beheerders, zodat het voor een Twiin Deelnemer makkelijker is om een GtK Beheerder te vinden.

Toegevoegde waarde

Door de verklaring te ondertekenen geeft de GtK Beheerder aan bereid te zijn om te voldoen aan de eisen die het Twiin Afsprakenstelsel stelt voor één of meer zorgtoepassingen. Door het afgeven van een Verklaring Twiin GtK Beheerder is het voor Twiin Deelnemers duidelijk welke partijen ze kunnen benaderen voor ondersteuning bij hun deelname aan Twiin.

Verantwoordelijkheden

- De GtK Beheerder is ervoor verantwoordelijk kennis te nemen van de lijst met taken en verantwoordelijkheden en de invulling hierover af te stemmen met de bij hen aangesloten Twiin Deelnemers.
- De Twiin Organisatie is verantwoordelijk voor het doorlopen van de lijst met taken en verantwoordelijkheden en indien nodig toelichting te geven. Na het doorlopen van de taken en verantwoordelijkheden ondertekent de GtK Beheerder een verklaring. De Twiin Organisatie tekent deze verklaring ook.

Toelichting processtappen aansluiten GtK Beheerder

1. Aanmelden	
Input	Intentie van een organisatie om aan te sluiten als GtK Beheerder
Activiteit	Een aspirant GtK Beheerder meldt zich bij de Twiin Organisatie.
Output	Informatie over de nieuwe GtK Beheerder

0. Aanmelden

Wie?	• Twiin Casemanager • GtK Beheerder

2. Intake

Input	Lijst Voorwaarden GtK Beheer
Activiteit	Een Twiin Casemanager doorloopt samen met de GtK Beheerder de lijst van taken en verantwoordelijkheden en legt vast welke taken en verantwoordelijkheden worden ondersteund.
Output	Ingevuld intakeformulier van taken en verantwoordelijkheden
Wie?	• Twiin Casemanager • GtK Beheerder

3. Tekenen verklaring

Input	Intakeformulier
Activiteit	Op basis van de ondersteunde taken en verantwoordelijkheden bepaalt de GtK Beheerder samen met de Twiin Organisatie of deze organisatie de rol kan vervullen. De Twiin Organisatie en de GtK Beheerder tekenen vervolgens de Verklaring GtK Beheerder.
Output	Verklaring GtK Beheerder
Wie?	• Twiin Organisatie • GtK Beheerder

4. Publiceren

Input	Verklaring GtK Beheerder
Activiteit	De Twiin Organisatie publiceert een actuele lijst met de nieuwe GtK Beheerders

0. Publiceren	
Output	Actuele lijst GtK Beheerders
Wie?	• Twiin Organisatie

8.1.4 | Aansluiten GtK Leverancier

Omschrijving van de dienst

Wanneer een organisatie kenbaar maakt als GtK Leverancier deel te willen nemen aan Twiin, dan kan dit door aan te sluiten bij het afsprakenstelsel. De dienst Aansluiten heeft als doel de aspirant GtK Leverancier te begeleiden bij het aansluitproces.

Doelstelling

De doelstelling van het proces Aansluiten GtK Leverancier is dat een partij die de rol GtK Leverancier zou willen invullen op de hoogte wordt gebracht van de stappen die doorlopen moeten worden om te komen tot het tekenen van de Verklaring GtK Leverancier. De taken en verantwoordelijkheden volgen uit de Voorwaarden GtK (see page 162). De Twiin Organisatie publiceert een actuele lijst met GtK Leveranciers zodat het voor een Twiin Deelnemer makkelijker is om een GtK te vinden.

Toegevoegde waarde

Door de verklaring te ondertekenen geeft de aspirant GtK Leverancier aan bereid te zijn om te gaan voldoen aan de eisen van het Twiin Afsprakenstelsel voor één of meer zorgtoepassingen. Door het afgeven van een Verklaring GtK Leverancier is het voor de Twiin Deelnemers duidelijk welke GtK's beschikbaar zijn om te komen tot validatie voor één of meer zorgtoepassing(en).

Verantwoordelijkheden

- De aspirant GtK Leverancier is ervoor verantwoordelijk kennis te nemen van de Voorwaarden GtK.
- De Twiin Organisatie is verantwoordelijk voor het samen met de aspirant GtK Leverancier doorlopen van de Voorwaarden GtK en geeft indien nodig toelichting. Na het doorlopen van de Voorwaarden GtK ondertekent de aspirant GtK Leverancier de verklaring. De Twiin Organisatie ondertekent deze verklaring ook.

Toelichting processtappen aansluiten GtK Leverancier

1. Aanmelden

Input	Intentie bij een leveranciers om aan te sluiten als GtK Leverancier
Activiteit	Een aspirant GtK Leverancier meldt zich bij de Twiin Organisatie.
Output	Informatie over de nieuwe GtK Leverancier
Wie?	• Twiin Casemanager • Aspirant GtK Leverancier

2. Intake

Input	Lijst Voorwaarden GtK
Activiteit	Een Twiin Casemanager doorloopt samen met de aspirant GtK Leverancier de Voorwaarden GtK voor één of meer zorgtoepassingen.
Output	Ingevuld intakeformulier van taken en verantwoordelijkheden
Wie?	• Twiin Casemanager • Aspirant GtK Leverancier

3. Tekenen Verklaring GtK Leverancier

Input	Intakeformulier
Activiteit	Op basis van de Voorwaarden GtK, bepaalt de aspirant GtK Leverancier samen met de Twiin Organisatie of het GtK ingezet kan worden voor één of meer zorgtoepassingen. De Twiin Organisatie en de aspirant GtK Leverancier tekenen vervolgens de Verklaring GtK Leverancier.
Output	Verklaring GtK Leverancier
Wie?	• Twiin Organisatie • Aspirant GtK Leverancier

4. Publiceren	
Input	Verklaring GtK Leverancier
Activiteit	De Twiin Organisatie publiceert een actuele lijst met de nieuwe aspirant GtK Leverancier.
Output	Actuele lijst van GtK Leveranciers
Wie?	• Twiin Organisatie

8.2 | Valideren

Een Twiin Deelnemer werkt vanaf het tekenen van de Deelnemersovereenkomst toe naar het valideren van één of meer zorgtoepassingen. Een GtK Leverancier werkt vanaf het tekenen van de Verklaring GtK Leverancier toe naar het valideren van het GtK voor één of meer zorgtoepassingen. Deelnemers kunnen zich enkel laten valideren voor een zorgtoepassing als zij gebruik maken van een GtK dat ook voor die zorgtoepassing gevalideerd is.

In de onderliggende pagina's staat een korte omschrijving van de dienst en de toegevoegde waarde.

- 8.2.1 | Validatie Twiin Deelnemer (see page 128)
- 8.2.2 | Validatie GtK (see page 132)

8.2.1 | Validatie Twiin Deelnemer

Omschrijving van de dienst

Wanneer een Twiin Deelnemer aangeeft gereed te zijn voor landelijke uitwisseling van een zorgtoepassing, start de Validatie. De dienst Validatie heeft als doel de Twiin Deelnemer te begeleiden bij dit proces. De Twiin Dienstverlener ondersteunt de Twiin Deelnemer hierbij.

Een Twiin Deelnemer dient zich te laten valideren per zorgtoepassing.

Doelstelling

Het proces Validatie Twiin Deelnemer heeft als doel om op een zorgvuldige en beheerste wijze aan te tonen dat een Twiin Deelnemer voldoet aan alle voorwaarden van het Twiin Afsprakenstelsel om landelijk gegevens uit te wisselen voor een zorgtoepassing. Dit met als achterliggend doel het onderlinge vertrouwen tussen Twiin Deelnemers te borgen dat aan alle voorwaarden is voldaan om landelijk gegevens uit te wisselen voor die zorgtoepassing. Een Twiin Deelnemer dient aan de Voorwaarden Twiin Deelnemer (see page 142) te voldoen om gevalideerd te worden.

Toegevoegde waarde

Met een validatie toont een Twiin Deelnemer aan andere aangesloten partijen aan dat zijn organisatie voldoet aan de eisen die het Twiin Afsprakenstelsel stelt aan een Twiin Deelnemer voor de betreffende zorgtoepassing. Twiin controleert of de Twiin Deelnemer aan alle voorwaarden voldoet. Doordat alle Twiin Deelnemers op dezelfde wijze worden getoetst, kunnen andere aangesloten partijen erop vertrouwen dat de Twiin Deelnemer aan alle voorwaarden voldoet. Twiin kan eventuele generieke problemen in het proces Validatie snel herkennen en daarvoor oplossingen zoeken.

De dienst Validatie Twiin Deelnemer beschrijft de stappen om zorgaanbieders te valideren zodat deze binnen Twiin als Twiin Deelnemer kunnen acteren.

Verantwoordelijkheden

Diverse partijen hebben verantwoordelijkheden en taken in het proces Validatie Twiin Deelnemer:

- De Twiin Deelnemer is verantwoordelijk voor het implementeren van de voorwaarden die het Twiin Afsprakenstelsel stelt. Tijdens de dienst Validatie moet de Twiin Deelnemer hiervoor documentatie aanleveren en testen doorlopen.
- De Twiin Dienstverlener ondersteunt de Twiin Deelnemer gedurende de dienst Validatie.
- De Twiin Casemanager voert de volgende taken uit bij de dienst Validatie Twiin Deelnemer:
  - Houdt het intakegesprek en geeft informatie over de procedure en voorwaarden.
  - Administreert het dossier validatie en controleert de volledigheid ervan.
  - Controleert of de deelnemer voldoet aan de voorwaarden.
  - Stelt het advies op.
- Het Twiin Bestuur beoordeelt de validatie o.b.v. het advies van de Twiin Casemanager en geeft een Bewijs van Validatie Twiin Deelnemer uit.

Hervalideren

Het opnieuw doorlopen van de dienst Validatie vindt plaats:

- Tijdig voor het verlopen van de geldigheid van de validatie. De geldigheidsduur wordt meegegeven in het Bewijs van Validatie Twiin Deelnemer.
- Bij grote wijzigingen in de voorwaarden die worden gesteld.
- Op basis van het proces Handhaving (see page 140).

Toelichting proces Validatie Twiin Deelnemer

1. Aanmelden	
Input	Intern besluit van Twiin Deelnemer dat zijn organisatie gereed is voor validatie voor een zorgtoepassing

0. Aanmelden

Activiteit	Een Twiin Deelnemer meldt zich bij Twiin met een verzoek tot validatie voor een zorgtoepassing. De Twiin Deelnemer vult daartoe het aanmeldformulier in. Dit formulier bevat alle relevante informatie over de Twiin Deelnemer.
Output	Informatie over de Twiin Deelnemer.
Wie?	• Twiin Deelnemer

2. Intake

Input	Aanmeldformulier Twiin Deelnemer met verzoek tot validatie voor een nieuwe zorgtoepassing.
Activiteit	Een Twiin Casemanager houdt een intake en informeert de Twiin Deelnemer over procedure en vereisten. De Twiin Casemanager licht toe op welke omgeving de Twiin Deelnemer de voorwaarden kan doorlopen, testen kan uitvoeren en bewijslast kan aanleveren. De Twiin Casemanager licht toe hoe de Twiin deelnemer een account voor de validatieomgeving aanvraagt. Tijdens de intake zal ook kenbaar gemaakt worden waar een Twiin Deelnemer gedurende het proces met zijn vragen terecht kan.
Output	Samenvatting van intake, plan voor vervolg en account voor Twiin Validatieomgeving
Wie?	• Twiin Casemanager • Twiin Deelnemer • Twiin Dienstverlener (optioneel)

3. Begeleiding van de Twiin Deelnemer en doorlopen voorwaarden

Input	Twiin voorwaarden en status Twiin Deelnemer

0. Begeleiding van de Twiin Deelnemer en doorlopen voorwaarden

Activiteit	De Twiin Deelnemer wordt begeleid in het voldoen aan de voorwaarden en de activiteiten die daarvoor moeten gebeuren. • Inrichting van processen en afspraken • Ondersteuning bij inrichting bij processen en afspraken • Beantwoording van vragen m.b.t. generieke voorwaarden en vastleggen van alle bewijslast • Inrichting van testomgeving • Ondersteuning bij inrichting van testomgeving • Uitvoeren van technische test • Ondersteuning bij uitvoering van technische test
Output	De Twiin Deelnemer levert alle stukken aan die nodig zijn voor validatie
Wie?	• Twiin Dienstverlener • Twiin Deelnemer • GtK Beheerder

4. Validatie

Input	Dossier validatie Twiin Deelnemer
Activiteit	Controle van het dossier door Twiin Casemanager
Output	Beoordeling van dossier met advies over toekennen Bewijs van Validatie
Wie?	• Twiin Casemanager

5. Beoordeling advies

Input	Beoordeling van het doorlopen proces van validatie
Activiteit	Bestuur van Twiin beoordeelt het doorlopen proces van validatie o.b.v. het advies van de Twiin Casemanager.
Output	Advies en besluit, positief of negatief, over het toekennen van het Bewijs van Validatie van een Zorgtoepassing van Twiin Deelnemer, inclusief een periode dat de validatie van kracht blijft.

0. Beoordeling advies	
Wie?	• Twiin Bestuur

6. Definitief maken validatie	
Input	Positief besluit over het toekennen van het Bewijs van Validatie Twiin Deelnemer door het Twiin Bestuur
Activiteit	Twiin Deelnemer ontvangt een Bewijs van Validatie Twiin Deelnemer
Output	Bewijs van Validatie Twiin Deelnemer voor een Zorgtoepassing
Wie?	• Twiin Deelnemer • Twiin Bestuur

8.2.2 | Validatie GtK

Omschrijving van de dienst

Wanneer een GtK Leverancier kenbaar maakt gereed te zijn voor uitwisseling van een zorgtoepassing start de Validatie. De dienst Validatie heeft als doel de GtK Leverancier te begeleiden bij het validatieproces.

Een leverancier van een GtK dient deze per zorgtoepassing te laten valideren door Twiin.

Doelstelling

De doelstelling van de dienst Validatie GtK is om op een zorgvuldige en beheerste wijze te gebruiken applicaties binnen Twiin te valideren. GtK Leveranciers moeten zorgen dat hun GtK voldoet aan de Voorwaarden (see page 162) genoemd in het Twiin Afsprakenstelsel om dit vertrouwen te kunnen waarborgen.

Toegevoegde waarde

Met een validatie toont een GtK Leverancier aan zijn klanten aan dat zijn applicatie voldoet aan de eisen die het Twiin Afsprakenstelsel stelt aan het GtK voor de betreffende zorgtoepassing. Twiin begeleidt het Proces Validatie van het GtK en controleert of deze aan alle eisen voldoet. Doordat Twiin alle validatieprocessen begeleidt, profiteren GtK Leveranciers direct van deze kennis en ervaring. Doordat alle GtK's op dezelfde wijze worden getoetst, kunnen klanten van de GtK Leverancier erop vertrouwen dat het GtK aan alle eisen voldoet. Twiin kan eventuele generieke problemen in het Proces Validatie snel herkennen en daarvoor oplossingen zoeken.

De dienst Validatie GtK beschrijft de stappen om applicaties te valideren zodat deze binnen Twiin als GtK gebruikt kunnen worden.

Verantwoordelijkheden

Diverse partijen hebben verantwoordelijkheden en taken in het Proces Validatie GtK:

- De GtK Leverancier is verantwoordelijk voor het implementeren van de voorwaarden die het Twiin Afsprakenstelsel stelt. Hij stelt de benodigde documentatie en bewijsstukken beschikbaar voor de toetsing.
- Een Twiin Casemanager voert de volgende taken uit bij het Proces Validatie GtK:
  - Houdt het intakegesprek en geeft informatie over de procedure en vereisten.
  - Administreert het validatiedossier en controleert op de volledigheid ervan.
  - Controleert of voldaan wordt aan de voorwaarden.
  - Stelt het advies op.
- Het Twiin Bestuur beoordeelt de validatie o.b.v. het advies van de Twiin Casemanager en geeft een Bewijs van Validatie GtK uit.

Hervalideren

Het Bewijs van Validatie GtK is enkel van toepassing op de gevalideerde versie van het GtK.

Het opnieuw doorlopen van de dienst Validatie vindt plaats:

- Tijdig voor het verlopen van de geldigheid van de validatie. De geldigheidsduur wordt meegegeven in het Bewijs van Validatie GtK.
- Bij grote wijzigingen in de voorwaarden die worden gesteld.
- Bij nieuwe versies (major release) van het GtK zelf.
- Als dat vereist is door de Twiin Organisatie op basis van de dienst Handhaving (see page 140).

Toelichting Proces Valideren GtK

1. Aanmelden	
Input	Besluit van een leverancier dat zijn GtK gereed is voor validatie van een zorgtoepassing
Activiteit	Een huidige of nieuwe GtK Leverancier meldt zich bij Twiin met een verzoek tot (uitbreiding) validatie.
Output	Informatie over de nieuwe leverancier, GtK en zorgtoepassing

0. Aanmelden

Wie?	• GtK Leverancier

2. Intake

Input	Intake van een nieuwe GtK of nieuwe zorgtoepassing
Activiteit	Twiin houdt een intake en informeert de verzoekende partij over procedure en voorwaarden. Hierbij zal ook kenbaar gemaakt worden waar een leverancier gedurende het proces met zijn vragen terecht kan.
Output	• Samenvatting van intake en plan voor vervolg
Wie?	• Twiin Casemanager • GtK Leverancier

3. Testen door leverancier

Input	GtK inclusief testscript en testomgeving van Twiin
Activiteit	• Leverancier ontvangt een account voor de Twiin validatieomgeving van de zorgtoepassing. • Leverancier koppelt zijn GtK aan de Twiin validatieomgeving van de zorgtoepassing. • Leverancier doorloopt de testscenario's van de desbetreffende zorgtoepassing. • Leverancier voegt de documentatie toe behorend bij de generieke voorwaarden indien het een nieuw GtK betreft De volgende testfases worden doorlopen: • Testen van de inhoud van berichten • Testen van de gehele keten op de validatieomgeving , zoals beschreven in de implementatiehandleiding van de desbetreffende zorgtoepassing,
Output	• Beide testfases zijn met succes doorlopen en het beoordelen van de output_kan starten.
Wie?	• Twiin Casemanager • GtK Leverancier

4. Validatie

Input	Testresultaten en aangeleverde documentatie
Activiteit	Gedurende de validatie zullen de resultaten uit de testfase gecontroleerd worden. Als alle testen die benodigd zijn voor validatie goed zijn afgerond kan het advies worden afgegeven om de applicatie het predicaat 'Twiin Gevalideerd' te geven.
Output	Beoordeling van de testresultaten en aangeleverde documentatie met een advies
Wie?	• Twiin Casemanager • Twiin Organisatie • GtK Leverancier

5. Beoordeling advies

Input	Advies naar aanleiding van de beoordeling van de testresultaten en aangeleverde documentatie
Activiteit	Bestuur van Twiin beoordeelt de testresultaten en aangeleverde documentatie o.b.v. het advies van de Twiin Casemanager.
Output	Besluit, positief of negatief, over validatie GtK door Twiin, inclusief een periode dat de validatie van kracht blijft en een hervalidatie benodigd is.
Wie?	• Twiin Bestuur

6. Definitief maken validatie

Input	Positief besluit validatie GtK door Twiin Bestuur
Activiteit	Leverancier GtK ontvangt een Bewijs van Validatie GtK
Output	Bewijs van Validatie GtK voor één of meer Zorgtoepassingen
Wie?	• Twiin Bestuur • GtK Leverancier

8.3 | Ketenregie

Uitgangspunten

Voor de dienst Ketenregie gelden de volgende uitgangspunten:

- De dienst Ketenregie is bedoeld om te zorgen voor een transparant en uniform proces voor het melden van incidenten bij Twiin Deelnemers voor zover die impact hebben op andere Twiin Deelnemers of hun GtK Beheerders.
- De Twiin Organisatie zorgt voor de inrichting van een communicatieplatform voor Ketenregie met contactgegevens, versiebeheer en gemelde Incidenten (hierna: Twiin Serviceportaal).
- De Twiin Deelnemer zorgt voor een aanspreekpunt van de eigen organisatie voor vermelding in het Twiin Serviceportaal en voor contact met de eigen GtK Beheerder. Ook zorgt de Twiin Deelnemer voor een aanspreekpunt voor privacy en informatiebeveiliging, zoals vereist op basis van het informatiebeveiligingsbeleid (see page 117).
- Twiin Deelnemers en hun GtK Beheerders hebben zelf de regie over de contactgegevens van hun medewerkers zoals opgenomen in het Twiin Serviceportaal zoals naam, e-mail, telefoonnummer en rol en kunnen deze indien nodig aanpassen.
- Twiin Deelnemers en hun GtK Beheerders zorgen dat de naamgeving van hun organisatie in lijn is met de registratie van het Bewijs van Validatie Twiin Deelnemers. De Twiin Organisatie kan zo nodig een correctie doorvoeren op de registratie om te zorgen voor eenduidige naamgeving van Twiin Deelnemer.
- Twiin Deelnemers richten een eigen servicedesk in inclusief contract met ondersteunende leveranciers of laten dat voor hen doen door een GtK Beheerder (hierna: “Servicedesk Twiin Deelnemer”).
- De dienst ketenregie richt zich op het informeren over Incidenten bij de informatie-uitwisseling tussen Twiin Deelnemers, maar niet op de inhoudelijke afwikkeling hiervan.
- De Twiin Organisatie is beschikbaar voor bemiddeling en eventuele handhaving in geval van conflicten die de Twiin Deelnemers en GtK Beheerders niet (tijdig) onderling kunnen oplossen.

Gelaagdheid Ketenregie

Ketenregie vindt op verschillende niveaus plaats:

- Een lokaal incident bij een Twiin Deelnemer: Twiin Deelnemers zijn gehouden om een lokaal incident lokaal af te handelen. Zij kunnen ook hun GtK Beheerder opdracht geven om lokale incidenten voor hen af te handelen.
- Meerdere samenwerkende Twiin Deelnemers aangesloten bij één GtK Beheerder: Bij een incident waarbij meerdere Twiin Deelnemers, aangesloten bij één GtK Beheerder, zijn betrokken, kan de GtK Beheerder zorgen voor de coördinatie. De GtK Beheerder kan voor dit doel het Twiin Serviceportaal gebruiken.

- Deelnemers aangesloten bij meerdere GtK Beheerders: Bij een incident waarbij meerdere GtK Beheerders en/of GtK's zijn betrokken, zullen zij onderling met elkaar in contact treden en via het Twiin Serviceportaal elkaar kunnen informeren.
- Op verzoek van Twiin Deelnemers en GtK Beheerders zorgt de Twiin Organisatie voor bemiddeling tussen Twiin Deelnemers en GtK Beheerders en zo nodig kan de Twiin Organisatie op hun verzoek of op eigen initiatief zorgen voor handhaving conform de dienst Handhaving (see page 140).

Beheer Twiin Deelnemer

De Twiin Deelnemer is verantwoordelijk voor het inregelen van het beheer van zijn eigen ICT-systemen met bijbehorende Servicedesk Twiin Deelnemer en voor het volgen van het proces Incidentmelding (see page 137). De Twiin Deelnemer kan deze taken beleggen bij een GtK Beheerder.

- Gebruikers melden eventuele problemen bij de Servicedesk Twiin Deelnemer.
- De Servicedesk Twiin Deelnemer onderzoekt het probleem en zoekt naar een mogelijke oplossing.
- Mocht het gemelde probleem door systemen bij een andere Twiin Deelnemer worden veroorzaakt, dan zoekt de Servicedesk Twiin Deelnemer daar zelf contact mee door gebruik te maken van de gegevens in het Twiin Serviceportaal.
- De Servicedesk Twiin Deelnemer kan via Twiin Serviceportaal nagaan of sprake is van incidenten bij andere Twiin Deelnemers, kan de gegevens daarvan inzien en kan zo nodig contactgegevens van die Twiin Deelnemers opzoeken.
- Incidenten waar andere Twiin Deelnemers en GtK Beheerders hinder van kunnen hebben, worden tijdig gemeld. Binnen het Twiin Serviceportaal is vervolgens te zien of er relevante meldingen zijn gedaan en indien nodig kunnen beheerders onderling contact met elkaar opnemen om meer informatie te achterhalen.

Beheer Twiin Ketenregie

Twiin zorgt voor de inrichting van het Twiin Serviceportaal voor Ketenregie met de volgende functies:

- vastleggen incidenten (met categorieën verstoring, onderhoud en activeren nieuwe applicatie)
- contactgegevens Servicedesk Twiin Deelnemers
- contactgegevens GtK Beheerder van Twiin Deelnemer (indien van toepassing)
- e-mailnotificaties
- zoeken op Servicedesk Twiin Deelnemer, Twiin Deelnemer, impact, soort melding en datum

8.3.1 | Incidentmelding

- Twiin Deelnemers zorgen voor goede afspraken met hun eigen GtK Beheerder en eventueel GtK Leverancier over het tijdig ontvangen van meldingen over tijdelijke verstoringen, (gepland) onderhoud, beveiligingsincidenten en datalekken ter zake van hun GtK. De Twiin Deelnemers zorgen ervoor dat hun Servicedesk Twiin Deelnemer de relevante informatie beoordeelt om te bepalen of sprake is van een Incident dat gemeld moet worden op basis van dit proces incidentmelding.

- De Servicedesk Twiin Deelnemer is gehouden om incidenten te melden en tevens AVG-verzoeken van cliënten zoals omschreven in nr. 2.6 van de Voorwaarden Twiin Deelnemer (see page 142).
    - Meldingen worden gedaan in het Twiin Serviceportaal als meerdere partijen (Twiin Deelnemers en hun GtK Beheerders en GtK's) er hinder van kunnen ondervinden. Denk aan tijdelijke verstoringen, (gepland) onderhoud, beveiligingsincidenten en datalekken voor zover die meerdere andere partijen raken.
    - Meldingen van incidenten en AVG-verzoeken waarbij bekend is welke specifieke andere partijen zijn betrokken worden gericht aan die andere partijen (Twiin Deelnemers en hun GtK Beheerders) via de contactgegevens die te vinden zijn in het Twiin Serviceportaal.
- De Servicedesk Twiin Deelnemer zorgt ervoor dat alle relevante feiten en omstandigheden worden gedeeld aan de andere Servicedesk Twiin Deelnemer bij het melden van incidenten, zowel aan het begin als tussentijds. En ook verstrekt Twiin Deelnemer na afloop een *root cause analysis*.
- Twiin Deelnemers zorgen dat hun eigen Servicedesk Twiin Deelnemer beschikbaar is via de contactgegevens zoals vastgelegd in het Twiin Serviceportaal.
- De Servicedesk Twiin Deelnemer meldt incidenten zo snel mogelijk. Als het gaat om een inbreuk in verband met persoonsgegevens dan meldt de Servicedesk Twiin Deelnemer het Incident zonder onredelijke vertraging zodanig dat de overige Twiin Deelnemers in staat zijn om te voldoen aan de wettelijke termijnen.
- De Twiin Organisatie ontvangt de meldingen van incidenten via het Twiin Serviceportaal en kan ook zelf meldingen indienen over Twiin Deelnemers en hun GtK Beheerders en GtK's. In geval van incidenten met privacy- en beveiligingsrisico's kan de Twiin Organisatie besluiten om het proces Handhaving (see page 140) te starten.

8.4 | Risicoanalyse

Beschikbaarheid, integriteit en vertrouwelijkheid

De Twiin Organisatie voert periodiek samen met Twiin Deelnemers, Twiin Dienstverleners, GtK Beheerders en GtK Leveranciers een risicoanalyse uit gericht op informatieveiligheidsrisico's, zoals vastgelegd in het informatiebeveiligingsbeleid (see page 117). Dit zijn risico's die kunnen leiden tot inbreuken op de beschikbaarheid, integriteit of vertrouwelijkheid van informatie. Hiermee geven partijen invulling aan de plicht in de NEN 7512. Het gaat hier om een risicoanalyse op stelselniveau, dat wil zeggen dat het om de risico's gaat in de onderlinge relatie tussen de betrokken partijen en niet de specifieke analyse bij een betrokken partij. Daarmee zijn alle onderdelen uit het Twiin Afsprakenstelsel onderwerp van de risicoanalyse. Maatregelen die voortkomen uit de analyse kunnen betrekking hebben op de Twiin Deelnemers, GtK Beheerders, GtK Leveranciers en de Twiin Organisatie.

De risicoanalyse is niet publiekelijk beschikbaar gelet op het vertrouwelijke karakter ervan, maar is wel op te vragen door Twiin Deelnemers en GtK Leveranciers die gevalideerd zijn voor één of meer zorgtoepassingen. Twiin Deelnemers kunnen de analyse delen met hun Twiin Dienstverlener.

Uitgangspunten bij de risicoanalyse

1. De scope van de risicoanalyse wordt bepaald door de architectuur, met name de principes. Op basis hiervan worden uitspraken gedaan over beschikbaarheid, vertrouwelijkheid en integriteit van de informatie binnen scope van het afsprakenstelsel.
2. De risicoanalyse wordt uitgevoerd op basis van de, op het moment van uitvoering, laatst gepubliceerde release van het Twiin Afsprakenstelsel.
3. In de analyse is een vertegenwoordiging van de Twiin Deelnemers, Twiin Dienstverleners, GtK Beheerders en GtK Leveranciers betrokken.
4. Voldoen aan geldende wet- en regelgeving is een startpunt voor alle partijen en een vereiste in de definitie van maatregelen.
5. Het bestuur van de Twiin Organisatie streeft naar een voor de betrokken partijen aanvaardbaar risiconiveau aan de hand van de impact op de volgende onderwerpen: gezondheid, privacy, financiën, imago en vertrouwen. De Twiin Organisatie bepaalt met betrokkenen wat dit aanvaardbare risiconiveau is. De Twiin Organisatie stelt de risicoanalyse, de risicotolerantie en beveiligingsmaatregelen vast.

Maatregelen

De risicoanalyse leidt tot het formuleren van drie typen maatregelen:

1. Maatregelen die direct betrekking hebben op risico’s voor de werking en veiligheid van het stelsel en daarom uniform moeten worden vastgesteld.
2. Maatregelen voor risico’s die kunnen leiden tot stelselrisico's (een gebeurtenis bij een Twiin Deelnemer die schade toebrengt aan andere deelnemers of de Twiin Organisatie). Deze zijn gespecificeerd in het stelsel om eenduidige interpretatie af te dwingen.
3. Maatregelen die vanuit het oogpunt van efficiëntie in het stelsel staan, zodat niet iedere partij deze afzonderlijk hoeft te definiëren.

De geformuleerde maatregelen kunnen op verschillende manieren worden opgenomen in het afsprakenstelsel. Er kunnen technische specificaties worden geformuleerd voor deelnemers in de technische kern. Beleid en operationele processen kunnen worden vormgegeven, dan wel de voorwaarden worden aangevuld.

Verwerking in het afsprakenstelsel

Aantoonbaar voldoen aan de NEN 7510 is wettelijk verplicht bij de gegevensuitwisseling tussen zorgaanbieders. Het Twiin Afsprakenstelsel verplicht de GtK Leverancier, GtK Beheerder en Twiin Deelnemer dan ook aan te tonen dat wordt voldaan aan NEN 7510.

Een NEN 7510-certificering in samenhang met het proces toetreding en aansluiten en het proces Valideren, dekt de belangrijkste informatiebeveiligingsrisico’s van het stelsel af.

Op een aantal onderwerpen zijn maatregelen uit de NEN 7512-norm meer specifiek ingevuld voor uitwisseling op basis van het Twiin Afsprakenstelsel. Deze maatregelen staan in het Normenkader

informatiebeveiliging (see page 115). Daarnaast staan in de architectuu (see page 37)r, de technische kern (see page 164) en in het proces Incidentmelding (see page 137) maatregelen uit de risicoanalyse op stelselniveau. De uitvoering van deze maatregelen wordt onder meer getoetst via het proces Validatie (see page 128).

Herijking risicoanalyse

De risicoanalyse is een dienst die periodiek en bij bepaalde wijzingen moet worden uitgevoerd. Herijking van de risicoanalyse is nodig op het moment dat:

- wijzigingen in het afsprakenstelsel van invloed kunnen zijn op de risicoanalyse
- er incidenten met aanzienlijke impact zijn
- er bekende wijzigingen zijn in het dreigingslandschap
- er significante technische wijzigingen zijn in de werking van het stelsel
- er wijziging is van wetgeving waar het Twiin Afsprakenstelsel aan moet voldoen
- één van de uitgangspunten wordt gewijzigd

8.5 | Handhaving

De dienst Handhaving is gericht op de naleving van het Twiin Afsprakenstelsel door Twiin Deelnemers, GtK Beheerders, Twiin Dienstverleners en GtK Leveranciers. Het proces kan worden opgestart op basis van verschillende signalen:

1. Op verzoek van een Twiin Deelnemer, GtK Beheerder, Twiin Dienstverlener of GtK Leverancier vanwege (vermoeden van) niet-naleving bij één of meer (andere) aangesloten partijen.
2. Op basis van meldingen over (het vermoeden van) niet-naleving bij één of meer incidenten.
3. Bij het constateren van niet-naleving in het kader van het doorlopen van de dienst Valideren Twiin Deelnemer en/of Valideren GtK.

De dienst Handhaving doorloopt de volgende stappen:

1. **Constatering en vastlegging:** De Twiin Organisatie beschrijft zo concreet mogelijk welke verplichting van het Twiin Afsprakenstelsel het betreft en wat de concrete omstandigheden van het geval zijn.
2. **Verificatie en verzoek om nadere toelichting:** De constatering van de niet-naleving wordt schriftelijk voorgelegd aan de desbetreffende Twiin Deelnemer, GtK Beheerder, Twiin Dienstverlener en/of GtK Leverancier. De Twiin Deelnemer, GtK Beheerder, Twiin Dienstverlener en/of GtK Leverancier moet hierop reageren en aangeven welke maatregelen binnen welke termijn worden getroffen om de niet-naleving op te lossen.
3. **Beoordeling nadere toelichting en communicatie besluit:** Op basis van de ontvangen informatie beoordeelt de Twiin Organisatie of, gelet op de aard en de ernst van de niet-nageleefde verplichting, de door de Twiin Deelnemer, GtK Beheerder, Twiin Dienstverlener en/of GtK

Leverancier voorgestelde maatregelen en het benodigde tijdbestek passend zijn. In geval van een Twiin Deelnemer en een GtK kan de Twiin Organisatie besluiten het Bewijs van Validatie Twiin Deelnemer en het Bewijs van Validatie GtK al dan niet tijdelijk op te schorten of in te trekken. In geval van een Twiin Dienstverlener en een GtK Beheerder kan de Twiin Organisatie besluiten de Verklaring Twiin Dienstverlener en de verklaring GtK Beheerder al dan niet tijdelijk op te schorten of in te trekken.

4. **Formele ingebrekestelling:** De formele ingebrekestelling is de laatste aanmaning om te voldoen aan de niet-naleving en gebeurt schriftelijk met afschrift naar de overlegtafels. De Twiin Organisatie draagt de betreffende partij op een voor hem geldende verplichting uit het Twiin Afsprakenstelsel, binnen een bepaalde termijn, na te komen. De ingebrekestelling is de laatste mogelijkheid die de Twiin Deelnemer, GtK Beheerder, Twiin Dienstverlener en/of GtK Leverancier krijgt om de niet-naleving op te heffen. Als de gestelde termijn wordt overschreden dan is de Twiin Deelnemer, GtK Beheerder, Twiin Dienstverlener en/of GtK Leverancier in verzuim en kan de overeenkomst door de Twiin Organisatie worden ontbonden.
5. **Formele beëindiging:** Nadat de termijn is verstreken die in de ingebrekestelling is opgenomen, is sprake van verzuim. Op dat moment kan de Twiin Deelnemersovereenkomst, Verklaring GtK Beheerder, Verklaring Twiin Dienstverlener of Verklaring GtK Leverancier door de Twiin Organisatie worden ontbonden.

Tijdens elk van deze stappen kan de Twiin Organisatie constateren dat er ofwel geen sprake (meer) is van niet-naleving, ofwel dat er voldoende zicht is op naleving. Als er geen sprake (meer) is van niet-naleving, dan wordt de procedure beëindigd en dit wordt ook schriftelijk kenbaar gemaakt aan de betrokken organisatie. Bij voldoende zicht op naleving wordt nog vinger aan de pols gehouden.

De Twiin Organisatie gaat vertrouwelijk om met dossiers aangaande lopende en afgesloten nalevingszaken. Besluiten over opschorting van het Bewijs van Validatie en ontbinding van een overeenkomst zijn wel openbaar.

De Twiin Organisatie houdt bij het bepalen van de redelijke termijn rekening met de ernst van de privacy- en beveiligingsrisico's en de gangbare doorlooptijd voor het nemen van de relevante maatregelen.

9 | Voorwaarden

In onderliggende pagina's worden de Twiin Voorwaarden uitgewerkt die gelden voor de Twiin Deelnemer, Twiin Dienstverlener en voor beheer van het GtK en daarnaast ook de validatievoorwaarden GtK.

De voorwaarden volgen uit het vertrouwensmodel, de diensten en de governance toegepast op de rollen (actoren) genoemd in de architectuur. De voorwaarden zijn voornamelijk organisatorisch van aard. Daarnaast zijn er met name technische specificaties waaraan Twiin Deelnemers moeten voldoen. Deze specificaties zijn te vinden in de technische kern (see page 164).

Onderliggende pagina's

9.1 | Voorwaarden Twiin Deelnemer

Zodra een Twiin Deelnemer de Deelnemersovereenkomst (see page 84) heeft ondertekend, is deze Twiin Deelnemer gebonden aan de voorwaarden die in het schema hieronder verplicht zijn gesteld. Vanaf de validatie moet de Twiin Deelnemer voldoen aan alle Twiin Voorwaarden zoals in het schema hieronder weergegeven. Na validatie ontvangt de Twiin Deelnemer een Bewijs van Validatie waarmee landelijk gegevens kunnen worden uitgewisseld.

Tot aan validatie gelden de Samenwerkingsvoorwaarden. Deze volgen de Twiin Voorwaarden, met de mogelijkheid tot afwijking op enkele onderdelen. Waar dat het geval is, beschrijven de Samenwerkingsvoorwaarden deze afwijking. Bij nieuwe versies van het Twiin Afsprakenstelsel kan de ruimte voor afwijking in een bepaalde Samenwerkingsvoorwaarde vervallen.

De Twiin Dienstverlener beheert de Samenwerkingsvoorwaarden voor de Twiin Deelnemer.

De Twiin Dienstverlener houdt bij met welke andere Twiin Deelnemers gegevens worden uitgewisseld op basis van deze voorwaarden.

1. Wet en regelgeving

Twiin Voorwaarden	*Samenwerkingsvoorwaarden*

#	Onderwerp	Omschrijving	Verplicht vanaf ondertekening Deelnemersovereenkomst	Verplicht van af validatie	Eventuele afwijking	Toelichting afwijking incl. tijdpad
1.1	Contracten	De Twiin Deelnemer heeft de Twiin Deelnemersovereenkomst ondertekend.	Ja	Ja		
1.2		De Twiin Deelnemer heeft een (sub)verwerkersovereenkomst getekend met verwerker(s) die toegang heeft/hebben tot persoonsgegevens ter zake van de (kandidaat) GtK, welke overeenkomst voldoet aan artikel 28 AVG.	Ja	Ja		

2. Organisatorisch

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
#	Onderwerp	Omschrijving	Verplicht vanaf ondertekening Deelnemersovereenkomst	Verplicht vanaf validatie	Eventuele afwijking	Toelichting afwijking incl. tijdpad
2.1	Algemeen	De Twiin Deelnemer is gevalideerd voor de desbetreffende zorgtoepassing.	Nee	Ja	In te vullen	In te vullen
2.2	Twiin Dienstverlener	De Twiin Deelnemer is verplicht een Twiin Dienstverlener in te schakelen. Voor iedere zorgtoepassing kan de Twiin Deelnemer maar één Twiin Dienstverlener inschakelen. De Twiin Deelnemer zorgt dat de Voorwaarden Twiin Dienstverlener (see page 151) worden vervuld. De Twiin Deelnemer kan ook zelf de rol van Twiin Dienstverlener vervullen voor zichzelf en voor andere Twiin Deelnemers. In dat geval is de deelnemer zelf gehouden om de voorwaarden van de Twiin Dienstverlener te vervullen.	Ja	Ja		

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
2.3	GtK Beheerder	De Twiin Deelnemer zorgt dat de Voorwaarden GtK Beheer worden vervuld. De Twiin Deelnemer kan deze verplichtingen nakomen door een GtK Beheerder in te schakelen.	Ja	Ja		
2.4	Beveiliging	De Twiin Deelnemer draagt overeenkomstig het bepaalde in NEN 7510 en NEN 7512* en NEN 7513, aantoonbaar zorg voor een veilig en zorgvuldig gebruik van het eigen zorginformatiesysteem en een veilig en zorgvuldig gebruik van het uitwisselingssysteem. De Twiin Deelnemer beschikt over een auditverklaring voor NEN 7510 of een vergelijkbare andere verklaring dat aan NEN 7510 wordt voldaan. * Door deel te nemen aan het Twiin Afsprakenstelsel geeft de Twiin Deelnemer invulling aan NEN 7512.	Ja, waarbij de verklaring nog geen vereiste is	Ja		In te vullen vanaf wanneer audit-verklaring beschikbaar is

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
2.5	Privacy	De Twiin Deelnemer is verplicht passende technische en organisatorische maatregelen te nemen om de (bijzondere) persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking (zoals onbevoegde kennisname, aantasting, wijziging of verstrekking van de persoonsgegevens), minstens op een niveau dat gelet op de stand van de techniek en de gevoeligheid van de persoonsgegevens redelijk is rekening houdend met de uitvoeringskosten en de waarschijnlijkheid en ernst van de risico's e.e.a. conform artikel 32 AVG. Voor zover de wet daartoe verplicht, is de Twiin Deelnemer gehouden om zelf een gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren. De Twiin Deelnemer beoordeelt zelf voor de eigen organisatie en de eigen GtK vermoedelijke datalekken zoals bedoeld in artikel 33 AVG. Als uit deze beoordeling blijkt dat één of meer andere Twiin Deelnemers betrokken zijn, zal de Twiin Deelnemer hen zo snel als redelijkerwijs mogelijk is, informeren over de aard van het datalek, de mogelijke impact van het datalek op de andere Twiin Deelnemers, en/of de betrokkene(n), alsmede de maatregelen die hij heeft genomen of zal nemen om de beveiliging te corrigeren en/of de gevolgen te beperken. De Twiin Deelnemer zal samenwerken met de andere Twiin Deelnemers om: i) het datalek zo nodig te melden aan de Autoriteit Persoonsgegevens en zo nodig de betrokkenen; en ii) de oorzaak van het datalek te onderzoeken en alle maatregelen nemen die Twiin Deelnemers nodig achten om een vergelijkbaar incident te voorkomen.	Ja	Ja		

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
2.6	Rechten van cliënten	De Twiin Deelnemer zorgt voor een adequaat proces waarmee de cliënt te allen tijde zijn wettelijke rechten ter bescherming van zijn persoonsgegevens kan uitoefenen. Als de Twiin Deelnemer een verzoek ontvangt, terwijl een andere Twiin Deelnemer voor dat verzoek verantwoordelijk is, dan zal de Twiin Deelnemer die het verzoek ontvangt, de andere Twiin Deelnemer hierover zo mogelijk informeren en de cliënt naar de juiste Twiin Deelnemer verwijzen. De Twiin Deelnemer stelt de andere Twiin Deelnemers die persoonsgegevens van een cliënt hebben ontvangen in kennis van de rectificatie of wissing van persoonsgegevens of beperking van de verwerking, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. De Twiin Deelnemer verstrekt de cliënt informatie over deze ontvangende Twiin Deelnemers indien de cliënt hierom vraagt.	Ja	Ja		

3. Zorgprocessen

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
#	Onderwerp	Omschrijving	Verplicht vanaf ondertekening Deelnemersovereenkomst	Verplicht vanaf validatie	Eventuele afwijking	Toelichting afwijking incl. tijdpad
3.1	Behandelrelatie	De Twiin Deelnemer moet controleren op de behandelrelatie tussen zorgverlener en cliënt. De Twiin Deelnemer zorgt voor een autorisatiestructuur met het doel om ervoor te zorgen dat een zorgverlener enkel met een behandelrelatie toegang krijgt tot gegevens van de cliënt.	Ja	Ja		

4. Informatie

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
#	Onderwerp	Omschrijving	Verplicht vanaf ondertekening Deelnemersovereenkomst	Verplicht van afvalidatie	Eventuele afwijking	Toelichting afwijking incl. tijdpad
4.1	Algemeen	De Twiin Deelnemer volgt per zorgtoepassing dezelfde en meest recente versie van de implementatiewijzer en is verantwoordelijk voor het doorvoeren van aanpassingen conform het Twiin Releasebeleid.	Nee	Ja	In te vullen	In te vullen
4.2		De Twiin Deelnemer zorgt ervoor dat ter beschikking gestelde gegevens voldoen aan semantiek, formaat en structuur conform het Twiin Afsprakenstelsel en gebruikte Nictiz-informatiestandaarden, zoals vastgelegd in de aansluit- en implementatiewijzer. De Twiin Deelnemer staat ervoor in dat de door hen verstrekte gegevens juist, actueel en volledig zijn.	Nee	Ja	In te vullen	In te vullen
4.3	Metadata	De Twiin Deelnemer is verantwoordelijk voor het juiste gebruik en invulling van metadata conform het Twiin Afsprakenstelsel en kan dit laten zien met een overzicht van de gebruikte bronsystemen en de gebruikte metadata.	Nee	Ja	In te vullen	In te vullen

5. Applicatie

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
#	Onderwerp	Omschrijving	Verplicht vanaf ondertekening Deelnemersovereenkomst	Verplicht vanaf validatie	Eventuele afwijking	Toelichting afwijking incl. tijdpad

5.1		De Twiin Deelnemer maakt voor de uitwisseling van de Twiin Zorgtoepassing uitsluitend gebruik van Gevalideerde Twiin Knooppunten (GtK's).	Nee	Ja	In te vullen	In te vullen
5.2		De Twiin Deelnemer is verantwoordelijk voor implementatie van het GtK conform het Twiin Afsprakenstelsel.	Nee	Ja	In te vullen	In te vullen
5.3		De Twiin Deelnemer volgt het releasebeleid van Twiin.	Ja	Ja		
5.4	Testmanagement	De Twiin Deelnemer moet, naast de productieomgeving, beschikken over een test-/acceptatieomgeving die voldoet aan de richtlijnen van NEN 7510-2.	Ja	Ja		
5.5		De Twiin Deelnemer doorloopt een ketentest.	Nee	Ja	In te vullen	In te vullen
5.6		De Twiin Deelnemer gebruikt een set testcliënten met een geldig fictief BSN.	Nee	Ja	In te vullen	In te vullen
5.7	Identificatie	De Twiin Deelnemer gebruikt geverifieerde en gevalideerde Burgerservicenummers (BSN) van cliënten.	Ja	Ja		
5.8		De Twiin Deelnemer zorgt voor het eenduidig identificeren van de eigen zorgverleners bij gebruik van het GtK. De Twiin Deelnemer zorgt voor identificatie van zorgverleners op basis van UZI als dit mogelijk is. Als dit niet kan is een ander identifier van de zorgverlener ook toegestaan (bijvoorbeeld het eigen medewerkernummer i.c.m. het URA. Deze identifier moet uniek voor de zorgverlener zijn én blijven)*. * Het hebben van een UZI-nummer is momenteel hard gekoppeld aan het aanvragen van een UZI-pas. Wanneer het niet mogelijk of gewenst is om de UZI-pas aan te vragen en/of te gebruiken kan een zorgverlener een ander identificatiemiddel gebruiken waaraan een andere identifier is gekoppeld. De eis uit de NEN7512 dat dit een eIDAS betrouwbaarheidsniveau 'hoog' identificatiemiddel moet zijn blijft staan.	Ja	Ja		
5.9		De Twiin Deelnemer identificeert zichzelf met het UZI-Register Abonneenummer (URA).	Nee	Ja	In te vullen	In te vullen

5.10	Authenticatie	De Twiin Deelnemer is verantwoordelijk voor de authenticatie van zorgverleners die het GtK gebruiken.	Ja	Ja		
5.11		De Twiin Deelnemer borgt dat zijn gebruikers van het GtK (zorgverleners) hiervoor een identificatiemiddel gebruiken dat voldoet aan eIDAS-hoog.	Nee	Ja	In te vullen	In te vullen
5.12	Autorisatie	De Twiin Deelnemer gebruikt het autorisatieprotocol zoals afgesproken voor de zorgtoepassing(en).	Ja	Ja		
5.13	Toestemming	De Twiin Deelnemer draagt zorg voor het (laten) uitvragen, vastleggen en toepassen van de toestemming van de cliënt. (Vastleggen van veronderstelde toestemming is overigens geen vereiste).	Ja	Ja		
5.14		De Twiin Deelnemer maakt gebruik van Mitz als toestemmingsvoorziening voor zover nodig voor de zorgtoepassing (bij communicatiepatronen (see page 169) raadpleegbaar maken en bij verzenden dossier als het gaat om de use case opvragen dossier).	Nee	Ja	In te vullen	In te vullen
5.15	Lokalisatie	De Twiin Deelnemer maakt gebruik van een lokalisatievoorziening zoals en wanneer de zorgtoepassing dit vereist (bij communicatiepatronen Pull en indexed Pull). Zie ook 10.2.6 | Generieke functie – Lokalisatie (see page 184)	Nee	Ja	In te vullen	In te vullen
5.16		{vervallen}				
5.17	Adressering	De Twiin Deelnemer zorgt dat de adresinformatie op betrouwbare wijze wordt verkregen.	Ja	Ja		

5.18		De Twiin Deelnemer levert zijn eigen adresgegevens aan bij de Twiin Beheerorganisatie voor publicatie in ZORG-AB*. Als de Twiin Deelnemer routering wil realiseren, deelt de Twiin Deelnemer de gegevens voor interne routering met andere Twiin Deelnemers. *Gebruik van ZORG-AB is een afspraak uit het Integraal Zorgakkoord (IZA): "Zorgaanbieders verbinden zich aan de door VWS en in afstemming met het Informatieberaad Zorg vastgestelde oplossingen voor de 6 generieke functies (zoals Mitz en ZORG-AB) en implementeren deze uiterlijk 2025 met hun leveranciers ter ondersteuning van hun zorgprocessen." Twiin kiest -ook bij gebrek aan andere beschikbare adresboeken- daarom nu voor voor ZORG-AB, maar stelt geen verplichting aan zorgaanbieders/deelnemers om ZORG-AB ook te gebruiken, zie ook 10.2.5 | Generieke functie - Adressering (see page 184)	Nee	Ja	In te vullen	Voorwaarde voor aanlevering routering is geldig tot opname Technische Afspraak Routering wordt opgenomen in het Twiin Afsprakenstelsel.
5.19	Logging	De Twiin Deelnemer is verantwoordelijk voor het loggen van transacties met gebruik van het GtK.	Ja	Ja		
5.20		De Twiin Deelnemer zorgt voor logging rapportages en procedures voor het opvragen en opstellen van rapportages van logging conform het Twiin Afsprakenstelsel.	Nee	Ja	In te vullen	In te vullen

6. Infrastructuur

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
#	Onderwerp	Omschrijving	Verplicht vanaf ondertekening Deelnemersovereenkomst	Verplicht vanaf validatie	Eventuele afwijking	Toelichting afwijking incl. tijdpad

6.1	Netwerk	De Twiin Deelnemer is verantwoordelijk voor het correct gebruik van een GtK. Dat betekent dat de Twiin Deelnemer zorgt dat het GtK is verbonden met andere GtK's via een netwerk dat voldoet aan de eisen voor veilig netwerk zoals omschreven in voorwaarde nr. 1.3 Voorwaarden GtK.	Nee	Ja	In te vullen	In te vullen

9.2 | Voorwaarden Twiin Dienstverlener

De Twiin Dienstverlener heeft een aantal taken en verantwoordelijkheden die op deze pagina zijn weergegeven. Het is de verantwoordelijkheid van de Twiin Deelnemer om te zorgen dat er een Twiin Dienstverlener is aangesteld en dat de voorwaarden van de Twiin Dienstverlener worden nagekomen.

Zodra de Twiin Deelnemer de Deelnemersovereenkomst (see page 84) heeft ondertekend, is Twiin Deelnemer verplicht om te zorgen dat de voorwaarden Twiin Dienstverlener worden nagekomen die in het schema hieronder verplicht zijn gesteld. Vanaf validatie moet de Twiin Deelnemer zorgen dat alle voorwaarden Twiin Dienstverlener worden nagekomen zoals in het schema hieronder weergegeven.

Tot aan validatie gelden de Samenwerkingsvoorwaarden. De Samenwerkingsvoorwaarden volgen de Twiin Voorwaarden, behalve dat op een aantal onderdelen afwijking mogelijk is. In die gevallen beschrijven de Samenwerkingsvoorwaarden deze afwijking. Bij nieuwe versies van het Twiin Afsprakenstelsel kan de ruimte voor afwijking in een bepaalde Samenwerkingsvoorwaarde vervallen.

De Twiin Dienstverlener beheert de Samenwerkingsvoorwaarden voor de Twiin Deelnemer. De Twiin Dienstverlener houdt voor de Twiin Deelnemer bij met welke andere Twiin Deelnemers hij uitwisselt op basis van de Samenwerkingsvoorwaarden.

1. Organisatorisch

Twiin Voorwaarden	*Samenwerkingsvoorwaarden*

#	Onderwerp	Omschrijving	Verplicht vanaf ondertekening Deelnemersovereenkomst	Verplicht vanaf validatie	Eventuele afwijking	Toelichting afwijking incl. tijdpad
1.1	Governance	Het ondersteunen van de Twiin Deelnemer om te komen tot naleving van alle afspraken in het Twiin Afsprakenstelsel waaronder alle Twiin Voorwaarden. Deelnemen aan overlegtafel Twiin om te zorgen voor afstemming van de samenwerkingsvoorwaarden met andere Twiin Dienstverleners.	Ja	Ja		

2. Zorgprocessen

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
#	Onderwerp	Omschrijving	Verplicht vanaf ondertekening Deelnemersovereenkomst	Verplicht vanaf validatie	Eventuele afwijking	Toelichting afwijking incl. tijdpad

2.1	Gebruik	Monitoren van het gebruik van de zorgtoepassing(en) met als doel om het gebruik door zorgverleners te optimaliseren. Monitoring betekent dat de Twiin Dienstverlener achterhaalt of een zorgtoepassing gebruikt wordt door eindgebruikers en indien nodig stappen onderneemt om eventuele knelpunten op te lossen. Bijvoorbeeld door zorgprocessen in overleg met Twiin Deelnemers beter op elkaar af te stemmen.	Ja	Ja

3. Informatie

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
#	**Onderwerp**	**Omschrijving**	**Verplicht vanaf ondertekening Deelnemersovereenkomst**	**Verplicht vanaf validatie**	**Eventuele afwijking**	**Toelichting afwijking incl. tijdpad**
3.1	Algemeen	Inrichten van een procedure die de Twiin Deelnemer ondersteunt om te voldoen aan het Twiin releasebeleid.	Nee	Ja	In te vullen	In te vullen

3.2	Zorgtoepassingen	De Twiin Deelnemer ondersteunen in het voldoen aan semantiek, formaat en structuur conform het Twiin Afsprakenstelsel en gebruikte Nictiz-informatiestandaarden, zoals per zorgtoepassing vastgelegd.	Nee	Ja	In te vullen	In te vullen
3.3	Logging	Ondersteunen van de Twiin Deelnemer(s) en hun GtK Beheerder(s) bij de logging van transacties tussen Twiin Deelnemer(s) en gemeenschappelijke voorzieningen conform het Twiin Afsprakenstelsel.	Nee	Ja	In te vullen	In te vullen

4. Applicatie

Twiin Voorwaarden	*Samenwerkingsvoorwaarden*

#	Onderwerp	Omschrijving	Verplicht vanaf ondertekening Deelnemersovereenkomst	Verplicht vanaf validatie	Eventuele afwijking	Toelichting afwijking incl. tijdpad
4.1	Algemeen	Beschikken over een actueel overzicht van de zorgtoepassingen van de Twiin Deelnemers waaraan de Twiin Dienstverlener ondersteuning biedt.	Ja	Ja		
4.2		Ondersteunen van Twiin Deelnemer(s) in de keuze van het GtK, de implementatie van het GtK, het opstellen van testscripts en het overkoepelende release en update management.	Nee	Ja	In te vullen	In te vullen
4.3	Generieke functies en gemeenschappelijke voorzieningen	Ondersteunen van Twiin Deelnemer(s) bij de aansluiting op de gemeenschappelijke voorzieningen en de toepassing van generieke functies.	Nee	Ja	In te vullen	In te vullen
4.4		Regie voeren op het gebruik van de gemeenschappelijke voorzieningen en generieke functies door de Twiin Deelnemer(s) te ondersteunen bij het voldoen aan de afspraken die hierover per zorgtoepassing zijn vastgelegd.	Nee	Ja	In te vullen	In te vullen

9.3 | Voorwaarden GtK Beheer

Het is de verantwoordelijkheid van de Twiin Deelnemer dat de voorwaarden GtK Beheer worden nagekomen. Zodra de Twiin Deelnemer de Deelnemersovereenkomst (see page 84) heeft ondertekend, is de Twiin Deelnemer verplicht om te zorgen dat de voorwaarden GtK Beheer worden nagekomen die in het schema hieronder verplicht zijn gesteld. Vanaf validatie moet de Twiin Deelnemer zorgen dat alle Voorwaarden GtK Beheer worden nagekomen zoals in het schema hieronder weergegeven.

Tot aan validatie gelden de Samenwerkingsvoorwaarden. De Samenwerkingsvoorwaarden volgen de Twiin Voorwaarden, behalve dat op een aantal onderdelen afwijking mogelijk is. In die gevallen beschrijven de Samenwerkingsvoorwaarden deze afwijking. Bij nieuwe versies

van het Twiin Afsprakenstelsel kan de ruimte voor afwijking in een bepaalde Samenwerkingsvoorwaarde vervallen.

1. Wet en regelgeving

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
#	**Onderwerp**	**Omschrijving**	**Verplicht vanaf ondertekening Deelnemersovereenkomst**	**Verplicht vanaf validatie**	**Eventuele afwijking**	**Toelichting afwijking incl. tijdpad**
1.1	Contracten	Afsluiten van een (sub)verwerkersovereenkomst met de partijen die toegang hebben tot persoonsgegevens ter zake van het GtK zoals een leverancier.	Ja	Ja		

1.2		In de (sub)verwerkersovereenkomst worden adequate beveiligingsafspraken gemaakt met de (sub)verwerker. Meer specifiek is de (sub)verwerker in bezit van een geldige NEN 7510-certificering (of ISO27001), inclusief de bijbehorende verklaring van toepasselijkheid en heeft (sub)verwerker een verklaring van een externe auditor overlegd. Bij gebreke hieraan toont de (sub)verwerker op andere wijze aan dat de beveiligingsmaatregelen adequaat zijn conform de eisen zoals opgenomen in NEN 7510.	Ja	Ja		

2. Organisatorisch

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
#	**Onderwerp**	**Omschrijving**	**Verplicht vanaf ondertekening Deelnemersovereenkomst**	**Verplicht vanaf validatie**	**Eventuele afwijking**	**Toelichting afwijking incl. tijdpad**

2.1	Servicedesk	Het (laten) inrichten van een servicedesk voor het uitvoeren van beheer vo or het GtK.	Ja	Ja		
2.2		Aansluiten op de supportorgani satie van Twiin.	Nee	Ja	In te vullen	In te vullen
2.3		Vastleggen van afspraken in een SLA over het melden en afhandelen van incidenten, storingen en aangetroffen kwetsbaarhed en ten aanzien van het GtK en beschikbaarhe id.	Ja	Ja		

2.4		Zo nodig voeren van overleg met derden, waaronder derde-leveranciers, bij incidenten en gebreken. Het overleg zal gericht zijn op het achterhalen van de oorzaak van de fouten en/of gebreken in de diensten en het uitwerken van een oplossing daarvoor, ongeacht of de oorzaak is gelegen in een prestatie aan de zijde van GtK Beheerder of aan de zijde van een derde partij.	Ja	Ja		

3. Informatie

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
#	**Onderwerp**	**Omschrijving**	**Verplicht vanaf ondertekening Deelnemers overeenkomst**	**Verplicht vanaf validatie**	**Eventuele afwijking**	**Toelichting afwijking incl. tijdpad**

3.1	Gegevens	Voert beheer van het GtK zodanig dat deze het gebruik van de informatiestandaard(en) ondersteunt conform het Twiin Afsprakenstelsel.	Nee	Ja	In te vullen	In te vullen
3.2		Voert beheer van het GtK zodanig dat deze het juiste gebruik van metadata ondersteunt conform het Twiin Afsprakenstelsel.	Nee	Ja	In te vullen	In te vullen

4. Applicatie

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
#	**Onderwerp**	**Omschrijving**	**Verplicht vanaf ondertekening Deelnemers overeenkomst**	**Verplicht vanaf validatie**	**Eventuele afwijking**	**Toelichting afwijking incl. tijdpad**
4.1	Adressering	Erop toezien dat de functie voor adressering op de correcte manier gebruikt wordt.	Ja	Ja		

4.2		Gebruikmaken van ZORG-AB voor adressering.	Nee	Ja		Vooralsnog geldt alleen de verplichting om de Twiin Beheerorganisatie de benodigde adresgegevens van de deelnemer en de GtK-diensten aan te leveren. De Twiin Beheerorganisatie publiceert dit vervolgens in ZORG-AB.
4.3	Logging	Beheer van logging faciliteiten voor het GtK. Zie (o.a.) PvE | Logging (see page 209) Log-02	Ja	Ja		
4.4		Deployment van nieuwe releases van het GtK.	Ja	Ja		
4.5		Volgt een uitgewerkt testscript dat doorlopen wordt voor het in productie nemen van nieuwe versies/ releases en upgrades van het GtK.	Nee	Ja	In te vullen	In te vullen

5. Infrastructuur

Twiin Voorwaarden	*Samenwerkingsvoorwaarden*

#	Onderwerp	Omschrijving	Verplicht vanaf ondertekening Deelnemers overeenkomst	Verplicht vanaf validatie	Eventuele afwijking	Toelichting afwijking incl. tijdpad
5.1	Beveiliging	Zorgen voor een beveiligde en stabiele verbinding tussen de zorginformatie systemen van Twiin Deelnemer en het GtK.	Ja	Ja		

9.4 | Voorwaarden GtK

Het GtK moet voldoen aan de voorwaarden die op deze pagina zijn weergegeven. Het GtK wordt op basis van deze voorwaarden getoetst, voordat deze door Twiin gevalideerd is. Het is de verantwoordelijkheid van de Twiin Deelnemer dat de voorwaarden GtK worden nagekomen

#	Onderwerp	Omschrijving
1.1	Releasebeleid	Een GtK dient door middel van het installeren van updates, upgrades en patches aan het Twiin 6.5 | Releasebeleid (see page 97) te voldoen.
1.2	Vertrouwens model	Het GtK ondersteunt het Twiin 5 | Vertrouwensmodel (see page 56) en het gebruik van de generieke functies en gemeenschappelijke voorzieningen zoals omschreven in de implementatiewijzer per zorgtoepassing.

#	Onderwerp	Omschrijving
1.3	Netwerk	Onderstaande invulling van een 'veilig netwerk' (NEN7512:2022) is een tijdelijke afspraak voor de duur van maximaal 1 jaar. De GtK's moeten onderling verbonden worden via een veilig netwerk op basis van publiek internet dat minimaal voldoet aan de volgende eisen (waarbij per Zorgtoepassing aanvullende eisen kunnen worden gesteld): 1. Er zijn maatregelen genomen waarmee met grote zekerheid wordt voorkomen dat communicatie binnen het GtK-netwerk buiten de Europese Economische Ruimte ("EER") kan komen, allereerst doordat de technische infrastructuur van het GtK zich in de EER bevindt. 2. Netwerkverkeer vanuit het GtK richting andere GtK's dient plaats te vinden zonder tussenkomst van andere applicaties en/of componenten van applicaties. Het netwerkverkeer tussen GtK's dient rechtstreeks plaats te vinden, zonder enige tussenkomst van externe applicaties of applicatiecomponenten, zodat een continue en ongehinderde datastroom wordt gewaarborgd. 3. Inlog op het GtK is uitsluitend toegestaan voor partijen waarvan de identiteit is vastgesteld met betrouwbaarheid die overeenkomt met eIDAS betrouwbaarheidsniveau 'hoog'. 4. Die delen van GtK Leverancier die betrokken zijn bij het leveren van een verbinding van het GtK met andere GtK's zijn in het bezit van een geldige NEN 7510 certificering (of ISO 27001). a. Het GtK moet worden beheerd door een GtK Beheerder die in bezit is van een geldige NEN 7510 certificering (of ISO 27001).
1.4	Netwerk	De GtK Leveranciers hebben een beleid m.b.t. reguliere scans van protocolstacks en m.b.t. encryptie conform NEN 7510-1:2024 Deel 1 A.8.8 Beheer van technische kwetsbaarheden en NEN 7510-2:2024 Deel 2 Beheersmaatregelen 8.24 Gebruik van cryptografie). Dit is te zien in de verklaring van toepasselijkheid van het NEN 7510 certificaat.

#	Onderwerp	Voorwaarden
2.1	Beeldbeschikbaarheid	Voor de Zorgtoepassing Beeldbeschikbaarheid dient het GtK te voldoen aan de eisen zoals beschreven in de Implementatiewijzer voor beeldbeschikbaarheid. (see page 414)
2.2	Basisgegevensset Zorg	Voor de Zorgtoepassing Basisgegevensset Zorg dient het GtK te voldoen aan de eisen zoals beschreven in de Implementatiewijzer voor Basisgegevensset Zorg. (see page 294)

10 | Technische kern

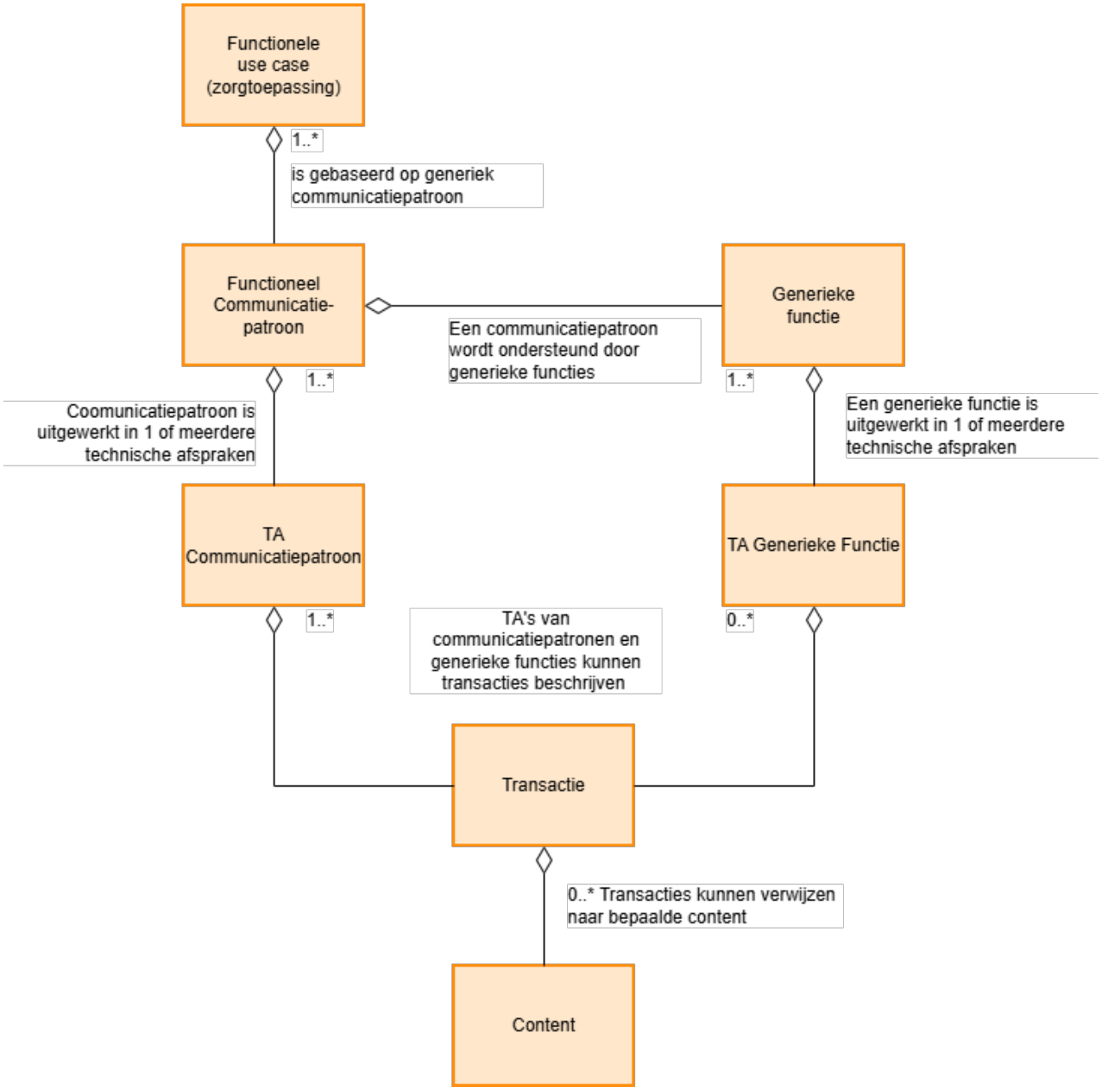
In dit onderdeel staat het generieke, technische en herbruikbare deel beschreven voor databeschikbaarheid. De implementatiewijzers van de zorgtoepassingen van Twiin zijn gebaseerd op deze generieke kern.

> Het metamodel beschrijft de componenten waaruit de technische kern is opgebouwd en welke onderlinge relaties er kunnen zijn. Het metamodel van de technische kern bevat geen afspraken, maar is toegevoegd voor een juiste interpretatie van de technische kern.

Componenten van de technische kern

Component	Korte omschrijving
Communicatiepatroon	Een communicatiepatroon beschrijft hoe gegevens worden uitgewisseld tussen zorgpartijen vanuit organisatorisch-juridisch (technologie-agnostisch) en technisch oogpunt. De functionele use case (een toepassing) zal bepalen welk of welke communicatiepatronen gebruikt moeten worden.
Generieke functie	Een generieke functie is een basisfunctionaliteit die zorgbreed nodig is voor elektronische gegevensuitwisseling en/of in meerdere toepassingen gebruikt wordt.

Component	Korte omschrijving
TA	Een Technical Agreement (TA) beschrijft de technische afspraken die gemaakt moeten worden om een bepaalde uitwisseling te kunnen implementeren. Een functionele use case die waarin een bepaald communicatiepatroon gebruikt zal hiervoor meerdere TA's voor moeten volgen om de gehele uitwisseling te implementeren, waaronder de TA's van de benodigde generieke functies. > Een functionele use case waarin de cliënt vanuit zorgaanbieder A verwezen wordt naar zorgaanbieder B en dat daarvoor een dossier bij de laatste moet belanden kan geïmplementeerd worden met het communicatiepatroon 'gericht beschikbaar stellen' (maar ook met het communicatiepatroon 'verzenden'). Om een implementatie te doen van het het uitwisselingen van het dossier tussen zorgaanbieder A en B via het communicatiepatroon gericht beschikbaar stellen zullen meerdere TA's geïmplementeerd worden, zoals bijvoorbeeld de TA voor authenticatie, de TA voor het verzenden en ontvangen van een notificatie, de TA voor het raadplegen van het dossier en de TA voor het implementeren van een veilig netwerk. Het kan zijn dat er meerdere varianten van een TA worden ontwikkeld. Bijvoorbeeld: een authenticatie kan gedaan worden op basis van SAML2, maar ook met OpenID Connect. Berichtuitwisseling kan Service Oriented (SOAP) of Resource Oriented (RESTfull) plaatsvinden. Deze keuzes leiden tot een verschillende implementatie van technologie. In het Twiin Afsprakenstelsel worden deze keuzes vastgelegd.
TTA	Twiin Technical Agreement (TTA): Het komt voor dat er TA's zijn ontwikkeld maar dat deze nog niet (geheel) aansluiten bij het vertrouwensmodel van Twiin. TTA's zijn technische afspraken die aanvullende afspraken bevat die in lijn liggen met het Twiin Vertrouwensmodel. Ook kan het zijn dat er een TTA is waar er nog helemaal geen (landelijke) invulling is gegeven aan een bepaald aspect van een gegevensuitwisseling en heeft Twiin hier noodzakelijkerwijs zelf keuzes moeten maken. Het is mogelijk dat een TA in verschillende technische alternatieven wordt uitgewerkt, zoals SOAP of FHIR.
Transactie	Transacties beschrijven de berichten benodigd voor de communicatie tussen Gevalideerde Twiin Knooppunten onderling of tussen Gevalideerde Twiin Knooppunten en gemeenschappelijke voorzieningen. Een TA kan meerdere transacties voorschrijven, maar een transactie zou niet in meerdere TA's moeten voorkomen (maar er mag vanuit een TA natuurlijk wel verwezen worden naar andere TA's en transacties.
Content	(Meta)data die nodig is om een transactie te implementeren. Denk bijvoorbeeld aan codelijsten of informatiestandaarden.



- Volume 0a bevat een functioneel overzicht van de communicatiepatronen die gebruikt kunnen worden bij gegevensuitwisseling en, in Volume 0b, de generieke functies die daarbij (mogelijk) nodig zijn. Dit volume is voor een breed publiek (informatiemanagers, architecten) geschreven in het Nederlands. Er zijn vier typen communicatiepatronen die een technische invulling zijn van de twee manieren van gegevens uitwisselen: verzenden en raadpleegbaar maken. In de technische kern worden deze manieren van gegevens uitwisselen op een generieke manier beschreven. Een zorgtoepassing (in het Twiin Afsprakenstelsel) kiest welk communicatiepatroon het best geschikt

is voor de betreffende use case(s). Afhankelijk van het type communicatiepatroon en de gekozen technische uitwerking (in volume 1) gelden andere voorwaarden voor validatie. Een communicatiepatroon beschrijft puur de vorm/volgorde van acties in een gegevensuitwisseling, maar dient ondersteund te worden door zogenaamde generieke functies, zoals identificatie en authenticatie (van zorgverleners, zorgaanbieders en hun informatiesystemen), autorisatie, logging en toestemming.

- Volume 1a bevat de technische uitwerking in Twiin Technical Agreements (de Twiin Technische Afspraken) van de communicatiepatronen tussen de GtK's (Gevalideerde Twiin Knooppunten), Let op dat er voor voor één communicatiepatroon meerdere technische uitwerkingen kunnen bestaan, zoals SOAP[25] of REST[26]. Volume 1b bevat de technische afspraken voor de uitwerking van de generieke functies. Dit volume is bestemd voor ontwerpers en solution architecten voor een internationale doelgroep en daarom geschreven in het Engels. Een technische uitwerking van een communicatiepatroon of generieke functie kan (als dit al voldoende is uitgewerkt) een Programma van Eisen (PvE) bevatten. Deze PvE's zijn (nog) in het Nederlands geschreven.
- Volume 2 bevat de gedetailleerde technische beschrijvingen van de berichten/transacties die in de communicatiepatronen (volume 2a) of generieke functies (volume 2b) worden gebruikt.
- Volume 3 bevat de content, zoals bijvoorbeeld metadata, die overkoepelend geldt voor de zorgtoepassingen.

Eisen

De kern bevat eisen voor de generieke functies. Deze zijn niet per definitie van toepassing bij een zorgtoepassing. Per zorgtoepassing wordt bepaald aan welke eisen moet worden voldaan. Dit zullen generieke en zorgtoepassing specifieke eisen zijn.

Statement

Twiin volgt de ontwikkelen op het vlak van Generieke Functies[27] en NEN-normeringen als onderdeel van de Wegiz. Twiin sluit aan op de keuzes die op landelijk niveau worden gemaakt en neemt deze op in het Twiin Afsprakenstelsel. Daarnaast volgt Twiin EHDS en sluit hierbij aan.

Inhoud

25. https://en.wikipedia.org/wiki/SOAP
26. https://en.wikipedia.org/wiki/REST
27. https://www.datavoorgezondheid.nl/generieke-functies

10.1 | Kern Volume 0a – Communicatiepatroon Overview

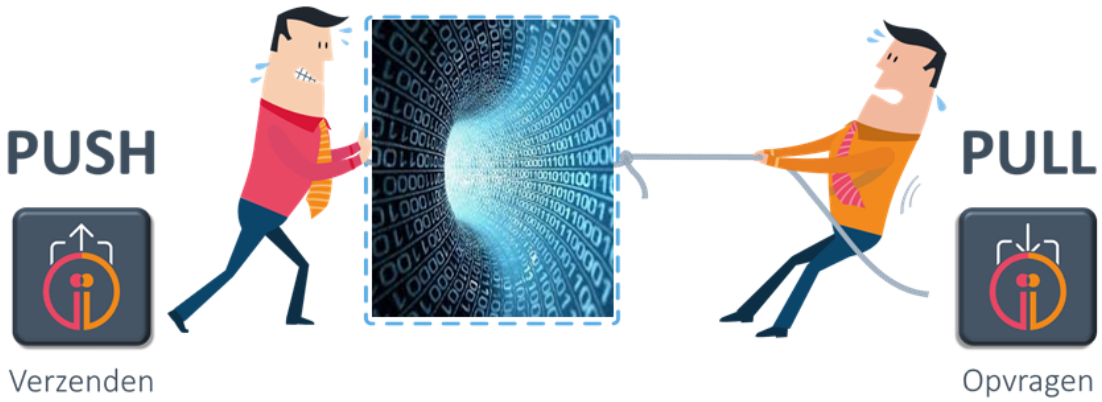
Voor het delen en uitwisselen (beschikbaar stellen) van data heeft Twiin vier communicatiepatronen uitgewerkt (zie ook 4.4 | Logische architectuur (see page 46)). De communicatiepatronen vallen uiteen in twee typen gegevensuitwisselingen. Functioneel ziet dit onderscheid op de initiator van de communicatie. Het gaat hierbij om verzenden en raadplegen. Is de initiator de houder van de gegevens dan wordt gesproken over 'verzenden'. Is de initiator niet de houder van de gegevens dan wordt functioneel gesproken over 'raadplegen'. Dit onderscheid in typen gegevensuitwisselingen is ook een juridisch onderscheid. De wet stelt bijzondere eisen aan een elektronisch uitwisselingssysteem zoals bedoeld in de Wabvpz. Bij het raadpleegbaar maken van gegevens is sprake van een elektronisch uitwisselingssysteem. Dit is verder uitgelegd in het juridische kader (see page 104) onder het kopje Wabvpz.

In dit volume 0 wordt op logisch niveau een overzicht gegeven van de communicatiepatronen tussen de GtK's (Gevalideerde Twiin Knooppunten) en generieke functies. Dit volume is voor een breed publiek (informatiemanagers, architecten) geschreven in het Nederlands.

In de zorgtoepassingen wordt bepaald hoe een functionele use case het beste ingevuld kan worden met één of meerdere communicatiepatronen.

Overzicht communicatiepatronen:

Een communicatiepatroon kan daarnaast verschillende technische uitwerkingen hebben namelijk SOAP (IHE XDS) gebaseerd of RESTful (HL7 FHIR) gebaseerd. In volume 1 worden wordt de technische uitwerking van de communicatiepatronen gedaan en eventuele technische varianten daarin.



10.1.1 | Communicatiepatroon: Pull

1. Use case

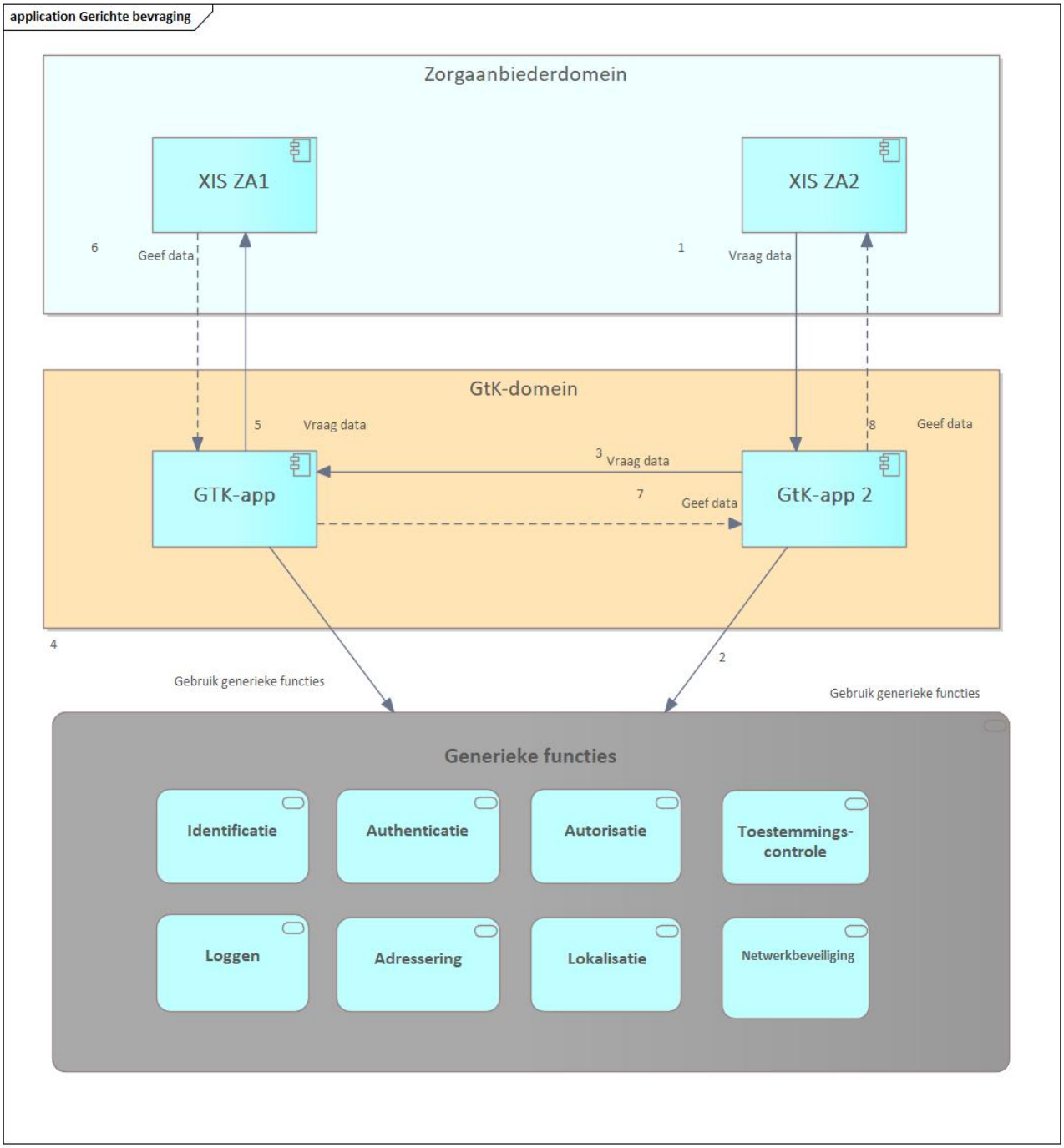
Vanuit Twiin zijn verschillende communicatiepatronen beschreven voor gegevensuitwisseling, hieronder staat een use case beschreven die van het communicatiepatroon Pull gebruik zou kunnen maken.

> Een cliënt onder behandeling bij een specialist geeft aan dat er reeds een specifieke type dataset van hem/haar beschikbaar is bij een andere zorgaanbieder. De zorgverlener wil direct die gegevens ophalen bij die specifieke zorgaanbieder.

De ‘gerichte bevraging’ biedt een oplossing voor de ‘juridische pull’", waarbij gegevens door de raadplegende organisatie bij de beschikbaarstellende organisatie kan worden opgevraagd. Van de raadplegende organisatie wordt verwacht dat alleen gegevens opgevraagd worden die noodzakelijk zijn in de context. Van de beschikbaarstellende organisatie wordt verwacht dat alleen gegevens worden opgeleverd waar expliciete toestemming van de cliënt voor is gegeven.

2. Applicatiediagram

Het applicatiediagram geeft een overzicht van de applicatierollen en de gegevensstroom hiertussen.



In bovenstaand applicatiediagram is globaal beschreven *wat* in de basis de bedoeling is. Verder in de uitwerking van de technische kern worden verschillende technieken beschreven in sequence transactiediagrammen om aan te geven *hoe* er tot een daadwerkelijke uitwisseling van data gekomen kan worden. De beschrijving hieronder is een, maar niet per se dé manier om dit communicatiepatroon in te vullen. Vaak is er een keuze om bepaalde functionaliteit in het GtK te beleggen waar het ook in het XIS kan. Generieke functies zijn in bovenstaand diagram apart gezet –om te benadrukken dat het

gebruik hiervan nodig is- maar de implementatie hiervan zou onderdeel van het XIS, het GtK of een centrale gemeenschappelijke voorziening kunnen zijn.

1. Vanuit een raadplegend XIS wordt aan het raadplegende GtK waarop hij aangesloten is een vraag gesteld. Hoe dit precies gebeurt valt buiten de scope van Twiin om te beschrijven.
2. Het raadplegende GtK gebruikt de gemeenschappelijke voorzieningen om het vervolg te bepalen.
3. Het raadplegende GtK stuurt de vraag door naar het bron-GtK.
4. Het bron GtK controleert de medische autorisatie en de cliënttoestemming bij de gemeenschappelijke voorzieningen.
5. Het bron GtK stuurt de vraag door aan het bron-XIS. Hoe dit precies gebeurt valt buiten de scope van Twiin om te beschrijven.
6. Het bron XIS geeft de gevraagde data terug aan het bron-GtK. Hoe dit precies gebeurt valt buiten de scope van Twiin om te beschrijven.
7. Het bron GtK stuurt het antwoord door aan het raadplegende GtK.
8. Het raadplegende GtK geeft het antwoord terug aan het raadplegende XIS. Hoe dit precies gebeurt valt buiten de scope van Twiin om te beschrijven.

3. Benodigde generieke functies

Voor de geïndexeerde uitwisseling zijn de volgende generieke functies nodig.

- 10.2.1 | Generieke functie - Identificatie en Authenticatie (see page 180)
- 10.2.2 | Generieke functie - Autorisatie (see page 180)
- 10.2.3 | Generieke functie - Toestemming (see page 181)
- 10.2.4 | Generieke functie - Logging (see page 182)
- 10.2.5 | Generieke functie - Adressering (see page 184)
- 10.2.6 | Generieke functie - Lokalisatie (see page 184)
- 10.2.7 | Generieke functie - Netwerkbeveiliging (see page 185)

10.1.2 | Communicatiepatroon: Indexed Pull

1. Use case

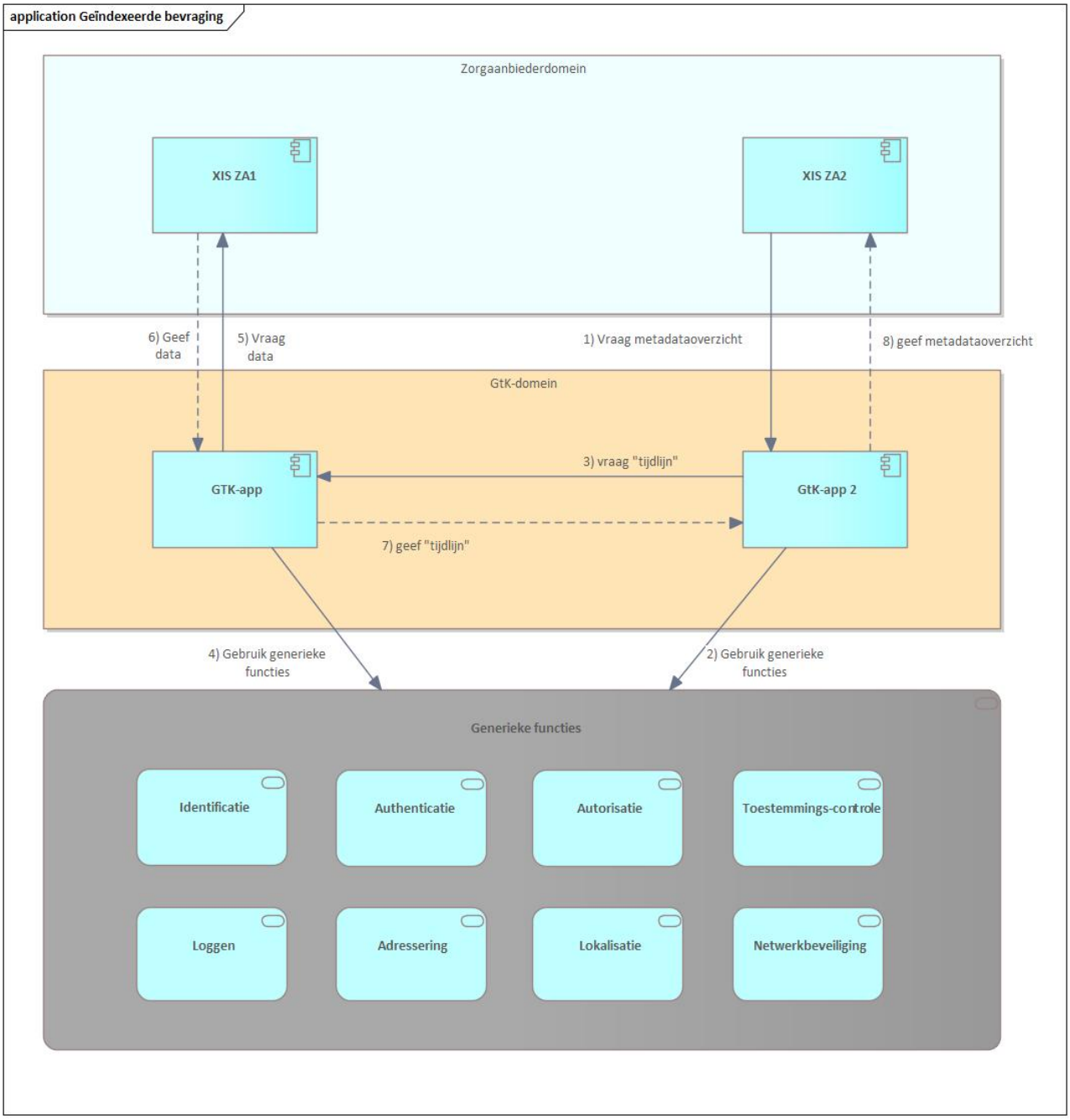
Vanuit Twiin zijn verschillende communicatiepatronen beschreven voor gegevensuitwisseling. Hieronder staat een use case beschreven, waarin van het communicatiepatroon Index Pull gebruik kan worden gemaakt. Dit is een invulling van 'opvragen'.

> Een uroloog in ziekenhuis A wil alle reeds bekende labuitslagen van de patiënt die bij haar onder behandeling is opvragen, om hiermee een zo compleet mogelijk dossier voor de patiënt op te bouwen.

1.1. Applicatiediagram

Het applicatiediagram geeft een overzicht van de applicatierollen en de gegevensstroom hiertussen. Het communicatiepatroon ‘geïndexeerde bevraging’ bevat twee stappen.

De eerste stap is nodig om een overzicht van beschikbare gegevens inzichtelijk te maken aan de zorgverlener, indien gewenst in de vorm van een tijdlijn. Dit overzicht bestaat uit verschillende metadata elementen, waaronder bijvoorbeeld cliëntnaam, cliëntnummer, type gegeven en de vindplaats van de data zelf. Het overzicht met metadata kan samengesteld worden vanuit de informatie uit verschillende zorgsystemen. Delen van het metadata overzicht worden beschikbaar gesteld via één of meerdere GtK’s. Om overvraging te voorkomen wordt gebruik gemaakt van een lokalisatievoorziening. Hieronder wordt deze eerste stap in een diagram weergegeven. Aan de hand van de metadataoverzicht kan de data opgehaald worden bij of via een GtK.



In bovenstaande applicatiediagram is globaal beschreven *wat* in de basis de bedoeling is voor de eerste stap. Verder in dit de uitwerking van de technische kern worden verschillende technieken beschreven in sequence transactiediagrammen om aan te geven *hoe* je tot een daadwerkelijke uitwisseling van data kunt komen. De beschrijving hieronder is een, maar niet per se dé manier om dit communicatiepatroon in te vullen. Vaak is er een keuze om bepaalde functionaliteit in het GtK te beleggen waar het ook in het XIS kan. Generieke functies zijn in bovenstaand diagram apart gezet –om te benadrukken dat het gebruik hiervan nodig is– maar de implementatie hiervan zou onderdeel van het XIS, het GtK of een centrale gemeenschappelijke voorziening kunnen zijn.

1. Vanuit een XIS wordt de vraag “geef metadataoverzicht” aan het GtK gesteld.

2. Het GtK stelt een lokalisatievraag aan een lokalisatievoorziening (bijvoorbeeld Mitz) om te achterhalen bij welke zorginstellingen gegevens van de cliënt bekend zijn. Indien nodig kan het GtK de hier bijbehorende technische adressen van opgehaald worden via ZORG-AB.

3. De vraag “geef metadataoverzicht” wordt doorgezet naar de bevraagde GtK’s.

4. Een bevraagd GtK controleert:

   - de medische autorisatie op basis van wat er voor de betreffende use case is afgesproken en
   - de cliënt toestemming bij de toestemmingsvoorziening.

5. Indien akkoord stuurt het GtK de vraag door naar het bevraagde XIS

6. Het bevraagde XIS stuurt de metadata als antwoord terug naar het GtK.

7. Het bevraagde GtK stuurt deze als antwoord terug naar het vragende GtK.

8. Het vragende GtK stuurt het antwoord op zijn beurt weer terug naar de vragende XIS.

1.2. Benodigde generieke functies

Voor de geïndexeerde uitwisseling zijn de volgende generieke functies nodig.

- 10.2.1 | Generieke functie – Identificatie en Authenticatie (see page 180)
- 10.2.2 | Generieke functie – Autorisatie (see page 180)
- 10.2.3 | Generieke functie – Toestemming (see page 181)
- 10.2.4 | Generieke functie – Logging (see page 182)
- 10.2.5 | Generieke functie – Adressering (see page 184)
- 10.2.6 | Generieke functie – Lokalisatie (see page 184)
- 10.2.7 | Generieke functie – Netwerkbeveiliging (see page 185)

10.1.3 | Communicatiepatroon: Push

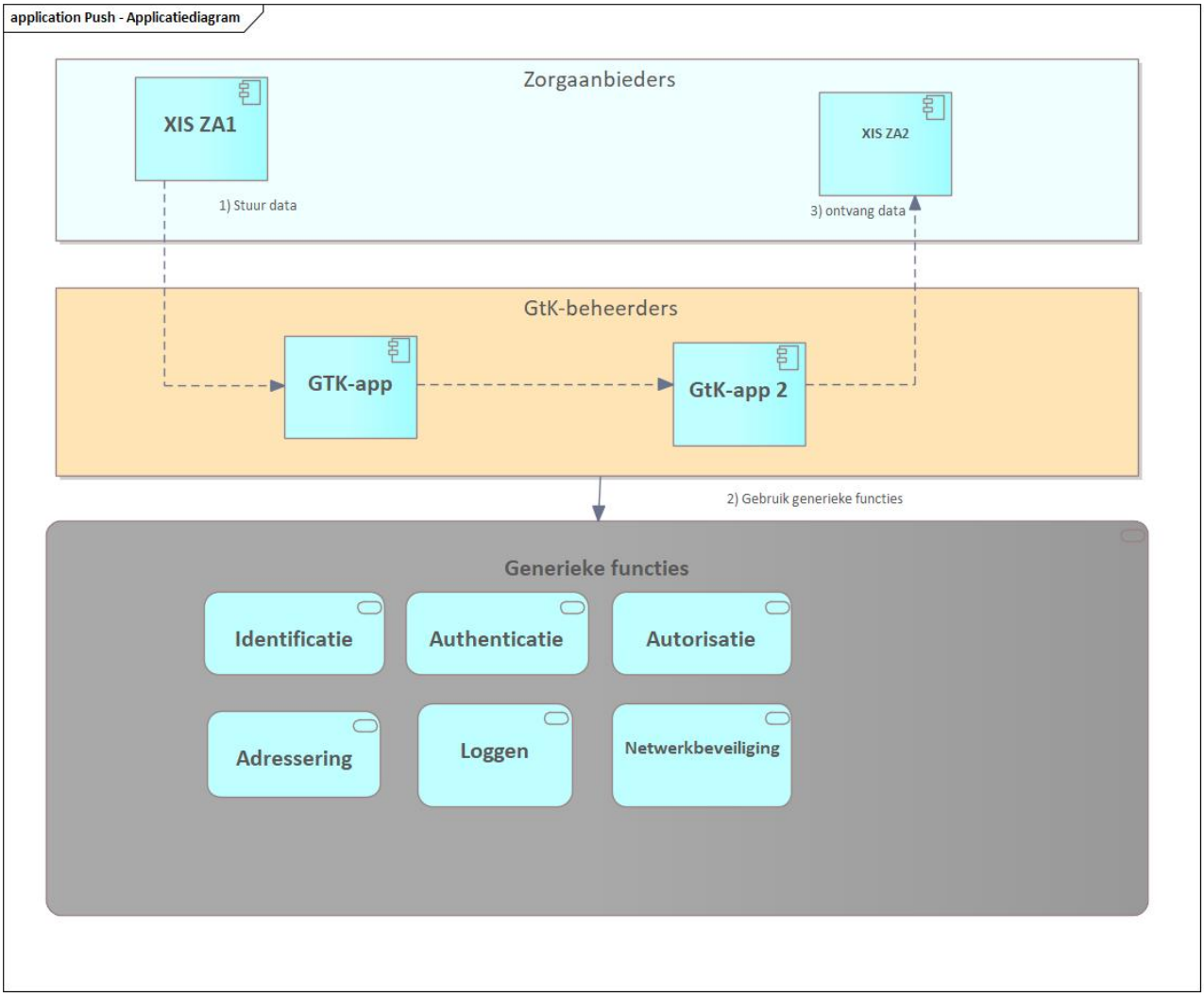
1. Use case

Vanuit Twiin zijn verschillende communicatiepatronen beschreven voor gegevensuitwisseling. Hieronder staat een use case beschreven, waarin van het communicatiepatroon Push gebruik kan worden gemaakt. Dit is een invulling van ‘verzenden’.

> Een zorgverlener besluit de cliënt die op dat moment bij hem/haar op bezoek is door te verwijzen. De zorgverlener stuurt bij de verwijzing direct de gegevens mee die hij/zij acht van belang te zijn bij de voortzetting van de behandeling.

2. Applicatiediagram

Het applicatiediagram geeft een overzicht van de applicatierollen en de gegevensstroom hiertussen.



Het communicatiepatroon Push A beschrijft een push mechanisme waarin direct de gegevens gestuurd worden van zorgverlener A naar zorgverlener B.
Er zijn verschillende generieke functies nodig om een transactie te bewerkstelligen. Deze beschrijving is een, maar niet per se dé manier om dit communicatiepatroon in te vullen. Vaak is er een keuze om bepaalde functionaliteit in het GtK te beleggen waar het ook in het XIS kan. Generieke functies zijn in bovenstaand diagram apart gezet -om te benadrukken dat het gebruik hiervan nodig is- maar de implementatie hiervan zou onderdeel van het XIS, het GtK of een centrale gemeenschappelijke voorziening kunnen zijn.

3. Benodigde generieke functies

Voor de geïndexeerde uitwisseling zijn de volgende generieke functies nodig.

10.1.4 | Communicatiepatroon: Notified Pull

1. Use case

Vanuit Twiin zijn verschillende communicatiepatronen beschreven voor gegevensuitwisseling, hieronder staat een use case beschreven die van het communicatiepatroon Notified Pull gebruik zou kunnen maken.

> Een cliënt is doorverwezen door een zorgverlener voor een onderzoek bij een zorgverlener in een andere zorgaanbieder. Zodra het onderzoek is uitgevoerd, brengt de uitvoerende zorgverlener de aanvragende zorgverlener op de hoogte dat de gegevens op te halen zijn.

Communicatiepatroon Notified Pull biedt een oplossing voor de 'juridische push', waarbij gegevens van de ene organisatie aan de andere worden beschikbaar worden gemaakt. Dit is bijvoorbeeld het geval bij een verwijzing, een second opinion of een overdracht. De Notified Pull-transactie verwacht dat bij de ontvangende organisatie zorgvuldig wordt geselecteerd door de verzendende organisatie. Deze actie bevestigt de geneeskundige behandelingsovereenkomst/behandelrelatie tussen de cliënt en de toekomstige zorgaanbieder/zorgverlener en kan worden gezien als een 'veronderstelde toestemming'. De cliënt is op de hoogte van de nieuwe behandelingsovereenkomst/behandelrelatie en begrijpt daarom dat zijn medische gegevens voor de andere partij beschikbaar gemaakt worden.

De Notified Pull zal een ontvangende organisatie op de hoogte stellen van medische dossiers die klaar zijn om te worden opgehaald. De ontvangende organisatie ontvangt alleen op eigen voorwaarden door te bepalen hoe en wanneer de Pull-operaties worden uitgevoerd die door de verzendende organisatie zijn voorgesteld.

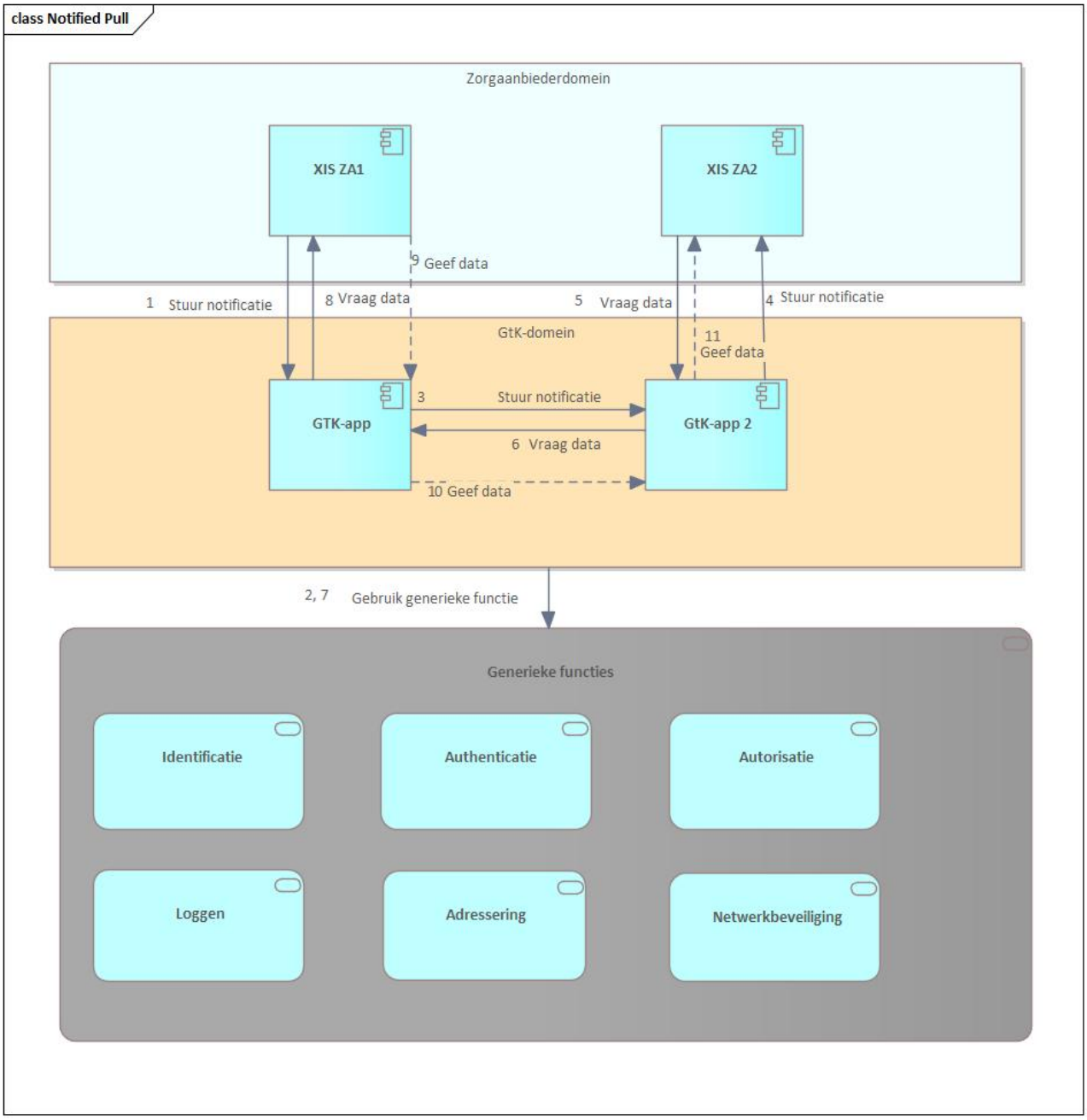
2. Applicatiediagram

Het applicatiediagram geeft een overzicht van de **applicatierollen** en de gegevensstroom hiertussen.

Er zijn twee type organisaties, een verzendende en een ontvangende organisatie. Beide organisaties hebben een GtK, een zendend GtK en een ontvangend GtK.

De applicaties van een zorgaanbieder worden ontsloten via een GtK. De systemen die we daarbij identificeren zijn een bronsysteem en een raadplegend systeem.

Organisatie	GtK	Systeem
Verzendende organisatie	Gtk verzender	Bronsysteem
Ontvangende organisatie	GtK ontvanger	Raadplegend systeem



Het communicatiepatroon Notified Pull beschrijft een push/pull-mechanisme dat start met het sturen van een notificatie van de zorgverlener waar iets opgehaald kan worden, naar de zorgverlener die de dataset uiteindelijk op moet halen.

Benodigde generieke functies

Voor de geïndexeerde uitwisseling zijn de volgende generieke functies nodig.

- 10.2.1 | Generieke functie - Identificatie en Authenticatie (see page 180)
- 10.2.2 | Generieke functie - Autorisatie (see page 180)
- 10.2.4 | Generieke functie - Logging (see page 182)
- 10.2.5 | Generieke functie - Adressering (see page 184)
- 10.2.7 | Generieke functie - Netwerkbeveiliging (see page 185)

10.2 | Kern Volume 0b - Generieke functies

Naast de communicatiepatronen, die op generiek niveau beschrijven welke vormen van gegevensuitwisselingen mogelijk zijn, zijn er ook zogenaamde generieke functies. Dit zijn functionaliteiten die door meerdere typen gegevensuitwisselingen ingevuld moeten worden. Veel van deze generieke functies borgen een stukje vertrouwen in de uitwisselingsketen, zoals identificatie en authenticatie, maar sommige generieke functies zijn ondersteunend zoals bijvoorbeeld het lokaliseren van medische gegevens of een terminologieserver die kan vertalen van en naar verschillende codestelsels (nu niet uitgewerkt binnen Twiin).

Omdat zorgaanbieders en ICT-leveranciers niet voor iedere gegevensuitwisseling een andere implementatie willen hebben van een generieke functie proberen we over de gegevensuitwisselingen heen eenzelfde technische uitwerking van een generieke functie te maken. Dit gebeurt, net als bij de communicatiepatronen, in een zogenaamde Technical Agreement/Technische Afspraak (TA).

Dit onderscheid in een techniek-agnostische functionele beschrijving van een generieke functie en de specifieke technische implementatie zie je weer terug in het onderscheid dat gemaakt is in de verschillende volumes.

Het kan zijn dat voor de implementatie van een generieke functie gekozen is/wordt om dit in een technische implementatie te ondersteunen die door meerdere partijen gebuikt wordt of zelfs moet worden. Dit noemen we dan een gemeenschappelijke voorziening, zie ook de definitie uit de NVS: https://www.datavoorgezondheid.nl/nationale-visie-en-strategie/begrippen .

Vanuit het Ministerie van Volksgezondheid, Welzijn en Sport is er een programma[28] gestart waarin bepaalde generieke functies op landelijk niveau worden ontworpen. Twiin is nauw betrokken bij deze ontwikkelingen en zal aansluiten op de keuzes die op landelijk niveau worden gemaakt.

Overzicht van (in Twiin uitgewerkte) generieke functies:

- 10.2.1 | Generieke functie - Identificatie en Authenticatie (see page 180)

28. https://www.datavoorgezondheid.nl/generieke-functies

10.2.1 | Generieke functie - Identificatie en Authenticatie

Zorgaanbieder

De communicerende zorgaanbieders dienen als identificatie het UZI-register Abonneenummer (URA) te gebruiken. De authenticatie van deze identiteit kan nog niet op een hoog niveau en door de gehele keten plaatsvinden.

Zorgverlener/gebruiker

Zorgverleners dienen geïdentificeerd te worden op basis van een uniek ID. Waar mogelijk is dit het UZI-nummer, maar ook een lokaal-id i.c.m. het URA mag gebruikt worden. De zorgverlener/gebruiker dient lokaal geauthenticeerd te worden op eIDAS-niveau hoog. Door de keten heen kan hier nog geen bewijs van worden meegeven zodat andere partijen de zorgverlener ook met zekerheid kunnen authenticeren. Twiin zal in de toekomst meegaan met de eisen die gesteld gaan worden uit het wetsvoorstel DIAZ[29], de NEN7518 en het DEZI-stelsel[30].

GtK

De GtK's dienen bij het opzetten van de gegevensuitwisseling elkaar te authenticeren op basis van een PKIo-servercertificaat.

10.2.2 | Generieke functie - Autorisatie

De bron van medische gegevens is verplicht om te zorgen dat niet meer gegevens worden geraadpleegd of vrijgegeven dan noodzakelijk. Dit wordt gedaan door afspraken te maken over autorisatie: wie mag wanneer en waar bij?

In een zorgtoepassing moet er een rolgebaseerde autorisatieafspraak gemaakt zijn. Hier zal ieder GtK zich aan moeten houden, maar kan ook betekenen dat de autorisatieregels van de eigen zorgaanbieder(s) worden overruled. Hierdoor kan een gebruiker mogelijk meer of minder rechten hebben doen dan (initieel) intern was afgesproken. Autorisatieafspraken worden momenteel per zorgtoepassing bepaald: er zijn twee scenario's.

1. Er zijn landelijke autorisatieafspraken. Ieder GtK dat deelneemt aan een toepassing dient zich hieraan te houden.
2. Er zijn (nog) geen landelijke autorisatieafspraken. Binnen Twiin maken we een (tijdelijke) afspraak.

In de NEN7520 wordt momenteel gewerkt aan een landelijk kader om te komen tot eenduidige autorisatieafspraken. Twiin zal de lijn uit de NEN7520 volgen indien deze gereed is.

29. https://wetgevingskalender.overheid.nl/Regeling/WGK015084
30. https://www.dezi.nl/

10.2.3 | Generieke functie - Toestemming

Wanneer (een onderdeel van) het medisch dossier door de bron alvast 'klaargezet' wordt voor een later (nog niet bekend) gebruik is er (ook) toestemming van de cliënt vereist, zie 7.1 | Juridisch kader (see page 104) en 5.5 | Vertrouwen: Toestemming (see page 74). De dossierhoudende zorgaanbieder is verantwoordelijk voor de controle op de toestemming. Deze cliënttoestemmingen worden vaak nog geregistreerd in het EPD van de zorgaanbieder en zijn vaak specifiek voor een uitwisselingsysteem. Het registreren hiervan is een administratieve last voor de zorgaanbieder. Daarnaast is het soms voor de cliënt niet duidelijk of overzichtelijk waar en waarvoor toestemming is gegeven. Mede om deze reden is de gemeenschappelijke voorziening Mitz[31] ontwikkeld, waar steeds meer zorgaanbieders op aansluiten.

Mitz biedt de functionaliteit voor het vastleggen van toestemmingen aan de zorgaanbieder en maakt het mogelijk dat deze voor meerdere elektronische uitwisselingssystemen te gebruiken is. Daarnaast biedt Mitz de cliënt de functionaliteit om een overzicht te hebben van de alle zorgaanbieders waar een behandeling heeft plaatsgevonden en om toestemmingen te beheren. De transitie om de registratie van toestemmingen over te hevelen naar Mitz is inmiddels ingezet.

Het Informatieberaad Zorg heeft Mitz in 2022 opgenomen als zogenaamde 'bouwsteen[32] van de basisinfrastructuur' [1] in het informatiestelsel in de zorg. Dit besluit geldt in ieder geval nog tot 2027 en wordt dan geëvalueerd. Dit besluit is ook opgenomen in het integraal zorg akkoord (IZA) [2]. Hieruit volgt dat Twiin voor Mitz een pas-toe-of-leg-uit-principe toepast. Voor de gegevensuitwisselingen die in Twiin worden ondersteund en waarvoor een uitdrukkelijke cliënttoestemming noodzakelijk is, volgt Twiin de hiervoor gemaakte afspraken dat Mitz gebruikt moet gaan worden (totdat er nieuwe landelijke afspraken over toestemming zijn gemaakt).

---

[1] De website van het Informatieberaad heeft het besluit niet meer direct beschikbaar. Het besluit is wel nog terug te vinden via nieuwsberichten en het archief van het Ministerie van VWS.

- https://archief25.sitearchief.nl/archives/sitearchief/20240624100213/https://www.informatieberaadzorg.nl/[33]
- https://www.icthealth.nl/nieuws/informatieberaad-zorg-kiest-voor-mitz-en-nuts
- https://smarthealth.live/2022/05/18/informatieberaad-zorg-kiest-voor-online-toestemmingsvoorziening-mitz/
- https://www.mitz-toestemming.nl/ons-verhaal

[2] "Zorgaanbieders verbinden zich aan de door VWS en in afstemming met het Informatieberaad Zorg vastgestelde oplossingen voor de 6 generieke functies (zoals Mitz en ZORG-AB) en implementeren deze uiterlijk 2025 met hun leveranciers ter ondersteuning van hun zorgprocessen."

31. https://www.mitz-toestemming.nl/
32. https://www.informatieberaadzorg.nl/actueel/nieuws/2022/05/12/informatieberaad-zorg-kiest-voor-mitz-en-nuts
33. https://archief25.sitearchief.nl/archives/sitearchief/20240624100213/https://www.informatieberaadzorg.nl/binaries/informatieberaad-zorg/documenten/vergaderstukken/2022/04/25/5a-oplegnotitie-opvolging-mitz-bouwsteen/5a+Oplegnotitie+Opvolging-Mitz-bouwsteen.pdf

10.2.4 | Generieke functie - Logging

Wat is logging?

De normen NEN 7510 en NEN 7513 definiëren loggen als 'het chronologisch vastleggen van gebeurtenissen' waarbij het resultaat en de bundeling ervan logging vormen. Het doel van het loggen is 'een betrouwbaar overzicht te kunnen leveren van de gebeurtenissen waarbij persoonlijke gezondheidsinformatie is verwerkt'.

Logging is een verplichting voor zorgaanbieders om zich tegenover hun cliënten, collega's, toezichthouders en anderen te verantwoorden over de zorgvuldigheid waarmee zij met de persoonsgegevens omgaan, conform de wetgeving (i.e. AVG, WABVPZ).

Logtypes

Logging kent verschillende vormen van logs met verschillende kenmerken voor specifieke doeleinden. Hieronder worden de verschillende logtypes beschreven: toegangslog, systeemlog en beheerlog.

Toegangslog

Een toegangslog wordt gebruikt om interacties van actoren/gebruikers met het systeem op te slaan (te loggen) die door het systeem worden ontvangen en verwerkt, evenals interacties van actoren die door het systeem worden gegenereerd en verzonden. Elke toegang of poging tot toegang, op elk moment, in elke situatie, tot gegevens opgeslagen in het Informatiesysteem wordt vastgelegd in de toegangslog, daarbij tevens de toegang tot de toegangslog zelf.

Actoren/gebruikers kunnen zijn personen, zorgverleners, zorgaanbieders, beheerders/ondersteuners, uitwisselsystemen of andere systemen die toegang tot het systeem hebben. Wanneer er sprake is van het ontvangen en/of verzenden van interacties van actoren door een systeem, bevat de toegangslog een logging van deze interacties. Interacties zijn gebeurtenissen waarbij acties plaatsvinden die betrekking hebben op inloggen, inzien van gegevens, wijzigen van gegevens en uitloggen. Deze interacties kunnen over meerdere domeinen plaatsvinden. De loggegeven in de toegangslog zij herleidbaar tot de actoren en de daarbij behorende gegevens en bevat datum, tijd, rol en naam gebruiker verantwoordelijk voor de toegang, dossierdeel, resultaat, rol en naam gebruiker, autorisatieprotocol, toestemmingsprofiel en noodknopprocedure (ja/nee).

Afhankelijk van de gebeurtenistypen, kan in de toegangslog onderscheid gemaakt worden tussen operationele gebeurtenissen (voor cliënten), gebeurtenissen die de toegangsregeling betreffen en gebeurtenissen die het loggen beïnvloeden. Verdere beschrijving van het datamodel kan worden gevonden in de NEN 7513.

Met de toegangslog kunnen incidenten gesignaleerd en gelokaliseerd worden.

Systeemlog

Een systeemlog is het traditionele logboek van gebeurtenissen en interne verwerkingsdetails van één systeem of applicatie. De systeemlog wordt gebruikt door beheerders en leveranciers voor het oplossen van gelogde fouten en ter voorkoming van toekomstige fouten.

- Systeem logt:

- fouten of
- statuswijzigingen

Beheerlog

In de beheerlog worden alle acties opgenomen die door een specifieke systeembeheerder (actor) worden uitgevoerd met betrekking tot beheer van het systeem. Het beheerlog geeft onder andere de gebeurtenissen aan die de toegangsregeling betreffen, zoals gebeurtenissen met betrekking tot structuurwijzigingen, granulariteit classificaties en rollen in het zorg informatiedomein en de algehele toegangsregeling aangaande applicaties, gegevens bevoegdheden en autorisatie protocollen.

Te loggen gebeurtenissen

De NEN 7513 bepaalt welke gegevens in de logging aanwezig moeten zijn, welke gebeurtenissen moeten worden gelogd, welke gegevens van die gebeurtenissen moeten worden vastgelegd en aan welke kwaliteitseisen het loggen en de logbestanden moeten voldoen. Ook bepaalt de norm hoe lang de logbestanden moeten worden bewaard. Verder biedt de norm houvast aan zorgaanbieders en andere beheerders van persoonlijke gezondheidsinformatie over het verstrekken van informatie over wie toegang heeft gehad tot haar of zijn elektronisch cliëntdossier.

Voor een betrouwbare logging moeten niet alleen operationele gebeurtenissen worden gelogd, maar ook gebeurtenissen die de toegangsregeling betreffen, zoals structuurinstellingen, toegangsregeling en het instellen van toestemmingsprofielen, en die het loggen en logging kunnen beïnvloeden.

De gebeurtenissen zijn in dit geval operationele gebeurtenissen waarbij acties of interacties plaatsvinden tussen systemen/stelsels die betrekking hebben op een cliënt (dossier). Gegevens worden vastgelegd, ingezien of anderszins verwerkt. Hiertoe behoren:

- zoekacties en gegevens ophalen
- gegevens aanmaken en/of muteren
- starten en/of stoppen van diensten
- notificeren
- foutafhandelingen

In de Twiin toolkit[34] staat een handreiking voor (dienstverleners en beheerders van) zorgaanbieders die te maken hebben met loggen en rapporteren.

In de NEN 7513:2024[35] is er een nieuwe tabel opgesteld die expliciet geldt voor de gebeurtenis gegevensuitwisseling. Om zorgaanbieders en softwareleveranciers te ondersteunen bij het toepassen van logging in de zorg, is de nieuwe Nederlandse Praktijkrichtlijn NPR 7523[36] gepubliceerd. Deze richtlijn biedt praktische handvatten en heldere use cases voor het implementeren van NEN 7513:2024

Ketenbrede traceerbaarheid

34. https://www.twiin.nl/downloads
35. https://www.nen.nl/nen-7513-2024-nl-329182
36. https://www.nen-egiz.nl/nieuwe-praktijkrichtlijn-npr-7523-gepubliceerd-concrete-hulp-bij-implementatie-loggingnorm-nen-7513/

- Logging is niet alleen relevant binnen individuele systemen, maar ook voor interacties tussen systemen in een keten van zorginformatiesystemen.
- In de NEN 7513:2024 zijn hiervoor ook nieuw te loggen elementen opgenomen die de ketenbrede traceerbaarheid bij gegevensuitwisseling kunnen te waarborgen.
- Twiin kiest voor het W3C Trace Context[37]-concept: dit internationale concept biedt een manier om een trace-id en span-id door te geven, zodat gebeurtenissen in meerdere systemen consistent gekoppeld kunnen worden.
- Toepassing van dit principe bevordert interoperabiliteit en consistentie, zonder dat Twiin een verplicht uitwisselingsformaat voorschrijft.

10.2.5 | Generieke functie - Adressering

GtK's dienen elkaars elektronische diensten te kunnen vinden. Hiervoor publiceert de Twiin Beheerorganisatie de elektronische adressen (en alle aanvullende gegevens die nodig zijn om te kunnen adresseren) van alle GtK-diensten in ZORG-AB, waardoor deze voor alle partijen vindbaar worden. ZORG-AB is een kandidaatbouwsteen in het duurzaam informatiestelsel van de Zorg. De Twiin Beheerorganisatie van Twiin zal de elektronische adressen van deelnemers in ZORG-AB opnemen; dit hoeft een deelnemer/GtK dus niet zelf te doen.

Het zoeken/vinden van elektronische adressen hoeft niet verplicht via ZORG-AB te gebeuren. Als een domein hier een andere oplossing voor bedenkt mag dat ook (bijvoorbeeld onderlinge afspraken tussen GtK's). Hiermee worden deelnemers niet verplicht om functionaliteit voor de ZORG-AB-interfaces in te bouwen.

De technische beschrijving van het gebruik van ZORG-AB door een GtK staat beschreven in 10.6.5 | Addressing - ZORG-AB Transacties (see page 288).

10.2.6 | Generieke functie - Lokalisatie

Als uitwisseling plaatsvindt via een elektronisch uitwisselingssysteem zoals bedoeld in de Wabvpz, is het ook nodig om een functie in te richten voor lokalisatie. Dit kan via een gemeenschappelijke voorziening of door het vragen aan de cliënt

Raadplegende zorgaanbieders mogen gegevens alleen opvragen bij andere zorgaanbieders waar de cliënt daadwerkelijk bekend is. Bijvoorbeeld: een brede uitvraag bij meerdere zorgaanbieder met de vraag of zij de cliënt toevallig kennen en gegevens beschikbaar hebben, is niet toegestaan. Hiermee wordt namelijk het feit dat cliënt bij de raadplegende partij onder behandeling staat gedeeld met zorgaanbieders die de cliënt mogelijk niet eens kennen. Het hebben van een behandelingsovereenkomst valt namelijk ook het beroepsgeheim en mag niet zonder meer gedeeld worden.

De toestemmingsvoorziening Mitz - waar nodig verplicht door Twiin - biedt een rudimentaire vorm van lokalisatie. Mitz biedt een dienst waarmee een zorgaanbieder kan vragen bij welke andere zorgaanbieders (potentiëel) gegevens van een bepaalde cliënt voor raadpleging (door de betreffende zorgaanbieder) beschikbaar zijn. Dit is de zogenaamde 'waar-vraag'. Vaak is het ook nog nodig of noodzakelijk om ook te weten welke type(n) gegevens dan beschikbaar zijn, de zogenaamde 'welke-vraag'. Deze functie biedt Mitz niet.

37. https://www.w3.org/TR/trace-context-1/

Tot op welk detailniveau de welke-vraag beantwoordt moet worden kan ook per toepassing verschillen. Deze zal daarom, indien van toepassing, per type gegevensuitwisseling in Twiin beschreven worden.

10.2.7 | Generieke functie - Netwerkbeveiliging

"Hoe groter een risico, des te groter de beveiliging, zo leert onder andere de AVG. Dit geld ook voor het versleutelen bij gegevensuitwisseling" (NEN7512:2022). Volgens de norm dient er in het kader van vertrouwelijkheid een gelaagde beveiliging ('defence in depth') toegepast te worden op de gegevensuitwisseling. Hierbij onderkent de norm de volgende beveiligingslagen:

- versleuteld bericht
- versleuteld kanaal
- veilig netwerk

Afhankelijk van het risiconiveau van de gegevensuitwisseling dienen één tot drie van deze maatregelen te worden toegepast. Twiin kiest voor de toepassing van een versleuteld kanaal en een veilig netwerk (see page 211).

10.3 | Kern Volume 1a - Technical Agreements - CP

The goal of this volume is to describe the Twiin generic, reuseable exchange patterns (Dutch: Twiin communicatiepatronen) in the format of Technical Agreements.

General remarks on the transaction schemas:

- The transaction schemas are intended for the availability of all forms of data. The term 'dataset' refers to:
  - zib-based datasets, such as BgZ
  - Individual healthcare information building blocks
  - Other datasets
  - Documents (e.g., PDFs for correspondence)
- Transaction specifications based on:
  - Documents: IHE XDS/XCA, HL7 FHIR
  - Resources: Based on HL7 FHIR

10.3.1 | TTA FHIR - Notified pull

This Twiin Technical Agreement (TTA) describes and specifies the technical responsibilities to which parties agree when connecting to exchange transactions to facilitate the Notified Pull. This TTA is based on the TA Notified Pull[38], with the normative specifications remaining unchanged. The informative specifications, however, have been described using a specific implementation.

The possibility to exchange a client's medical record is for example required in case of a patient referral or transfer. When different healthcare organizations are involved in a client's treatment plan, attention should be paid to the required legal permission and the possible 'burden' for the receiving system when a medical record is transferred.

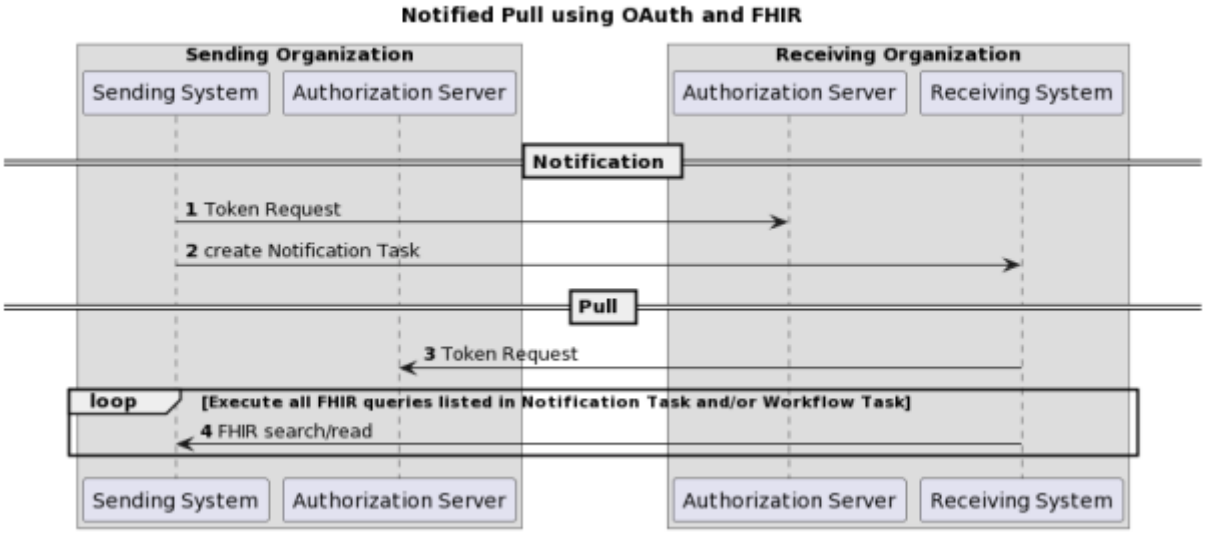
Relation to other documents

This document is written with the following documents as references:

- Nictiz – Informatiestandaard BgZ MSZ
- TA Notified Pull v1.x.x (latest version)[39]

Format

The format of this section follows the main interactions as presented below in the simplified sequence diagram of the Notified Pull sequence.



Interaction numbers 1 and 3 are described in the 10.4.2 | TTA FHIR – Authorization (see page 206). Interaction number 2 is described in10.3.1.1 Notified Pull – Data interactions (see page 190). A part of interaction number 4 is also described in 10.3.1.1 Notified Pull – Data interactions (see page 190). For specifics of the context of the Notified Pull, see Nictiz information standards.

The sequence diagram below provides a complete overview that covers both the resource interactions and the authorization interactions of the complete Notified Pull interaction sequence.

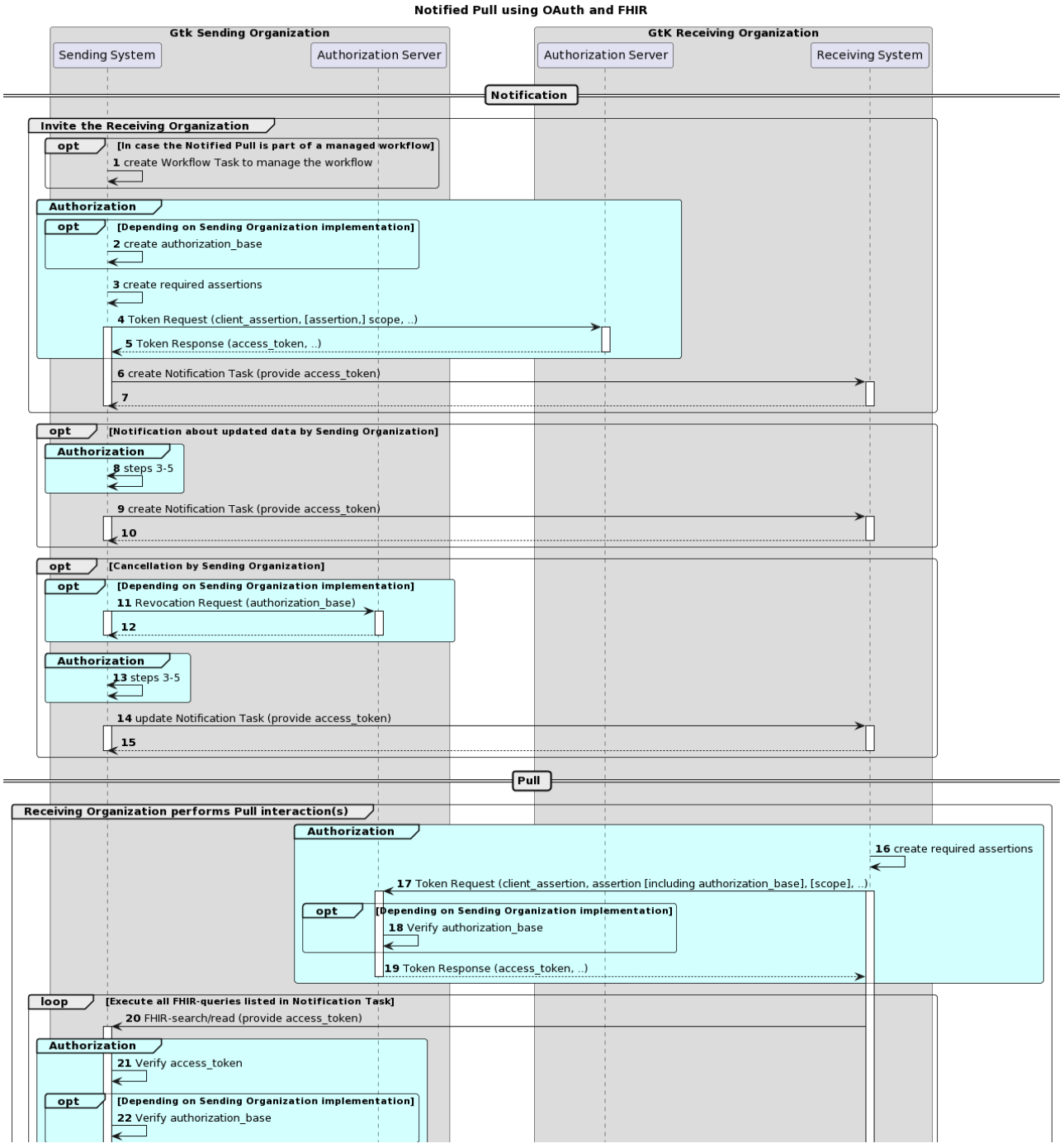
The Twiin specific solutions for identification and addressing can be found in 10.4.2 | TTA FHIR – Authorization (see page 206) and 10.4.5 | TTA – Addressing (see page 210) respectively.

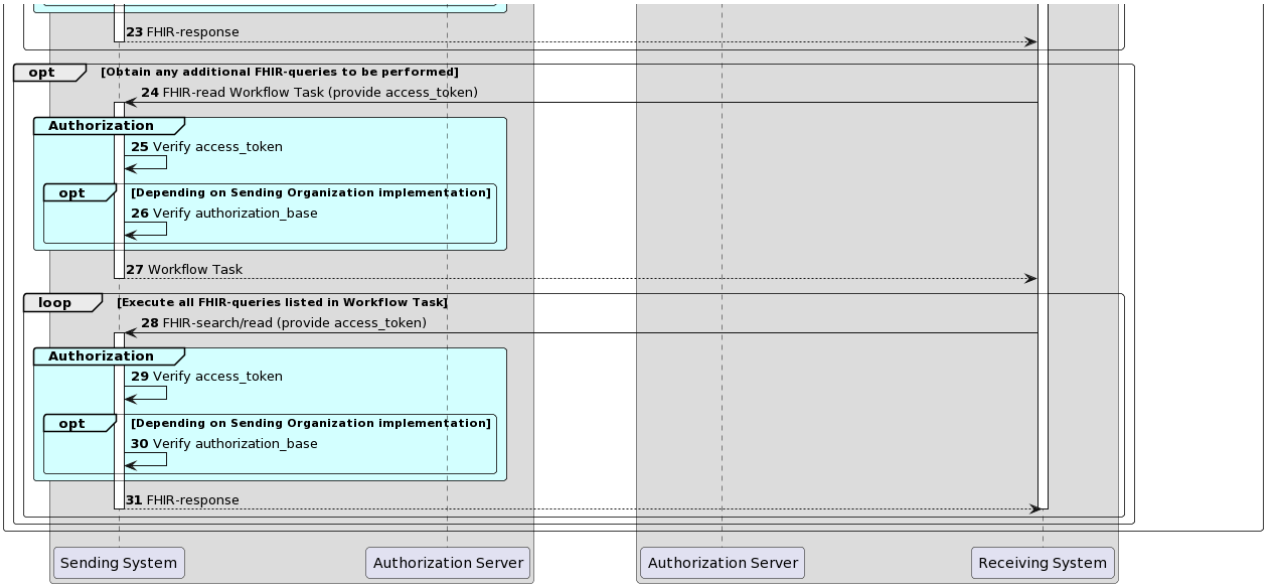
38. https://www.twiin.nl/tanp
39. https://www.twiin.nl/tanp

Sequence diagram

The sequence diagram below visualizes the full flow for the Notified Pull interaction sequence, including both interactions in the data layer using HL7 FHIR (described in 10.3.1.1 Notified Pull – Data interactions (see page 190)) and in authorization layer using OAuth 2.0 (marked cyan, described in 10.4.7 | Network level security (see page 211)).

Each section consists of several steps. The steps correspond to the numbers in the sequence diagram.





Section	Step	Description
Invite the Receiving Organization	1	If the Notified Pull is part of a managed workflow involving both the Sending Organization and the Receiving Organization, and this workflow specifies the creation of a FHIR Task ('workflow task') at the Sending System, then the flow starts with the creation of this task on the Sending System.
	2	The Sending System creates an authorization base, which is used later to communicate a presumed consent for the exchange of patient information. The Receiving System must treat the authorization base as an opaque element. The Receiving System should not depend on any information contained in the authorization base.
	3	The Sending System creates one or two assertions, which can be used to request an access token in the next step.
	4–5	The Sending System requests an access token which can be used in step 6. The Receiving System processes the token request and returns a token response containing, among other elements, an access token. The Sending System must treat the access token as opaque. The Sending System should not depend on any information contained in the access token.

	6–7	By invoking a create interaction regarding a FHIR Task ('notification task') on the Receiving System, the Sending System invites the Receiving System to perform one or more Pull interactions. The Receiving System processes the invitation and sends a technical response to complete the create interaction.
Notification about updated data by Sending Organization	8	The Sending System repeats steps 3–5.
	9–10	The Sending System updates the notification task on the Receiving System using the create interaction. The Receiving System returns a technical response message.
Cancellation by Sending Organization	11–12	The 'cancellation by Sending Organization' option provides a means for the Sending System to cancel/revoke an erroneously created notification. Depending on the implementation at the Sending Organization, the Sending System might have to start the cancellation by revoking the authorization base created in step 2, by sending a revocation request to the Sending Organization's authorization server. The authorization server processes the request and returns a response.
	13	The Sending System repeats steps 3–5.
	14–15	The Sending Organization informs the Receiving Organization by updating the Notification Task on the Receiving System (Task.status is set to "cancelled"). The Receiving System returns a technical response message.
Receiving Organization performs Pull interaction(s)	16	The Receiving System creates one or two assertions, which can be used to request an access token in the next step.
	17–19	The Receiving System requests an access token which can be used to perform the intended Pull interactions. The Sending Organization's authorization server processes the token request and returns a token response containing (among others) an access token. Depending on the Sending System implementation, the Sending System can choose to verify the consent before issuing an access token (preferred option). The Receiving System must treat the access token as an opaque element. The Receiving System should not depend on any information contained in the access token.
	20–23	The Receiving System initiates the intended interactions and processes the responses. The Sending System verifies the access token and can additionally decide to verify the authorization base at this point in the flow.

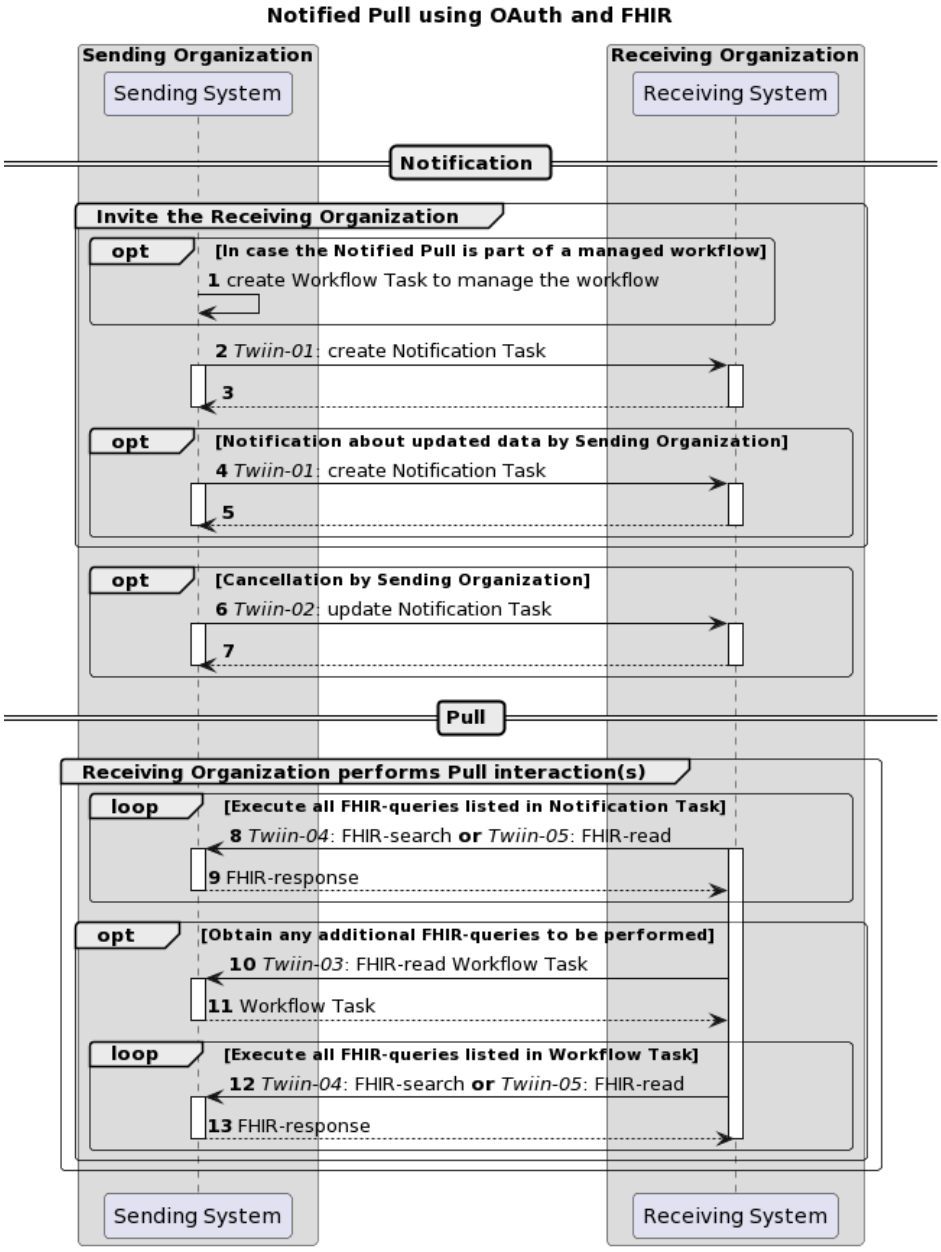
24–27	In case the notification task indicates that a workflow task is available that contains (additional) Pull interactions to be performed, the Receiving System obtains this workflow task from the Sending System.
28–31	The Receiving System initiates the (additional) Pull interactions listed in the workflow task, and processes the responses.

10.3.1.1 Notified Pull - Data interactions

This chapter describes all relevant interactions for the Notified Pull interaction sequence on data level.

Notified Pull interaction sequence

All relevant interactions for the Notified Pull interaction sequence on data level are displayed in the sequence diagram below.



Description of the interactions in this sequence diagram:

Steps	Description

1	If the Notified Pull is part of a managed workflow involving both the Sending Organization and the Receiving Organization, and this workflow specifies the creation of a FHIR 'workflow task' at the sending system, then the flow starts with a creation of this task on the sending system. See Notification Task vs Workflow Task for additional details.
2-3	The sending system invites the receiving system to perform one or more Pull interactions (FHIR requests) by sending a FHIR task resource ('notification task') to the receiving system using a FHIR create interaction. The receiving system processes the invitation and sends a technical response to complete the create interaction. See 10.5.1 | Twiin-01 | Send Notification Task (see page 217) for a detailed description.
4-5	When the data set for which a notification message has been sent is updated in the sending system, the sending system must inform the receiving system about this update by sending a new notification message. The receiving system processes the invitation and sends a technical response to complete the create interaction. See 10.5.1 | Twiin-01 | Send Notification Task (see page 217) for a detailed description.
6-7	The 'cancellation by Sending Organization' option provides a means for the sending system to cancel or revoke an erroneously created notification. The sending system communicates the cancellation to the receiving system by sending an updated notification task to the receiving system using a FHIR conditional update interaction. The receiving system processes the interaction and sends a technical response to complete the conditional update interaction. See 10.5.2 | Twiin-02 | Cancel Notification Task (see page 225) for a detailed description.
8-9	The receiving system extracts the intended FHIR requests from the notification task listed in Task.input:read-available-resource and Task.input:query-available-resources. Subsequently, the receiving system initiates these FHIR requests and processes the responses. See 10.5.5 | Twiin-05 | Retrieve Resource (see page 232) for a detailed description for the retrieval of resources referenced in Task.input:read-available-resources. See 10.5.4 | Twiin-04 | Search Resource(s) (see page 230) for a detailed description for the retrieval of resources referenced in Task.input:query-available-resources.
10-11	In case that the notification task contains an indication that there is a workflow task at the sending system that contains additional FHIR requests (i.e. when Task.input:get-worflow-task.valueBoolean is true), the receiving system requests the workflow task at the sending system. See 10.5.3 | Twiin-03 | Get Workflow Task (see page 228)
12-13	The receiving system extracts the intended FHIR requests from the workflow task. Subsequently, the receiving system initiates these FHIR requests and processes the responses. See 10.5.5 | Twiin-05 | Retrieve Resource (see page 232) for a detailed description for the retrieval of resources referenced in Task.input:read-available-resources. See 10.5.4 | Twiin-04 | Search Resource(s) (see page 230) for a detailed description for the retrieval of resources referenced in Task.input:query-available-resources.

Notification task vs workflow task

The FHIR task resource used in the notification payload is not meant to track the status of a workflow or healthcare process that initiated the data exchange. When the data that is exchanged using the Notified Pull pattern serves for instance a patient referral or transfer, the status of that process should be tracked using a separate FHIR task resource that is maintained and hosted by the initiator of that process, i.e. the sending system. To keep a clear distinction between these two task resources, the task resource used as notification payload is referred to as the 'notification task', while the task resource that is used to track a healthcare process or workflow is referred to as a 'workflow task'. The notification task is sent from the sending system to the receiving system using a Push interaction (HTTP POST or PUT), while the workflow task is hosted at the sending system, and can be requested by the receiving system using a Pull interaction.

The use of a notification task as notification payload does not require the presence of a workflow task, but when a Notification task is sent in the context of a workflow that is maintained by the initiator of that workflow using a workflow task, the notification task MUST contain a reference to that workflow task.

Availability of BSN

For correct handling the BSN should be available as soon as possible, when this is legally required. The sending system has two possibilities:

- The BSN is sent in the authorization assertion (see page 206) used in the access token request before sending the notification task.
- The BSN is made available through the workflow task resource which is referenced in the basedOn attribute of the notification task resource. The workflow task resource must have a for reference with the identifier filled with the BSN.

The receiving system must support both. Since both variants are possible for the sending system to use, both must be supported by the receiving system, to be able to process from any sending system.

10.3.1 | TTA FHIR – Notified pull (see page 185)

10.4.7 | Network level security (see page 211)

PvE | Notified Pull

BgZ-2a-TANP-01	Aanbieden notificatie-endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-ontvanger** dient een notificatie-endpoint aan te bieden aan de GtK-verzender. Een endpoint kan worden gedeeld door meerdere Twiin Deelnemers (bijv. een endpoint per GtK/ SaaS-dienst) of er kan sprake zijn van een endpoint per Twiin Deelnemer.
Prescription Level/Type	Verplicht

BgZ-2a-TANP-01	Aanbieden notificatie-endpoint
Toetsing	Validatie
Transactie/verwijzing	Zie o.a. Z1.2.1 | TTA Exchanging BgZ - FHIR Notified Pull (see page 302)

BgZ-2a-TANP-02	Aanbieden resource-endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** dient een resource-endpoint aan te bieden aan GtK-ontvanger. Een endpoint kan worden gedeeld door meerdere Twiin Deelnemers (bijv. een endpoint per GtK/ SaaS-dienst) of er kan sprake zijn van een endpoint per Twiin Deelnemer.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie o.a. Z1.2.1 | TTA Exchanging BgZ - FHIR Notified Pull (see page 302)

BgZ-2a-TANP-03	Aanbieden token-endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** en de **GtK-ontvanger** dienen een token-endpoint aan elkaar aan te bieden. Een endpoint kan worden gedeeld door meerdere Twiin Deelnemers (bijv. een endpoint per GtK/ SaaS-dienst) of er kan sprake zijn van een endpoint per Twiin Deelnemer.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie o.a. Z1.2.1 | TTA Exchanging BgZ - FHIR Notified Pull (see page 302)

BgZ-2a-AA-06	Aanmaken authorization_base
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** is in staat een digitale representatie van de in de context van een verwijzing veronderstelde toestemming aan te maken (`authorization_base`). Omdat de `authorization_base` alleen door GtK-verzender wordt verwerkt, worden de vorm en inhoud ervan bepaald door GtK-verzender. GtK-ontvanger mag niet afhankelijk zijn van het formaat of de inhoud van `authorization_base` . De vorm en inhoud van de `authorization_base` is (nog) niet gebonden aan normatieve eisen. Het bepalen van vorm en inhoud doet GtK-verzender bij voorkeur in afstemming met de gebruikte infrastructuur.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie (TA141) Z1.2.1.2 | BgZ: Authentication & Authorization#Authorization-base

BgZ-2a-AA-07 / BgZ-2a-AA-12	Aanmaken autorization_grant
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** en **GtK-ontvanger** zijn in staat een `authorization_grant` aan te maken die voldoet aan de specificaties
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Specificaties: (TA141) 10.4.2 | TTA FHIR - Authorization#id-10.2.5|TTAFHIR-Authentication&Authorization-Authorization-grant

BgZ-2a-AA-08	Aanmaken access token request voor notification-endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** is in staat conform de specificaties een access token request voor toegang tot het notificatie-endpoint aan te maken en aan GtK-ontvanger te versturen.
Prescription Level/Type	Verplicht

BgZ-2a-AA-08	Aanmaken access token request voor notification-endpoint
Toetsing	Validatie
Transactie/verwijzing	Specificaties: (TA141) Z1.2.1.2 | BgZ: Authentication & Authorization#Access-token-request Twiin-07 | Token Request (see page 270)

BgZ-2a-AA-09	Gelijke waardes in authentication_grant en access token request
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** en **GtK-ontvanger** dienen ervoor te zorgen dat het veld `sub` in de `authentication_grant` en het veld `client_id` in het access token request dezelfde waarde bevatten.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Specificaties: (TA141) Z1.2.1.2 | BgZ: Authentication & Authorization#Access-token-request Twiin-07 | Token Request (see page 270)

BgZ-2a-AA-10	Afhandelen access token request voor notification server endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-ontvanger** is in staat conform de specificaties een access token request van GtK-verzender voor toegang tot het notificatie server endpoint af te handelen
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Specificaties: (TA141) Z1.2.1.2 | BgZ: Authentication & Authorization#Access-token-request Twiin-07 | Token Request (see page 270)

BgZ-1-authz-03	Controleren autorization_base
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** dient te controleren of de grondslag (`authorization_base`) waarmee de GtK-ontvanger een verzoek doet daadwerkelijk is uitgegeven (aan de GtK-ontvanger). Wanneer de grondslag niet meekomt in de uitwisseling, is er geen sprake van het notified pull communicatiepatroon en dient de GtK-ontvanger op basis van de in de autorisatierichtlijn beschreven rollen het verzoek te autoriseren.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Autorisatiematrix: (TA141) Z1.4.4 | BgZ: Autorisatie#autorisatiematrix-BgZ (see page 375) Transacties: 10.5.4 | Twiin-04 | Search Resource(s) (see page 230) , 10.5.5 | Twiin-05 | Retrieve Resource (see page 232) Autorisatierichtlijn: https://www.aorta-lsp.nl/over-aorta-lsp/autorisatierichtlijnen/autorisatierichtlijn-basisgegevensset-zorg-bgz

BgZ-2b-trans-01	Aanmaken Workflow-Taks
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** is in staat een Workflow-Task aan te maken indien verzender geen Workflow-Task stuurt als payload van de Notification-Task.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 1 van Z1.2.1.1 | BgZ - data interactions (see page 306)

BgZ-2b-trans-02	Versturen notificatie-create-request
Omschrijving/Toelichting/ Uitleg/Implicaties	**GtK-verzender** is in staat een notificatie-create-request te versturen.
Prescription Level/Type	Verplicht
Toetsing	Validatie

BgZ-2b-trans-02	Versturen notificatie-create-request
Transactie/verwijzing	Transactie 2 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: (TA141) 10.5.1 | Twiin-01 | Send Notification Task#id-10.3.1| Twiin-01|SendNotificationTask-Request-message

BgZ-2b-trans-03	Afhandelen notificatie-create-request
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-ontvanger** is in staat een binnenkomend notificatie-create-request af te handelen en een passende response te versturen
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 3 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: (TA141) 10.5.1 | Twiin-01 | Send Notification Task#id-10.3.1| Twiin-01|SendNotificationTask-Response-message

BgZ-2b-trans-04	Versturen notificatie-create-request bij updates
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** is in staat een notificatie-create-request te versturen wanneer de dataset van de verwijzing is geüpdatet
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 4 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie:(TA141) 10.5.1 | Twiin-01 | Send Notification Task#id-10.3.1|Twiin-01| SendNotificationTask-Request-message

BgZ-2b-trans-05	Afhandelen notificatie-create-request bij updates
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-ontvanger** is in staat een naar aanleiding van een geüpdatete dataset binnenkomend notificatie-create-request af te handelen en een passende response te versturen
Prescription Level/Type	Verplicht

BgZ-2b-trans-05	Afhandelen notificatie-create-request bij updates
Toetsing	Validatie
Transactie/verwijzing	Transactie 5 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: (TA141) 10.5.1 | Twiin-01 | Send Notification Task#id-10.3.1| Twiin-01|SendNotificationTask-Response-message

BgZ-2b-trans-06	Versturen annulering
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** is in staat een notificatie-update-request te versturen wanneer GtK-verzender de notificatie wil annuleren of intrekken.
Prescription Level/Type	Optioneel
Toetsing	Validatie
Transactie/verwijzing	Transactie 6 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: (TA141) 10.5.2 | Twiin-02 | Cancel Notification Task#id-10.3.2| Twiin-02|CancelNotificationTask-Request-message

BgZ-2b-trans-07	Afhandeling annulering
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK-ontvanger is in staat een binnenkomend notificatie-update-request af te handelen en een passende response te versturen.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 7 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: (TA141) 10.5.2 | Twiin-02 | Cancel Notification Task#id-10.3.2| Twiin-02|CancelNotificationTask-Notification-response

BgZ-2b-trans-08.read	Uitvoeren read-operaties
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-ontvanger** is in staat read-operaties uit de notificatie-taak uit te voeren op het resource-endpoint van GtK-verzender.

BgZ-2b-trans-08.read	Uitvoeren read-operaties
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 8 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.5 | Twiin-05 | Retrieve Resource (see page 232) De read-operaties zijn opgenomen in de notificatie-task onder Task.input:read-available-resources.

BgZ-2b-trans-09.read	Afhandelen read-requests
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK-verzender is in staat binnenkomende read-requests af te handelen en een passende response te versturen.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 9 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.5 | Twiin-05 | Retrieve Resource (see page 232)

BgZ-2b-trans-08.search	Uitvoeren search-operaties resource-endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK-ontvanger is in staat search-operaties uit de notificatie-taak uit te voeren op het resource-endpoint van GtK-verzender.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 8 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.4 | Twiin-04 | Search Resource(s) (see page 230) De search-operaties zijn opgenomen in de notificatie-task onder Task.input:query-available-resources.

BgZ-2b-trans-09.search	Afhandelen search-requests resource-endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK-verzender is in staat binnenkomende search-requests af te handelen en een passende response te versturen.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 9 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.4 | Twiin-04 | Search Resource(s) (see page 230)

BgZ-2b-trans-10	Uitvoeren read-operatie ophalen workflow-task
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-ontvanger** is in staat een read-operatie voor het ophalen van de Workflow-task uit te voeren op het resource-endpoint van GtK-verzender.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 10 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.3 | Twiin-03 | Get Workflow Task (see page 228) De indicator voor de aanwezigheid van een workflow-task is opgenomen in de notificatie-task onder Task.input:get-worflow-task.valueBoolean (waarde is `true`).

BgZ-2b-trans-11	Afhandelen read-operatie workflow-task
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** is in staat een binnenkomende read-request op de workflow-task af te handelen en een passende response te versturen.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 11 van Z1.2.1.1 | BgZ - data interactions (see page 306)

BgZ-2b-trans-12.read	Uitvoeren read-operatie uit workflow-task
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK-ontvanger is in staat read-operaties uit de workflow-taak uit te voeren op het resource-endpoint van GtK-verzender.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 12 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.5 | Twiin-05 | Retrieve Resource (see page 232) De read-operaties zijn opgenomen in de workflow-task onder `Task.input:read-available-resources`.

BgZ-2b-trans-13.read	Afhandelen read-request
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK-verzender is in staat binnenkomende read-requests af te handelen en een passende response te versturen.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 13 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.5 | Twiin-05 | Retrieve Resource (see page 232)

BgZ-2b-trans-12.search	Uitvoeren search-operaties op resource-endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK-ontvanger is in staat search-operaties uit de workflow-taak uit te voeren op het resource-endpoint van GtK-verzender.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 12 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.4 | Twiin-04 | Search Resource(s) (see page 230) De search-operaties zijn opgenomen in de workflow-task onder `Task.input:query-available-resources`.

BgZ-2b-trans-13.search	Afhandelen search-operaties op resource-endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK-verzender is in staat binnenkomende search-requests af te handelen en een passende response te versturen
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 13 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.4 | Twiin-04 | Search Resource(s) (see page 230)

10.4 | Kern Volume 1b - Technical Agreements - GF

In this section the technical agreements for the generic functions (GF's) are described.

10.4.1 | TTA - Identification & Authentication

The world of identification and authentication in (Dutch) healthcare is changing rapidly. New regulation on European level (EHDS) is recently published and will come into effect the coming years. Also on and national level (DIAZ[40] law) and NEN7518 are currently developed. The UZI-register[41] will be replaced by the DEZI-register[42] and new technologies for authentication, like digital wallets and supporting technical standards (Verifiable Credentials[43], Decentralized Identifiers[44]) will be come more broadly available and supported. Therefore Twiin does not set technical requirements that won't be future-proof in a few years.

Identification and and authentication of healthcare workers and healthcare providers is important, though. Identification and authentication across the entire network help build the trust required for the exchange of medical data, therefore it is not surprising that NEN7512 defines specific requirements for this.

40. https://wetgevingskalender.overheid.nl/Regeling/WGK015084
41. https://www.uziregister.nl/
42. https://www.dezi.nl/
43. https://www.w3.org/TR/vc-overview/
44. https://www.w3.org/TR/did-1.1/

PvE | Identificatie en authenticatie

Id-01	Zorgverleners dienen geïdentificeerd te worden op basis van een uniek ID
Omschrijving/Toelichting/ Uitleg/Implicaties	UZI of een ander uniek tot één persoon te herleiden nummer. Wanneer een eigen id wordt gebruikt moet dit een **unieke combinatie** van persoons-id en organisatie-id opleveren en dat dit **herleidbaar blijft** (ook na, bijvoorbeeld, vertrek van zorgverlener), uitgegeven op het op het juiste betrouwbaarheidsniveau
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	alle Twiin-transacties

Auth-01	Zorgverlener/gebruiker (van het GtK) dienen (lokaal) geauthentiseerd te worden op eIDAS-niveau hoog
Omschrijving/Toelichting/ Uitleg/Implicaties	Door de keten heen kan hier nog geen bewijs van worden meegeven zodat andere partijen de zorgverlener ook met zekerheid kunnen authenticeren.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	alle Twiin-transacties

BgZ-2a-AA-01 / BgZ-2a-AA-02	Opzoekbaar maken publieke sleutel gebruikt voor ondertekening
Omschrijving/Toelichting/ Uitleg/Implicaties	**GtK-verzender** en **GtK-ontvanger** dienen de publieke sleutel(s) die zij gebruiken voor de ondertekening van JWT's via `kid` opzoekbaar te maken voor GtK-ontvanger. De wijze waarop de uitwisseling van publieke sleutels tussen GtK-verzender en GtK-ontvanger plaatsvindt is (nog) niet gebonden aan normatieve eisen. GtK-verzender en GtK-ontvanger moeten daarom onderling en in afstemming met de gebruikte infrastructuur afspraken maken over de wijze van uitwisseling van publieke sleutels.

BgZ-2a-AA-01 / BgZ-2a-AA-02	Opzoekbaar maken publieke sleutel gebruikt voor ondertekening
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Z1.2.1.2 | BgZ: Authentication & Authorization (see page 310)

BgZ-2a-AA-03	Aanmaken client assertion
Omschrijving/Toelichting/ Uitleg/Implicaties	**GtK-verzender** is in staat een client assertion in de vorm van een `authentication_grant` aan te maken die voldoet aan de specificaties
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Specificaties: 10.4.2 | TTA FHIR - Authorization | id 10.2.5 | TTA FHIR Authentication & Authorization Client authentication

BgZ-2a-AA-05	Identifiers GtK
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK-verzender en GtK-ontvanger dienen gebruik te maken van dezelfde identifiers voor de systemen die opereren als autorisatie-servers (authorization server token endpoints) Het toekennen en gebruiken van identifiers van systemen is (nog) niet gebonden aan landelijke normatieve eisen. GtK-verzender en GtK-ontvanger moeten daarom onderling en in afstemming met de gebruikte infrastructuur afspraken maken over de te gebruiken identifiers van systemen. Voor de BgZ is nu afgestemd dat de systeem identifiers zelf gekozen moeten zijn, maar de vorm van een FQDN of OID mogen hebben.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie `aud` -velden in Twiin-07 | Token Request (see page 270)

10.4.2 | TTA FHIR - Authorization

> Attention! The specifications and requirements in this chapter are still a specific implementation for the Notified Pull communication pattern and have not yet been generalized to work for other communication patterns.

Resource server authorization: OAuth 2.0

On application level both the Notification endpoint of the Receiving System and the FHIR endpoint of Sending System are considered as resource endpoints that must be secured by https://www.rfc-editor.org/rfc/rfc6749. This implies that a client that wants to interact with a resource server (FHIR or Notification endpoint) must obtain an access token from an authorization server before it can interact with that resource server. The client must present this access token as bearer token in the HTTP Authorization header of each request to the resource server as specified in https://www.rfc-editor.org/rfc/rfc6750#section-2.1.

For further information on the transaction involved, please go to Twiin-07 | Token Request (see page 270)

PvE | Autorization

BgZ-2a-AA-04	Systeem identifiers autorisatie-clients
Omschrijving/Toelichting/ Uitleg/Implicaties	**GtK-verzender** en **GtK-ontvanger** dienen gebruik te maken van dezelfde identifiers voor de systemen die opereren als autorisatie-clients (OAuth clients). Het toekennen en gebruiken van identifiers van systemen is (nog) niet gebonden aan normatieve eisen. GtK-verzender en GtK-ontvanger moeten daarom onderling en in afstemming met de gebruikte infrastructuur afspraken maken over de te gebruiken identifiers van systemen.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie `iss`-velden in Z1.2.1.2	BgZ: Authentication & Authorization (see page 310)

BgZ-2a-AA-04	Systeem identifiers autorisatie-servers
Omschrijving/Toelichting/ Uitleg/Implicaties	**GtK-verzender** en **GtK-ontvanger** dienen gebruik te maken van dezelfde identifiers voor de systemen die opereren als autorisatie-servers (authorization server token endpoints). Het toekennen en gebruiken van identifiers van systemen is (nog) niet gebonden aan landelijke normatieve eisen. GtK-verzender en GtK-ontvanger moeten daarom onderling en in afstemming met de gebruikte infrastructuur afspraken maken over de te gebruiken identifiers van systemen. Voor de BgZ is nu afgestemd dat de systeem identifiers zelf gekozen moeten zijn, maar de vorm van een FQDN of OID mogen hebben
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie `aud`-velden in Z1.2.1.2 | BgZ: Authentication & Authorization (see page 310)

BgZ-2a-AA-13	Aanmaken access token request voor resource endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-ontvanger** is in staat conform de specificaties een access token request voor toegang tot het resource-endpoint aan te maken en aan GtK-verzender te versturen. Eventueel inclusief een eerder van GtK-verzender ontvangen `authorization_grant`, welke de digitale representatie van de veronderstelde toestemming (`authorization_base`) bevat.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Specificaties: (TA141) Z1.2.1.2 | BgZ: Authentication & Authorization#Access-token-request (TA141) Twiin-07 | Token Request#Authorization-grant (TA141) Twiin-07 | Token Request#Authorization-base

BgZ-2a-AA-14	Aanmaken access token request voor resource endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	**GtK-verzender** is in staat conform de specificaties een access token request van GtK-ontvanger voor toegang tot het resource server endpoint af te handelen.

BgZ-2a-AA-14	Aanmaken access token request voor resource endpoint
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Specificaties: (TA141) Z1.2.1.2 | BgZ: Authentication & Authorization#Access-token-request

10.4.3 | TTA - Patient Consent

In certain use cases that require specific patient consent, Twiin mandates the use of Mitz. Mitz is an online consent management system that allows patients to manage their consent choices for the exchange of medical data between healthcare providers.

If a component is a (source) GtK and needs to offer Mitz Connector functionality, it must support multiple Mitz interfaces as specified in the Mitz Afsprakenstelsel to be able to check a patient consent registered in Mitz.

PvE | Toestemming

Toestemming-01	Een GtK dient een aansluiting op Mitz te hebben
Omschrijving/Toelichting/ Uitleg/Implicaties	Een GtK die uitwisselingen ondersteunt waar uitdrukkelijke toestemming voor nodig is, dient een Mitz Connector Aansluiting te ondersteunen
Prescription Level/Type	Conditioneel verplicht
Toetsing	n.v.t.
Transactie/verwijzing	Introductie

10.4.4 | TTA - Logging

In the context of exchanging medical information, every component involved is required to keep a record of its actions. This process is called logging. The logging of actions follows two standards: NEN7513 and IHE ATNA profile.

If a component is an Audit Record Repository (server), it must support all transactions. On the other hand, if a component sends logging (client), it can choose any transaction it wants to use.

IHE ITI-20 | Record Audit Event (see page 284)

> Both the NEN7513:2024 standard and the IHE ATNA profile only cover the logging of an access/ data exchange events. The fact that, in an OAuth implementation, access tokens are first requested, issued, and possibly revoked is not explicitly addressed in these logging standards and profiles. Therefore, there does not appear to be any mandatory requirement to log such events. As a result, this may create a challenge later on when setting up monitoring and alerting for abuse patterns or unauthorized use.

PvE | Logging

Log-01	**Het GtK moet alle berichtuitwisseling met andere GtK's loggen**
Omschrijving/Toelichting/ Uitleg/Implicaties	Wat er functioneel gelogd moet worden is gespecificeerd in de norm NEN 7513:2024, tabel 21.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	alle Twiin-transacties

Log-02	**Het GtK moeten loggegevens over uitwisselingen met andere GtK's kunnen aanleveren aan die GtK's.**
Omschrijving/Toelichting/ Uitleg/Implicaties	Wat de procedures en uitwisselformaat hiervoor gaat zijn is nog niet bepaald.
Prescription Level/Type	Verplicht
Toetsing	n.v.t.
Transactie/verwijzing	Eis uit NEN7512:2022 6.2.9: "De communicatiepartijen moeten afspraken maken over de wederzijdse inzage in de logbestanden en de termijn waarbinnen deze mogelijk wordt gemaakt." Zolang er nog geen landelijke procedures en afspraken zijn opgesteld over de uitwisseling van de logging tussen GtK's zal dit in de (uitzonderlijke) gevallen wanneer dit toch nodig is op ad hoc basis gedaan moeten worden.

10.4.5 | TTA - Addressing

To communicate between GtK's, the technical endpoints must be known. Twiin offers ZORG-AB as a service to find the technical endpoints of other GtK applications. These endpoints are registered in ZORG-AB by the Twiin governance. In this way Twiin makes addressing information public to all GtK applications. However, the use of ZORG-AB is not requirement, and alternate means of obtaining addressing information is permitted. It is not mandatory to use the ZORG-AB interfaces, it is mandatory for the GtK management organisations to inform Twiin about (changes in) the addressing information.

To search for GtK endpoints with ZORG-AB, you can use the Get_Organization and Get_Endpoint transactions.

When additional internal routing is necessary, the Twiin Participant in question is responsible to communicate the relevant information to the other participants until Twiin can adopt the technical agreement on routing and addressing, which is currently under development.

PvE | Adressering

BgZ-2a-TANP-04 / BgZ-2a-TANP-05	**Publiceren adresinformatie endpoints**
Omschrijving/Toelichting/ Uitleg/Implicaties	De GtK-ontvanger en GtK-verzender dienen de technische adressen van het resource-endpoint, het notificatie-endpoint en het token-endpoint kenbaar te maken aan de Twiin Beheerorganisatie. De wijze waarop technische adressen tussen GtK-verzender en GtK-ontvanger worden gecommuniceerd is (nog) niet gebonden aan normatieve eisen. De Twiin Beheerorganisatie publiceert de endpoints en technische adressen in ZORG-AB. Om de technische adressen van een andere partij te achterhalen kan er worden gekozen om ZORG-AB te raadplegen (10.6.5 | Addressing - ZORG-AB Transacties (see page 288)) maar dit is niet verplicht. GtK-verzender en GtK-ontvanger kunnen bijvoorbeeld ook onderling afspraken maken over de wijze waarop technische adressen worden gecommuniceerd.
Prescription Level/Type	Verplicht
Toetsing	n.v.t.
Transactie/verwijzing	De procedures hiervoor moeten nog worden opgesteld.

10.4.6 | TTA - Localisation

Localisation is searching the sources that (might) have relevant information on the client. Localisation on a broad level is done via an interface Mitz offers. This means the GtK should offer Mitz Connector functionality when an explicit patient consent is necessary for the information exchange the GtK supports.

With the so-called open authorization query[45] a healthcare provider can ask Mitz which other healthcare providers maintain records of a certain client may and can be consulted for one or more data categories. The result gives 0 or more healthcare providers (identified with URA) that have client consent to share the requested datatype and *might* have it. The URA-identifier in combination with the type of electronic service(s) that need to be addressed can be used as search parameter to find corresponding Twiin GtK interfaces in ZORG-AB (see addressing (see page 210)).

10.4.7 | Network level security

The network connections between GtK's must be secure. In a secure network, certificates play a crucial role by enabling the establishment of secure connections using TLS. They also ensure the authenticity and integrity of data in transit. Therefore mutual TLS shall be used between GtK's.

Both the Sending System and Receiving System expose endpoints that must be protected from unauthorized and malicious interactions. More specifically, access control measures must be applied to the following endpoints:

- Receiving System: Notification endpoint (FHIR Task endpoint)
- Sending System: Resource endpoint

Mutual TLS shall be used to protect these endpoints in the following ways:

- Authentication: The sending and receiving systems are mutually verifying each other's identity before establishing a secure connection. In this way only systems that are trusted are allowed to set up connections.
- Encryption: an mTLS connection is encrypted. This means that only the sending and receiving systems can read the exchanged data and no third, unauthorized party can 'listen in'.
- Integrity: mTLS assures that the data has not been modified by any unauthorized party during transmission. Any tampering attempts would alert the recipient.
- Protection against replay attacks: Each message sent over the connection includes a sequence number, and the recipient keeps track of the sequence numbers it has received. If a message with a previously received sequence number arrives, it is considered a replayed message and is rejected. This prevents attackers from intercepting and resending previously valid messages.

> There are endpoints where access control measures do not need to be enforced. For example, the endpoint where the JWKS is available. Mutual TLS does not need to be enforced there, because there is virtually no opportunity to do any real harm. On the other hand, in the technical core we do indeed also refer to those endpoints elsewhere—just not in the sense that they require extra attention from a network-level security perspective.

45. https://www.mitz-toestemming.nl/sites/default/files/2022-05/VZVZ_Mitz_Implementatiehandleiding_OpenGesloten_v3.8.0.pdf

Terminology

- Certificate Authority (CA): A trusted entity responsible for issuing and managing certificates used in secure network connections.
- Certificate Revocation List (CRL): A list maintained by a Certificate Authority, containing revoked certificates to prevent the use of compromised or invalid certificates.
- Public Key Infrastructure overheid (PKIo): A PKI structure controlled by the Dutch government, governing the issuance and management of certificates in the Netherlands.
- Trusted Service Provider (TSP): A party authorized to issue PKIo certificates within the PKIo infrastructure, ensuring the integrity and security of the certificates they issue.

Network level security: mTLS 1.3

At the network level, mutual TLS (mTLS) must be applied. The TLS-implementation must comply with the security level "Good" as specified by the National Cyber Security Centre (NCSC). At the time of writing, the https://www.ncsc.nl/documenten/publicaties/2025/juni/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2025-05 (Security guidelines for Transport Layer Security 2025-05) require version 1.3 of the TLS standard for the security level "Good". In the case one or more of the cipher suites (Appendix B of the Security guidelines) are declassified by NCSC will this be described in a future version of the Twiin specification.

The exchange of a client certificate during the mTLS handshake does not only enable the server to authenticate the client on network level, but it also enables the server to issue certificate bound access tokens as specified in https://www.rfc-editor.org/rfc/rfc8705 as an additional security measure on application level. See section Resource server authorization: OAuth 2.0 (see page 211) for requirements on application level security using OAuth 2.0.

CRL / OCSP / CPS

The validity of a certificate shall be verified using a CRL, OCSP, or CPS check. A determined validity may be relied upon for a maximum of one hour, after which the verification must be performed again. If the validity of a certificate cannot be established, the connection shall be terminated, as it shall also be terminated if the certificate is found to be invalid.

PKIoverheid

Both the client and server certificates must be PKIo-certificates that are issued under the CA "Staat der Nederlanden Private Services CA – G1" (this includes UZI server certificates issued by UZI-registry (CIBG)). https://cert.pkioverheid.nl/

Note: the requirements specified in this chapter apply to Notification, FHIR, and token endpoints.

PvE | Netwerkbeveiliging

5.010 / BgZ-2a-NS-02	Authenticeren met PKI
Omschrijving/Toelichting/ Uitleg/Implicaties	Om zich te kunnen authenticeren, kunnen alle systemen betrokken bij transacties in het kader van Twiin een geldig PKIo-certificaat overleggen. Gebruikte PKIo-certificaten dienen te zijn uitgegeven onder de CA "Staat der Nederlanden Private Services CA – G1". Deze omvatten: • UZI-servercertificaat of • PKIoverheid Private Services CA – G1 certificate Het betreft de systemen in de rol van token-server en -client, notification-server en -client en resource-server en -client. Zie 10.4.7 | Network level security (see page 211)
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	

5.020	mTLS
Omschrijving/Toelichting/ Uitleg/Implicaties	Alle transacties in het kader van Twiin zijn beveiligd met Mutual Transport Layer Security[46] (mTLS).
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	

46. https://datatracker.ietf.org/doc/html/rfc8705

5.030 / BgZ-2a-NS-03	**Volgen TLS-richtlijnen NCSC**
Omschrijving/Toelichting/ Uitleg/Implicaties	**GtK-verzender** en **GtK-ontvanger** maken gebruik van TLS versies en -algoritmen die zijn geclassificeerd als beveiligingsniveau "goed" in de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS), 2025-5[47] van het NCSC: Verplicht gebruik van de volgende cryptografische algoritmes: • Certificate Verification: ECDSA, RSA en EdDSA* • Key exchange: ECDHE* is afgewaardeerd van goed naar voldoende. Met X25519MLKEM768, SecP256r1MLKEM768, SecP384r1MLKEM1024 zijn er alternatieven, maar deze algoritmes zijn (relatief) nieuw en maken nog geen deel uit van de TLS standaarden. ECDHE moet daarom nog gebruikt worden. • Bulk encryption: AES-256-GCM of ChaCha20-Poly1305 • Hash functions: SHA-512 of SHA-384 of SHA-256 Het is verplicht om *alle*** algoritmen aan te bieden die in de genoemde richtlijnen als "goed" zijn geclassificeerd. Hiermee wordt er voor gezorgd dat wanneer onverhoopt een algoritme in veiligheidsniveau daalt er andere alternatieven overblijven van niveau goed. *Deze algoritmen zijn afgewaardeerd naar beveiligingsniveau 'voldoende'. Maar zijn geen (beschikbare) varianten die geclassificeerd is met beveiligingsniveau 'goed'. Hierdoor is het noodzakelijk om ook deze algoritmen op het niveau 'voldoende' te gebruiken. **Er geldt een uitzondering voor ChaCha20-Poly1305. Voor bulk encryptie wordt door sommige partijen de keuze gemaakt voor AES-256-GCM en **niet** voor ondersteuning van ChaCha20-Poly1305. De laatste is namelijk niet compliant met de eisen (Federal Information Processing Standards) die het Amerikaanse NIST (National Institute of Standards and Technology) stelt. Het is voor een GtK-server niet verboden om ook andere algoritmen en TLS-versies te ondersteunen van een lager niveau dan goed. De rationale hierachter is dat hard- en software waar de GtK-server gebruik van maakt ook voor andere use cases buiten het Twiin Afsprakenstelsel ingezet kan worden. De GtK-verzender MOET in het kader van Twiin echter wel altijd de door Twiin beschreven algoritmen en TLS-versie bij de GtK-ontvanger aanbieden.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS), versie 2.1[48]

47. https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2025/juni/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2025-05/TLS-Richtlijnen-2025-05.pdf
48. https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1

5.040	Versleuteling volgens TLS
Omschrijving/Toelichting/ Uitleg/Implicaties	Transacties in het kader van Twiin worden versleuteld volgens TLS, zoals bedoeld in eis 5.020.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	

5.050 / BgZ-2a-NS-04	Controleren geldigheid TLS-certificaat
Omschrijving/Toelichting/ Uitleg/Implicaties	**GtK-verzender** en **GtK-ontvanger** controleren minimaal ieder uur door middel van CRL of OCSP de geldigheid van de certificaten van systemen waarmee transacties plaatsvinden.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	

5.060 / BgZ-2a-NS-05	CPS van het UZI-register
Omschrijving/Toelichting/ Uitleg/Implicaties	Systemen die de geldigheid van het UZI-servercertificaat van de andere Systemen dienen te controleren, voldoen aan de verplichting van het Certification Practice Statement (CPS) UZI-register.
Prescription Level/Type	Conditioneel Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie https://www.zorgcsp.nl/certification-practice-statement-cps , artikel 4.5.2 CRL's: https://www.zorgcsp.nl/certificate-revocation-lists-crl-s

BgZ-2a-NS-06	CPS van PKIo
Omschrijving/Toelichting/ Uitleg/Implicaties	Wanneer GtK-verzender en GtK-ontvanger de geldigheid van een PKIo-servercertficaat controleren, doen zij dit op basis van de afspraken in het Certification Practice Statement (CPS) PKIoverheid.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie https://cps.pkioverheid.nl/pkioverheid-cps-unified-v5.4.html , hoofdstuk 2

5.070	Gebruik CRL of OSCP
Omschrijving/Toelichting/ Uitleg/Implicaties	Systemen die de geldigheid van het PKIo-servercertificaat van de andere Systemen dienen te controleren, doen dit door middel van de meest recent gepubliceerde Certificaten Revocatie Lijst (CRL) of via het Online Certificate Status Protocol (OCSP), minimaal ieder uur.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie https://cps.pkioverheid.nl/pkioverheid-cps-unified-v5.4.html , paragraaf 2.2.

5.080	Ondertekening volgens DNSSEC
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK zijn in hun rol als DNS Server moet er voor zorgen dat de *name records* behorende bij de hostnames van GtK'en zijn ondertekend volgens DNSSEC. (proudly copied from MedMij (core.dns.300))[49]
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	

49. https://afsprakenstelsel.medmij.nl/asverplicht/mmverplicht/verantwoordelijkheden-core

5.090	Controleren ondertekenning DNSSEC
Omschrijving/Toelichting/ Uitleg/Implicaties	Elke GtK, in zijn rol als DNS resolver in het Domain Name System, controleert of de ontvangen name records zijn voorzien van ondertekening volgens DNSSEC en valideert deze volgens DNSSEC. Indien deze controle en validatie niet beide slagen, ziet hij af van verbinding met de betreffende hostname. Het gebruik van DNSSEC vermindert de kwetsbaarheid van het Domain Name System voor bijvoorbeeld DNS spoofing[50].
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	(proudly copied from MedMij (core.dns.301))[51]

10.5 | Kern Volume 2a – Transactions – CP

Under this section, the transactions are described of the generic core of Twiin herein all transactions between GtK applications are described and a reference is made to the transactions of the common facilities.

- 10.5.1 | Twiin-01 | Send Notification Task (see page 217)
- 10.5.2 | Twiin-02 | Cancel Notification Task (see page 225)
- 10.5.3 | Twiin-03 | Get Workflow Task (see page 228)
- 10.5.4 | Twiin-04 | Search Resource(s) (see page 230)
- 10.5.5 | Twiin-05 | Retrieve Resource (see page 232)
- 10.5.6 | Twiin-06 | WADO-WS (see page 234)
- 10.5.7 | IHE ITI-38 | Cross Gateway Query (see page 237)
- 10.5.8 | IHE ITI-39 | Cross Gateway Retrieve (see page 249)
- 10.5.9 | IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set (see page 256)

These transactions are generic and used within multiple “zorgtoepassingen”. Each Twiin “zorgtoepassingen” has its own implementation guide containing references to this section.

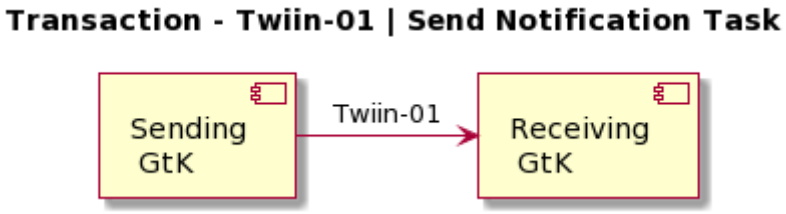
In this section, the IHE transactions of the generic core of Twiin are described, all IHE transactions between GtK applications are described and a reference is made to the transactions of the common facilities.

10.5.1 | Twiin-01 | Send Notification Task

This section describes the transaction needed for the notification.

50. https://datatracker.ietf.org/doc/html/rfc5452#section-3
51. https://afsprakenstelsel.medmij.nl/asverplicht/mmverplicht/verantwoordelijkheden-core

Scope



This transaction delivers a notification from the Sending GtK to the Receiving GtK based on the specified referral.

Use Case Roles

Actor: Sending GtK

Role: Sends Notification Tasks on behalf of a referring user.

Actor: Receiving GtK

Role: Receives and processes Notification Tasks

Referenced Standards

- HL7® FHIR® standard STU3 https://hl7.org/fhir/stu3

Messages

Request message

The Notification message is sent by the Sending GtK when it needs to notify the Receiving GtK about one or more FHIR® resources that have been made available to the Receiving GtK.

The Notification that is sent to the Receiving GtK must be able to convey at least the following details:

- Identification of Sending GtK, Sending Organization and practitioner
- Identification of Receiving Organization
- References to individual FHIR® resources that have been made available at the Sending GtK
- FHIR® search or read queries that can be used to retrieve FHIR® resources that have been made available at the Sending GtK
- Authorization base (see (TA141) Twiin-07 | Token Request#Authorization-base)

The payload of this message consists of a https://hl7.org/fhir/stu3/task.html resource that contains at least the details mentioned above. This message is sent to communicate both a new and an updated

data set to the Receiving GtK. The message results in a Task instance that will be referred to as the Notification Task.

> For the time being, the STU3 version of the FHIR® standard will be used because this TA will first be applied in the context of the BgZ (Basisgegevensset Zorg). Within that context, data is exchanged based on FHIR® STU3. As soon as data has to be exchanged using the Notified Pull pattern for newer FHIR® versions, it becomes opportune to provide or adopt a specification of the Notification for the corresponding FHIR® version.

The Sending GtK must initiate the Notification message using a create[52] interaction, i.e. sending an HTTP POST request to the Task endpoint of the Receiving GtK.

The media type of the HTTP body must be either *application/fhir+json* or *application/fhir+xml*.

When generating the Notification message, the Sending GtK must set the Task attributes as specified in the table below. For complete information on constructing a FHIR® Task Resource, see https://hl7.org/fhir/stu3/task.html .

Attribute	Card.	Description

52. https://hl7.org/fhir/STU3/http.html#create

definitionReference	0..1	This element will be used for routing purposes. The value could determine the organisational unit which will handle the notification. The display of this reference should be filled if no reference to a workflow Task exists and this value shall reference a valid ActivityDefinition resource. See also: 10.4.5 | TTA – Addressing (see page 210) Temporary agreement: We expect the activity definition reference to be in the same section as the references to the substantive resources: • In a thick notification, it will be referenced in the notification itself • In a thin notification, it will be referenced in the workflow task Until additional and more explicit agreements will be specified in the TA Routing, we will use this temporary agreement.
basedOn	0..*	Optional reference to a request–Type resource[53] that produced this event. If a workflow has been initiated and a Workflow Task is present, this must be referenced.
groupIdentifier	1..1	Unique identifier of the data set that is made available. An update to an existing data set at the Sending GtK triggers a new Notification Task, and thus a new Notification Task instance. Multiple Notifications Tasks on the same data set must share one unique identifier so that the Receiving GtK can identify them as relating to the same data set at the Sending GtK.
identifier	**1..1**	Business identifier of the task. This is a required field for traceability and cancellation of individual Notifications.

53. https://hl7.org/fhir/workflow.html#list

status	1..1	The state communicated by this event. Fixed value: • requested See also: https://hl7.org/fhir/stu3/valueset-request-status.html
intent	1..1	Indicates the "level" of actionability associated with the Task[2] (see page 217). Preferred value: • proposal See also: https://hl7.org/fhir/stu3/valueset-request-intent.html
code.coding	**1**..1	A code briefly describing what the task involves: • system = "http://fhir.twiin.nl/fhir/CodeSystem/TaskCode" • code = "pull-notification"
restriction.period	0..1	The period during which the data will be available for retrieval.
requester.agent.identifier	1..1	Identifier of the system that created this Notification. This could be the originating EHR System or the routing gateway system, dependent on which system created the Notification Task.
requester.onBehalfOf.identifier	**1**..1	Identifier of the Organization at which the data has been made available. The identifier shall be in the system “http://fhir.nl/fhir/NamingSystem/ura”
owner.identifier	**1**..1	Identifier of the Receiving Healthcare Organization. The identifier shall be in the system “http://fhir.nl/fhir/NamingSystem/ura”

input:authorization-base	**1..1**	The (TA141) Twiin-07 | Token Request#Authorization-base to be used when retrieving the data.
		Constraints:
		• type.coding
		  • system = "http://fhir.twiin.nl/fhir/CodeSystem/TaskParameter"
		  • code = "authorization-base".
		• valueString

input:get-workflow-task	0..1	An indicator to show whether or not all available resources are part of this Notification.
		Constraints:
		• type.coding
		  • system = "http://fhir.twiin.nl/fhir/CodeSystem/TaskParameter"
		  • code = “get-workflow-task”
		• valueBoolean
		Where valueBoolean:
		• true, the basedOn Workflow Task must be retrieved to get all available resources;
		• false (default), all available resources are available in the next (two) input slices.
		If this input slice is not added, the presumed value shall be false.

input: read-available-resource	0..*	The FHIR®-read interactions that can be performed to retrieve the data that was made available.
		Constraints:
		• type.coding (one or more of:)
		  • *Generic typing:*
		  • system = "http://hl7.org/fhir/restful-interaction"
		  • code = "read"
		  • *SNOMED CT typing **(deprecated)**:*
		  • system = "http://snomed.info/sct"
		  • code = a SNOMED CT code
		  • *LOINC typing **(deprecated)**:*
		  • system = "http://loinc.org"
		  • code = a LOINC code
		  • *FHIR profile typing **(prefered)**:*
		  • system = "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile"
		  • code = a FHIR profile-id, e.g. "http://nictiz.nl/fhir/StructureDefinition/zib-DrugUse"
		• valueReference format
		  • [resourcetype]/[id]
		Where:
		• resourcetype denotes a FHIR® resourcetype;
		• id represents a logical id of a FHIR® resource instance.

input: query-available-resources	0..*	The FHIR®-search interactions that can be performed to retrieve the data that was made available.
		Constraints:
		• type.coding (one or more of:)
		  • *Generic typing:*
		  • system = "http://hl7.org/fhir/restful-interaction"
		  • code = "search-type"
		  • *SNOMED CT typing **(deprecated)**:*
		  • system = "http://snomed.info/sct"
		  • code = a SNOMED CT code
		  • LOINC typing ***(deprecated)***:
		  • system = "http://loinc.org"
		  • code = a LOINC code
		  • *FHIR profile typing **(prefered)***:
		  • system = "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile"
		  • code = a FHIR profile-id, e.g. "http://nictiz.nl/fhir/StructureDefinition/zib-DrugUse"
		• valueString format
		  • [resourcetype]{?[parameters]}
		Where:
		• Resourcetype denotes a FHIR® resourcetype;
		• parameters can be added to refine a FHIR®-search.

The Sending GtK MAY choose not to list the available FHIR® resources in Task.input. In that case, the Sending GtK MUST provide a reference to a Workflow Task resource in Task.basedOn. This Workflow Task MUST list the available FHIR® resources in Task.input, in the same format that is specified for the Notification Task. Additionally, in this case the Notification Task MUST have an entry in Task.input with the following values:

- Task.input.type.coding.system: "http://fhir.twiin.nl/fhir/CodeSystem/TaskParameter"
- Task.input.type.coding.value: "get-workflow-task"
- Task.input.valueBoolean: true

The Receiving GtK must accept both media types *application/fhir+json* and *application/fhir+xml*.

On receiving the submission, the Receiving GtK must validate the resource and respond with one of the HTTP codes defined in the 10.5.1 | Twiin-01 | Send Notification Task .

The Notification should trigger an event in the Receiving GtK to facilitate the expected Pull.

Persistence of the Notification Task as a FHIR® resource is not required, whether it is necessary to persist is purely up to the receiving GtK and its internal implementation.

When the data set for which a Notification message has been sent is updated in the Sending GtK, the Sending GtK must inform the Receiving GtK about this update by sending a new Notification Message. In this case, Task.input:read-available-resource and Task.input:query-available-resources should only list the updated FHIR® resources. This way, the update can be communicated as a delta to the original data set. This relieves the Receiving GtK of determining which resources have changed in a larger set of resources. Note that the value of Task.identifier for the new Notification Task must differ from the value of Task.identifier Notification Task for the original data set, while the value of Task.groupIdentifier must be the same for all Notification Tasks on the same data set. This way, consecutive Notification Tasks on the same data set can be related to each other by the value of Task.groupIdentifier.

Response message

This message must be provided when a success or error condition needs to be communicated in response to an inbound request message. Success is only indicated once the Notification is received and completely processed.

To enable the Sending GtK to know the outcome of technical / syntactic processing of the Notification Task, the Receiving GtK must return either an empty body or an OperationOutcome resource. This body must be accompanied with the correct HTTP status code, e.g.:

- 200 OK – Notification received and not persisted.
- 201 Created – Notification received and persisted. In this case http-headers Location and Etag should be filled.
- 400 Bad Request – Notification could not be parsed or failed basic FHIR® validation rules.
- 404 Not Found – Resource type not supported, or wrong endpoint.
- 412 Precondition Failed – The processing of the Notification Task could not be finished, since the criteria were not selective enough.
- 422 Unprocessable Entity – The Notification Task resource violated applicable server business rules. This should be accompanied by an OperationOutcome resource providing additional detail.

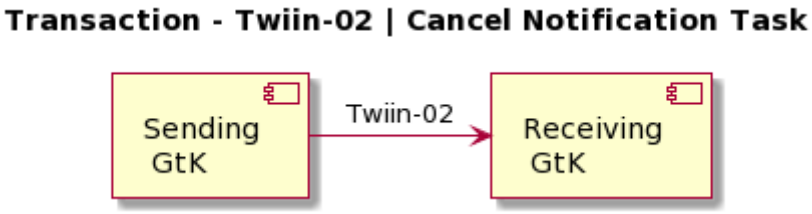
Whether or not the resources referenced from any of the input elements can be retrieved shall not be a factor in the HTTP status.

The Sending GtK processes the response according to application defined rules.

10.5.2 | Twiin-02 | Cancel Notification Task

This section describes the transaction needed for the cancellation of the notification.

Scope



This transaction delivers a cancellation notification from the Sending GtK to the Receiving GtK based on the specified referral. Twiin only requires that a GtK can receive this message, sending and processing the message is optional.

Actor	Sending Twiin-02	Receiving Twiin-02	Processing Twiin-02
Sending GtK	Optional	N/A	N/A
Receiving GtK	N/A	Mandatory	Optional

Use Case Roles

Actor: Sending GtK

Role: Sends Cancellation Notification Tasks on behalf of a referring user.

Actor: Receiving GtK

Role: Receives and processes Cancellation Notification Tasks

Referenced Standards

- HL7® FHIR® standard STU3 https://hl7.org/fhir/stu3

Messages

Request message

The Notification Cancellation request message is sent when the Sending GtK needs to send a cancellation of a previous Notification to the Receiving GtK. Just as the Notification message, the payload of this message consists of a FHIR® STU3 Task resource.

The Sending GtK can cancel a previous Notification using a conditional update[54] interaction on the Task that represents that previous Notification. This is done by sending an HTTP PUT request to the Task

endpoint of the Receiving GtK, where the value of Task.identifier of that previous Notification is included in the query parameters of the PUT request.

The media type of the HTTP body must be either *application/fhir+json* or *application/fhir+xml*.

When generating the Notification Cancellation message, the Sending GtK must set the Task attributes as specified in the table below. For complete information on constructing a FHIR® Task Resource, see https://hl7.org/fhir/stu3/task.html .

Attribute	Card.	Description
identifier	1..1	Business identifier of the Notification Task; the value of this identifier must be equal to the value of the identifier of the Notification Task that is to be cancelled.
status	1..1	The state communicated by this event. Fixed value: • cancelled
intent	1..1	Indicates the "level" of actionability associated with the Task[1] (see page 225). Preferred value: • proposal See also: https://hl7.org/fhir/stu3/valueset-request-intent.html
code.coding	1..1	A code briefly describing what the task involves: • system = "http://fhir.twiin.nl/fhir/CodeSystem/TaskCode" • code = "pull-notification"

In the absence of a reference to the patient (for example, within the Workflow Task), the token request for this cancellation SHALL include the patient's BSN within the assertion.

The Receiving GtK must accept both media types *application/fhir+json* and *application/fhir+xml*.

On receipt of the submission, the Receiving GtK must validate the resource and respond to the cancellation message according to the requirements specified in Notification response (see page 225).

The Notification SHOULD trigger an event in the Receiving GtK to cancel any intended Pull interaction.

Persistence of the Notification Task as a FHIR® resource is not necessary.

54. http://hl7.org/fhir/stu3/http.html#cond-update

Notification response

This message must be provided when a success or error condition needs to be communicated in response to an inbound Notification message. Success is only indicated once the Notification is received and completely processed.

To enable the Sending GtK to know the outcome of technical / syntactic processing of the Notification Task, the Receiving GtK must return either an empty body or an OperationOutcome resource. This body must be accompanied with the correct HTTP status code, e.g.:

- 200 OK – Notification received and not persisted.
- 201 Created – Notification received and persisted. In this case http-headers Location and Etag should be filled.
- 400 Bad Request – Notification could not be parsed or failed basic FHIR® validation rules.
- 404 Not Found – Resource type not supported, or wrong endpoint.
- 412 Precondition Failed – The processing of the Notification Task could not be finished, since the criteria were not selective enough.
- 422 Unprocessable Entity – The Notification Task resource violated applicable server business rules. This should be accompanied by an OperationOutcome resource providing additional detail.

The Sending GtK processes the response according to application defined rules.

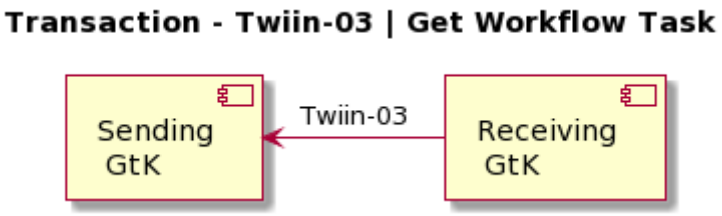
10.5.3 | Twiin-03 | Get Workflow Task

This section describes the transaction of the retrieval of the Workflow Task.

> If a workflow Taks is used its definitionReference must be filled and shall reference a valid ActivityDefinition resource.

> Temporary agreement: We expect the activity definition reference to be in the same section as the references to the substantive resources:
>
> - In a thick notification, it will be referenced in the notification itself
> - In a thin notification, it will be referenced in the workflow task
>
> Until additional and more explicit agreements will be specified in the TA Routing, we will use this temporary agreement.

Scope



This transaction supports getting the Workflow Task by the Requesting System at the Resource Server.

Use Case Roles

Actor: Requesting GtK

Role: Requests the workflow Task on behalf of a requesting user.

Actor: Responding GtK

Role: Processes the request and responds with the requested resource.

Referenced Standards

- HL7® FHIR® standard STU3 https://hl7.org/fhir/stu3

Messages

Request message

The requesting system wants to obtain the workflow Task for information about a known workflow. The workflow Task is retrieved using a the FHIR® read interaction, i.e. executing an HTTP GET request to the Task endpoint of the resource server.

```
GET [base]/Task/[id]
```

The requesting system may provide the HTTP Accept header. Valid values for this header are *application/fhir+json* or *application/fhir+xml*. If none is set, the resource server will use its default.

Response message

The resource server returns the workflow Task that is requested.

The payload of this message consists of a https://hl7.org/fhir/stu3/task.html resource that contains relevant information to the workflow. This message is returned to the Receiving System.

The media type of the HTTP body must be either *application/fhir+json* or *application/fhir+xml*, based on the Accept header or default response content type.

At this time there is no generic specification of the contents of the workflow Task more specific than the FHIR® specification.

Persistence of the Workflow Task as a FHIR® resource is not necessary.

When an error occurs an OperationOutcome resource must be returned with more details on the reason.

The HTTP response must be accompanied with the correct HTTP status code, e.g.:

- `200` OK – The request is accepted and responded
- `401` Not Authorized - Authorization is required for the interaction that was attempted
- `404` Not Found – The request could not be processed, i.e. the resource with that id doesn't exist.
- `410` Gone – The request could not be processed, because the resource does not exist anymore.

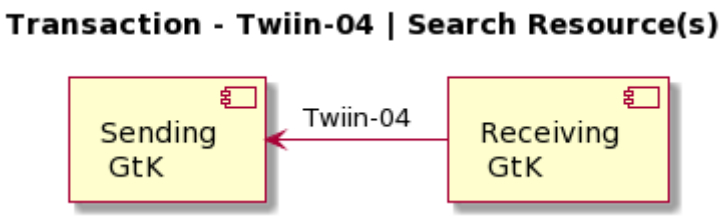
The requesting system processes the response according to application defined rules.

10.5.4 | Twiin-04 | Search Resource(s)

This section describes the transaction of the retrieval of the FHIR® resources.

> In the communication pattern notified pull these resources are referenced in the input field of the Notification or Workflow Task.
> These input fields contain valueString in the input slice: query-available-resources.

1. Scope



This transaction supports the request of resources by the Requesting GtK to the Resource Server.

2. Use Case Roles

Actor: Requesting GtK

Role: Sends a request for resources on behalf of a retrieving user.

> In the communication pattern notified pull, this is the Receiving GtK.

Actor: Responding GtK

Role: Processes the request and responds with the requested resources.

> Note: In the communication pattern notified pull, this is the Sending GtK.

3. Referenced Standards

- HL7® FHIR® standard STU3 https://hl7.org/fhir/stu3

4. Messages

4.1. Request message

The requesting GtK wants to obtain the resources that were referenced in the Task. These resources are retrieved using a FHIR® search interaction, i.e. executing an HTTP GET request to the resource servers FHIR® endpoint. If there is a relative path, the input valueString must be appended to the FHIR® base-url.

```
GET [base]/<ResourceType>?parameter=value
```

> **Percent-encoding of query parameters**
>
> When constructing URLs that include query parameters (e.g., code=...), it is important to percent-encode any reserved characters that could cause syntactic ambiguity, in accordance with https://datatracker.ietf.org/doc/html/rfc3986.
>
> **Exception**
> The slash character (/) may appear unencoded in query parameter values, as it is explicitly allowed in the query component of a URI per RFC 3986 (see Appendix A), and is commonly accepted by web servers and FHIR implementations.

The requesting GtK may provide the HTTP Accept header. Valid values for this header are *application/fhir+json* or *application/fhir+xml*. If none is set, the resource server will use its default.

4.2. Response message

The responding GtK returns the resource(s) that are requested.

The payload of this message consists of a FHIR® Bundle resource that contains the requested resource(s). This message is returned to the Receiving GtK.

The media type of the HTTP body must be either *application/fhir+json* or *application/fhir+xml*, based on the Accept header or default response content type.

When an error occurs an OperationOutcome resource must be returned with more details on the reason.

The HTTP response must be accompanied with the correct HTTP status code, e.g.:

- `200` OK - The search was processed and a valid response was returned
- `400` Bad Request - The search could not be processed or failed basic FHIR® validation rules
- `401` Not Authorized - Authorization is required for the interaction that was attempted
- `404` Not Found - The resource type not supported

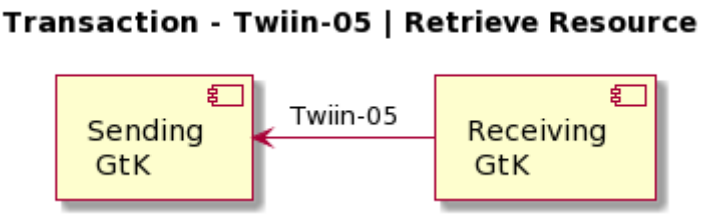
The requesting GtK processes the response according to application defined rules.

10.5.5 | Twiin-05 | Retrieve Resource

This page describes the transaction of the retrieval of the FHIR® resources.

> In the communication pattern notified pull these resources are referenced in the input field of the Notification or Workflow Task.
> These input fields contain valueReference in the input slice: read-available-resource.

Scope



This transaction supports the request of resources by the Requesting System to the Resource Server.

Use Case Roles

Actor: Requesting GtK

Role: Sends a request for a specific resource on behalf of a retrieving user.

> In the communication pattern notified pull, this is the Receiving GtK.

Actor: Responding GtK

Role: Processes the request and responds with the requested resource.

> Note: In the communication pattern notified pull, this is the Sending GtK.

Referenced Standards

- HL7® FHIR® standard STU3 https://hl7.org/fhir/stu3

Messages

Request message

The requesting GtK wants to obtain the resources that were referenced in the Task. These resources are retrieved using a FHIR® read interaction, i.e. executing an HTTP GET request to the resource servers FHIR® endpoint. If there is a relative path, the input valueReference must be appended to the FHIR® base-url.

```
GET [base]/<ResourceType>/<id>
```

> The requesting GtK may provide the HTTP Accept header. Valid values for this header are *application/fhir+json* or *application/fhir+xml*. If none is set, the resource server will use its default.

Response message

The responding GtK returns the resource that is requested.

The payload of this message is the requested FHIR® resource. This message is returned to the requesting GtK.

The media type of the HTTP body must be either *application/fhir+json* or *application/fhir+xml*, based on the Accept header or default response content type.

When an error occurs an OperationOutcome resource must be returned with more details on the reason.

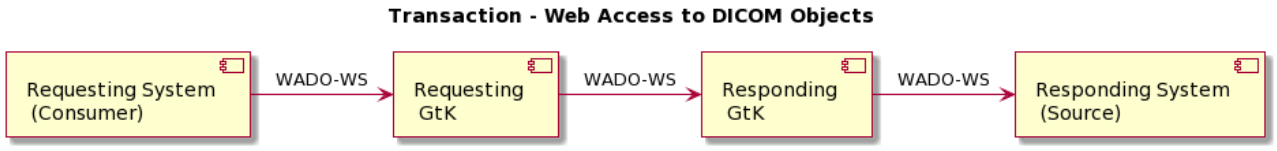
The HTTP response must be accompanied with the correct HTTP status code, e.g.:

- `200` OK – The search was processed and a valid response was returned
- `401` Not Authorized – Authorization is required for the interaction that was attempted
- `404` Not Found – The resource could not be found
- `410` Gone – The resource was deleted

The requesting GtK processes the response according to application defined rules.

10.5.6 | Twiin-06 | WADO-WS

> In the Netherlands the WADO-WS transaction is used in the SOAP based exchange pattern Indexed Pull.
>
> Although this is a deprecated transaction it is still used by most consumers to 'stream' images. Which means, request images in other formats than the 'full DICOM' format. (for example JPEG in lower resolution)
>
> A Requesting GtK can choose to implement the WADO-WS transaction
>
> An Responding GtK should be able to receive the WADO-WS transaction



```
<?xml version="1.0" encoding="UTF-8"?>
<!-- This wsdl file is for an XDS-I.b Imaging Document Source Actor
It can be used 'as is' to support Retrieve Imaging Document Set Transaction [RAD-69]
using Synchronous Web Services.-->
<definitions name="ImagingDocumentSource" targetNamespace="urn:ihe:rad:xdsi-b:2009"
xmlns="http://schemas.xmlsoap.org/wsdl/" xmlns:wsdl="http://schemas.xmlsoap.org/
wsdl/" xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/" xmlns:wsaw="http://
www.w3.org/2006/05/addressing/wsdl" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:tns="urn:ihe:rad:xdsi-b:2009" xmlns:wadows="urn:dicom:wado:ws:2011"
xmlns:deprecatedwadows="urn:dicom:ws:wado:2011" xmlns:ihe="urn:ihe:iti:xds-b:2007"
xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"> <documentation>IHE XDS-I.b
Imaging Document Source</documentation> <types>
<xsd:schema elementFormDefault="qualified">
<xsd:import namespace="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0" /> <xsd:import
namespace="urn:ihe:iti:xds-b:2007" />
<xsd:import namespace="urn:ihe:rad:xdsi-b:2009" />
</xsd:schema> </types>
<message name="RetrieveImagingDocumentSetRequest_Message"> <documentation>Retrieve
Imaging Document Set</documentation>
<part name="body" element="tns:RetrieveImagingDocumentSetRequest" />
</message>
<message name="RetrieveRenderedImagingDocumentSetRequest_Message">
<documentation>Retrieve Rendered Imaging Document Set</documentation>
<part name="body" element="wadows:RetrieveRenderedImagingDocumentSetRequest" /> </
message>
<message name="DeprecatedRetrieveRenderedImagingDocumentSetRequest_Message">
<documentation>Deprecated Retrieve Rendered Imaging Document Set</documentation>
<part name="body"
element="deprecatedwadows:RetrieveRenderedImagingDocumentSetRequest" /> </message>
<message name="RetrieveRenderedImagingDocumentSetResponse_Message">
<documentation>Retrieve Rendered Imaging Document Set Response</documentation>
<part name="body" element="wadows:RetrieveRenderedImagingDocumentSetResponse" /> </
message>
<message name="RetrieveDocumentSetResponse_Message">
<documentation>Retrieve Document Set Response</documentation>
<part name="body" element="ihe:RetrieveDocumentSetResponse" /> </message>
<portType name="ImagingDocumentSource_PortType">
<operation name="ImagingDocumentSource_RetrieveImagingDocumentSet"> <input
message="tns:RetrieveImagingDocumentSetRequest_Message"
wsaw:Action="urn:ihe:rad:2009:RetrieveImagingDocumentSet" /> <output
message="tns:RetrieveDocumentSetResponse_Message"
wsaw:Action="urn:ihe:iti:2007:RetrieveDocumentSetResponse" /> </operation>
```

```
<operation name="ImagingDocumentSource_RetrieveRenderedImagingDocumentSet"> <input
message="tns:RetrieveRenderedImagingDocumentSetRequest_Message"
wsaw:Action="urn:dicom:wado:ws:2011:RetrieveRenderedImagingDocumentSet" /> <output
message="tns:RetrieveRenderedImagingDocumentSetResponse_Message"
wsaw:Action="urn:dicom:wado:ws:2011:RetrieveRenderedImagingDocumentSetResponse" />
</operation>
<operation
name="ImagingDocumentSource_DeprecatedRetrieveRenderedImagingDocumentSet"> <input
message="tns:DeprecatedRetrieveRenderedImagingDocumentSetRequest_Message"
wsaw:Action="urn:dicom:ws:wado:2011:RetrieveRenderedImagingDocumentSet" /> <output
message="tns:RetrieveDocumentSetResponse_Message"
wsaw:Action="urn:ihe:iti:2007:RetrieveDocumentSetResponse" /> </operation>
</portType>
<binding name="ImagingDocumentSource_Binding"
type="tns:ImagingDocumentSource_PortType">
<soap12:binding style="document" transport="http://schemas.xmlsoap.org/soap/http" />
<wsaw:UsingAddressing wsdl:required="true" />
<operation name="ImagingDocumentSource_RetrieveImagingDocumentSet">
<soap12:operation soapActionRequired="false" /> <input>
<soap12:body use="literal" />
</input> <output>
<soap12:body use="literal" /> </output>
</operation>
<operation name="ImagingDocumentSource_RetrieveRenderedImagingDocumentSet">
<soap12:operation soapActionRequired="false" /> <input>
<soap12:body use="literal" /> </input>
<output>
<soap12:body use="literal" />
</output>
</operation>
<operation
name="ImagingDocumentSource_DeprecatedRetrieveRenderedImagingDocumentSet">
<soap12:operation soapActionRequired="false" /> <input>
<soap12:body use="literal" /> </input>
<output>
<soap12:body use="literal" />
</output> </operation>
</binding>
<service name="ImagingDocumentSource_Service">
<port name="ImagingDocumentSource_Port_Soap12"
binding="tns:ImagingDocumentSource_Binding"> <soap12:address location="http://
servicelocation/ImagingDocumentSource_Service" />
</port> </service> </definitions>
```

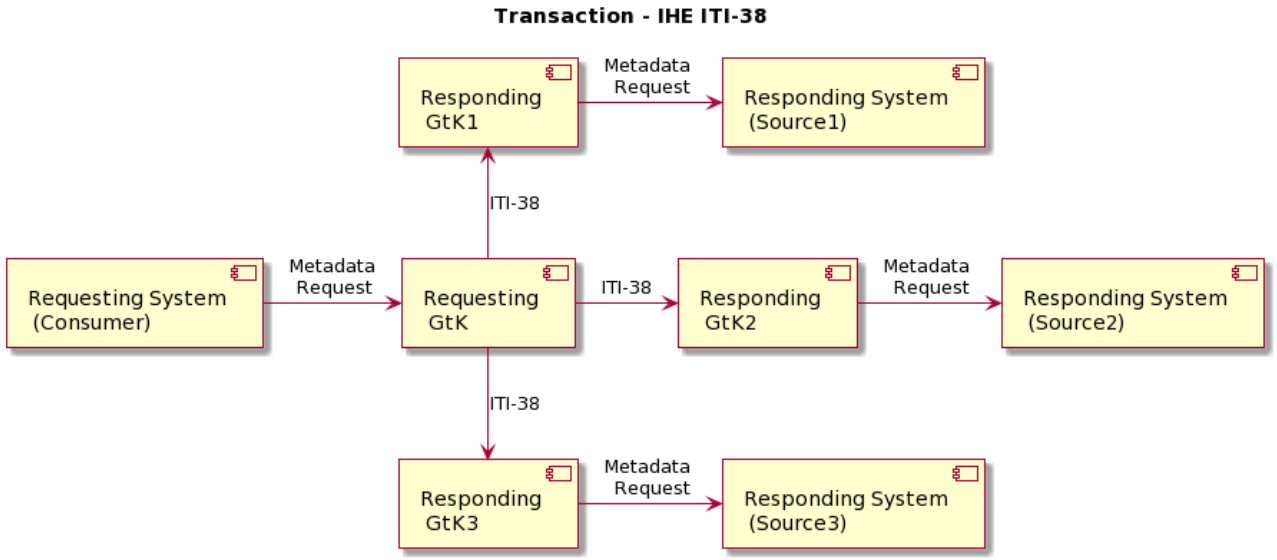
10.5.7 | IHE ITI-38 | Cross Gateway Query

Scope

This transaction is used by the Requesting GtK to retrieve metadata. The Requesting GtK sends this request to all Responding GtK's where information is available. Prior to this transaction the Requesting GtK first needs to retrieve information about where metadata can be retrieved. This is needed to prevent excessive usage of the transaction to GtK's where no information is available.

> The Mitz open question specifications can be found on their website: Bijlage | Architectuurdocumenten

Use Case Roles



This transaction uses SOAP v1.2 and Synchronous Web Services.

Referenced standards

Implementers of this transaction shall comply with all requirements described in Web Services for IHE Transactions.[55]

ebRIM	OASIS/ebXML Registry Information Model v3.0
ebRS	OASIS/ebXML Registry Services Specifications v3.0
ITI TF-3:4	Metadata used in Document Sharing profiles

Messages

Cross Gateway Query

For more technical specification, see the original document: https://profiles.ihe.net/ITI/TF/Volume2/ITI-38.html

NB: This transaction is always performed in combination with the transaction ITI-40 (see page 265) where user data is added in a SAML token.
NB: All transactions are logged with an ITI-20 audit transaction, see IHE:ITI volume 2 for the correct implementation."

10.5.7.1 | ITI-38 examples

For reference only

55. https://profiles.ihe.net/ITI/TF/Volume2/ch-V.html#Appendix%20V

ITI-38 request

```
<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing"
    xmlns:s="http://www.w3.org/2003/05/soap-envelope">
    <s:Header xmlns:s="http://www.w3.org/2003/05/soap-envelope">
        <a:Action s:mustUnderstand="1">urn:ihe:iti:2007:CrossGatewayQuery</a:Action>
        <a:MessageID>urn:uuid:7948cf8b-81fa-486d-a7d6-ca121b6b9c98</a:MessageID>
        <a:ReplyTo>
            <a:Address> http://www.w3.org/2005/08/addressing/anonymous </a:Address>
        </a:ReplyTo>
        <a:To s:mustUnderstand="1"> http://testing.interoplab.eu:8080 /
interoplab__responding_gateway/rg/xcq</a:To>
    </s:Header>
    <s:Body xmlns:s="http://www.w3.org/2003/05/soap-envelope">
        <query:AdhocQueryRequest xmlns:lcm="urn:oasis:names:tc:ebxml-
regrep:xsd:lcm:3.0"
            xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
            xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
            xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
            xmlns:xdsb="urn:ihe:iti:xds-b:2007"
            xmlns:xop="http://www.w3.org/2004/08/xop/include">
            <query:ResponseOption returnComposedObjects="true"
returnType="LeafClass"/>
            <rim:AdhocQuery home="1.1.4567334.1.4"
id="urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d">
                <rim:Slot name="$XDSDocumentEntryPatientId">
                    <rim:ValueList>
                        <rim:Value>'999999011^^^&2.16.840.1.113883.2.4.6.3&ISO'</
rim:Value>
                    </rim:ValueList>
                </rim:Slot>
                <rim:Slot name="$XDSDocumentEntryStatus">
                    <rim:ValueList>
                        <rim:Value>('urn:oasis:names:tc:ebxml-
regrep:StatusType:Approved')</rim:Value>
                    </rim:ValueList>
                </rim:Slot>
            </rim:AdhocQuery>
        </query:AdhocQueryRequest>
    </s:Body>
</s:Envelope>
```

ITI-38 response

```
<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope">
    <S:Header>
        <wsa:Action xmlns:s="http://www.w3.org/2003/05/soap-envelope"
            xmlns:wsa="http://www.w3.org/2005/08/addressing"
s:mustUnderstand="1">urn:ihe:iti:2007:CrossGatewayQueryResponse</wsa:Action>
        <wsa:RelatesTo xmlns:wsa="http://www.w3.org/2005/08/
addressing">urn:uuid:7948cf8b-81fa-486d-a7d6-ca121b6b9c98</wsa:RelatesTo>
    </S:Header>
    <S:Body>
        <query:AdhocQueryResponse xmlns:query="urn:oasis:names:tc:ebxml-
regrep:xsd:query:3.0" status="urn:oasis:names:tc:ebxml-
regrep:ResponseStatusType:Success">
            <rim:RegistryObjectList xmlns:rim="urn:oasis:names:tc:ebxml-
regrep:xsd:rim:3.0">
                <rim:ExtrinsicObject id="urn:uuid:4da76db2-30ba-4822-b495-
a42b5841394d" lid="urn:uuid:3dc68646-5432-4334-997c-b8db58baad0d"
objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1" mimeType="text/xml"
status="urn:oasis:names:tc:ebxml-regrep:StatusType:Approved"
home="urn:oid:1.1.4567334.1.4">
                    <rim:Slot name="hash">
                        <rim:ValueList>
                            <rim:Value>0a177cec96cc04e2fe4443cb213f7816abfe72b6</
rim:Value>
                        </rim:ValueList>
                    </rim:Slot>
                    <rim:Slot name="languageCode">
                        <rim:ValueList>
                            <rim:Value>nl-NL</rim:Value>
                        </rim:ValueList>
                    </rim:Slot>
                    <rim:Slot name="repositoryUniqueId">
                        <rim:ValueList>
                            <rim:Value>1.1.4567332.1.1</rim:Value>
                        </rim:ValueList>
                    </rim:Slot>
                    <rim:Slot name="size">
                        <rim:ValueList>
                            <rim:Value>2459</rim:Value>
                        </rim:ValueList>
                    </rim:Slot>
                    <rim:Slot name="sourcePatientId">
                        <rim:ValueList>
```

```
                        <rim:Value>999999011^^^&2.16.840.1.113883.2.4.6.3&ISO</
rim:Value>
                    </rim:ValueList>
                </rim:Slot>
                <rim:Slot name="creationTime">
                    <rim:ValueList>
                        <rim:Value>20191023024209</rim:Value>
                    </rim:ValueList>
                </rim:Slot>
                <rim:Slot name="sourcePatientInfo">
                    <rim:ValueList/>
                </rim:Slot>
                <rim:Name>
                    <rim:LocalizedString xml:lang="us-en" charset="UTF-8"
value="Poliklinische brief"/>
                </rim:Name>
                <rim:VersionInfo versionName="2"/>
                <rim:Classification id="urn:uuid:4d85ee12-4876-4b97-914d-
c0284b937484" objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a"
classifiedObject="urn:uuid:4da76db2-30ba-4822-b495-a42b5841394d"
nodeRepresentation="405624007">
                    <rim:Slot name="codingScheme">
                        <rim:ValueList>
                            <rim:Value>2.16.840.1.113883.6.96</rim:Value>
                        </rim:ValueList>
                    </rim:Slot>
                    <rim:Name>
                        <rim:LocalizedString xml:lang="us-en" charset="UTF-8"
value="Administratieve documentatie"/>
                    </rim:Name>
                    <rim:VersionInfo versionName="-1"/>
                </rim:Classification>
                <rim:Classification id="urn:uuid:2a8e553f-27f0-49a0-9f74-
f5737dfa2b4c" objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f"
classifiedObject="urn:uuid:4da76db2-30ba-4822-b495-a42b5841394d"
nodeRepresentation="N">
                    <rim:Slot name="codingScheme">
                        <rim:ValueList>
                            <rim:Value>2.16.840.1.113883.5.25</rim:Value>
                        </rim:ValueList>
                    </rim:Slot>
```

```
                        <rim:Name>
                            <rim:LocalizedString xml:lang="us-en" charset="UTF-8"
value="Normaal"/>
                        </rim:Name>
                        <rim:VersionInfo versionName="-1"/>
                    </rim:Classification>
                    <rim:Classification id="urn:uuid:736d2cfd-
c936-446d-93d6-94170e155fe7" objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
classificationScheme="urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d"
classifiedObject="urn:uuid:4da76db2-30ba-4822-b495-a42b5841394d"
nodeRepresentation="urn:ihe:rad:TEXT">
                        <rim:Slot name="codingScheme">
                            <rim:ValueList>
                                <rim:Value>1.3.6.1.4.1.19376.1.2.3</rim:Value>
                            </rim:ValueList>
                        </rim:Slot>
                        <rim:Name>
                            <rim:LocalizedString xml:lang="us-en" charset="UTF-8"
value="Radiology XDS-I Text"/>
                        </rim:Name>
                        <rim:VersionInfo versionName="-1"/>
                    </rim:Classification>
                    <rim:Classification id="urn:uuid:4250718b-3eee-4cb2-bd96-
f1c814166971" objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1"
classifiedObject="urn:uuid:4da76db2-30ba-4822-b495-a42b5841394d"
nodeRepresentation="V6">
                        <rim:Slot name="codingScheme">
                            <rim:ValueList>
                                <rim:Value>2.16.840.1.113883.2.4.15.1060</rim:Value>
                            </rim:ValueList>
                        </rim:Slot>
                        <rim:Name>
                            <rim:LocalizedString xml:lang="us-en" charset="UTF-8"
value="Algemeen ziekenhuis"/>
                        </rim:Name>
                        <rim:VersionInfo versionName="-1"/>
                    </rim:Classification>
```

```
                    <rim:Classification
id="urn:uuid:2fcf8117-5821-4f0a-9fd9-9d04b1e80815"
objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
classificationScheme="urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead"
classifiedObject="urn:uuid:4da76db2-30ba-4822-b495-a42b5841394d"
nodeRepresentation="309964003">
                        <rim:Slot name="codingScheme">
                            <rim:ValueList>
                                <rim:Value>2.16.840.1.113883.6.96</rim:Value>
                            </rim:ValueList>
                        </rim:Slot>
                        <rim:Name>
                            <rim:LocalizedString xml:lang="us-en" charset="UTF-8"
value="Radiologie"/>
                        </rim:Name>
                        <rim:VersionInfo versionName="-1"/>
                    </rim:Classification>
                    <rim:Classification
id="urn:uuid:20515fbf-56af-4a78-9396-9aadcfba9462"
objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
classificationScheme="urn:uuid:f0306f51-975f-434e-a61c-c59651d33983"
classifiedObject="urn:uuid:4da76db2-30ba-4822-b495-a42b5841394d"
nodeRepresentation="304784009">
                        <rim:Slot name="codingScheme">
                            <rim:ValueList>
                                <rim:Value>2.16.840.1.113883.6.96</rim:Value>
                            </rim:ValueList>
                        </rim:Slot>
                        <rim:Name>
                            <rim:LocalizedString xml:lang="us-en" charset="UTF-8"
value="Administratief document"/>
                        </rim:Name>
                        <rim:VersionInfo versionName="-1"/>
                    </rim:Classification>
                    <rim:ExternalIdentifier id="urn:uuid:09f046ee-f100-4765-995c-
f4a7231789f5" objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
identificationScheme="urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427"
value="999907025^^^&2.16.840.1.113883.2.4.6.3&ISO"
registryObject="urn:uuid:4da76db2-30ba-4822-b495-a42b5841394d">
                        <rim:Name>
                            <rim:LocalizedString xml:lang="en-US"
value="XDSDocumentEntry.patientId"/>
```

```
                        </rim:Name>
                        <rim:VersionInfo versionName="-1"/>
                    </rim:ExternalIdentifier>
                    <rim:ExternalIdentifier id="urn:uuid:7757ca3a-cff9-4ddb-91b6-
d6469703a305" objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
identificationScheme="urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab"
value="1.3.6.1.4.1.12559.11.13.2.1.227" registryObject="urn:uuid:4da76db2-30ba-4822-
b495-a42b5841394d">
                        <rim:Name>
                            <rim:LocalizedString xml:lang="en-US"
value="XDSDocumentEntry.uniqueId"/>
                        </rim:Name>
                        <rim:VersionInfo versionName="-1"/>
                    </rim:ExternalIdentifier>
                </rim:ExtrinsicObject>
            </rim:RegistryObjectList>
        </query:AdhocQueryResponse>
    </S:Body>
</S:Envelope>
```

ITI-38 request incl. SAML-token (ITI-40)

```
<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing"
    xmlns:s="http://www.w3.org/2003/05/soap-envelope">
    <s:Header xmlns:s="http://www.w3.org/2003/05/soap-envelope">
        <wsse:Security xmlns:wsse=http://docs.oasis-open.org/wss/2004/01/
oasis-200401-wss-wssecurity-secext-1.0.xsd xmlns:wsu="http://docs.oasis-open.org/
wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" soap:mustUnderstand="true">
            <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                xmlns:xsd="http://www.w3.org/2001/XMLSchema"
ID="_a7dc0f5d-5300-4fac-80a5-5c6d08b808c3" IssueInstant="2018-10-30T08:11:47.187Z"
Version="2.0">
                <saml2:Issuer>xds-bridge-xua-proxy</saml2:Issuer>
                <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                    <ds:SignedInfo>
                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/
2001/10/xml-exc-c14n#"/>
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#rsa-sha1"/>
                        <ds:Reference URI="#_a7dc0f5d-5300-4fac-80a5-5c6d08b808c3">
                            <ds:Transforms>
                                <ds:Transform Algorithm="http://www.w3.org/2000/09/
xmldsig#enveloped-signature"/>
                                <ds:Transform Algorithm="http://www.w3.org/2001/10/
xml-exc-c14n#">
                                    <ec:InclusiveNamespaces xmlns:ec="http://
www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd"/>
                                </ds:Transform>
                            </ds:Transforms>
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#sha1"/>
                            <ds:DigestValue>u0aMCbaPxaD3NKUcm9RTKJ8nYu0=</
ds:DigestValue>
                        </ds:Reference>
                    </ds:SignedInfo>

<ds:SignatureValue>ca4w0ETLyPgQHWjUQS8FFTzNNrjt5fZ5+5LFWrao11H354IwHw0CksI8qD/
GVZ6pkmbkwNPZV8Pf DlGsvzDstsytnSB7/8PNVberVJVehg7CwC/
nd3SoL7aRpj96c8yxL9gaUDrU3EzoPy4j9Vb2UbF2
W8EXATeosHJjPTTnsnBGHVYBRfarqAv32Ll99cTG4fN03Vlz+IJAp/qBofD2Mgz0iJRoucwqjOes
9O5I8qRB60CIhEd7Z/P8X3hRNZULQQoZn8AyRHdoqY/AgLLUKE/JUQsxYKa3BbGJw7JmFPtI7I4c
+wlM577HcMbfq8VjeS31QL8Pzj48rQV4AnsS9w==</ds:SignatureValue>
                    <ds:KeyInfo>
                        <ds:X509Data>
```

```
<ds:X509Certificate>MIIDyzCCArMCAQEwDQYJKoZIhvcNAQELBQAwgasxCzAJBgNVBAYTAk5MMRUwEwYD
VQQIDAxadWlk
LUhvbGxhbmQxHzAdBgNVBAcMFkNhcGVsbGUgYWFuIGRlbiBJSnNzZWwxGjAYBgNVBAoMEVZBTkFE
IEhlYWx0aCBDYXJlMRQwEgYDVQQLDAtEZXZlbG9wbWVudDELMAkGA1UEAwwCY2ExJTAjBgkqhkiG
9w0BCQEWFnhkc3RlYW1AdmFuYWRncm91cC5jb20wHhcNMTcxMTI4MTQyMzM5WhcNMTgxMTI4MTQy
MzM5WjCBqjELMAkGA1UEBhMCTkwxFTATBgNVBAgMDFp1aWQtSG9sbGFuZDEfMB0GA1UEBwwWQ2Fw
ZWxsZSBhYW4gZGVuIElkc3NlbDEaMBgGA1UECgwRVkFOQUQgSGVhbHRoIENhcmUxFDASBgNVBAsM
C0RldmVsb3BtZW50MQowCAYDVQQDDAF4MSUwIwYJKoZIhvcNAQkBFhZ4ZHN0ZWFtQHZhbmFkZ3Jv
dXAuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuv+sbPxoGUh3H2FUBr3dnBEZ
fUSMqbD/2rrADDrMZVh/RqZ+oBeQhOuD0enWt5+IMA/eZ4d8g5qUiU8gXAdpJ/49A7+kFZOL82jd
zwga/XP2WPBLucmjw9rwjM3clHdWRdFsjF5Iw+NVo8cmY7Vebi673q7mWPIKY4vdFC2UBNQtblot
YnswbvoQHRhXaTKjQ/zEp6viK/gD+o32ee0MSn/0d0jKhMVufvR1P3tzwAQnK6J/i5fDI3QnghKx
5KC7IHETv0/qskSTYQge40GJtjtOpgrP1xTEII2TnadBVevyBPdes4Wi/5RLYxpj8aWDNUXzRbcj
HTRPDx5FUnOHGwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQARV+dsvKrfU1w46a3LTiAWn+V2Fx3c
1kHyj8FkOLFouHp8H/55nhOFlW7qskWHiILuEA7HN29kO+JenNUF0V9K2wrNV5tEMrvTKIFqXOxu
VwO5Vu0tHE43VGNdbucuR2zD3irmsIpLdwDxkN/9NPMEBPLYu4g7+v896EM5c/3uJtaBfP0ufOGv
Abx+nEBlGyTuMUPbgstTvwT/Tvkc0YFzIuz7wNAaWpkELd6Hj+9r/DMzbNshjKTs0WK9wffQxphJ
NI4LW1L5LF6W84HQFGrP9+gwODLAHQ4bBKIOWXDxPXyLeMwjbm5hCKB/PE1oMu84iFsQwSzcPERz
HbXy1EJU</ds:X509Certificate>
                        </ds:X509Data>
                    </ds:KeyInfo>
                </ds:Signature>
                <saml2:Subject>
                    <saml2:NameID SPProvidedID="Anton Bibber">anton@ziekenhuis.nl</
saml2:NameID>
                    <saml2:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
                </saml2:Subject>
                <saml2:Conditions NotBefore="2018-10-30T08:11:47.187Z"
NotOnOrAfter="2018-10-30T09:11:47.187Z">
                    <saml2:AudienceRestriction>
                        <saml2:Audience>OTV-ABB-REGISTER</saml2:Audience>
                    </saml2:AudienceRestriction>
                </saml2:Conditions>
                <saml2:AuthnStatement AuthnInstant="2018-10-30T08:11:47.187Z">
                    <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</
saml2:AuthnContextClassRef>
                    </saml2:AuthnContext>
                </saml2:AuthnStatement>
                <saml2:AttributeStatement>
                    <!-- Beroepsgroep verantwoordelijke zorgverlener -->
```

```
                    <saml2:Attribute
Name="urn:oasis:names:tc:xacml:2.0:subject:role">
                        <saml2:AttributeValue>
                            <Role xmlns="urn:hl7-org:v3"
                                xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
code="01.013" codeSystem="2.16.840.1.113883.2.4.15.111" codeSystemName="RoleCodeNL"
originalText="Arts v. maag-darm-leverziekten" xsi:type="CE"/>
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                    <!-- Identificatienummer Verantwoordelijke -->
                    <saml2:Attribute Name="urn:ihe:iti:xua:2017:subject:provider-
identifier">
                        <saml2:AttributeValue>
                            <id xmlns="urn:hl7-org:v3"
                                xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" assigningAuthorityName="CIBG" displayable="true" extension="123456782"
root="2.16.528.1.1007.3.1" xsi:type="II"/>
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                    <!-- Identificatienummer Raadpleger -->
                    <saml2:Attribute
Name="urn:nl:otv:names:tc:1.0:subject:mandated">
                        <saml2:AttributeValue>
                            <id xmlns="urn:hl7-org:v3"
                                xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" assigningAuthorityName="CIBG" displayable="true" extension="123456789"
root="2.16.528.1.1007.3.1" xsi:type="II"/>
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                    <!–Raadplegende organisatieID -->
                    <saml2:Attribute Name="urn:nl:otv:names:tc:1.0:subject:provider-
institution">
                        <saml2:AttributeValue DataType="urn:hl7-org:v3#II">
                            <InstanceIdentifier xmlns="urn:hl7-org:v3"
extension="00014332" root=" 2.16.528.1.1007.3.3" />
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                    <!-- Raadpleegsituatie -->
                    <saml2:Attribute
Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
                        <saml2:AttributeValue>
                            <saml2:AttributeValue DataType=" urn:hl7-org:v3#CV">
                                <CodedValue xmlns="urn:hl7-org:v3" code="TREAT"
codeSystem="2.16.840.1.113883.1.11.20448" displayName="treatment" />
                            </saml2:AttributeValue>
```

```
                        </saml2:Attribute>
                    </saml2:AttributeStatement>
                </saml2:Assertion>
            </wsse:Security>
            <a:Action s:mustUnderstand="1">urn:ihe:iti:2007:CrossGatewayQuery</
a:Action>
            <a:MessageID>urn:uuid:ba8fc617-bcd1-467b-b1f7-87957a7ad16f</a:MessageID>
            <a:ReplyTo>
                <a:Address>http://www.w3.org/2005/08/addressing/anonymous</
a:Address>
            </a:ReplyTo>
            <a:To s:mustUnderstand="1">http://testing.interoplab.eu:8080/
interoplab__responding_gateway/rg/xcq</a:To>
        </s:Header>
        <s:Body xmlns:s="http://www.w3.org/2003/05/soap-envelope">
            <query:AdhocQueryRequest xmlns:lcm="urn:oasis:names:tc:ebxml-
regrep:xsd:lcm:3.0"
                xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
                xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
                xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
                xmlns:xdsb="urn:ihe:iti:xds-b:2007"
                xmlns:xop="http://www.w3.org/2004/08/xop/include">
                <query:ResponseOption returnComposedObjects="true"
returnType="LeafClass"></query:ResponseOption>
                <rim:AdhocQuery home="1.1.4567334.1.4"
id="urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d">
                    <rim:Slot name="$XDSDocumentEntryPatientId">
                        <rim:ValueList>

<rim:Value>'999999011^^^&2.16.840.1.113883.2.4.6.3&ISO'</rim:Value>
                        </rim:ValueList>
                    </rim:Slot>
                    <rim:Slot name="$XDSDocumentEntryStatus">
                        <rim:ValueList>
                            <rim:Value>('urn:oasis:names:tc:ebxml-
regrep:StatusType:Approved')</rim:Value>
                        </rim:ValueList>
                    </rim:Slot>
                    <rim:Slot name="$XDSDocumentEntryEventCodeList">
                        <rim:ValueList>
                            <rim:Value>('CT^^1.2.840.10008.2.16.4')</rim:Value>
                        </rim:ValueList>
                    </rim:Slot>
                    <rim:Slot name="$XDSDocumentEntryPracticeSettingCode">
                        <rim:ValueList>
```

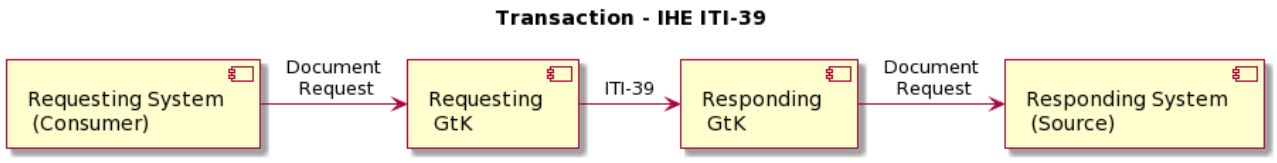
```
                            <rim:Value>('309964003^^2.16.840.1.113883.6.96')</
rim:Value>
                        </rim:ValueList>
                    </rim:Slot>
                </rim:AdhocQuery>
            </query:AdhocQueryRequest>
        </s:Body>
    </s:Envelope>
```

10.5.8 | IHE ITI-39 | Cross Gateway Retrieve

Scope

This transaction is used by the Requesting GtK to retrieve one of more documents from the Responding GtK.

Use Case Roles



> This transaction uses SOAP v1.2 and Synchronous Web Services.

Referenced standards

Implementers of this transaction shall comply with all requirements described in Web Services for IHE Transactions.[56]

ebRIM	OASIS/ebXML Registry Information Model v3.0
ebRS	OASIS/ebXML Registry Services Specifications v3.0
ITI TF-3:4	Metadata used in Document Sharing profiles

56. https://profiles.ihe.net/ITI/TF/Volume2/ch-V.html#Appendix%20V

MTOM	SOAP Message Transmission Optimization Mechanism http://www.w3.org/TR/soap12-mtom/

Messages

Cross Gateway Retrieve

> For more technical specification, see the original document: https://profiles.ihe.net/ITI/TF/Volume2/ITI-39.html

NB: This transaction is always performed in combination with the transaction ITI-40 (see page 265) where user data is added in a SAML token.
NB: All transactions are logged with an ITI-20 audit transaction, see IHE:ITI volume 2 for the correct implementation."

10.5.8.1 | ITI-39 examples

> For reference only

ITI-39 request

In the example below, two documents are retrieved

```
<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing"
    xmlns:s="http://www.w3.org/2003/05/soap-envelope">
    <s:Header>
        <a:Action s:mustUnderstand="1">urn:ihe:iti:2007:RetrieveDocumentSet</
a:Action>
        <a:MessageID>urn:uuid:6d090619-abb5-4758-8146-f71a9e1868a4</a:MessageID>
        <a:ReplyTo>
            <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
        </a:ReplyTo>
        <a:To s:mustUnderstand="1">http://testing.interoplab.eu:8080/
interoplab__repository/rep/ret</a:To>
    </s:Header>
    <s:Body>
        <xdsb:RetrieveDocumentSetRequest xmlns:lcm="urn:oasis:names:tc:ebxml-
regrep:xsd:lcm:3.0"
            xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
            xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
            xmlns:xdsb="urn:ihe:iti:xds-b:2007"
            xmlns:xop="http://www.w3.org/2004/08/xop/include">
            <xdsb:DocumentRequest>
                <xdsb:HomeCommunityId>urn:oid:1.1.4567334.1.4</xdsb:HomeCommunityId>
                <xdsb:RepositoryUniqueId>1.1.4567332.1.1</xdsb:RepositoryUniqueId>
                <xdsb:DocumentUniqueId>1.3.6.1.4.1.12559.11.13.2.1.227</
xdsb:DocumentUniqueId>
            </xdsb:DocumentRequest>
            <xdsb:DocumentRequest>
                <xdsb:HomeCommunityId>urn:oid:1.1.4567334.1.4</xdsb:HomeCommunityId>
                <xdsb:RepositoryUniqueId>1.1.4567332.1.1</xdsb:RepositoryUniqueId>
                <xdsb:DocumentUniqueId>1.3.6.1.4.1.12559.11.13.2.1.231</
xdsb:DocumentUniqueId>
            </xdsb:DocumentRequest>
        </xdsb:RetrieveDocumentSetRequest>
    </s:Body>
</s:Envelope>
```

ITI-39 response

In the example below, the response shows a DICOM object (KOS). The multipart is not shown in the example.

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
    <soap:Header>
        <Action xmlns="http://www.w3.org/2005/08/
addressing">urn:ihe:iti:2007:CrossGatewayRetrieveResponse</Action>
        <MessageID xmlns="http://www.w3.org/2005/08/
addressing">urn:uuid:818cf943-1127-47b9-b5d7-16feedac311b</MessageID>
        <To xmlns="http://www.w3.org/2005/08/addressing">http://www.w3.org/2005/08/
addressing/anonymous</To>
        <RelatesTo xmlns="http://www.w3.org/2005/08/addressing">uuid:353219ca-
e86a-4590-b49a-3587dd7394ed</RelatesTo>
    </soap:Header>
    <soap:Body>
        <ns2:RetrieveDocumentSetResponse xmlns:ns6="urn:oasis:names:tc:ebxml-
regrep:xsd:lcm:3.0"
            xmlns:ns5="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
            xmlns:ns4="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
            xmlns:ns3="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
            xmlns:ns2="urn:ihe:iti:xds-b:2007">
            <ns4:RegistryResponse status="urn:oasis:names:tc:ebxml-
regrep:ResponseStatusType:Success"/>
            <ns2:DocumentResponse>
                <ns2:RepositoryUniqueId>1.3.6.1.4.1.12559.11.34.1.3.1</
ns2:RepositoryUniqueId>
                <ns2:DocumentUniqueId>2.25.329127271855121542029064767251061713151</
ns2:DocumentUniqueId>
                <ns2:NewRepositoryUniqueId>1.3.6.1.4.1.12559.11.34.1.3.1</
ns2:NewRepositoryUniqueId>

<ns2:NewDocumentUniqueId>2.25.329127271855121542029064767251061713151</
ns2:NewDocumentUniqueId>
                <ns2:mimeType>application/dicom</ns2:mimeType>
                <ns2:Document>
                    <xop:Include xmlns:xop="http://www.w3.org/2004/08/xop/include"
href="cid:a404d989-33e5-4bf9-bbf0-e3e8cafab474-1@urn%3Aihe%3Aiti%3Axds-b%3A2007"/>
                </ns2:Document>
            </ns2:DocumentResponse>
        </ns2:RetrieveDocumentSetResponse>
    </soap:Body>
</soap:Envelope>
```

ITI-39 request including SAML-Token

```
<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing"
    xmlns:s="http://www.w3.org/2003/05/soap-envelope">
    <s:Header>
        <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
            xmlns:xsd="http://www.w3.org/2001/XMLSchema"
ID="_a7dc0f5d-5300-4fac-80a5-5c6d08b808c3" IssueInstant="2018-10-30T08:11:47.187Z"
Version="2.0">
            <saml2:Issuer>xds-bridge-xua-proxy</saml2:Issuer>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/
xml-exc-c14n#"/>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#_a7dc0f5d-5300-4fac-80a5-5c6d08b808c3">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2000/09/
xmldsig#enveloped-signature"/>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#">
                                <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/
2001/10/xml-exc-c14n#" PrefixList="xsd"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#sha1"/>
                        <ds:DigestValue>u0aMCbaPxaD3NKUcm9RTKJ8nYu0=</
ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>

<ds:SignatureValue>ca4w0ETLyPgQHWjUQS8FFTzNNrjt5fZ5+5LFWrao11H354IwHw0CksI8qD/
GVZ6pkmbkwNPZV8Pf DlGsvzDstsytnSB7/8PNVberVJVehg7CwC/
nd3SoL7aRpj96c8yxL9gaUDrU3EzoPy4j9Vb2UbF2
W8EXATeosHJjPTTnsnBGHVYBRfarqAv32Ll99cTG4fN03Vlz+IJAp/qBofD2Mgz0iJRoucwqjOes
9O5I8qRB60CIhEd7Z/P8X3hRNZULQQoZn8AyRHdoqY/AgLLUKE/JUQsxYKa3BbGJw7JmFPtI7I4c
+wlM577HcMbfq8VjeS31QL8Pzj48rQV4AnsS9w==</ds:SignatureValue>
                <ds:KeyInfo>
                    <ds:X509Data>

<ds:X509Certificate>MIIDyzCCArMCAQEwDQYJKoZIhvcNAQELBQAwgasxCzAJBgNVBAYTAk5MMRUwEwYD
VQQIDAxadWlk
```

```
LUhvbGxhbmQxHzAdBgNVBAcMFkNhcGVsbGUgYWFuIGRlbiBJSnNzZWwxGjAYBgNVBAoMEVZBTkFE
IEhlYWx0aCBDYXJlMRQwEgYDVQQLDAtEZXZlbG9wbWVudDELMAkGA1UEAwwCY2ExJTAjBgkqhkiG
9w0BCQEWFnhkc3RlYW1AdmFuYWRncm91cC5jb20wHhcNMTcxMTI4MTQyMzM5WhcNMTgxMTI4MTQy
MzM5WjCBqjELMAkGA1UEBhMCTkwxFTATBgNVBAgMDFp1aWQtSG9sbGFuZDEfMB0GA1UEBwwWQ2Fw
ZWxsZSBhYW4gZGVuIElkKc3NlbDEaMBgGA1UECgwRVkFOQUQgSGVhbHRoIENhcmUxFDASBgNVBAsM
C0RldmVsb3BtZW50MQowCAYDVQQDDAF4MSUwIwYJKoZIhvcNAQkBFhZ4ZHN0ZWFtQHZhbmFkZ3Jv
dXAuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuv+sbPxoGUh3H2FUBr3dnBEZ
fUSMqbD/2rrADDrMZVh/RqZ+oBeQhOuD0enWt5+IMA/eZ4d8g5qUiU8gXAdpJ/49A7+kFZOL82jd
zwga/XP2WPBLucmjw9rwjM3clHdWRdFsjF5Iw+NVo8cmY7Vebi673q7mWPIKY4vdFC2UBNQtblot
YnswbvoQHRhXaTKjQ/zEp6viK/gD+o32ee0MSn/0d0jKhMVufvR1P3tzwAQnK6J/i5fDI3QnghKx
5KC7IHETv0/qskSTYQge40GJtjtOpgrP1xTEII2TnadBVevyBPdes4Wi/5RLYxpj8aWDNUXzRbcj
HTRPDx5FUnOHGwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQARV+dsvKrfU1w46a3LTiAWn+V2Fx3c
1kHyj8FkOLFouHp8H/55nhOFlW7qskWHiILuEA7HN29kO+JenNUF0V9K2wrNV5tEMrvTKIFqXOxu
VwO5Vu0tHE43VGNdbucuR2zD3irmsIpLdwDxkN/9NPMEBPLYu4g7+v896EM5c/3uJtaBfP0ufOGv
Abx+nEBlGyTuMUPbgstTvwT/Tvkc0YFzIuz7wNAaWpkELd6Hj+9r/DMzbNshjKTs0WK9wffQxphJ
NI4LW1L5LF6W84HQFGrP9+gwODLAHQ4bBKIOWXDxPXyLeMwjbm5hCKB/PE1oMu84iFsQwSzcPERz
HbXy1EJU</ds:X509Certificate>
                    </ds:X509Data>
                </ds:KeyInfo>
            </ds:Signature>
            <saml2:Subject>
                <saml2:NameID SPProvidedID="Anton Bibber">anton@ziekenhuis.nl</
saml2:NameID>
                <saml2:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
            </saml2:Subject>
            <saml2:Conditions NotBefore="2018-10-30T08:11:47.187Z"
NotOnOrAfter="2018-10-30T09:11:47.187Z">
                <saml2:AudienceRestriction>
                    <saml2:Audience>OTV-ABB-REGISTER</saml2:Audience>
                </saml2:AudienceRestriction>
            </saml2:Conditions>
            <saml2:AuthnStatement AuthnInstant="2018-10-30T08:11:47.187Z">
                <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</
saml2:AuthnContextClassRef>
                </saml2:AuthnContext>
            </saml2:AuthnStatement>
            <saml2:AttributeStatement>
                <!-- Beroepsgroep verantwoordelijke zorgverlener -->
                <saml2:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">
                    <saml2:AttributeValue>
                        <Role xmlns="urn:hl7-org:v3"
```

```
                        xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
code="01.013" codeSystem="2.16.840.1.113883.2.4.15.111" codeSystemName="RoleCodeNL"
originalText="Arts v. maag-darm-leverziekten" xsi:type="CE"/>
                    </saml2:AttributeValue>
                </saml2:Attribute>
                <!-- Identificatienummer Verantwoordelijke -->
                <saml2:Attribute Name="urn:ihe:iti:xua:2017:subject:provider-
identifier">
                    <saml2:AttributeValue>
                        <id xmlns="urn:hl7-org:v3"
                            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
assigningAuthorityName="CIBG" displayable="true" extension="123456782"
root="2.16.528.1.1007.3.1" xsi:type="II"/>
                    </saml2:AttributeValue>
                </saml2:Attribute>
                <!-- Identificatienummer Raadpleger -->
                <saml2:Attribute Name="urn:nl:otv:names:tc:1.0:subject:mandated">
                    <saml2:AttributeValue>
                        <id xmlns="urn:hl7-org:v3"
                            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
assigningAuthorityName="CIBG" displayable="true" extension="123456789"
root="2.16.528.1.1007.3.1" xsi:type="II"/>
                    </saml2:AttributeValue>
                </saml2:Attribute>
                <!–Raadplegende organisatieID -->
                <saml2:Attribute Name="urn:nl:otv:names:tc:1.0:subject:provider-
institution">
                    <saml2:AttributeValue DataType="urn:hl7-org:v3#II">
                        <InstanceIdentifier xmlns="urn:hl7-org:v3"
extension="00014332" root=" 2.16.528.1.1007.3.3" />
                    </saml2:AttributeValue>
                </saml2:Attribute>
                <!-- Raadpleegsituatie -->
                <saml2:Attribute
Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
                    <saml2:AttributeValue>
                        <saml2:AttributeValue DataType=" urn:hl7-org:v3#CV">
                            <CodedValue xmlns="urn:hl7-org:v3"code="TREAT"
codeSystem="2.16.840.1.113883.1.11.20448" displayName="treatment" />
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                </saml2:AttributeStatement>
            </saml2:Assertion>
        </wsse:Security>
```

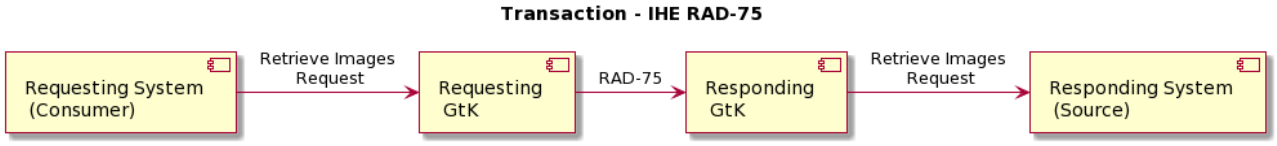
```
        <a:Action s:mustUnderstand="1">urn:ihe:iti:2007:RetrieveDocumentSet</
a:Action>
        <a:MessageID>urn:uuid:6d090619-abb5-4758-8146-f71a9e1868a4</a:MessageID>
        <a:ReplyTo>
            <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
        </a:ReplyTo>
        <a:To s:mustUnderstand="1">http://testing.interoplab.eu:8080/
interoplab__repository/rep/ret</a:To>
    </s:Header>
    <s:Body>
        <xdsb:RetrieveDocumentSetRequest xmlns:lcm="urn:oasis:names:tc:ebxml-
regrep:xsd:lcm:3.0"
            xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
            xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
            xmlns:xdsb="urn:ihe:iti:xds-b:2007"
            xmlns:xop="http://www.w3.org/2004/08/xop/include">
            <xdsb:DocumentRequest>
                <xdsb:HomeCommunityId>urn:oid:1.1.4567334.1.4</xdsb:HomeCommunityId>
                <xdsb:RepositoryUniqueId>1.1.4567332.1.1</xdsb:RepositoryUniqueId>
                <xdsb:DocumentUniqueId>1.3.6.1.4.1.12559.11.13.2.1.227</
xdsb:DocumentUniqueId>
            </xdsb:DocumentRequest>
            <xdsb:DocumentRequest>
                <xdsb:HomeCommunityId>urn:oid:1.1.4567334.1.4</xdsb:HomeCommunityId>
                <xdsb:RepositoryUniqueId>1.1.4567332.1.1</xdsb:RepositoryUniqueId>
                <xdsb:DocumentUniqueId>1.3.6.1.4.1.12559.11.13.2.1.231</
xdsb:DocumentUniqueId>
            </xdsb:DocumentRequest>
        </xdsb:RetrieveDocumentSetRequest>
    </s:Body>
</s:Envelope>
```

10.5.9 | IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set

Scope

This transaction is used by the Requesting GtK to retrieve images from sources behind Responding GtK's. Prior to this transaction, the '10.5.7 | IHE ITI-38 | Cross Gateway Query (see page 237) is used for the necessary information (specifically the metadata of the KOS Objects and the KOS objects of the set of images to be requested)

Use Case Roles



This transaction uses SOAP v1.2 and Synchronous Web Services.

Referenced standards

Implementers of this transaction shall comply with all requirements described in Web Services for IHE Transactions.[57]

ebRIM	OASIS/ebXML Registry Information Model v3.0
ebRS	OASIS/ebXML Registry Services Specifications v3.0
ITI TF-3:4	Metadata in Document Sharing profiles
MTOM	SOAP Message Transmission Optimization Mechanism http://www.w3.org/TR/soap12-mtom/
XOP	XML-binary Optimized Packaging http://www.w3.org/TR/2005/REC-xop10-20050125/

Messages

Cross Gateway Retrieve Imaging Document Set

For more technical specification, see the original document: https://www.ihe.net/uploadedFiles/Documents/Radiology/IHE_RAD_TF_Vol3.pdf

NB: This transaction is always performed in combination with the transaction ITI-40 where user data is added in a SAML token.

57. https://profiles.ihe.net/ITI/TF/Volume2/ch-V.html#Appendix%20V

NB: All transactions are logged with an ITI-20 audit transaction, see IHE:ITI volume 2 for the correct implementation."

10.5.9 | RAD-75 examples

> For reference only

RAD-75 request

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope"
    xmlns:enc="http://www.w3.org/2003/05/soap-encoding">
    <env:Header>
        <Action xmlns="http://www.w3.org/2005/08/
addressing">urn:ihe:rad:2009:RetrieveImagingDocumentSet</Action>
        <To xmlns="http://www.w3.org/2005/08/addressing">http://
xtdchixjenkins01:8086/XCAI</To>
        <MessageID xmlns="http://www.w3.org/2005/08/
addressing">urn:uuid:ab70c66b-7f7f-42d1-bfac-e2afcc4ad6f2</MessageID>
        <ReplyTo xmlns="http://www.w3.org/2005/08/addressing"
            xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
soapenv:mustUnderstand="1">
            <wsa:Address xmlns:wsa="http://www.w3.org/2005/08/addressing">http://
www.w3.org/2005/08/addressing/anonymous</wsa:Address>
        </ReplyTo>
        <Security xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"/>
    </env:Header>
    <env:Body>
        <ns3:RetrieveImagingDocumentSetRequest xmlns:ns2="urn:ihe:iti:xds-b:2007"
            xmlns:ns3="urn:ihe:rad:xdsi-b:2009">
            <ns3:StudyRequest studyInstanceUID="21">
                <ns3:SeriesRequest seriesInstanceUID="22">
                    <ns2:DocumentRequest>
                        <ns2:HomeCommunityId>urn:oid:1.2.34.567.8.6</
ns2:HomeCommunityId>
                        <ns2:RepositoryUniqueId>23</ns2:RepositoryUniqueId>
                        <ns2:DocumentUniqueId>24</ns2:DocumentUniqueId>
                    </ns2:DocumentRequest>
                </ns3:SeriesRequest>
            </ns3:StudyRequest>
            <ns3:TransferSyntaxUIDList>
                <ns3:TransferSyntaxUID>6</ns3:TransferSyntaxUID>
            </ns3:TransferSyntaxUIDList>
        </ns3:RetrieveImagingDocumentSetRequest>
    </env:Body>
</env:Envelope>
```

RAD-75 response

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
    <soap:Header>
        <Action xmlns="http://www.w3.org/2005/08/
addressing">urn:ihe:rad:2011:CrossGatewayRetrieveImagingDocumentSetResponse</Action>
        <MessageID xmlns="http://www.w3.org/2005/08/
addressing">urn:uuid:8f62a0f3-1906-4b32-9b22-e37585fb4cc5</MessageID>
        <To xmlns="http://www.w3.org/2005/08/addressing">http://www.w3.org/2005/08/
addressing/anonymous</To>
        <RelatesTo xmlns="http://www.w3.org/2005/08/
addressing">uuid:abb813bb-9c7b-48ec-a26f-6779b219cccf</RelatesTo>
    </soap:Header>
    <soap:Body>
        <RetrieveDocumentSetResponse xmlns="urn:ihe:iti:xds-b:2007"
            xmlns:ns6="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
            xmlns:ns5="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0"
            xmlns:ns2="urn:ihe:rad:xdsi-b:2009"
            xmlns:ns4="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
            xmlns:ns3="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
            <ns4:RegistryResponse status="urn:oasis:names:tc:ebxml-
regrep:ResponseStatusType:Success"/>
            <DocumentResponse>
                <HomeCommunityId>urn:oid:1.3.6.1.4.1.21367.2011.2.6.169</
HomeCommunityId>
                <RepositoryUniqueId>1.3.6.1.4.1.21367.2011.2.1.304</
RepositoryUniqueId>

<DocumentUniqueId>1.2.40.0.13.1.1.192.168.0.2.20060712144818517.32770</
DocumentUniqueId>
                <mimeType>application/dicom</mimeType>
                <Document>
                    <xop:Include xmlns:xop="http://www.w3.org/2004/08/xop/include"
href="cid:02efdfb6-377b-4adf-a1f5-b78c5b16fad1-10@urn%3Aihe%3Aiti%3Axds-b%3A2007"/>
                </Document>
            </DocumentResponse>
        </RetrieveDocumentSetResponse>
    </soap:Body>
</soap:Envelope>
```

RAD-75 request incl. SAML-token

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope"
    xmlns:enc="http://www.w3.org/2003/05/soap-encoding">
    <env:Header>
        <Action xmlns="http://www.w3.org/2005/08/
addressing">urn:ihe:rad:2009:RetrieveImagingDocumentSet</Action>
        <To xmlns="http://www.w3.org/2005/08/addressing">http://
xtdchixjenkins01:8086/XCAI</To>
        <MessageID xmlns="http://www.w3.org/2005/08/
addressing">urn:uuid:ab70c66b-7f7f-42d1-bfac-e2afcc4ad6f2</MessageID>
        <ReplyTo xmlns="http://www.w3.org/2005/08/addressing"
            xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
soapenv:mustUnderstand="1">
            <wsa:Address xmlns:wsa="http://www.w3.org/2005/08/addressing">http://
www.w3.org/2005/08/addressing/anonymous</wsa:Address>
        </ReplyTo>
        <wsse:Security xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-secext-1.0.xsd">
            <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                xmlns:xsd="http://www.w3.org/2001/XMLSchema"
ID="_a7dc0f5d-5300-4fac-80a5-5c6d08b808c3" IssueInstant="2018-10-30T08:11:47.187Z"
Version="2.0">
                <saml2:Issuer>xds-bridge-xua-proxy</saml2:Issuer>
                <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                    <ds:SignedInfo>
                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/
2001/10/xml-exc-c14n#"/>
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#rsa-sha1"/>
                        <ds:Reference URI="#_a7dc0f5d-5300-4fac-80a5-5c6d08b808c3">
                            <ds:Transforms>
                                <ds:Transform Algorithm="http://www.w3.org/2000/09/
xmldsig#enveloped-signature"/>
                                <ds:Transform Algorithm="http://www.w3.org/2001/10/
xml-exc-c14n#">
                                    <ec:InclusiveNamespaces xmlns:ec="http://
www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd"/>
                                </ds:Transform>
                            </ds:Transforms>
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#sha1"/>
                            <ds:DigestValue>u0aMCbaPxaD3NKUcm9RTKJ8nYu0=</
ds:DigestValue>
```

```
                        </ds:Reference>
                    </ds:SignedInfo>

<ds:SignatureValue>ca4w0ETLyPgQHWjUQS8FFTzNNrjt5fZ5+5LFWrao11H354IwHw0CksI8qD/
GVZ6pkmbkwNPZV8Pf DlGsvzDstsytnSB7/8PNVberVJVehg7CwC/
nd3SoL7aRpj96c8yxL9gaUDrU3EzoPy4j9Vb2UbF2
W8EXATeosHJjPTTnsnBGHVYBRfarqAv32Ll99cTG4fN03Vlz+IJAp/qBofD2Mgz0iJRoucwqjOes
9O5I8qRB60CIhEd7Z/P8X3hRNZULQQoZn8AyRHdoqY/AgLLUKE/JUQsxYKa3BbGJw7JmFPtI7I4c
+wlM577HcMbfq8VjeS31QL8Pzj48rQV4AnsS9w==</ds:SignatureValue>
                    <ds:KeyInfo>
                        <ds:X509Data>

<ds:X509Certificate>MIIDyzCCArMCAQEwDQYJKoZIhvcNAQELBQAwgasxCzAJBgNVBAYTAk5MMRUwEwYD
VQQIDAxadWlk
LUhvbGxhbmQxHzAdBgNVBAcMFkNhcGVsbGUgYWFuIGRlbiBJSnNzZWwxGjAYBgNVBAoMEVZBTkFE
IEhlYWx0aCBDYXJlMRQwEgYDVQQLDAtEZXZlbG9wbWVudDELMAkGA1UEAwwCY2ExJTAjBgkqhkiG
9w0BCQEWFnhkc3RlYW1AdmFuYWRncm91cC5jb20wHhcNMTcxMTI4MTQyMzM5WhcNMTgxMTI4MTQy
MzM5WjCBqjELMAkGA1UEBhMCTkwxFTATBgNVBAgMDFp1aWQtSG9sbGFuZDEfMB0GA1UEBwwWQ2Fw
ZWxsZSBhYW4gZGVuIElKc3NlbDEaMBgGA1UECgwRVkFOQUQgSGVhbHRoIENhcmUxFDASBgNVBAsM
C0RldmVsb3BtZW50MQowCAYDVQQDDAF4MSUwIwYJKoZIhvcNAQkBFhZ4ZHN0ZWFtQHZhbmFkZ3Jv
dXAuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuv+sbPxoGUh3H2FUBr3dnBEZ
fUSMqbD/2rrADDrMZVh/RqZ+oBeQhOuD0enWt5+IMA/eZ4d8g5qUiU8gXAdpJ/49A7+kFZOL82jd
zwga/XP2WPBLucmjw9rwjM3clHdWRdFsjF5Iw+NVo8cmY7Vebi673q7mWPIKY4vdFC2UBNQtblot
YnswbvoQHRhXaTKjQ/zEp6viK/gD+o32ee0MSn/0d0jKhMVufvR1P3tzwAQnK6J/i5fDI3QnghKx
5KC7IHETv0/qskSTYQge40GJtjtOpgrP1xTEII2TnadBVevyBPdes4Wi/5RLYxpj8aWDNUXzRbcj
HTRPDx5FUnOHGwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQARV+dsvKrfU1w46a3LTiAWn+V2Fx3c
1kHyj8FkOLFouHp8H/55nhOFlW7qskWHiILuEA7HN29kO+JenNUF0V9K2wrNV5tEMrvTKIFqXOxu
VwO5Vu0tHE43VGNdbucuR2zD3irmsIpLdwDxkN/9NPMEBPLYu4g7+v896EM5c/3uJtaBfP0ufOGv
Abx+nEBlGyTuMUPbgstTvwT/Tvkc0YFzIuz7wNAaWpkELd6Hj+9r/DMzbNshjKTs0WK9wffQxphJ
NI4LW1L5LF6W84HQFGrP9+gwODLAHQ4bBKIOWXDxPXyLeMwjbm5hCKB/PE1oMu84iFsQwSzcPERz
HbXy1EJU</ds:X509Certificate>
                        </ds:X509Data>
                    </ds:KeyInfo>
                </ds:Signature>
                <saml2:Subject>
                    <saml2:NameID SPProvidedID="Anton Bibber">anton@ziekenhuis.nl</
saml2:NameID>
                    <saml2:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
                </saml2:Subject>
                <saml2:Conditions NotBefore="2018-10-30T08:11:47.187Z"
NotOnOrAfter="2018-10-30T09:11:47.187Z">
                    <saml2:AudienceRestriction>
                        <saml2:Audience>OTV-ABB-REGISTER</saml2:Audience>
                    </saml2:AudienceRestriction>
```

```
                </saml2:Conditions>
                <saml2:AuthnStatement AuthnInstant="2018-10-30T08:11:47.187Z">
                    <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</
saml2:AuthnContextClassRef>
                    </saml2:AuthnContext>
                </saml2:AuthnStatement>
                <saml2:AttributeStatement>
                    <!-- Beroepsgroep verantwoordelijke zorgverlener -->
                    <saml2:Attribute
Name="urn:oasis:names:tc:xacml:2.0:subject:role">
                        <saml2:AttributeValue>
                            <Role xmlns="urn:hl7-org:v3"
                                xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
code="01.013" codeSystem="2.16.840.1.113883.2.4.15.111" codeSystemName="RoleCodeNL"
originalText="Arts v. maag-darm-leverziekten" xsi:type="CE"/>
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                    <!-- Identificatienummer Verantwoordelijke -->
                    <saml2:Attribute Name="urn:ihe:iti:xua:2017:subject:provider-
identifier">
                        <saml2:AttributeValue>
                            <id xmlns="urn:hl7-org:v3"
                                xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" assigningAuthorityName="CIBG" displayable="true" extension="123456782"
root="2.16.528.1.1007.3.1" xsi:type="II"/>
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                    <!-- Identificatienummer Raadpleger -->
                    <saml2:Attribute
Name="urn:nl:otv:names:tc:1.0:subject:mandated">
                        <saml2:AttributeValue>
                            <id xmlns="urn:hl7-org:v3"
                                xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" assigningAuthorityName="CIBG" displayable="true" extension="123456789"
root="2.16.528.1.1007.3.1" xsi:type="II"/>
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                    <!—Raadplegende organisatieID -->
                    <saml2:Attribute Name="urn:nl:otv:names:tc:1.0:subject:provider-
institution">
                        <saml2:AttributeValue DataType="urn:hl7-org:v3#II">
                            <InstanceIdentifier xmlns="urn:hl7-org:v3"
extension="00014332" root=" 2.16.528.1.1007.3.3" />
```

```
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                    <!-- Raadpleegsituatie -->
                    <saml2:Attribute
Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
                        <saml2:AttributeValue>
                            <saml2:AttributeValue DataType=" urn:hl7-org:v3#CV">
                                <CodedValue xmlns="urn:hl7-org:v3" code="TREAT"
codeSystem="2.16.840.1.113883.1.11.20448" displayName="treatment" />
                            </saml2:AttributeValue>
                        </saml2:Attribute>
                    </saml2:AttributeStatement>
                </saml2:Assertion>
            </wsse:Security>
        </env:Header>
        <env:Body>
            <ns3:RetrieveImagingDocumentSetRequest xmlns:ns2="urn:ihe:iti:xds-
b:2007"
                xmlns:ns3="urn:ihe:rad:xdsi-b:2009">
                <ns3:StudyRequest studyInstanceUID="21">
                    <ns3:SeriesRequest seriesInstanceUID="22">

<ns2:DocumentRequest>ns2:HomeCommunityId>urn:oid:1.2.34.567.8.6</
ns2:HomeCommunityId>
                        <ns2:RepositoryUniqueId>23</ns2:RepositoryUniqueId>
                        <ns2:DocumentUniqueId>24</ns2:DocumentUniqueId>
                    </ns2:DocumentRequest>
                </ns3:SeriesRequest>
            </ns3:StudyRequest>
            <ns3:TransferSyntaxUIDList>
                <ns3:TransferSyntaxUID>6</ns3:TransferSyntaxUID>
            </ns3:TransferSyntaxUIDList>
        </ns3:RetrieveImagingDocumentSetRequest>
    </env:Body>
</env:Envelope>
```

10.6 | Kern Volume 2b - Transactions - GF

Deze transacties worden binnen meerdere zorgtoepassingen gebruikt en vinden plaats tussen een GtK-applicatie en een gemeenschappelijke voorziening. De transacties staan niet inhoudelijk beschreven in dit afsprakenstelsel. Vanuit deze pagina wordt er een verwijzing gemaakt naar de gemeenschappelijke voorziening.

Voor wat betreft de transacties met de gemeenschappelijke voorzieningen:

- 10.6.5 | Addressing - ZORG-AB Transacties (see page 288)
- 10.6.3 | Patient Consent - Mitz Transacties (see page 284)

10.6.1 | Identification and Authentication

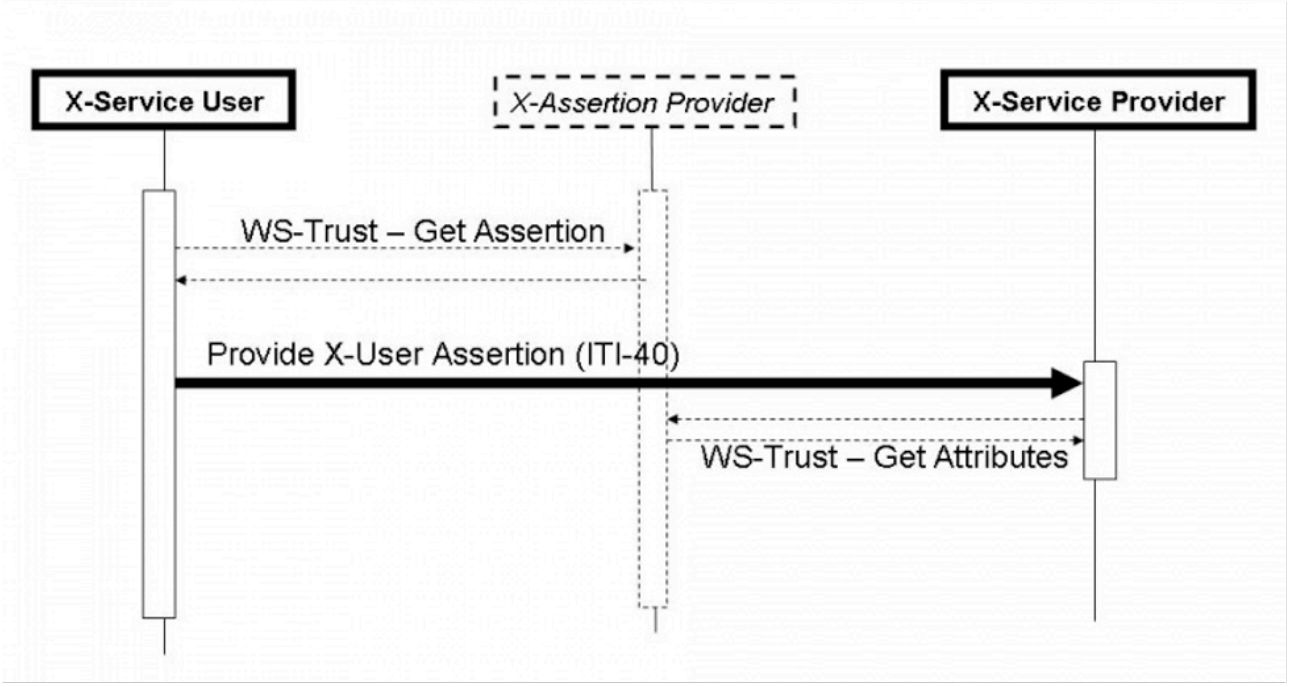
In this section the transactions needed / used by the function identification and authentication are described.

IHE ITI-40 | Provide X-User Assertion

Scope

This transaction is used to add user attributes in the SOAP TTA transactions. The attributes are placed in a SAML-token in the security header of a, for example, ITI-75 transaction.

Use Case Roles



Referenced Standards

- OASIS http://www.oasis-open.org/committees/security/
- SAMLCore[58] SAML V2.0 Core standard

58. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

- WSS10[59] OASIS Standard, "OASIS Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)", March 2004.
- WSS11[60] OASIS Standard, "OASIS Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)", February 2006.
- WSS:SAMLTokenProfile1.0[61] OASIS Standard, "Web Services Security: SAML Token Profile", December 2004
- WSS:SAMLTokenProfile1.1[62] OASIS Standard, "Web Services Security: SAML Token Profile 1.1", February 2006
- XSPA-SAMLv1.0 OASIS Standard, "Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of the Security Assertion Markup Language (SAML) for Healthcare v1.0" , November 2009
- SAML 2.0 Profile For XACML 2.0 OASIS Standard, February 2005

Informative -- assist with understanding or implementing this transaction

- IHE Profiles
  - Personnel White Pages[63] Profile
  - Enterprise User Authentication[64] Profile
  - Basic Patient Privacy Consents[65] Profile
- OASIS
  - SAML V2.0 Standards http://www.oasis-open.org/committees/security/ .
  - SAML V2.0 Technical Overview
  - SAML Executive Overview
  - SAML Tutorial presentation by Eve Maler of Sun Microsystems
  - SAML Specifications
  - WS-Trust - OASIS Web Services Secure Exchange (WS-SX) TC
  - XSPA-XACMLv1.0 OASIS Standard, "Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare v1.0" , November 2009

Messages

Provide X-User Assertion

> For more technical specification, see the original document: https://profiles.ihe.net/ITI/TF/Volume2/ITI-40.html

59. http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf
60. http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
61. http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0.pdf
62. http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf
63. https://profiles.ihe.net/ITI/TF/Volume1/ch-11.html
64. https://profiles.ihe.net/ITI/TF/Volume1/ch-4.html
65. https://profiles.ihe.net/ITI/TF/Volume1/ch-19.html

Twiin implementation

The SAML token is only valid for 10 minutes. The SAML token has the following attributes (in addition to the required attributes from the SAML-standard)

Element	Opt.	DataType
urn:nl:otv:names:tc:1.0:subject:mandated	**C**	HL7 V3 II
urn:ihe:iti:xua:2017:subject:provider-identifier	R	HL7 V3 II
urn:oasis:names:tc:xacml:2.0:subject:role	R	HL7 V3 CE
urn:ihe:iti:appc:2016:document-entry:event-code	O	HL7 V3 CV
urn:nl:otv:names:tc:1.0:subject:provider-institution	R	HL7 V3 II
urn:oasis:names:tc:xspa:1.0:subject:organization	O	String
urn:oasis:names:tc:xspa:1.0:subject:organization-id	O	anyURI
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	R	HL7 V3 CV

> The SAML token is only required in the transactions **between** GtK (external traffic).

Identification Raadpleger	
Name:	urn:nl:otv:names:tc:1.0:subject:mandated
Type:	urn:hl7-org:v3:II
Example:	`extension="123456789" root="2.16.528.1.1007.3.1" assigningAuthorityName="CIBG"`
Opt.:	**Conditional**, required if the person is mandated by the *verantwoordelijke-id.*

Identification Verantwoordelijke	
Name:	urn:ihe:iti:xua:2017:subject:provider-identifier
Type:	urn:hl7-org:v3:II
Example:	`extension="123456782" root="2.16.528.1.1007.3.1" assigningAuthorityName="CIBG"`
Opt.:	**Required,** UZI-nummer *verantwoordelijke.*

Rolcode verantwoordelijke healthcare provider	
Name:	urn:oasis:names:tc:xacml:2.0:subject:role
Type:	urn:hl7-org:v3:CE
Example:	`code="01.013" codeSystem="2.16.840.1.113883.2.4.15.111" codeSystemName="RoleCodeNL" displayName="Arts v. maag-darm-leverziekten"`
Opt.:	**Required,** UZI *rolcode*

Data category	
Name:	urn:ihe:iti:appc:2016:document-entry:event-code
Type:	urn:hl7-org:v3:CV
Example:	`code="GGC007" codeSystem="2.16.840.1.113883.2.4.3.111.5.10.1"`

Opt.:	**Optional**
Identification *verantwoordelijke* provider	
Name:	urn:nl:otv:names:tc:1.0:subject:provider-institution
Type:	urn:hl7-org:v3:II
Example:	`<AttributeValue DataType="urn:hl7-org:v3#II" ><InstanceIdentifier xmlns="urn:hl7-org:v3" extension="00014332" root="2.16.528.1.1007.3.3" /></AttributeValue>`
Opt.:	**Required, URA**
Alternative Identification *verantwoordelijke* provider	
Name:	urn:oasis:names:tc:xspa:1.0:subject:organization
Type:	String
Example:	`<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization"><saml:AttributeValue>Family Medical Clinic</saml:AttributeValue> </saml:Attribute>`
Opt.:	**Conditional, required if** urn:oasis:names:tc:xspa:1.0:subject:organization-id is not empty

Alternative Identification *verantwoordelijke* provider (id)	
Name:	urn:oasis:names:tc:xspa:1.0:subject:organization-id
Type:	AnyURI
Example:	`<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id"> <saml:AttributeValue>http://familymedicalclinic.org</ saml:AttributeValue> </saml:Attribute>`
Opt.:	**Conditional, required if** urn:oasis:names:tc:xspa:1.0:subject:organization is not empty

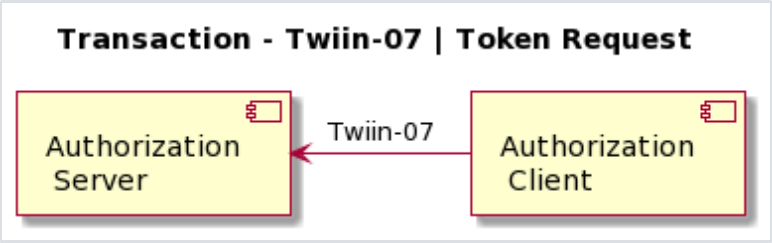
Purpose of use	
Name:	urn:oasis:names:tc:xspa:1.0:subject:purposeofuse
Type:	urn:hl7-org:v3#CV
Example:	<AttributeValue DataType=" urn:hl7-org:v3#CV"> <CodedValue xmlns="urn:hl7-org:v3" code="TREAT" codeSystem="2.16.840.1.113883.1.11.20448" displayName="treatment" /> </AttributeValue>
Opt.:	**Required**

10.6.2 | Authorization

Twiin-07 | Token Request

This page describes the transaction of the retrieval of the OAuth tokens

Scope



This transaction supports the request of an authentication token by the Requesting System to the Resource Server.

Use Case Roles

Actor: Authorization Client

Role: Client requesting an access token to authorize RESTful transactions.

Actor: Authorization Server

Role: Server that grants access tokens

Relevant Standards

- *OAuth 2.1*: The OAuth 2.1 Authorization Framework, published as draft-ietf-oauth-v2-1-01, 1 February 2021.
- *JWT Access Token*: JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens, published as draft-ietf-oauth-access-token-jwt-10, September 2020.
- *RFC4648*: The Base16, Base32, and Base64 Data Encodings, October 2006
- RFC6749: The OAuth 2.0 Authorization Framework, October 2012.
- *RFC7519*: JSON Web Token (JWT), May 2015.
- *RFC7522*: Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants, May 2015.
- *RFC7523*: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants, May 2015.
- *RFC7515*: JSON Web Signature (JWS), May 2015.
- *RFC7518*: JSON Web Algorithms (JWA), May 2015.
- *RFC8705*: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens, February 2020.

Messages

Request message

The resource server must be able to authenticate the client as a trusted client. The client is specified as the **system** that submits the access token request (not to be confused with the **organization** for which that system is acting). The OAuth specs leave room for different authentication methods for client authentication. The authentication methods that are proposed in the OAuth 2.0 core specifications (https://www.rfc-editor.org/rfc/rfc6749.html#section-2.3) all rely on the exchange of shared secrets. The use of shared secrets is considered as a security risk since they are prone to leakage. The use of an authentication method that relies on digital signatures using asymmetric cryptography offers better security. Therefore, the client must authenticate itself by providing a client assertion by means of a signed JWT as specified in https://www.rfc-editor.org/rfc/rfc7523#section-2.2.

The client assertion is a JWS Compact Serialized JWT that consists of a header, a payload, and a signature. The signature is created using a key pair belonging to the initiating system or to a third party trusted by the initiating system.

The header carries the claims listed below:

Claim	Description	Required
typ	Token type, must be “JWT”	Yes
alg	Cryptographic algorithm used to sign the client assertion. See https://www.rfc-editor.org/rfc/rfc7518#section-3.1 . All algorithms are described at Twiin-07 | Token Request.	Yes
kid	Identifier of the key pair used to sign this JWT. See https://www.rfc-editor.org/rfc/rfc7515#section-4.1.4.	Yes

The payload contains a set of claims listed below:

Claim	Description	Required

jti	Unique identifier of the client assertion. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.7. The jti (JWT ID) is a unique identifier for a token and must not be reused. An assertion containing a duplicate jti (i.e., one that has been previously processed) shall be rejected to prevent replay attacks. Implementations should maintain a mechanism to track used jti values for the duration of their validity period.	Yes
iss	Identifier of the system that issued the client assertion. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.1 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	Yes
iat	The time at which the client assertion was issued. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.6. If there is an agreed age of a client assertion.	Conditional
exp	The expiration time on or after which the client assertion shall not be accepted for processing. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.4 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3. The expiration time (exp) claim in the assertion shall not exceed 5 minutes (300 seconds) from the time of issuance. Any assertion with an exp value set beyond this limit must be rejected.	Yes
nbf	The time before which the token shall not be accepted for processing. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.5 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	No
aud	Identifier of the authorization server token endpoint where this client assertion is to be used. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.3 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	Yes

sub	Identifier of the OAuth client that requests access. This claim must match the value of the client_id parameter in the access token request. Note that the client is specified as the system that submits the access token request.	Yes

The Issuer of the client assertion may include additional claims in the assertion, but the Issuer shall not require the authorization server to process these claims.

The exchange of the public key that corresponds to the private key that was used to sign the client assertion between the Assertion Issuer and the authorization server is beyond the scope of this normative specification. This is the added value of Twiin. Twiin unambiguously describes the agreements that system providers typically need to make with each other.Note that the authorization server can authenticate the client on network level by the client certificate that the client must present during the mTLS handshake (see section Network level security (see page 206)). In theory, this could be used by the authorization server to authenticate the client on application level. However, this may cause problems since it introduces additional and potentially unwanted requirements on TLS termination and related matters. Therefore, a client must always provide a client assertion in the access token request.

Authorization grant

OAuth 2.0 requires the use of an authorization grant to request an access token. As specified in https://www.rfc-editor.org/rfc/rfc6749#section-1.3 “an authorization grant is a credential representing the resource owner's authorization (to access its protected resources) used by the client to obtain an access token.” OAuth 2.0 specifies several different authorization grants. Additionally, there are several RFC’s that specify extension grants, e.g. https://www.rfc-editor.org/rfc/rfc6749#section-4.5. Because this TA applies to situations where a resource client is acting on behalf of a user (health professional) that works for an organization (healthcare provider), the use of the JWT Bearer Assertion authorization grant as specified in https://www.rfc-editor.org/rfc/rfc7523#section-2.1 is the most suitable authorization grant. This means that the resource client must provide an authorization assertion in each access token request to identify the acting user, organization, and authorization base to prove that it is authorized to access the requested data. This authorization assertion acts as the authorization grant that the client can present to prove that it is authorized to access the protected resources.

The authorization assertion is a JWS Compact Serialized JWT that consists of a header, a payload, and a signature. The signature is created using a key pair belonging to the initiating organization or to a third party trusted by the initiating organization.

The header carries the claims listed below:

Claim	Description	Required
typ	Token type, must be “JWT”	Yes
alg	Cryptographic algorithm used to sign the authorization assertion. See https://www.rfc-editor.org/rfc/rfc7518#section-3.1 . All algorithms are described at Twiin-07 | Token Request.	Yes

kid	Identifier of the key pair used to sign this JWT. See https://www.rfc-editor.org/rfc/rfc7515#section-4.1.4.	Yes

The payload contains a set of claims that carry information required by NEN 7512 and NEN 7513.

Claim	Description	Required
jti	Unique identifier of the authorization assertion. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.7. The jti (JWT ID) is a unique identifier for a token and must not be reused. An assertion containing a duplicate jti (i.e., one that has been previously processed) shall be rejected to prevent replay attacks. Implementations should maintain a mechanism to track used jti values for the duration of their validity period.	Yes
iss	Identifier of the system that issued the authorization assertion. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.1 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	Yes
iat	The time at which the authorization assertion was issued. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.6. This is only required if there is an agreed age of an authorization assertion.	Conditional
exp	The expiration time on or after which the authorization assertion shall not be accepted for processing. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.4 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3. The expiration time (exp) claim in the assertion shall not exceed 5 minutes (300 seconds) from the time of issuance. Any assertion with an exp value set beyond this limit must be rejected.	Yes

nbf	The time before which the token shall not be accepted for processing. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.5 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	No
aud	Identifier of the authorization server token endpoint where this authorization assertion is to be used. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.3 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	Yes
sub	Identifier of the **healthcare organization** that requests access. **URA nummer** is mandatory, *additionaly* other identifiers may be added. The codesystem (`issuing_system`) for the identifier is also mandatory. For the URA this is OID: 2.16.528.1.1007.3.3 5.1 | Vertrouwen: Identificatie (see page 62) Allowed format for this identifier is: • `http://fhir.nl/fhir/NamingSystem/ura|<URA>`	Yes
sub_role	Code of the type of the **organization** (healthcare supplier) that requests access. **RoleCodeNL** is mandatory. The codesystem (`issuing_system`) for the identifier is also mandatory. For the RoleCodeNL this is OID: 2.16.840.1.113883.2.4.15.1060 Sub role is required when the responding party needs to check the patient consent. For instance when a user does not have an authorization base when requesting patient information.	Conditional

user_id	Identifier of the **responsible user** (healthcare professional) who requests access. **Preferred: UZI nummer** Allowed formats for this identifier are: • `urn:oid:2.16.528.1.1007.3.1.<UZI>` (without leading zero of UZI) • `http://fhir.nl/fhir/NamingSystem/uzi-nr-pers|<UZI>` 5.1 | Vertrouwen: Identificatie (see page 62) **User or system** In some cases a system is allowed to access data without a specific user being involved. Whenever there is a request for patient information, the identifier of the responsible user MUST be communicated. The only known exception to this rule is the retrieval of the Workflow Task that is requested based on the Notification Task in the TTA Notified Pull.	Yes
user_role	Code of the role of the responsible user (healthcare professional) who requests access. **Preferred: UZI rolcode** Allowed formats for this code are: • `urn:oid:2.16.840.1.113883.2.4.15.111.<UZI rolcode` (without leading zero, both before and after the . within the UZI rolcode) • `http://fhir.nl/fhir/NamingSystem/uzi-rolcode|<UZI rolcode>` 5.1 | Vertrouwen: Identificatie (see page 62) User identification (user_id and user_role claims) is only required in the authorization assertion when access to patient data is requested. This implies that these claims are not required in authorization assertions used in access token requests for Notification endpoints.	Conditional

authorizer	Identifier of the **healthcare organization** that grants access. **URA nummer** is mandatory, *additionaly* other identifiers may be added. The codesystem (`issuing_system`) for the identifier is also mandatory. For URA this is OID: 2.16.528.1.1007.3.3 5.1 | Vertrouwen: Identificatie (see page 62) Allowed format for this identifier is: • `http://fhir.nl/fhir/NamingSystem/ura|<URA>`	Yes
authorization_base	See Authorization base	No
patient	Identifier of the patient for whom data is exchanged. 5.1 | Vertrouwen: Identificatie (see page 62) Allowed format for this identifier is: • `urn:oid:2.16.840.1.113883.2.4.6.3.<BSN>` (without leading zero of BSN) Patient identification is only required when the Sending System requests access to the Notification endpoint of the Receiving System and the Sending System does not provide a Workflow Task that refers to a Patient resource containing the BSN of the patient. This way, the Receiving System is always able to identify a patient by BSN based on a Notification. The Receiving System must support receiving the BSN through the patient claim.	Conditional

The Issuer of the authorization assertion may include additional claims in the authorization assertion, but the Issuer shall not require the authorization server to process these claims.

The exchange of the public key that corresponds to the private key that was used to sign the authorization assertion between the Assertion Issuer and the authorization server is beyond the scope of this normative specification. Therefore, system vendors have to make mutual agreements about the exchange of these public keys.

Authorization scope

The scope defines the requested access to the FHIR Server as specified in https://www.rfc-editor.org/rfc/rfc6749#section-3.3 . If a scope is provided in the access token request or access token response, it must be expressed in a string of space delimited scopes as defined in http://hl7.org/fhir/smart-app-launch/scopes-and-launch-context.html#scopes-for-requesting-clinical-data . The following additional requirements apply to the scope values:

- When requesting an access token for a Notification endpoint at the Receiving System, the scope value must be one of:
  - system/Task.c?code=http://fhir.twiin.nl/fhir/CodeSystem/TaskCode|pull-notification (create)
  - system/Task.u?code=http://fhir.twiin.nl/fhir/CodeSystem/TaskCode|pull-notification (update)
- When requesting an access token for a FHIR endpoint at the Sending System, the query parameters in the scopes must match (a subset of) the queries in the FHIR search requests listed in Task.input of the Notification Task (see Notification message (see page 217)).

The client must provide the requested scope in the access token request, except for cases where an authorization base is provided in the access token request as part of the authorization assertion.

The authorization server must provide the granted access scope in the access token response in accordance with https://www.rfc-editor.org/rfc/rfc6749#section-5.1 and the requirements mentioned above. The issued access token must grant access to the granted scope that the authorization server specifies in the access token response. The granted scope must be equal to or less than the scope that can be derived from the authorization base consent token.

Access token request

Based on the paragraphs above each access token request contains the parameters listed below:

Parameter	Value	Required
grant_type	"urn:ietf:params:oauth:grant-type:jwt-bearer"	Yes
assertion	JWT authorization assertion as specified in paragraph Authorization grant.	Yes
client_assertion_type	"urn:ietf:params:oauth:client-assertion-type:jwt-bearer"	Yes
client_assertion	JWT client assertion as specified in paragraph Request message.	Yes
client_id	ID of the resource client. This ID is issued by the authorization server. The value of the "client_id" parameter must identify the same client as is identified by the client assertion.	Yes

scope	Space separated list of requested scopes, see paragraph Authorization scope. The scope must not be encoded before the `x-www-form-urlencoded` encoding. e.g. before encoding it should look like: `patient/Observation.s?code=http://loinc.org|29463-7`	Conditional

Note that the access token request effectively contains two JWT assertions:

1. A client assertion that is used to authenticate the client. This assertion identifies and authenticates the **system** that is requesting access.
2. An authorization assertion that is used as an authorization grant. This assertion identifies both the **organization** and **user** that are requesting access.

Separating client authentication from client authorization in two separate assertions enables the client to select different Assertion Issuers for the two assertions. The targeted authorization server must register both Issuers as trusted Assertion Issuers for a specific client.

Access token requirements

The access token will be processed only by the party that issued the access token. Therefore, the form and contents of the token are determined by the authorization server (audience), so the access token is opaque to the resource client. The resource client should not take any dependency on the format or contents of an access token. The authorization server MAY issue certificate bound access tokens as specified in https://www.rfc-editor.org/rfc/rfc8705 , but this is not mandatory. To enable the server to issue certificate bound access tokens, the client MUST support mTLS for access token and resource requests as specified in section Network level security: mTLS 1.3.

The validity period of an OAuth 2.0 access token shall not exceed 15 minutes. Implementations must ensure that the exp (expiration) claim in the token is set accordingly, with a maximum lifetime of 900 seconds (15 minutes) from the time of issuance.

Clients should be designed to handle token expiration by obtaining a new access token as required.

Authorization base

When the Sending System receives a request from the Receiving System to access certain data, it is the primary responsibility of the Sending System to verify that the Receiving System is authorized to access that data. When a system receives an authorization base, it shall not use the UZI-rolcode to determine whether access should be granted. When publishing data on a resource server to be collected by the Receiving System, many Sending Systems register the authorization to access that data as an

authorization base of some kind. To facilitate that authorization process, the Sending System may submit the authorization base (or a reference to it) to the Receiving System as part of the Notification (see section Notification message (see page 218)). If the Receiving System received an authorization base in the Notification, it must include that authorization base in the access token request to the Sending System (see section Authorization grant). This enables the authorization server of the Sending System to determine if the requested access can be granted based on the provided authorization base.

Since an authorization base is to be processed by the Sending System only, the form and contents of an authorization base are determined by the Sending System. The Receiving System should not take any dependency on the format or contents of an authorization base.

User authentication

Healthcare professionals are identified in their EHR system by logging in with their personal account. When a user of the Receiving System wants to request resources at the Sending System, the Sending System must be able to identify the user at the Receiving System as a legitimate healthcare professional who is working for the receiving organization before it can provide the requested data. Therefore, the Receiving System must implement the appropriate means to ensure the authenticity of the user.

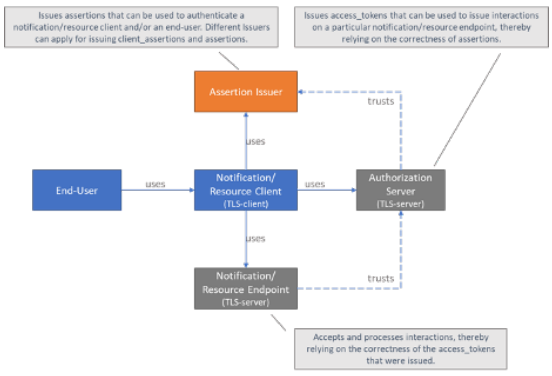
The Sending System can identify the healthcare professional at the receiving organization that is requesting patient data by the following claims in the authorization assertion of the access token request (see Authorization grant):

- **sub**: Identifier of the healthcare organization
- **user_id**: Identifier of the responsible user (healthcare professional)
- **user_role**: Code of the role of the responsible user (healthcare professional)

The type of identifiers used for organizations and users is beyond the scope of this TA. The same applies to the use of role codes.

Trust relationships

The picture below shows the different roles involved in the interactions, and clarifies the dependencies between these roles.



The Sending System hereby performs the following roles:

- Notification Client;

- Resource Server Endpoint.

The Receiving System performs the roles:

- Notification Server Endpoint;
- Resource Client.

Sending System and Receiving System both implement the role of Authorization Server.

The role of Assertion Issuer can be performed by a third-party, but can also be performed by the Sending System or by the Receiving System. Assertion Issuers producing client assertions do not necessarily have to produce authorization assertions as well. Different Issuers can be used for these types of assertions. Before issuing a client assertion or an authorization assertion, the Assertion Issuer has to make sure that applicable requirements regarding user authentication and other mutual security agreements between the Sending System and Receiver System have been met.

Trust and required level of user authentication between parties has to be arranged and agreed upon prior to performing the interaction.

Signature Algorithms

For verifying cryptographic tokens, we enforce the use of the following algorithms:

- **ES256** (Elliptic Curve P-256 with SHA-256)
- **ES512** (Elliptic Curve P-521 with SHA-512)
- ***PS256*** *(RSASSA-PSS with SHA-256) – Planned for future use*

Implementations must explicitly reject any other algorithms to ensure security and compliance with best practices.

For signing cryptographic tokens, one of the supported algorithms should be used.

Appendix: Token Request Examples

Token Request

request

```
POST /receiver-auth-server/token
Host: sending-server.example.com
Content-Type: application/x-www-form-urlencoded

grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Ajwt-bearer
assertion=ew0KICAidHlwIjogIkp[...omitted for brevity...]
client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-type%3Ajwt-
bearer
client_assertion=ew0KICAidHlwIjogIkp[...omitted for brevity...]
```

client_assertion jwt payload

```
{
 "jti": "4f0dfb37-7f9d-45fa-8187-9e260b80f949",
 "iss": "sending-ehr-issuer-id",
 "iat": "1572468316",
 "exp": "1572468916",
 "aud": "auth-server-id",
 "sub": "sending-ehr-system-id"
}
```

assertion jwt payload

```
{
 "jti": "4f0dfb37-7f9d-45fa-8187-9e260b80f949",
 "iss": "sending-ehr-issuer-id",
 "iat": "1572468316",
 "exp": "1572468916",
 "aud": "auth-server-id",
 "sub": "sending-organization-id",
 "user_id": "responsible-user-id",
 "user_role": "responsible-user-role",
 "authorizer": "receiving-organization-id",
 "authorization_base": "ZGFhNDFjY2MtZGFmMi00YjZkLThiNDYtN2JlZDk1MWEyYzk2",
 "patient": "urn:oid:2.16.840.1.113883.2.4.6.3.123456782"
}
```

10.6.3 | Patient Consent - Mitz Transacties

Beschreven in de "Implementatiehandleiding Mitz (Open & gesloten autorisatievraag)".

> Dit is een externe transactie. Zie voor meer informatie: Mitz Afsprakenstelsel 1.0.
>
> Binnen Twiin worden de volgende transacties gebruikt:
>
> - Open toestemmingsvraag Request conform XCPD [TR-0020]
> - Open toestemmingsvraag Request [TR-0030]
> - Gesloten toestemmingsvraag Request [TR-0040]
> - Gesloten toestemmingsvraag Response [TR-0041]
>
> voor een directe link naar de Mitz Implementatie handleiding kan onderstaande link gebruikt worden
>
> https://vzvz.atlassian.net/wiki/spaces/MA11/pages/828314367/Bijlage+Architectuurdocumenten

10.6.4| Logging

Logging is an internal responsibility for a GtK. IHE has defined transactions to log and retrieve the log. It is not mandatory to implement these transactions.

IHE ITI-20 | Record Audit Event

Scope

At every non-logging transaction an audit event is recorded and sent to the Audit Record Repository.

Use Case Roles

Referenced standards

RFC5424	The Syslog Protocol.
RFC5425	Transmission of Syslog Messages over TLS
RFC5426	Transmission of Syslog Messages over UDP
RFC7525	Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)

DICOM	DICOM PS3.15 Annex A.5 http://medical.nema.org/medical/dicom/current/output/chtml/part15/sect_A.5.html
ASTM E2147-01	Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems
NIST SP 800-92	Guide to Computer Security Log Management.
W3C XML 1.0	Extensible Markup Language (XML) 1.0
HL7 FHIR	*Release 4 http://hl7.org/fhir/R4/index.html*
RFC4627	*The application/json Media Type for JavaScript Object Notation (JSON)*

Messages

Send Audit Event – Syslog Interaction

> For more technical specification, see the original document: https://profiles.ihe.net/ITI/TF/Volume2/ITI-20.html

NB: This transaction is always performed in combination with the transaction ITI-40 (see page 265) where user data is added in a SAML token.
NB: All transactions are logged with an ITI-20 audit transaction, see IHE:ITI volume 2 for the correct implementation.

Send Audit Resource Rerquest Message – FHIR Feed Interaction

> This is part of the ITI TF Supplement: Add RESTful ATNA (Query and Feed) - Status: Trial Implementation

> For more technical specification, see the original document: paragraph 3.20.4.2 of https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RESTful-ATNA.pdf

Send Audit Bundle Request Message - FHIR Feed Interaction

This is part of the ITI TF Supplement: Add RESTful ATNA (Query and Feed) - Status: Trial Implementation

For more technical specification, see the original document: paragraph 3.20.4.3 of https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RESTful-ATNA.pdf

IHE ITI-81 | Retrieve Audit Record

This transaction is informative. Not for implementation in Twiin 1.4

Scope

An Audit Viewer requests (a selection of) audit events from the Audit Record Repository based on FHIR.

Use Case Roles

Referenced standards

RFC2616	IETF Hypertext Transfer Protocol – HTTP/1.1
RFC4627	The application/json Media Type for JavaScript Object Notation (JSON)
RFC6585	IETF Additional HTTP Status Codes
RFC5424	The Syslog Protocol
RFC3339	Date and Time on the Internet: Timestamps
HL7 FHIR	Release 4 http://hl7.org/fhir/R4/index.html

Messages

Retrieve ATNA Audit Events Message

This is part of the ITI TF Supplement: Add RESTful ATNA (Query and Feed) - Status: Trial Implementation

For more technical specification, see the original document: paragraph 3.81.4.1 of https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RESTful-ATNA.pdf

IHE ITI-82 | Retrieve Syslog Event

This transaction is informative. Not for implementation in Twiin 1.4

Scope

An Audit Viewer requests (a selection of) syslog events from the Audit Record Repository.

Use Case Roles

Referenced standards

RFC2616	IETF Hypertext Transfer Protocol – HTTP/1.1
RFC4627	The application/json Media Type for JavaScript Object Notation (JSON)
RFC6585	IETF Additional HTTP Status Codes
RFC5424	The Syslog Protocol
RFC3339	Date and Time on the Internet: Timestamps

Messages

Send Audit Resource Rerquest Message - FHIR Feed Interaction

> This is part of the ITI TF Supplement: Add RESTful ATNA (Query and Feed) - Status: Trial Implementation

> For more technical specification, see the original document: paragraph 3.82.4.1 of https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RESTful-ATNA.pdf

10.6.5 | Addressing - ZORG-AB Transacties

Beschreven in de "VZVZ ZORG-AB Implementatiehandleiding". Voor meer informatie:

> Dit is een externe transactie. Zie voor meer informatie: https://www.vzvz.nl/diensten/gemeenschappelijke-diensten/zorg-ab/implementeren-leveranciers
>
> Binnen Twiin worden de volgende transacties gebruikt:
>
> - GET Organization
> - GET Endpoint

ZORG-AB 2.9.1[66] kent twee type interfaces die gebruikt kunnen worden: Native REST (OData URL conventies) en een HL7 FHIR interface. De GtK-applicatie kan kiezen of, en zo ja welke interface van ZORG-AB gebruikt wordt. ZORG-AB dient nog wel aangepast te worden om ook Twiin Electronic Services te kunnen registreren. Hiervoor komt dan ook een zoekparameter, maar een gebruiker zou ook alle elektronische diensten van een bepaalde zorgaanbieder kunnen opvragen en daaruit een passende dienst kiezen (bijv die binnen het eigen domein).

Twiin publiceert de GtK informatie in ZORG-AB. Het gebruik van de ZORG-AB transacties door een GtK is niet verplicht.

10.6.6 | Localisation

> This is a placeholder page

66. https://www.vzvz.nl/diensten/gemeenschappelijke-diensten/zorg-ab/releases

10.6.7 | Network level security

In this section the generic transactions are described to keep the network safe and secure.

HTTP-header hygiene

HTTP header hygiene refers to the practice of using HTTP headers to enhance web security and performance by properly configuring and implementing headers that enforce security policies, provide necessary information about the client and server, and control caching and other response behaviors, but not more then is needed.

HTTP headers included in transactions **must adhere to the principle**:

Only transmit HTTP headers that are necessary for the functioning of the HTTP protocol and the web application.

(NCSC; U/PW.02 principle 4)

Important Notes

- This list is **not exhaustive**. Additional headers may be required depending on specific application or integration needs (e.g., FHIR version negotiation, content encoding, CORS, etc.).
- Any **custom or non-standard headers** must be documented and justified for their relevance to the functioning of the service.
- Headers revealing **internal infrastructure details** (e.g., Server, X-Powered-By) **must not be exposed** unless strictly necessary.

IHE ITI-1 | Maintain Time

Scope

This transaction is used to synchronize time among multiple systems.

Referenced Standards

NTP Network Time Protocol Version 3. RFC1305

SNTP Simple Network Time Protocol (SNTP) RFC4330

Messages

> For more technical specification, see the original document: https://profiles.ihe.net/ITI/TF/Volume2/ITI-1.html#3.1.1

10.7 | Kern Volume 3 - Content

Dit volume bevat de content, zoals bijvoorbeeld metadata, die overkoepelend voor de zorgtoepassingen geldt alsmede relevante verwijzingen naar de content van andere afsprakenstelsels en voorzieningen voor generieke functies.

10.7.1 | Document/beeld gebaseerde Metadata

Metadata geïndexeerde bevraging

> Disclaimer
>
> Voor de vulling van metadata is gebruik gemaakt van de Nictiz Metadataset: XDS metadata - Nictiz[67]
>
> De Nictiz metadata set is document gebaseerd en niet 1 op 1 van toepassing op b.v. resource gebaseerde uitwisseling.

APPLICATIE-LAAG

Het communicatiepatroon geïndexeerde bevraging (see page 172) maakt gebruik van metadata. De metadata wordt gebruikt binnen een use case om informatie te vinden bij verschillende zorgaanbieders.

Binnen Twiin passen we voor document gebaseerde bevragingen de volgende metadata-velden toe. De invulling van deze metadata-velden is vastgesteld binnen de use case.

Parameter	Opt	voorbeeld	beschrijving
Author	R	('Dr. Lewis Zimmerman')	Auteur van document
confidentialityCode	R	('N^^2.16.840.1.113883.5.25')	vertrouwelijkheidsniveau
creationTime	R	20100101230000	Tijd van aanmelden
DocumentEntryStatus	R	('urn:oasis:names:tc:ebxml-regrep:StatusType:Approved')	De status van het document

67. https://nictiz.nl/standaarden/overzicht-van-standaarden/xds-metadata/

patientId	R	'123456789^^^&2.16.840.1.113883.2.4.6.3&ISO '	BSN van cliënt
referenceIdList	O	642356235^^^&1.2.3.4.5.6&ISO^urn:ihe:iti:xds:2013:accession	Koppeling met ander document of beeld
repositoryUniqueId	R	1.1.4567332.1.1	Identificeert document Archief
serviceStartTime	R	20100101230000	Start van onderzoek
serviceStopTime	R	20100101230000	Stop van onderzoek
Document uniqueId	R	1.3.6.1.4.1.12559.11.13.2.1.231	Identificeert document
practiceSettingCode	R	('309964003^^2.16.840.1.113883.6.96')	Specialisme (in voorbeeld Radiology Department)
DocumentEntryType	R	urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1	Stable of On Demand
healthcareFacilityTypeCode	R	('V4^^ 2.16.840.1.113883.2.4.15.1060')	Type ZA (Zie nictiz metadata)
formatCode	R	('urn:ihe:rad:PDF^^1.3.6.1.4.1.19376.1.2.3')	Format van document
classCode	R	('9491000146107^^2.16.840.1.113883.6.96')	Imaging Documentation
typeCode	R	('722124004^^2.16.840.1.113883.6.96')	radiologisch verslag
mimeType	R	application/pdf	pdf

In het geval er DICOM beelden gedeeld worden is de volgende aanvullende metadata nodig.

Parameter	Opt	voorbeeld	beschrijving
StudyInstanceUID	R	Dicom tag (0020.000D)	Identificeert study
SeriesInstanceUID	R	Dicom tag (0020.000E)	Identificeert serie

Parameter	Opt	voorbeeld	beschrijving
eventCodeList	R	Dicom tag (0008,0060) (bijvoorbeeld MR) Anatomic Region	Geeft modaliteit aan Geeft lichaamsonderdeel aan

Toelichting algemene metadata

confidentialityCode

Code om het vertrouwelijkheidsniveau van het document te classificeren. De Nictiz metadata schrijft voor welke codes er gebruikt kunnen worden. Het is aan de bronhouder van de data om te bepalen welke documenten er als 'normal' geclassificeerd worden en of er documenten of beelden zijn die een hoger vertrouwelijkheidsniveau nodig hebben.

DocumentEntryStatus

Status van het document, kan de waarde 'Approved' of 'Deprecated' bevatten. Een deprecated document is een document dat vervangen is.

referenceIdList

De waarde in de referenceIdList wordt gebruikt om meerdere documenten aan elkaar te relateren. Meest praktische voorbeeld is het 'koppelen' van het verslag aan de beelden. IHE schrijft het volgende voor;

> The referenceIdList may be populated with the Accession Number and assigning authority.

Bron: *https://www.ihe.net/uploadedFiles/Documents/Radiology/IHE_RAD_TF_Vol2.pdf* table 4.68.4.1.2.3-1
Door bovenstaand te volgen zal er een unieke waarde zijn om toe te kennen aan de referenceIdList. Op deze waarde zal niet specifiek gezocht worden. Het is een manier voor de brondossierhouder om de data gestructureerd aan te bieden. De Nictiz metadataset schrijft hier de waarden voor die gebruikt moeten worden.

practiceSettingCode

Beschrijft het (zorg)specialisme. Een raadpleger kan een specifieke vraag (query) stellen om enkel data terug te krijgen over een specifiek specialisme, of alle binnengekomen data filteren op een specifiek specialisme.
De Nictiz metadataset schrijft hier de waarden voor die gebruikt moeten worden.

healthcareFacilityTypeCode

Beschrijft het zorgaanbiedertype. Een raadpleger kan een specifieke vraag (query) stellen om enkel data terug te krijgen over een specifiek zorgaanbiedertype, of alle binnengekomen data filteren op een

specifiek zorgaanbiedertype.

De Nictiz metadataset schrijft hier de waarden voor die gebruikt moeten worden.

Twiin Implementatiewijzer Zorgtoepassingen

De implementatiewijzers zijn bedoeld voor leveranciers en zorgaanbieders. Leveranciers hebben een vooraanstaande rol om het landelijk dekkend netwerk te realiseren; zonder leveranciers geen uitwisseling. Twiin werkt daarom samen met leveranciers van zorginformatiesystemen. Bij de oplossingen die we samen bedenken, gaan we uit van de functionele behoeften van de eindgebruikers. Deelnemende zorgaanbieders geven hun leveranciers opdracht te voldoen aan de eisen van het Twiin Afsprakenstelsel, zodat zorgaanbieders gezondheidsgegevens kunnen uitwisselen binnen het Twiin Samenwerkingsverband.

In het afsprakenstelsel staan deze eisen helder beschreven. Leveranciers kunnen ook de rol van GtK Beheerder op zich nemen in opdracht van een deelnemer. Daarnaast kunnen ze hun applicaties laten valideren als GtK-applicatie.

Belangrijke gerelateerde onderdelen van het afsprakenstelsel: 10 | Technische kern (see page 164) 5 | Vertrouwensmodel (see page 56) 9 | Voorwaarden (see page 142)

In de onderliggende pagina's zijn de implementatiewijzers beschreven voor de databeschikbaarheid van de zorgtoepassingen:

- Z1 | BgZ: Implementatiewijzer Basisgegevensset Zorg (see page 294)
- Z2 | BB: Implementatiewijzer Beeldbeschikbaarheid – Trial (see page 414)
- Z3 | COR: Implementatiewijzer Correspondentie (see page 469)

Volgens het releasebeleid (see page 97) onderkennen we de status **Trial** in de implementatiewijzer.

Z1 | BgZ: Implementatiewijzer Basisgegevensset Zorg

Inleiding

Deze implementatiewijzer is bedoeld voor leveranciers en zorgaanbieders. Leveranciers hebben een vooraanstaande rol om het landelijke dekkend netwerk te realiseren; zonder leveranciers geen uitwisseling. Twiin werkt daarom samen met leveranciers van zorginformatiesystemen. Bij de oplossingen die we samen bedenken, gaan we uit van de functionele behoeften van de eindgebruikers. Deelnemende zorgaanbieders geven hun leveranciers opdracht te voldoen aan de eisen van het Twiin Afsprakenstelsel, zodat zorgaanbieders gezondheidsgegevens kunnen uitwisselen.

In het afsprakenstelsel staan deze eisen helder beschreven. Leveranciers kunnen ook de rol van GtK Beheerder op zich nemen in opdracht van een deelnemer. Daarnaast kunnen ze hun applicaties laten valideren als GtK-applicatie.

- Belangrijke gerelateerde onderdelen van het afsprakenstelsel: Technische kern (see page 164), Twiin Implementatiewijzer Zorgtoepassingen (see page 294), Vertrouwensmodel (see page 56), Voorwaarden (see page 142),

De implementatiewijzer

Dit onderdeel beschrijft de technische implementatie voor de beschikbaarheid van data van de Twiin zorgtoepassing BgZ.

De Basisgegevensset Zorg (afgekort BgZ) is de minimale set van patiëntgegevens die specialisme-, ziektebeeld- en beroepsgroepoverstijgend relevant is en van belang voor de continuïteit van zorg. Dit betreft vooral situaties waarbij overdracht van zorg tussen zorgaanbieders plaatsvindt en/of behoefte bestaat aan een patiëntsamenvatting met eerdere behandelingen die in verschillende instellingen hebben plaatsgevonden. Deze medische samenvatting op basis van zorginformatiebouwstenen (zibs) is inmiddels omarmd als landelijke dataset. Steeds meer partijen implementeren de BgZ met voorrang in hun systemen. Mede vanwege verplichtingen van diverse regelingen (zoals VIPP 5) en aanstaande wet- en regelgeving bestaat een toenemende behoefte om de BgZ op een veilige en gestandaardiseerde wijze beschikbaar te stellen tussen zorgaanbieders. VIPP 5 module 3 gaat over de uitwisseling van de BgZ tussen zorgaanbieders binnen de medisch specialistische zorg. De zorgaanbieder kan digitaal de BgZ en relevante correspondentie uitwisselen met een andere instelling. Begin 2021 is door Nictiz de informatiestandaard BgZ[68] voor uitwisseling tussen medisch specialistische instellingen ontwikkeld.

- Volume 1 geeft een functioneel overzicht voor de databeschikbaarheid van de zorgtoepassing BgZ en de daarbij behorende eisen (see page 295).
- Volume 2a bevat de technische afspraken voor de uitwisseling van de BgZ. Dit noemen we ook wel de Twiin Technische Afspraak (TTA) (see page 301).
- Volume 2b bevat alle losse transacties die gebruikt worden voor de uitwisseling van de BgZ. (see page 316)
- Volume 3 is een verwijzing naar de informatiestandaard en de meta-informatie (see page 345).

Vanuit bovenstaande 4 secties zijn ook de eisen overzichtelijk beschreven. Deze zijn terug te vinden via de BgZ: Samenvatting PvE. (see page 377)

Vanuit Twiin wensen we je veel lees- en ontwikkelplezier.

Z1.1 | BgZ Volume 0 - Functioneel overzicht

Inleiding

In dit volume:

- een beschrijving van de functionele use case van de zorgtoepassing;
- een overzicht van de uitwisselpatronen die worden gebruikt voor deze zorgtoepassing;
- een beschrijving van de invulling van het vertrouwensmodel met de daarbij behorende voorwaarden voor deze zorgtoepassing;

68. https://informatiestandaarden.nictiz.nl/wiki/Landingspagina_BgZ

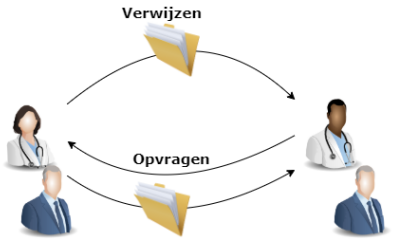
- een beschrijving of verwijzing naar de eisen die gesteld zijn door organisaties, programma's en/of informatiestandaarden.

In volume 2 volgt de uitwerking van de transacties van de uitwisselpatronen voor de zorgtoepassing BgZ (in het Engels).

Functionele use cases

In de NEN 7540 (BgZ)[69] en de informatiestandaard BgZ[70] voor uitwisseling tussen medisch specialistische instellingen zijn twee use cases uitgewerkt:

1. uitwisselen BgZ bij verwijzing of overdracht;
2. opvragen BgZ van een eerdere behandeling.



De meest gebruikte processen waar de BgZ een rol in speelt zijn:

- Verwijzing / overdracht
- Consult / advies
- Ketenzorg / netwerkzorg
- Ad hoc dossier opvragen
- Uitbesteed onderzoek / behandeling

Vanuit deze processen zijn er volgens de informatiestandaard functioneel twee manieren om de BgZ beschikbaar te stellen:

1. Uitwisselen BgZ en correspondentie bij verwijzing of overdracht (versturen, functionele push)
2. Opvragen BgZ en correspondentie bij eerdere behandelaar (opvragen, functionele pull)

Binnen het Twiin Afsprakenstelsel hergebruiken we graag relevante informatie. We gebruiken daarom voor deze use cases het beleid “proudly copied from” voor de Nictiz informatiestandaard BgZ[71].

Deze zijn overgenomen in de onderliggende pagina’s.

69. https://www.nen.nl/nen-7540-2024-nl-319920
70. https://informatiestandaarden.nictiz.nl/wiki/Landingspagina_BgZ
71. https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Use_cases

Z1.1.1 | Uitwisseling BgZ bij verwijzing of overdracht

Deze pagina beschrijft de uitwisseling in het geval van het versturen van de BgZ bij een verwijzing of overdracht. De Z1.2.1 | TTA Exchanging BgZ – FHIR Notified Pull (see page 302) beschrijft de technische invulling van deze uitwisseling binnen Twiin.

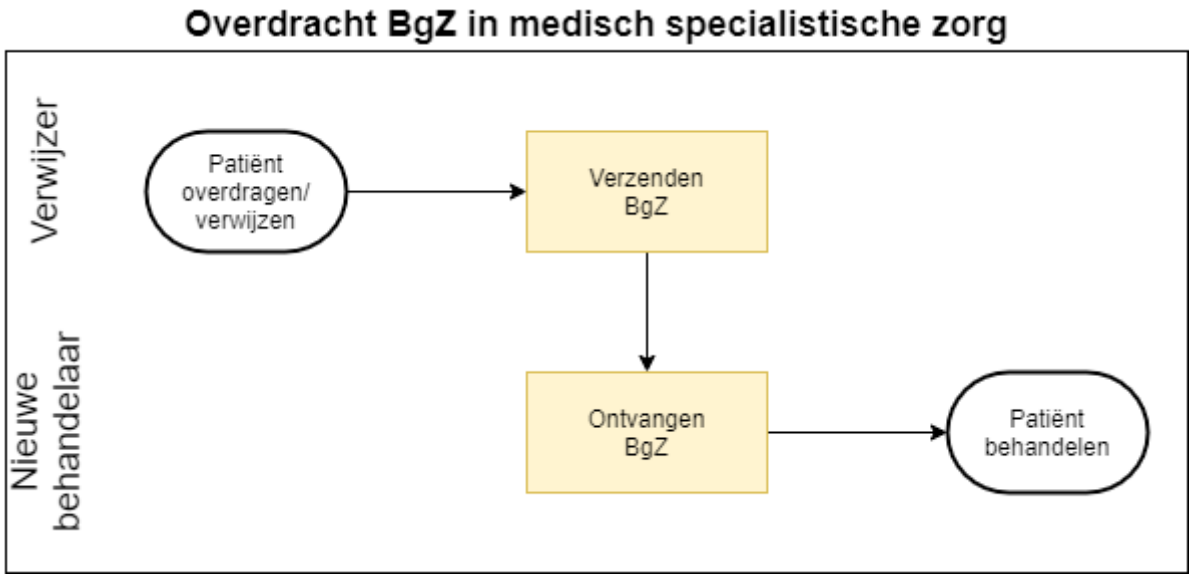
> Proudly copied from Nictiz: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Use_case_1:_Uitwisseling_BgZ_bij_verwijzing_of_overdracht

Doel en relevantie

Bij het verzenden van een BgZ naar een andere instelling kan van verschillende varianten sprake zijn.

- Een arts verwijst naar een andere arts, of er is een overdracht van een patiënt naar die andere instelling (en afdeling daarbinnen) en de eigen behandeling is daarmee afgelopen.
- Een tweede arts doet een deel van de behandeling zonder dat de eerdere arts de (eigen) behandeling beëindigt.

In al deze gevallen spreken we in deze informatiestandaard van verwijzing en/of overdracht. We maken geen strikt onderscheid tussen verwijzen en overdracht, en ook niet op de vraag of de verwijzende arts al dan niet bij de behandeling betrokken blijft. Dat kan per zorgproces nader bepaald worden. De essentie hier is dat de tweede arts een eigen, zelfstandige behandelovereenkomst met de patiënt aangaat.



Bedrijfsrollen

Rol	Toelichting
Verwijzer	De arts die een patiënt verwijst of overdraagt naar een andere arts bij een andere instelling en in het kader daarvan de BgZ deelt.
Nieuwe behandelaar	De arts van de andere instelling die de BgZ ontvangt en een behandelovereenkomst met de patiënt aangaat (of voortzet).

Proces en context

Patient journey

Een patiënt is onder behandeling bij een oncoloog in een regionaal ziekenhuis. De patiënt heeft een complexe aandoening, waarvoor de behandeling beter voortgezet kan worden in een nabij academisch ziekenhuis. De behandelend arts verwijst de patiënt door naar het academisch ziekenhuis, en verstrekt daarbij (alle of een deel van) de volgende documenten:

1. een verwijsbrief;
2. de BgZ van de patiënt;
3. eventuele verdere bijlagen of verwijzingen.

De patiënt komt op een consult in het academisch ziekenhuis. De behandelend arts daar opent het eigen EPD en ziet de BgZ en de overige informatie uit het regionale ziekenhuis in. Het academisch ziekenhuis zet de behandeling voort.

Precondities

- De patiënt is onder behandeling in een instelling.
- De behandelend arts is geautoriseerd om de BgZ te mogen versturen
- De behandelend arts besluit tot verwijzing of overdracht.
- De gegevens van de patiënt zijn vastgelegd in het EPD.
- Behandelend en ontvangend ziekenhuis kunnen digitaal de BgZ uitwisselen.

Trigger event

Het besluit van een arts om een patiënt te verwijzen of over te dragen aan een andere instelling, waar de patiënt onder behandeling zal komen.

Proces

1. De behandelend arts kiest een instelling en specialisme (en mogelijk een zorgverlener binnen die instelling) waarnaar verwezen wordt.

2. De behandelend arts rondt de verwijzing af.
3. De BgZ wordt verzonden.
    - De stap: "verzenden BgZ" kan expliciet zijn, maar kan ook "onder water" geschieden, bijvoorbeeld als deel van het afronden van de verwijzing.
4. Een arts in de ontvangende instelling ziet de BgZ in, en neemt (indien gewenst) alle of een deel van de gegevens over. Denk eraan dat opvragen binnen dient te gebeuren binnen de geldigheidsduur waarbinnen gegevensuitwisseling in het kader van de verwijzing mag plaatsvinden. De geldigheidsduur van een verwijzing dan wel overdracht binnen de tweede lijn is gebaseerd op de geldigheidsduur die gehanteerd wordt tussen de eerste en tweedelijns verwijzingen, namelijk **één jaar**. Dit is afgestemd met de koepels FMS, NVZ, NFU en ZKN en wordt tot nader order gehanteerd als veldnorm.

Annuleren

Het kan zijn dat er redenen zijn waarom de communicatiepartner de BgZ niet meer op hoeft te vragen. Het uitgestuurde verzoek om de BgZ op te vragen kan geannuleerd worden met een bericht (see page 324), maar het is niet verplicht dit bericht te versturen. Dit annuleringsbericht moet wel ontvangen kunnen worden. Over de verdere inhoudelijke verwerking van het annuleringsbericht doet Twiin nog geen uitspraak.

Tijdens de eerste uitwisseling onder 1.3.x en 1.4 zal onderzocht worden wat het effect kan zijn van het annuleren op het zorgproces en eventueel al geraadpleegde informatie. De details volgen bij tafels bij (opzet van) een kwaliteitsrichtlijn, norm of informatiestandaard.

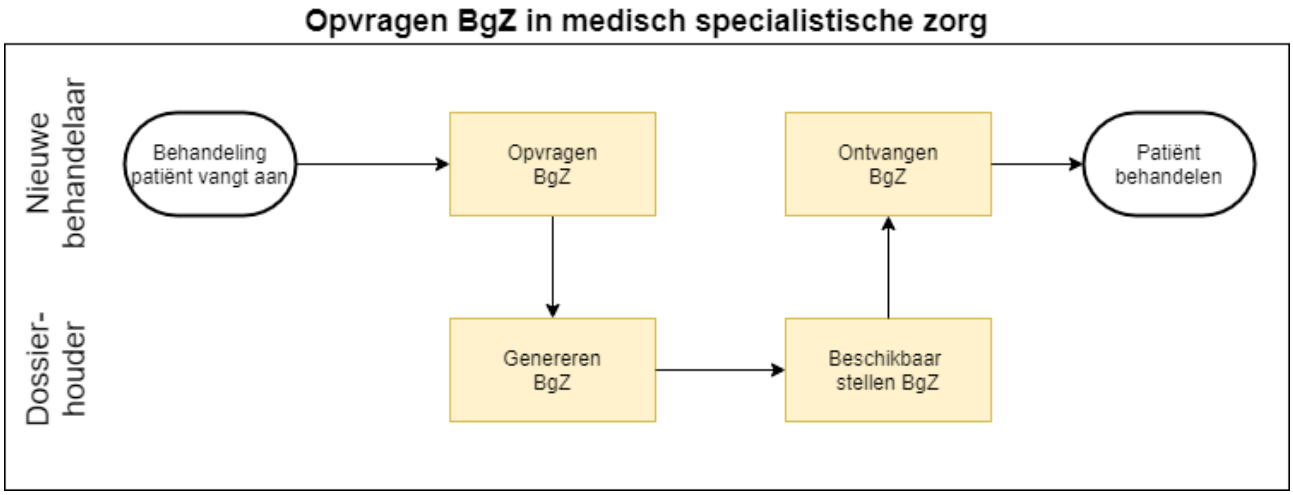
Z1.1.2 | Opvraging BgZ bij eerdere behandelaar

Deze pagina beschrijft de uitwisseling in het geval van een opvraging van de BgZ bij een eerdere behandelaar. De Z1.2.2 | TTA Retrieving BgZ – FHIR Direct Pull (see page 310) beschrijft de technische invulling van deze uitwisseling binnen Twiin.

> Proudly copied from Nictiz: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Use_case_2:_Opvraging_BgZ_bij_eerdere_behandelaar

Doel en relevantie

Bij deze use case is sprake van een behandeling waarbij gegevens van een andere instelling, waar een eerdere behandeling heeft plaatsgevonden, worden opgevraagd.



Bedrijfsrollen

Rol	Toelichting
Nieuwe behandelaar	De arts die een patiënt behandelt en gegevens wil opvragen van een eerdere behandeling bij een andere zorginstelling.
Dossierhouder	De instelling waar de patiënt eerder behandeld is, en die de BgZ deelt met de (huidige) behandelend arts bij een andere instelling.

Proces en context

Patient journey

Een patiënt komt voor behandeling bij een zorgverlener. Uit de anamnese blijkt een eerdere behandeling bij een andere instelling. De zorgverlener vraagt de BgZ op bij de andere instelling.

We maken een voorlopig onderscheid in twee subcasussen: opvraag met en zonder collegiaal contact.

- Met collegiaal contact volgt de gebruikelijke handelwijze waarbij een arts een eerdere arts belt om nadere informatie over de patiënt en naar eerdere behandelingen/bevindingen te informeren.

Variant: Opvraging met collegiaal contact

De huidige behandelaar neemt contact op met de dossierhoudende instelling en wordt doorverwezen naar de eerdere behandelaar. Beiden spreken de casus door. De eerdere behandelaar verstrekt de BgZ aan de huidige behandelaar en heeft daarbij de optie:

- een collegiale brief mee te zenden;
- aanvullende documentatie (brieven, beelden, verslagen etc.) mee te zenden.

Variant: Opvraging zonder collegiaal contact

Wanneer de eerdere behandelaar niet meer werkzaam is bij de dossierhoudende instelling, of wanneer collegiaal contact niet nodig of wenselijk is, vraagt de huidige zorgverlener de BgZ op bij de dossierhoudende instelling. De zorgverleners bij die instelling hoeven daarbij geen rol te spelen op dat moment. De dossierhoudende instelling levert de BgZ (zoals die op dat moment uit het EPD gegenereerd kan worden) op aan de huidige behandelaar.

Precondities

- Er is sprake van een eerdere behandeling.
- De gegevens van de patiënt zijn daar vastgelegd in het EPD.
- Er is een volgende behandeling in een andere instelling voor medisch-specialistische zorg.
- De (huidig) behandelend arts wil de gegevens van de eerdere behandeling inzien.

Trigger event

Het verzoek van een behandelend arts om eerder vastgelegde gegevens van een andere instelling in te zien.

Proces

1. De behandelend arts vraagt een BgZ op.
2. De eerdere instelling stelt de BgZ beschikbaar aan de opvragende instelling.
    - Niet alle instellingen hebben de mogelijkheid een BgZ direct aan te maken. Soms is deze pas na enige tijd beschikbaar. Het heeft uiteraard de voorkeur wanneer een opvragende arts de gegevens direct ook in kan zien. Dat is echter geen verplichting: ook een proces met opvragen van de BgZ op het moment dat een consult gepland wordt om tijdens of voor het consult in te zien heeft meerwaarde.
    - De BgZ mag ook de laatste BgZ zijn wanneer een instelling deze na iedere wijziging opslaat: opnieuw genereren hoeft niet als geborgd is dat het de laatste stand van zaken is.
3. De BgZ wordt ter beschikking gesteld aan de huidige behandelend arts.
4. De behandelend arts raadpleegt de BgZ, en neemt (indien gewenst) alle of een deel van de gegevens over.

Z1.2 | BgZ Volume 1 – Twiin Technical Agreement

This volume describes the technical side of the agreements to exchange information described in the Dutch standard Basisgegevensset Zorg. This technical agreement provides the exchange patterns in which this standard will be transmitted between two Twiin participants. In both patterns the consulting party should only query the data that is necessary.

Pushing the information

Because of the potential size of and potential security issues with the dataset BgZ, a traditional push was not preferred. The Notified Pull exchange pattern provides more possibilities surrounding these potential

problems, like data minimisation by only querying the data that is needed and using user authentication on privacy data.

Pulling the information

Due to the nature of the dataset, the natural pull is the exchange pattern direct pull. There is only one dataset in each datasource, which means there is no need for further indexing. Localising the datasources is enough to find the dataset.

- Z1.2.1 | TTA Exchanging BgZ – FHIR Notified Pull (see page 302)
- Z1.2.2 | TTA Retrieving BgZ – FHIR Direct Pull (see page 310)
- Z1.2.3 | TTA Retrieving BgZ – SOAP Indexed Pull (see page 312)
- Z1.2.4 | TTA Exchanging BgZ – SOAP PUSH (see page 316)

Z1.2.1 | TTA Exchanging BgZ – FHIR Notified Pull

For this use case the exchange pattern Notified Pull with FHIR is used. Below you will find the description of this exchange pattern.

> Original page can be found at 10.3.1 | TTA FHIR – Notified pull (see page 185)

This Twiin Technical Agreement (TTA) describes and specifies the technical responsibilities to which parties agree when connecting to exchange transactions to facilitate the Notified Pull. This TTA is based on the TA Notified Pull[72], with the normative specifications remaining unchanged. The informative specifications, however, have been described using a specific implementation.

The possibility to exchange a client's medical record is for example required in case of a patient referral or transfer. When different healthcare organizations are involved in a client's treatment plan, attention should be paid to the required legal permission and the possible 'burden' for the receiving system when a medical record is transferred.

Relation to other documents

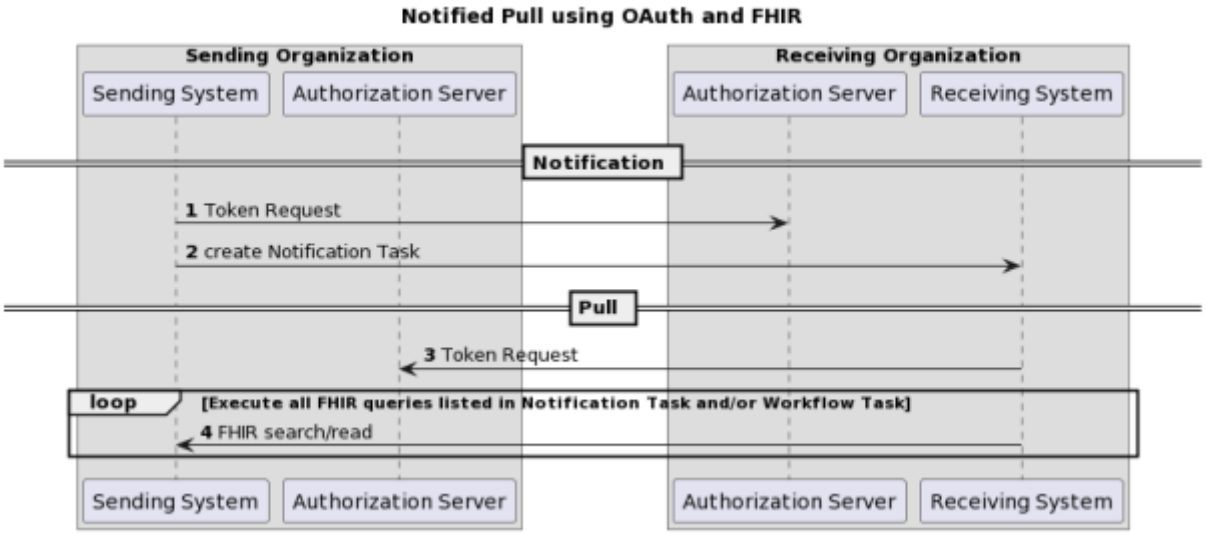
This document is written with the following documents as references:

- Nictiz – Informatiestandaard BgZ MSZ
- TA Notified Pull v1.x.x (latest version)[73]

72. https://www.twiin.nl/tanp
73. https://www.twiin.nl/tanp

Format

The format of this section follows the main interactions as presented below in the simplified sequence diagram of the Notified Pull sequence.



Interaction numbers 1 and 3 are described in the 10.4.2 | TTA FHIR – Authorization (see page 206). Interaction number 2 is described in10.3.1.1 Notified Pull – Data interactions (see page 190). A part of interaction number 4 is also described in 10.3.1.1 Notified Pull – Data interactions (see page 190). For specifics of the context of the Notified Pull, see Nictiz information standards.

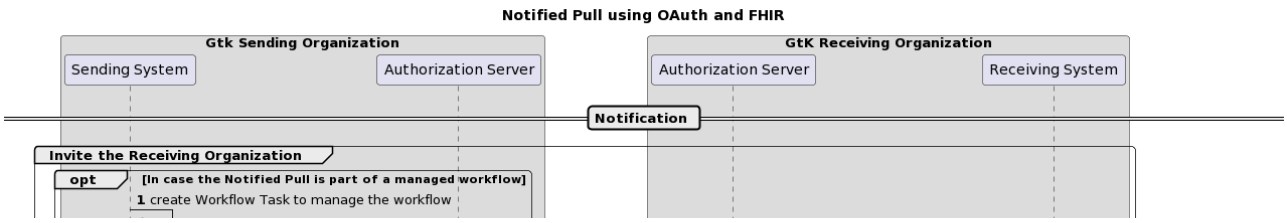
The sequence diagram below provides a complete overview that covers both the resource interactions and the authorization interactions of the complete Notified Pull interaction sequence.

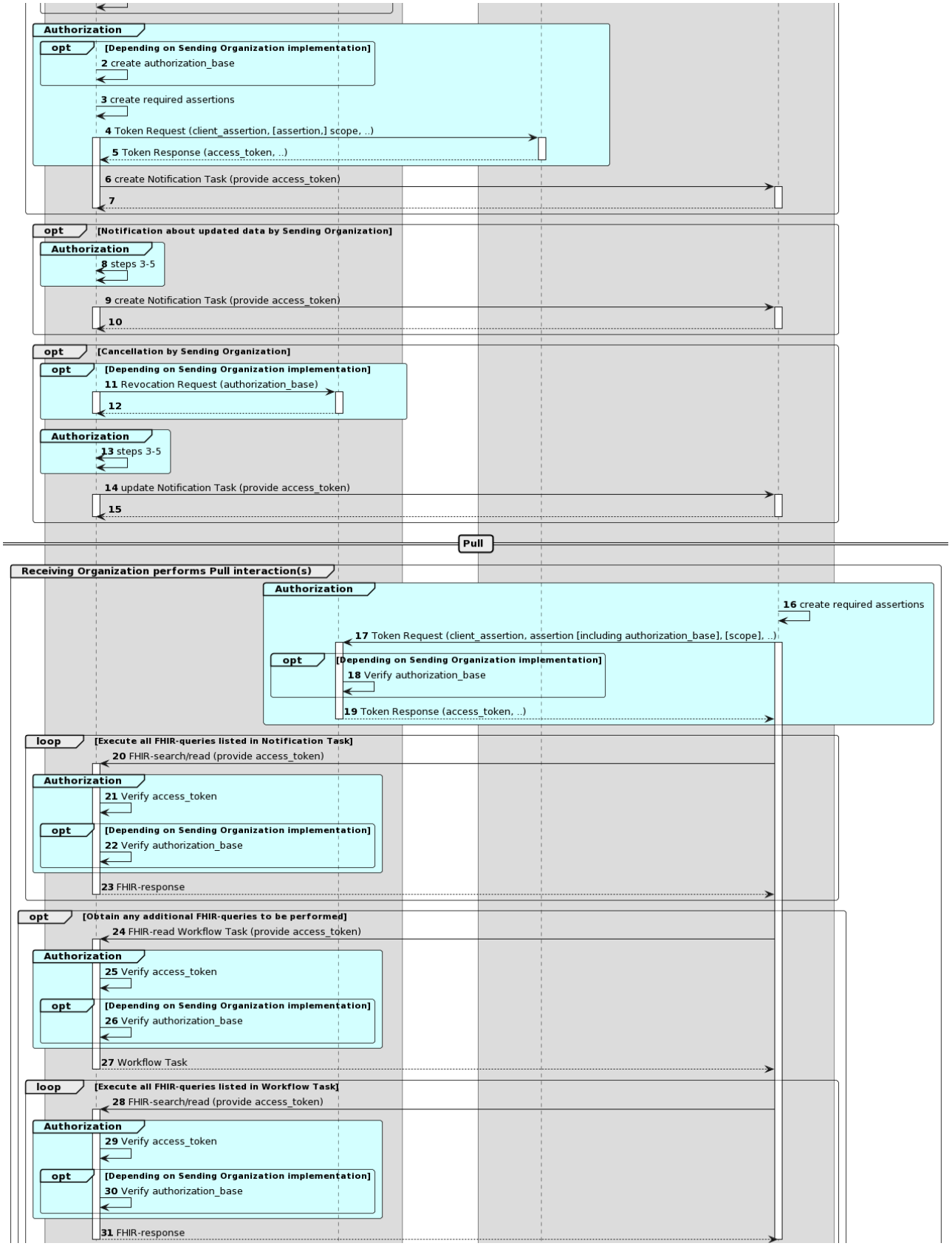
The Twiin specific solutions for identification and addressing can be found in 10.4.2 | TTA FHIR – Authorization (see page 206) and 10.4.5 | TTA – Addressing (see page 210) respectively.

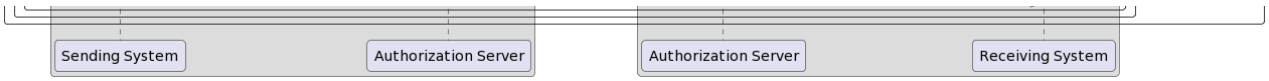
Sequence diagram

The sequence diagram below visualizes the full flow for the Notified Pull interaction sequence, including both interactions in the data layer using HL7 FHIR (described in 10.3.1.1 Notified Pull – Data interactions (see page 190)) and in authorization layer using OAuth 2.0 (marked cyan, described in 10.4.7 | Network level security (see page 211)).

Each section consists of several steps. The steps correspond to the numbers in the sequence diagram.




Authorization
opt
[Depending on Sending Organization implementation]
2 create authorization_base
3 create required assertions
4 Token Request (client_assertion, [assertion,] scope, ..)
5 Token Response (access_token, ..)
6 create Notification Task (provide access_token)
7
opt
[Notification about updated data by Sending Organization]
Authorization
8 steps 3-5
9 create Notification Task (provide access_token)
10
opt
[Cancellation by Sending Organization]
opt
[Depending on Sending Organization implementation]
11 Revocation Request (authorization_base)
12
Authorization
13 steps 3-5
14 update Notification Task (provide access_token)
15
Pull
Receiving Organization performs Pull interaction(s)
Authorization
16 create required assertions
17 Token Request (client_assertion, assertion [including authorization_base], [scope], ..)
opt
[Depending on Sending Organization implementation]
18 Verify authorization_base
19 Token Response (access_token, ..)
loop
[Execute all FHIR-queries listed in Notification Task]
20 FHIR-search/read (provide access_token)
Authorization
21 Verify access_token
opt
[Depending on Sending Organization implementation]
22 Verify authorization_base
23 FHIR-response
opt
[Obtain any additional FHIR-queries to be performed]
24 FHIR-read Workflow Task (provide access_token)
Authorization
25 Verify access_token
opt
[Depending on Sending Organization implementation]
26 Verify authorization_base
27 Workflow Task
loop
[Execute all FHIR-queries listed in Workflow Task]
28 FHIR-search/read (provide access_token)
Authorization
29 Verify access_token
opt
[Depending on Sending Organization implementation]
30 Verify authorization_base
31 FHIR-response



Section	Step	Description
Invite the Receiving Organization	1	If the Notified Pull is part of a managed workflow involving both the Sending Organization and the Receiving Organization, and this workflow specifies the creation of a FHIR Task ('workflow task') at the Sending System, then the flow starts with the creation of this task on the Sending System.
	2	The Sending System creates an authorization base, which is used later to communicate a presumed consent for the exchange of patient information. The Receiving System must treat the authorization base as an opaque element. The Receiving System should not depend on any information contained in the authorization base.
	3	The Sending System creates one or two assertions, which can be used to request an access token in the next step.
	4–5	The Sending System requests an access token which can be used in step 6. The Receiving System processes the token request and returns a token response containing, among other elements, an access token. The Sending System must treat the access token as opaque. The Sending System should not depend on any information contained in the access token.
	6–7	By invoking a create interaction regarding a FHIR Task ('notification task') on the Receiving System, the Sending System invites the Receiving System to perform one or more Pull interactions. The Receiving System processes the invitation and sends a technical response to complete the create interaction.
Notification about updated data by Sending Organization	8	The Sending System repeats steps 3–5.
	9–10	The Sending System updates the notification task on the Receiving System using the create interaction. The Receiving System returns a technical response message.

Cancellation by Sending Organization	11–12	The 'cancellation by Sending Organization' option provides a means for the Sending System to cancel/revoke an erroneously created notification. Depending on the implementation at the Sending Organization, the Sending System might have to start the cancellation by revoking the authorization base created in step 2, by sending a revocation request to the Sending Organization's authorization server. The authorization server processes the request and returns a response.
	13	The Sending System repeats steps 3–5.
	14–15	The Sending Organization informs the Receiving Organization by updating the Notification Task on the Receiving System (Task.status is set to "cancelled"). The Receiving System returns a technical response message.
Receiving Organization performs Pull interaction(s)	16	The Receiving System creates one or two assertions, which can be used to request an access token in the next step.
	17–19	The Receiving System requests an access token which can be used to perform the intended Pull interactions. The Sending Organization's authorization server processes the token request and returns a token response containing (among others) an access token. Depending on the Sending System implementation, the Sending System can choose to verify the consent before issuing an access token (preferred option). The Receiving System must treat the access token as an opaque element. The Receiving System should not depend on any information contained in the access token.
	20–23	The Receiving System initiates the intended interactions and processes the responses. The Sending System verifies the access token and can additionally decide to verify the authorization base at this point in the flow.
	24–27	In case the notification task indicates that a workflow task is available that contains (additional) Pull interactions to be performed, the Receiving System obtains this workflow task from the Sending System.
	28–31	The Receiving System initiates the (additional) Pull interactions listed in the workflow task, and processes the responses.

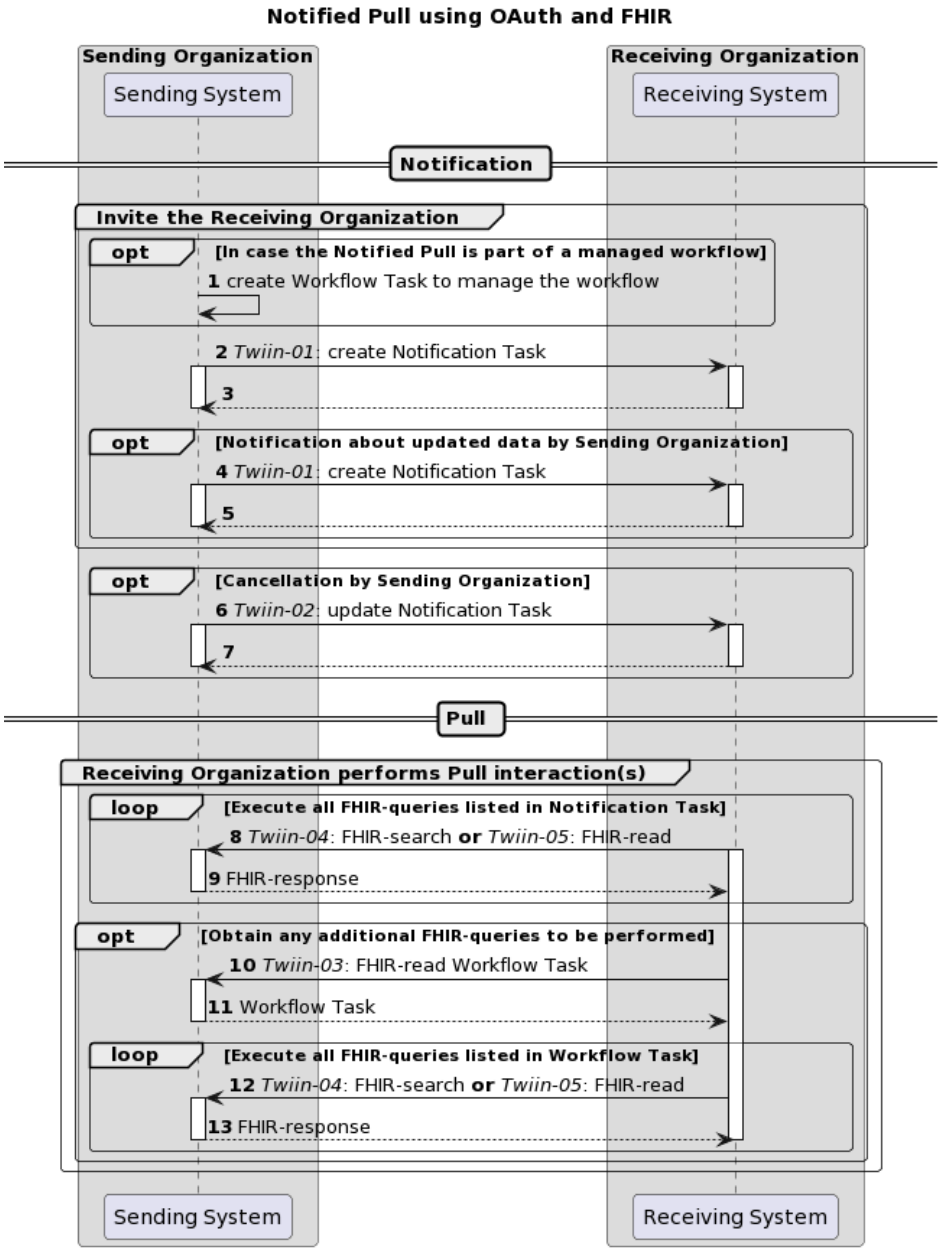
Z1.2.1.1 | BgZ – data interactions

> Original page can be found at: 10.3.1.1 Notified Pull – Data interactions (see page 190)

This chapter describes all relevant interactions for the Notified Pull interaction sequence on data level.

Notified Pull interaction sequence

All relevant interactions for the Notified Pull interaction sequence on data level are displayed in the sequence diagram below.



Description of the interactions in this sequence diagram:

Steps	Description
1	If the Notified Pull is part of a managed workflow involving both the Sending Organization and the Receiving Organization, and this workflow specifies the creation of a FHIR 'workflow task' at the sending system, then the flow starts with a creation of this task on the sending system. See Notification Task vs Workflow Task for additional details.
2-3	The sending system invites the receiving system to perform one or more Pull interactions (FHIR requests) by sending a FHIR task resource ('notification task') to the receiving system using a FHIR create interaction. The receiving system processes the invitation and sends a technical response to complete the create interaction. See 10.5.1 | Twiin-01 | Send Notification Task (see page 217) for a detailed description.
4-5	When the data set for which a notification message has been sent is updated in the sending system, the sending system must inform the receiving system about this update by sending a new notification message. The receiving system processes the invitation and sends a technical response to complete the create interaction. See 10.5.1 | Twiin-01 | Send Notification Task (see page 217) for a detailed description.
6-7	The 'cancellation by Sending Organization' option provides a means for the sending system to cancel or revoke an erroneously created notification. The sending system communicates the cancellation to the receiving system by sending an updated notification task to the receiving system using a FHIR conditional update interaction. The receiving system processes the interaction and sends a technical response to complete the conditional update interaction. See 10.5.2 | Twiin-02 | Cancel Notification Task (see page 225) for a detailed description.
8-9	The receiving system extracts the intended FHIR requests from the notification task listed in Task.input:read-available-resource and Task.input:query-available-resources. Subsequently, the receiving system initiates these FHIR requests and processes the responses. See 10.5.5 | Twiin-05 | Retrieve Resource (see page 232) for a detailed description for the retrieval of resources referenced in Task.input:read-available-resources. See 10.5.4 | Twiin-04 | Search Resource(s) (see page 230) for a detailed description for the retrieval of resources referenced in Task.input:query-available-resources.
10-11	In case that the notification task contains an indication that there is a workflow task at the sending system that contains additional FHIR requests (i.e. when Task.input:get-worflow-task.valueBoolean is true), the receiving system requests the workflow task at the sending system. See 10.5.3 | Twiin-03 | Get Workflow Task (see page 228)

12–13	The receiving system extracts the intended FHIR requests from the workflow task. Subsequently, the receiving system initiates these FHIR requests and processes the responses. See 10.5.5 | Twiin–05 | Retrieve Resource (see page 232) for a detailed description for the retrieval of resources referenced in Task.input:read–available–resources. See 10.5.4 | Twiin–04 | Search Resource(s) (see page 230) for a detailed description for the retrieval of resources referenced in Task.input:query–available–resources.

Notification task vs workflow task

The FHIR task resource used in the notification payload is not meant to track the status of a workflow or healthcare process that initiated the data exchange. When the data that is exchanged using the Notified Pull pattern serves for instance a patient referral or transfer, the status of that process should be tracked using a separate FHIR task resource that is maintained and hosted by the initiator of that process, i.e. the sending system. To keep a clear distinction between these two task resources, the task resource used as notification payload is referred to as the 'notification task', while the task resource that is used to track a healthcare process or workflow is referred to as a 'workflow task'. The notification task is sent from the sending system to the receiving system using a Push interaction (HTTP POST or PUT), while the workflow task is hosted at the sending system, and can be requested by the receiving system using a Pull interaction.

The use of a notification task as notification payload does not require the presence of a workflow task, but when a Notification task is sent in the context of a workflow that is maintained by the initiator of that workflow using a workflow task, the notification task MUST contain a reference to that workflow task.

Availability of BSN

For correct handling the BSN should be available as soon as possible, when this is legally required. The sending system has two possibilities:

- The BSN is sent in the authorization assertion (see page 206) used in the access token request before sending the notification task.
- The BSN is made available through the workflow task resource which is referenced in the basedOn attribute of the notification task resource. The workflow task resource must have a for reference with the identifier filled with the BSN.

The receiving system must support both. Since both variants are possible for the sending system to use, both must be supported by the receiving system, to be able to process from any sending system.

10.3.1 | TTA FHIR – Notified pull (see page 185)

10.4.7 | Network level security (see page 211)

Z1.2.1.2 | BgZ: Authentication & Authorization

Original page can be found at: 10.4.2 | TTA FHIR – Authorization (see page 206)

Attention! The specifications and requirements in this chapter are still a specific implementation for the Notified Pull communication pattern and have not yet been generalized to work for other communication patterns.

Resource server authorization: OAuth 2.0

On application level both the Notification endpoint of the Receiving System and the FHIR endpoint of Sending System are considered as resource endpoints that must be secured by https://www.rfc-editor.org/rfc/rfc6749. This implies that a client that wants to interact with a resource server (FHIR or Notification endpoint) must obtain an access token from an authorization server before it can interact with that resource server. The client must present this access token as bearer token in the HTTP Authorization header of each request to the resource server as specified in https://www.rfc-editor.org/rfc/rfc6750#section-2.1.

For further information on the transaction involved, please go to Twiin-07 | Token Request (see page 270)

Z1.2.2 | TTA Retrieving BgZ – FHIR Direct Pull

Informative only. Please contact info@twiin.nl[74] if you are implementing this exchange pattern.

For this use case the exchange pattern Direct Pull with FHIR is used. Below you will find the description of this exchange pattern.

Original page can be found at: 10.3.4 | TTA FHIR – Pull

This exchange pattern (Direct Pull) is Draft, intended for further coordination with suppliers and healthcare providers.

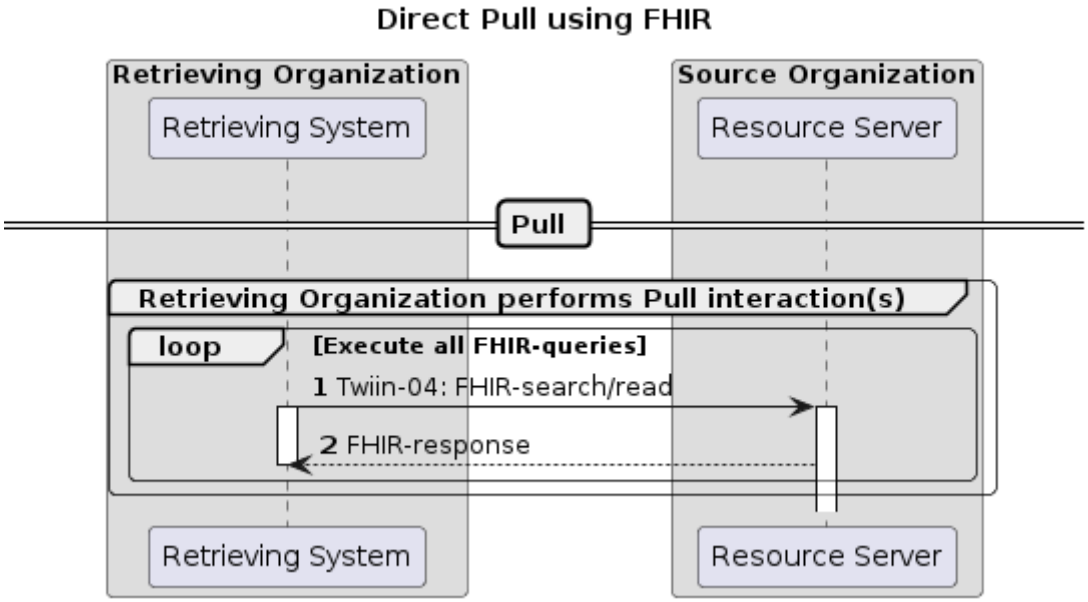
This Twiin Technical Agreement (TTA) describes and specifies technical responsibilities to which parties agree when connecting to exchange transactions to facilitate the Direct Pull.

74. mailto:info@twiin.nl

The retrieval of a patient's medical record might for instance be initiated to retrieve history when the patient is scheduled for a patient requested second opinion. This transaction will only be supported with explicit consent of the patient.

Sequence diagram

The sequence diagram below visualises the flow for the Direct Pull interaction sequence based on HL7 FHIR®.



The section consists of two steps. The steps correspond to the numbers in the sequence diagram.

Retrieving Organization performs Pull interaction(s)	1-2	The Retrieving System executes the necessary FHIR queries to retrieve the necessary information for the usecase. See 10.5.4 | Twiin-04 | Search Resource(s) (see page 230) for a detailed description for the retrieval of resources.

Z1.2.3 | TTA Retrieving BgZ – SOAP Indexed Pull

> Informative only. Please contact info@twiin.nl[75] if you are implementing this exchange pattern.

For this use-case the exchange pattern Index pull via SOAP is used. Below you will find the description of this exchange pattern.

> Original page can be found at: TTA SOAP – Pull – Indexed Pull

This Twiin Technical Agreement (TTA) describes and specifies technical responsibilities to which parties agree when connecting to exchange transactions to facilitate the Indexed Pull.

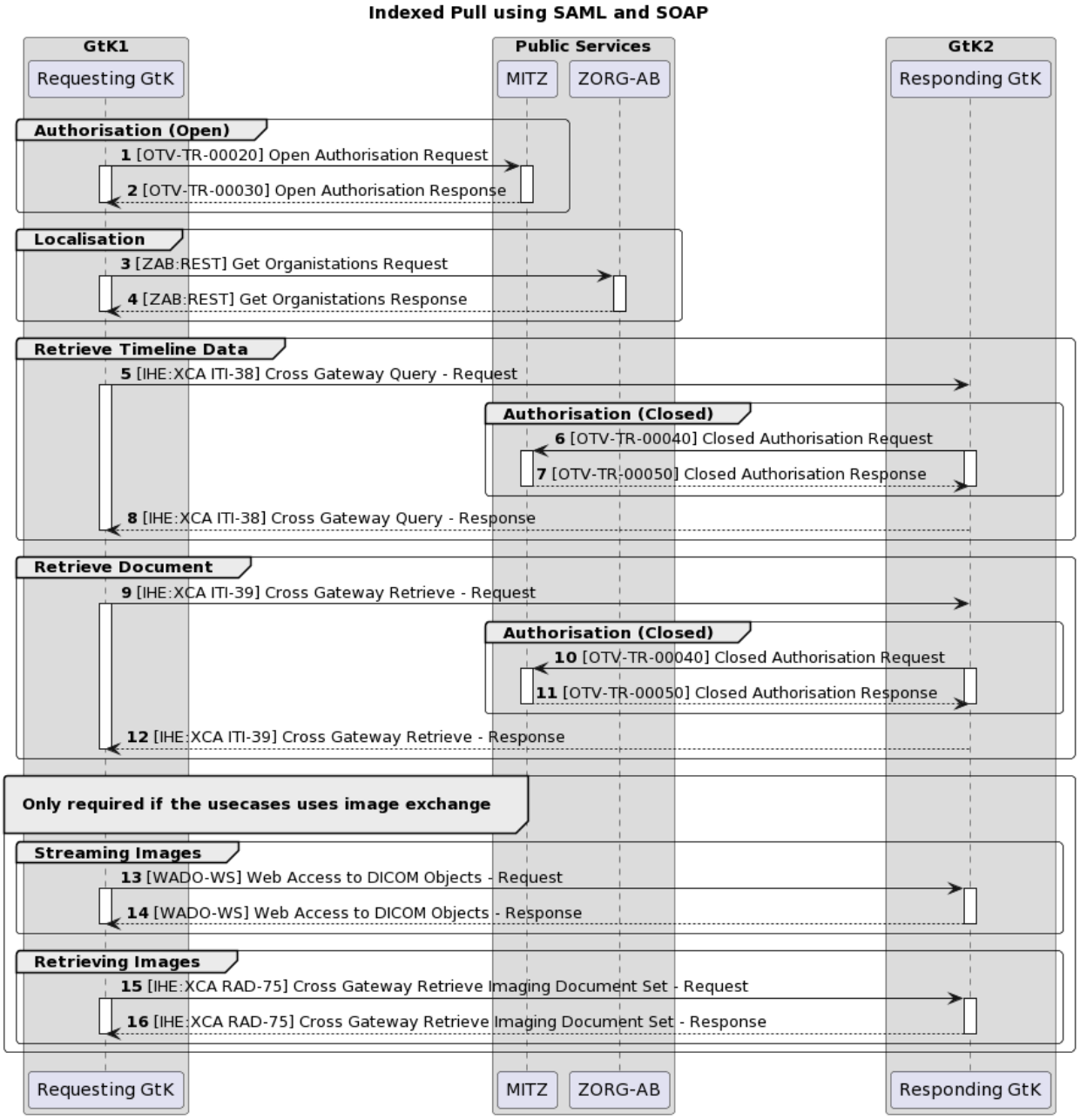
The Indexed Pull starts with several transactions required to locate where data is to be retrieved, aswell as the required endpoints where this data can be retrieved.

Sequence diagram

The sequence diagram below visualizes the full flow for the Indexed Pull interaction sequence.

Twiin describes the transaction between the GtK applications, applications behind these GtK applications can communicate with a GtK in any way they want, as long as the GtK uses the transactions as in this diagram

75. mailto:info@twiin.nl


Indexed Pull using SAML and SOAP
GtK1
Requesting GtK
Public Services
MITZ
ZORG-AB
GtK2
Responding GtK
Authorisation (Open)
1 [OTV-TR-00020] Open Authorisation Request
2 [OTV-TR-00030] Open Authorisation Response
Localisation
3 [ZAB:REST] Get Organistations Request
4 [ZAB:REST] Get Organistations Response
Retrieve Timeline Data
5 [IHE:XCA ITI-38] Cross Gateway Query - Request
Authorisation (Closed)
6 [OTV-TR-00040] Closed Authorisation Request
7 [OTV-TR-00050] Closed Authorisation Response
8 [IHE:XCA ITI-38] Cross Gateway Query - Response
Retrieve Document
9 [IHE:XCA ITI-39] Cross Gateway Retrieve - Request
Authorisation (Closed)
10 [OTV-TR-00040] Closed Authorisation Request
11 [OTV-TR-00050] Closed Authorisation Response
12 [IHE:XCA ITI-39] Cross Gateway Retrieve - Response
Only required if the usecases uses image exchange
Streaming Images
13 [WADO-WS] Web Access to DICOM Objects - Request
14 [WADO-WS] Web Access to DICOM Objects - Response
Retrieving Images
15 [IHE:XCA RAD-75] Cross Gateway Retrieve Imaging Document Set - Request
16 [IHE:XCA RAD-75] Cross Gateway Retrieve Imaging Document Set - Response
Requesting GtK
MITZ
ZORG-AB
Responding GtK

Each section consists of several steps. The steps correspond to the numbers in the sequence diagram.

> For all IHE transactions it is required to include a SAML token. This is usually included in the request the XIS (source) sends to a GtK.
>
> As Twiin decribes the transactions between GtK's, the transaction between a XIS and a GtK can be however the implementators of these applications see fit, as long as the transactions between GtK's include the SAML token as Twiin decribes it to be.
>
> IHE ITI-40 | Provide X-User Assertion (see page 265)

Section	Step	Description
Authorisation (Open)	1	Before initiating the retrieval of the Timeline data, a XIS behind the Initiating GtK sends a request to this GtK. After this request is recieved the GtK first sends an 'open' authorisation request to the Public Service know as 'MITZ' 10.6.3 | Patient Consent – Mitz Transacties (see page 284) – OTV-TR-00020
	2	This request is replied to by MITZ, in this request, the GtK's where data is available, are given back to the Initiating GtK 10.6.3 | Patient Consent – Mitz Transacties (see page 284) – OTV-TR-00030
Localisation	3	After the GtK 'knows' where available data can be retrieved, the Initiating GtK then requests the endpoints at the Public Service know as ZORG-AB 10.6.5 | Addressing – ZORG-AB Transacties (see page 288)
	4	ZORG-AB replies to this request with the endpoints 10.6.5 | Addressing – ZORG-AB Transacties (see page 288)
Retrieve Timeline data	5	Using the endpoints the GtK uses this information to send the query. With this transaction a SAML token is included 10.5.7 | IHE ITI-38 | Cross Gateway Query (see page 237) (TA141) 10.5.7.1 | ITI-38 examples#ITI-38-request
	6	The responding GtK then checks if the patients permission is in check at MITZ 10.6.3 | Patient Consent – Mitz Transacties (see page 284) – OTV-TR-00040
	7	A response is sent back 10.6.3 | Patient Consent – Mitz Transacties (see page 284) – OTV-TR-00050

	8	After the 'closed authentication' transaction is done, the Responding GtK retrieves the metadata at the XIS(es) connected with the Responding Gtk and sends this back to the Initiating Gateway. 10.5.7 | IHE ITI-38 | Cross Gateway Query (see page 237) (TA141) 10.5.7.1 | ITI-38 examples#ITI-38-response The Initiating GtK bundles the replies of the one or more Responding GtK's and sends this back to the XIS application originally requesting the data from the Initiation Request. A Timeline can now be built using this data in the XIS
Retrieve Document	9	Using the Timeline data, a request for a document can now be done from within the XIS (Consumer, connected to the Initiating GtK). The XIS then sends this request to the Initiating GtK. The Initiating GtK then sends a request including a SAML token to the Responding GtK where the XIS (Source, connected to the Responding GtK) is behind and the requested document is available. 10.5.8 | IHE ITI-39 | Cross Gateway Retrieve (see page 249) (TA141) 10.5.8.1 | ITI-39 examples#ITI-39-request
	10	(see step 6) 10.6.3 | Patient Consent - Mitz Transacties (see page 284) - OTV-TR-00040
	11	(see step 7) 10.6.3 | Patient Consent - Mitz Transacties (see page 284) - OTV-TR-00050
	12	After the 'closed authentication' transaction is done, the Responding GtK retrieves the document from the XIS where this document is available and sends this back to the Initiating Gateway 10.5.8 | IHE ITI-39 | Cross Gateway Retrieve (see page 249) (TA141) 10.5.8.1 | ITI-39 examples#ITI-39-response The Initiating Gateway on its turn returns this document to the XIS from where the document is requested from.
Streaming Images	13	the WADO-WS transaction can be used by a Requesting GtK to retrieve DICOM images in a different format and resolution. 10.5.6 | Twiin-06 | WADO-WS (see page 234)
	14	The images are sent back in the requested format 10.5.6 | Twiin-06 | WADO-WS (see page 234)

Retrieving Images	15	It is also possible the request is done for images instead of documents. Prior to this transaction a KOS object is retrieved using steps 9-12. Using the information in the retrieved KOS object images can be requested. 10.5.9 | IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set (see page 256) (TA141) 10.5.9 | RAD-75 examples#RAD-75-request
	16	The images are sent back 10.5.9 | IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set (see page 256) (TA141) 10.5.9 | RAD-75 examples#RAD-75-response

10.3 | Kern Volume 1a - Technical Agreements - CP (see page 185)

10.3.1.1 Notified Pull - Data interactions (see page 190)

Z1.2.4 | TTA Exchanging BgZ - SOAP PUSH

Informative only. Please contact info@twiin.nl[76] if you are implementing this exchange pattern.

For this use-case the exchange pattern PUSH via SOAP is used. Below you will find the description of this exchange pattern.

Original page can be found at: TTA SOAP - Push - Versturen

Work in progress. Please inform us via info@twiin.nl[77] if you use IHE XDR in a production scenario.

Z1.3 | BgZ Volume 2 - Transactions

Within this volume the transactions that are used within the exchange of the BgZ are described.

- Z1.3.1 | Twiin-01 | Send BgZ Notification Task (see page 317)
- Z1.3.2 | Twiin-02 | Cancel BgZ Notification Task (see page 324)
- Z1.3.3 | Twiin-03 | Get BgZ workflow Task (see page 327)

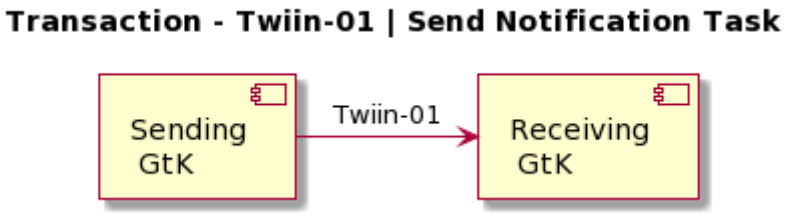
76. mailto:info@twiin.nl
77. mailto:info@twiin.nl

Z1.3.1 | Twiin-01 | Send BgZ Notification Task

> This section is the same as the generic 10.5.1 | Twiin-01 | Send Notification Task (see page 217)

This section describes the transaction needed for the notification.

Scope



This transaction delivers a notification from the Sending GtK to the Receiving GtK based on the specified referral.

Use Case Roles

Actor: Sending GtK

Role: Sends Notification Tasks on behalf of a referring user.

Actor: Receiving GtK

Role: Receives and processes Notification Tasks

Referenced Standards

- HL7® FHIR® standard STU3 https://hl7.org/fhir/stu3

Messages

Request message

The Notification message is sent by the Sending GtK when it needs to notify the Receiving GtK about one or more FHIR® resources that have been made available to the Receiving GtK.

The Notification that is sent to the Receiving GtK must be able to convey at least the following details:

- Identification of Sending GtK, Sending Organization and practitioner
- Identification of Receiving Organization
- References to individual FHIR® resources that have been made available at the Sending GtK
- FHIR® search or read queries that can be used to retrieve FHIR® resources that have been made available at the Sending GtK
- Authorization base (see (TA141) Twiin-07 | Token Request#Authorization-base)

The payload of this message consists of a https://hl7.org/fhir/stu3/task.html resource that contains at least the details mentioned above. This message is sent to communicate both a new and an updated data set to the Receiving GtK. The message results in a Task instance that will be referred to as the Notification Task.

> For the time being, the STU3 version of the FHIR® standard will be used because this TA will first be applied in the context of the BgZ (Basisgegevensset Zorg). Within that context, data is exchanged based on FHIR® STU3. As soon as data has to be exchanged using the Notified Pull pattern for newer FHIR® versions, it becomes opportune to provide or adopt a specification of the Notification for the corresponding FHIR® version.

The Sending GtK must initiate the Notification message using a create[78] interaction, i.e. sending an HTTP POST request to the Task endpoint of the Receiving GtK.

The media type of the HTTP body must be either *application/fhir+json* or *application/fhir+xml*.

When generating the Notification message, the Sending GtK must set the Task attributes as specified in the table below. For complete information on constructing a FHIR® Task Resource, see https://hl7.org/fhir/stu3/task.html .

Attribute	Card.	Description

78. https://hl7.org/fhir/STU3/http.html#create

definitionReference	0..1	This element will be used for routing purposes. The value could determine the organisational unit which will handle the notification. The display of this reference should be filled if no reference to a workflow Task exists and this value shall reference a valid ActivityDefinition resource. See also: 10.4.5 | TTA – Addressing (see page 210) Temporary agreement: We expect the activity definition reference to be in the same section as the references to the substantive resources: • In a thick notification, it will be referenced in the notification itself • In a thin notification, it will be referenced in the workflow task Until additional and more explicit agreements will be specified in the TA Routing, we will use this temporary agreement.
basedOn	0..*	Optional reference to a request–Type resource[79] that produced this event. If a workflow has been initiated and a Workflow Task is present, this must be referenced.
groupIdentifier	1..1	Unique identifier of the data set that is made available. An update to an existing data set at the Sending GtK triggers a new Notification Task, and thus a new Notification Task instance. Multiple Notifications Tasks on the same data set must share one unique identifier so that the Receiving GtK can identify them as relating to the same data set at the Sending GtK.
identifier	**1..1**	Business identifier of the task. This is a required field for traceability and cancellation of individual Notifications.

79. https://hl7.org/fhir/workflow.html#list

status	1..1	The state communicated by this event. Fixed value: • requested See also: https://hl7.org/fhir/stu3/valueset-request-status.html
intent	1..1	Indicates the "level" of actionability associated with the Task[2] (see page 217). Preferred value: • proposal See also: https://hl7.org/fhir/stu3/valueset-request-intent.html
code.coding	**1**..1	A code briefly describing what the task involves: • system = "http://fhir.twiin.nl/fhir/CodeSystem/TaskCode" • code = "pull-notification"
restriction.period	0..1	The period during which the data will be available for retrieval.
requester.agent.identifier	1..1	Identifier of the system that created this Notification. This could be the originating EHR System or the routing gateway system, dependent on which system created the Notification Task.
requester.onBehalfOf.identifier	**1**..1	Identifier of the Organization at which the data has been made available. The identifier shall be in the system “http://fhir.nl/fhir/NamingSystem/ura”
owner.identifier	**1**..1	Identifier of the Receiving Healthcare Organization. The identifier shall be in the system “http://fhir.nl/fhir/NamingSystem/ura”

input:authorization-base	**1..1**	The (TA141) Twiin-07 | Token Request#Authorization-base to be used when retrieving the data.
		Constraints:
		• type.coding
		  • system = "http://fhir.twiin.nl/fhir/CodeSystem/TaskParameter"
		  • code = "authorization-base".
		• valueString

input:get-workflow-task	0..1	An indicator to show whether or not all available resources are part of this Notification.
		Constraints:
		• type.coding
		  • system = "http://fhir.twiin.nl/fhir/CodeSystem/TaskParameter"
		  • code = “get-workflow-task”
		• valueBoolean
		Where valueBoolean:
		• true, the basedOn Workflow Task must be retrieved to get all available resources;
		• false (default), all available resources are available in the next (two) input slices.
		If this input slice is not added, the presumed value shall be false.

input: read-available-resource	0..*	The FHIR®-read interactions that can be performed to retrieve the data that was made available.
		Constraints:
		• type.coding (one or more of:)
		  • *Generic typing:*
		  • system = "http://hl7.org/fhir/restful-interaction"
		  • code = "read"
		  • *SNOMED CT typing **(deprecated)**:*
		  • system = “http://snomed.info/sct”
		  • code = a SNOMED CT code
		  • *LOINC typing **(deprecated)**:*
		  • system = “http://loinc.org”
		  • code = a LOINC code
		  • *FHIR profile typing **(prefered)**:*
		  • system = “http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
		  • code = a FHIR profile-id, e.g. "http://nictiz.nl/fhir/StructureDefinition/zib-DrugUse"
		• valueReference format
		  • [resourcetype]/[id]
		Where:
		• resourcetype denotes a FHIR® resourcetype;
		• id represents a logical id of a FHIR® resource instance.

input: query-available-resources	0..*	The FHIR®-search interactions that can be performed to retrieve the data that was made available.
		Constraints:
		• type.coding (one or more of:)
		  • *Generic typing:*
		  • system = "http://hl7.org/fhir/restful-interaction"
		  • code = "search-type"
		  • *SNOMED CT typing **(deprecated)**:*
		  • system = "http://snomed.info/sct"
		  • code = a SNOMED CT code
		  • LOINC typing ***(deprecated)***:
		  • system = "http://loinc.org"
		  • code = a LOINC code
		  • *FHIR profile typing **(prefered)***:
		  • system = "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile"
		  • code = a FHIR profile-id, e.g. "http://nictiz.nl/fhir/StructureDefinition/zib-DrugUse"
		• valueString format
		  • [resourcetype]{?[parameters]}
		Where:
		• Resourcetype denotes a FHIR® resourcetype;
		• parameters can be added to refine a FHIR®-search.

The Sending GtK MAY choose not to list the available FHIR® resources in Task.input. In that case, the Sending GtK MUST provide a reference to a Workflow Task resource in Task.basedOn. This Workflow Task MUST list the available FHIR® resources in Task.input, in the same format that is specified for the Notification Task. Additionally, in this case the Notification Task MUST have an entry in Task.input with the following values:

- Task.input.type.coding.system: "http://fhir.twiin.nl/fhir/CodeSystem/TaskParameter"
- Task.input.type.coding.value: "get-workflow-task"
- Task.input.valueBoolean: true

The Receiving GtK must accept both media types *application/fhir+json* and *application/fhir+xml*.

On receiving the submission, the Receiving GtK must validate the resource and respond with one of the HTTP codes defined in the (TA141) 10.5.1 | Twiin-01 | Send Notification Task .

The Notification should trigger an event in the Receiving GtK to facilitate the expected Pull.

Persistence of the Notification Task as a FHIR® resource is not required, whether it is necessary to persist is purely up to the receiving GtK and its internal implementation.

When the data set for which a Notification message has been sent is updated in the Sending GtK, the Sending GtK must inform the Receiving GtK about this update by sending a new Notification Message. In this case, Task.input:read-available-resource and Task.input:query-available-resources should only list the updated FHIR® resources. This way, the update can be communicated as a delta to the original data set. This relieves the Receiving GtK of determining which resources have changed in a larger set of resources. Note that the value of Task.identifier for the new Notification Task must differ from the value of Task.identifier Notification Task for the original data set, while the value of Task.groupIdentifier must be the same for all Notification Tasks on the same data set. This way, consecutive Notification Tasks on the same data set can be related to each other by the value of Task.groupIdentifier.

Response message

This message must be provided when a success or error condition needs to be communicated in response to an inbound request message. Success is only indicated once the Notification is received and completely processed.

To enable the Sending GtK to know the outcome of technical / syntactic processing of the Notification Task, the Receiving GtK must return either an empty body or an OperationOutcome resource. This body must be accompanied with the correct HTTP status code, e.g.:

- 200 OK – Notification received and not persisted.
- 201 Created – Notification received and persisted. In this case http-headers Location and Etag should be filled.
- 400 Bad Request – Notification could not be parsed or failed basic FHIR® validation rules.
- 404 Not Found – Resource type not supported, or wrong endpoint.
- 412 Precondition Failed – The processing of the Notification Task could not be finished, since the criteria were not selective enough.
- 422 Unprocessable Entity – The Notification Task resource violated applicable server business rules. This should be accompanied by an OperationOutcome resource providing additional detail.

Whether or not the resources referenced from any of the input elements can be retrieved shall not be a factor in the HTTP status.

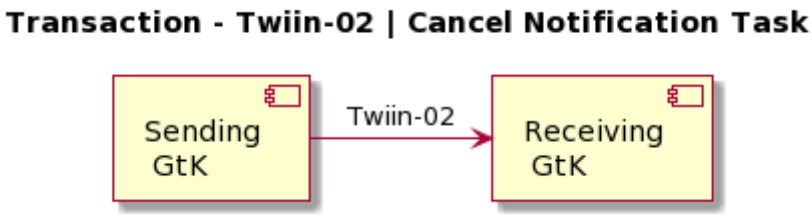
The Sending GtK processes the response according to application defined rules.

Z1.3.2 | Twiin-02 | Cancel BgZ Notification Task

> This page is the same as the generic 10.5.2 | Twiin-02 | Cancel Notification Task (see page 225)

This section describes the transaction needed for the cancellation of the notification.

Scope



This transaction delivers a cancellation notification from the Sending GtK to the Receiving GtK based on the specified referral. Twiin only requires that a GtK can receive this message, sending and processing the message is optional.

Actor	Sending Twiin-02	Receiving Twiin-02	Processing Twiin-02
Sending GtK	Optional	N/A	N/A
Receiving GtK	N/A	Mandatory	Optional

Use Case Roles

Actor: Sending GtK

Role: Sends Cancellation Notification Tasks on behalf of a referring user.

Actor: Receiving GtK

Role: Receives and processes Cancellation Notification Tasks

Referenced Standards

- HL7® FHIR® standard STU3 https://hl7.org/fhir/stu3

Messages

Request message

The Notification Cancellation request message is sent when the Sending GtK needs to send a cancellation of a previous Notification to the Receiving GtK. Just as the Notification message, the payload of this message consists of a FHIR® STU3 Task resource.

The Sending GtK can cancel a previous Notification using a conditional update[80] interaction on the Task that represents that previous Notification. This is done by sending an HTTP PUT request to the Task

endpoint of the Receiving GtK, where the value of Task.identifier of that previous Notification is included in the query parameters of the PUT request.

The media type of the HTTP body must be either *application/fhir+json* or *application/fhir+xml*.

When generating the Notification Cancellation message, the Sending GtK must set the Task attributes as specified in the table below. For complete information on constructing a FHIR® Task Resource, see https://hl7.org/fhir/stu3/task.html .

Attribute	Card.	Description
identifier	1..1	Business identifier of the Notification Task; the value of this identifier must be equal to the value of the identifier of the Notification Task that is to be cancelled.
status	1..1	The state communicated by this event. Fixed value: • cancelled
intent	1..1	Indicates the "level" of actionability associated with the Task[1] (see page 225). Preferred value: • proposal See also: https://hl7.org/fhir/stu3/valueset-request-intent.html
code.coding	1..1	A code briefly describing what the task involves: • system = "http://fhir.twiin.nl/fhir/CodeSystem/TaskCode" • code = "pull-notification"

In the absence of a reference to the patient (for example, within the Workflow Task), the token request for this cancellation SHALL include the patient's BSN within the assertion.

The Receiving GtK must accept both media types *application/fhir+json* and *application/fhir+xml*.

On receipt of the submission, the Receiving GtK must validate the resource and respond to the cancellation message according to the requirements specified in Notification response (see page 225).

The Notification SHOULD trigger an event in the Receiving GtK to cancel any intended Pull interaction.

Persistence of the Notification Task as a FHIR® resource is not necessary.

80. http://hl7.org/fhir/stu3/http.html#cond-update

Notification response

This message must be provided when a success or error condition needs to be communicated in response to an inbound Notification message. Success is only indicated once the Notification is received and completely processed.

To enable the Sending GtK to know the outcome of technical / syntactic processing of the Notification Task, the Receiving GtK must return either an empty body or an OperationOutcome resource. This body must be accompanied with the correct HTTP status code, e.g.:

- 200 OK – Notification received and not persisted.
- 201 Created – Notification received and persisted. In this case http-headers Location and Etag should be filled.
- 400 Bad Request – Notification could not be parsed or failed basic FHIR® validation rules.
- 404 Not Found – Resource type not supported, or wrong endpoint.
- 412 Precondition Failed – The processing of the Notification Task could not be finished, since the criteria were not selective enough.
- 422 Unprocessable Entity – The Notification Task resource violated applicable server business rules. This should be accompanied by an OperationOutcome resource providing additional detail.

The Sending GtK processes the response according to application defined rules.

Z1.3.3 | Twiin-03 | Get BgZ workflow Task

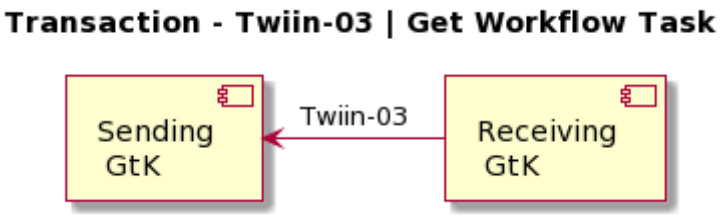
> This page is the same as the generic 10.5.3 | Twiin-03 | Get Workflow Task (see page 228)

This section describes the transaction of the retrieval of the Workflow Task.

> If a workflow Taks is used its definitionReference must be filled and shall reference a valid ActivityDefinition resource.

> Temporary agreement: We expect the activity definition reference to be in the same section as the references to the substantive resources:
>
> - In a thick notification, it will be referenced in the notification itself
> - In a thin notification, it will be referenced in the workflow task
>
> Until additional and more explicit agreements will be specified in the TA Routing, we will use this temporary agreement.

Scope



This transaction supports getting the Workflow Task by the Requesting System at the Resource Server.

Use Case Roles

Actor: Requesting GtK

Role: Requests the workflow Task on behalf of a requesting user.

Actor: Responding GtK

Role: Processes the request and responds with the requested resource.

Referenced Standards

- HL7® FHIR® standard STU3 https://hl7.org/fhir/stu3

Messages

Request message

The requesting system wants to obtain the workflow Task for information about a known workflow. The workflow Task is retrieved using a the FHIR® read interaction, i.e. executing an HTTP GET request to the Task endpoint of the resource server.

```
GET [base]/Task/[id]
```

The requesting system may provide the HTTP Accept header. Valid values for this header are *application/fhir+json* or *application/fhir+xml*. If none is set, the resource server will use its default.

Response message

The resource server returns the workflow Task that is requested.

The payload of this message consists of a https://hl7.org/fhir/stu3/task.html resource that contains relevant information to the workflow. This message is returned to the Receiving System.

The media type of the HTTP body must be either *application/fhir+json* or *application/fhir+xml*, based on the Accept header or default response content type.

At this time there is no generic specification of the contents of the workflow Task more specific than the FHIR® specification.

Persistence of the Workflow Task as a FHIR® resource is not necessary.

When an error occurs an OperationOutcome resource must be returned with more details on the reason.

The HTTP response must be accompanied with the correct HTTP status code, e.g.:

- `200` OK – The request is accepted and responded
- `401` Not Authorized - Authorization is required for the interaction that was attempted
- `404` Not Found – The request could not be processed, i.e. the resource with that id doesn't exist.
- `410` Gone – The request could not be processed, because the resource does not exist anymore.

The requesting system processes the response according to application defined rules.

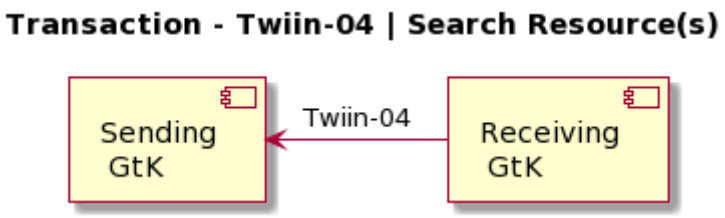
Z1.3.4 | Twiin-04 | Search BgZ Resource(s)

> This page is the same as the generic 10.5.4 | Twiin-04 | Search Resource(s) (see page 230)

This section describes the transaction of the retrieval of the FHIR® resources.

> In the communication pattern notified pull these resources are referenced in the input field of the Notification or Workflow Task.
> These input fields contain valueString in the input slice: query-available-resources.

1. Scope



This transaction supports the request of resources by the Requesting GtK to the Resource Server.

2. Use Case Roles

Actor: Requesting GtK

Role: Sends a request for resources on behalf of a retrieving user.

> In the communication pattern notified pull, this is the Receiving GtK.

Actor: Responding GtK

Role: Processes the request and responds with the requested resources.

> Note: In the communication pattern notified pull, this is the Sending GtK.

3. Referenced Standards

- HL7® FHIR® standard STU3 https://hl7.org/fhir/stu3

4. Messages

4.1. Request message

The requesting GtK wants to obtain the resources that were referenced in the Task. These resources are retrieved using a FHIR® search interaction, i.e. executing an HTTP GET request to the resource servers FHIR® endpoint. If there is a relative path, the input valueString must be appended to the FHIR® base-url.

```
GET [base]/<ResourceType>?parameter=value
```

> **Percent-encoding of query parameters**
>
> When constructing URLs that include query parameters (e.g., code=...), it is important to percent-encode any reserved characters that could cause syntactic ambiguity, in accordance with https://datatracker.ietf.org/doc/html/rfc3986.
>
> **Exception**
> The slash character (/) may appear unencoded in query parameter values, as it is explicitly allowed in the query component of a URI per RFC 3986 (see Appendix A), and is commonly accepted by web servers and FHIR implementations.

The requesting GtK may provide the HTTP Accept header. Valid values for this header are *application/fhir+json* or *application/fhir+xml*. If none is set, the resource server will use its default.

4.2. Response message

The responding GtK returns the resource(s) that are requested.

The payload of this message consists of a FHIR® Bundle resource that contains the requested resource(s). This message is returned to the Receiving GtK.

The media type of the HTTP body must be either *application/fhir+json* or *application/fhir+xml*, based on the Accept header or default response content type.

When an error occurs an OperationOutcome resource must be returned with more details on the reason.

The HTTP response must be accompanied with the correct HTTP status code, e.g.:

- `200` OK – The search was processed and a valid response was returned
- `400` Bad Request – The search could not be processed or failed basic FHIR® validation rules
- `401` Not Authorized – Authorization is required for the interaction that was attempted
- `404` Not Found – The resource type not supported

The requesting GtK processes the response according to application defined rules.

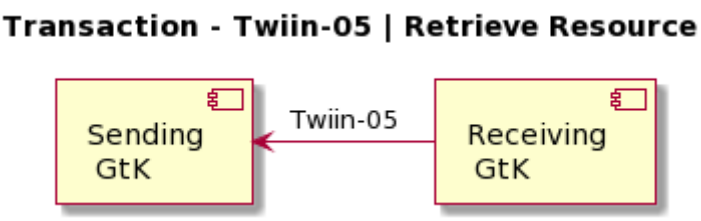
Z1.3.5 | Twiin-05 | Retrieve BgZ Resource

> This page is the same as the generic 10.5.5 | Twiin-05 | Retrieve Resource (see page 232)

This page describes the transaction of the retrieval of the FHIR® resources.

> In the communication pattern notified pull these resources are referenced in the input field of the Notification or Workflow Task.
> These input fields contain valueReference in the input slice: read-available-resource.

Scope



This transaction supports the request of resources by the Requesting System to the Resource Server.

Use Case Roles

Actor: Requesting GtK

Role: Sends a request for a specific resource on behalf of a retrieving user.

> In the communication pattern notified pull, this is the Receiving GtK.

Actor: Responding GtK

Role: Processes the request and responds with the requested resource.

> Note: In the communication pattern notified pull, this is the Sending GtK.

Referenced Standards

- HL7® FHIR® standard STU3 https://hl7.org/fhir/stu3

Messages

Request message

The requesting GtK wants to obtain the resources that were referenced in the Task. These resources are retrieved using a FHIR® read interaction, i.e. executing an HTTP GET request to the resource servers FHIR® endpoint. If there is a relative path, the input valueReference must be appended to the FHIR® base-url.

```
GET [base]/<ResourceType>/<id>
```

> The requesting GtK may provide the HTTP Accept header. Valid values for this header are *application/fhir+json* or *application/fhir+xml*. If none is set, the resource server will use its default.

Response message

The responding GtK returns the resource that is requested.

The payload of this message is the requested FHIR® resource. This message is returned to the requesting GtK.

The media type of the HTTP body must be either *application/fhir+json* or *application/fhir+xml*, based on the Accept header or default response content type.

When an error occurs an OperationOutcome resource must be returned with more details on the reason.

The HTTP response must be accompanied with the correct HTTP status code, e.g.:

- `200` OK – The search was processed and a valid response was returned
- `401` Not Authorized – Authorization is required for the interaction that was attempted
- `404` Not Found – The resource could not be found
- `410` Gone – The resource was deleted

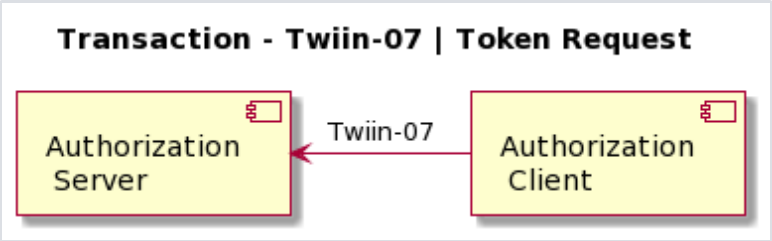
The requesting GtK processes the response according to application defined rules.

Z1.3.7 | Twiin-07 | Token Request

> This page is the same as the generic 10.3.7 | Twiin – 07 | Token Request (see page 270)

This page describes the transaction of the retrieval of the OAuth tokens

Scope



This transaction supports the request of an authentication token by the Requesting System to the Resource Server.

Use Case Roles

Actor: Authorization Client

Role: Client requesting an access token to authorize RESTful transactions.

Actor: Authorization Server

Role: Server that grants access tokens

Relevant Standards

- *OAuth 2.1*: The OAuth 2.1 Authorization Framework, published as draft-ietf-oauth-v2-1-01, 1 February 2021.
- *JWT Access Token*: JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens, published as draft-ietf-oauth-access-token-jwt-10, September 2020.
- *RFC4648*: The Base16, Base32, and Base64 Data Encodings, October 2006
- RFC6749: The OAuth 2.0 Authorization Framework, October 2012.
- *RFC7519*: JSON Web Token (JWT), May 2015.
- *RFC7522*: Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants, May 2015.
- *RFC7523*: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants, May 2015.
- *RFC7515*: JSON Web Signature (JWS), May 2015.
- *RFC7518*: JSON Web Algorithms (JWA), May 2015.
- *RFC8705*: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens, February 2020.

Messages

Request message

The resource server must be able to authenticate the client as a trusted client. The client is specified as the **system** that submits the access token request (not to be confused with the **organization** for which that system is acting). The OAuth specs leave room for different authentication methods for client authentication. The authentication methods that are proposed in the OAuth 2.0 core specifications (https://www.rfc-editor.org/rfc/rfc6749.html#section-2.3) all rely on the exchange of shared secrets. The use of shared secrets is considered as a security risk since they are prone to leakage. The use of an authentication method that relies on digital signatures using asymmetric cryptography offers better security. Therefore, the client must authenticate itself by providing a client assertion by means of a signed JWT as specified in https://www.rfc-editor.org/rfc/rfc7523#section-2.2.

The client assertion is a JWS Compact Serialized JWT that consists of a header, a payload, and a signature. The signature is created using a key pair belonging to the initiating system or to a third party trusted by the initiating system.

The header carries the claims listed below:

Claim	Description	Required

typ	Token type, must be “JWT”	Yes
alg	Cryptographic algorithm used to sign the client assertion. See https://www.rfc-editor.org/rfc/rfc7518#section-3.1 . All algorithms are described at (TA141) Twiin-07 | Token Request.	Yes
kid	Identifier of the key pair used to sign this JWT. See https://www.rfc-editor.org/rfc/rfc7515#section-4.1.4.	Yes

The payload contains a set of claims listed below:

Claim	Description	Required
jti	Unique identifier of the client assertion. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.7. The jti (JWT ID) is a unique identifier for a token and must not be reused. An assertion containing a duplicate jti (i.e., one that has been previously processed) shall be rejected to prevent replay attacks. Implementations should maintain a mechanism to track used jti values for the duration of their validity period.	Yes
iss	Identifier of the system that issued the client assertion. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.1 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	Yes
iat	The time at which the client assertion was issued. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.6. If there is an agreed age of a client assertion.	Conditional

exp	The expiration time on or after which the client assertion shall not be accepted for processing. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.4 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3. > The expiration time (exp) claim in the assertion shall not exceed 5 minutes (300 seconds) from the time of issuance. Any assertion with an exp value set beyond this limit must be rejected.	Yes
nbf	The time before which the token shall not be accepted for processing. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.5 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	No
aud	Identifier of the authorization server token endpoint where this client assertion is to be used. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.3 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	Yes
sub	Identifier of the OAuth client that requests access. This claim must match the value of the client_id parameter in the access token request. Note that the client is specified as the system that submits the access token request.	Yes

The Issuer of the client assertion may include additional claims in the assertion, but the Issuer shall not require the authorization server to process these claims.

The exchange of the public key that corresponds to the private key that was used to sign the client assertion between the Assertion Issuer and the authorization server is beyond the scope of this normative specification. This is the added value of Twiin. Twiin unambiguously describes the agreements that system providers typically need to make with each other.Note that the authorization server can authenticate the client on network level by the client certificate that the client must present during the mTLS handshake (see section Network level security (see page 206)). In theory, this could be used by the authorization server to authenticate the client on application level. However, this may cause problems since it introduces additional and potentially unwanted requirements on TLS termination and related matters. Therefore, a client must always provide a client assertion in the access token request.

Authorization grant

OAuth 2.0 requires the use of an authorization grant to request an access token. As specified in https://www.rfc-editor.org/rfc/rfc6749#section-1.3 “an authorization grant is a credential representing the resource owner's authorization (to access its protected resources) used by the client to obtain an access token.” OAuth 2.0 specifies several different authorization grants. Additionally, there are several RFC’s that specify extension grants, e.g. https://www.rfc-editor.org/rfc/rfc6749#section-4.5. Because this TA applies to situations where a resource client is acting on behalf of a user (health professional) that works

for an organization (healthcare provider), the use of the JWT Bearer Assertion authorization grant as specified in https://www.rfc-editor.org/rfc/rfc7523#section-2.1 is the most suitable authorization grant. This means that the resource client must provide an authorization assertion in each access token request to identify the acting user, organization, and authorization base to prove that it is authorized to access the requested data. This authorization assertion acts as the authorization grant that the client can present to prove that it is authorized to access the protected resources.

The authorization assertion is a JWS Compact Serialized JWT that consists of a header, a payload, and a signature. The signature is created using a key pair belonging to the initiating organization or to a third party trusted by the initiating organization.

The header carries the claims listed below:

Claim	Description	Required
typ	Token type, must be "JWT"	Yes
alg	Cryptographic algorithm used to sign the authorization assertion. See https://www.rfc-editor.org/rfc/rfc7518#section-3.1 . All algorithms are described at (TA141) Twiin-07 | Token Request.	Yes
kid	Identifier of the key pair used to sign this JWT. See https://www.rfc-editor.org/rfc/rfc7515#section-4.1.4.	Yes

The payload contains a set of claims that carry information required by NEN 7512 and NEN 7513.

Claim	Description	Required
jti	Unique identifier of the authorization assertion. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.7. > The jti (JWT ID) is a unique identifier for a token and must not be reused. An assertion containing a duplicate jti (i.e., one that has been previously processed) shall be rejected to prevent replay attacks. Implementations should maintain a mechanism to track used jti values for the duration of their validity period.	Yes
iss	Identifier of the system that issued the authorization assertion. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.1 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	Yes

iat	The time at which the authorization assertion was issued. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.6. This is only required if there is an agreed age of an authorization assertion.	Conditional
exp	The expiration time on or after which the authorization assertion shall not be accepted for processing. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.4 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3. The expiration time (exp) claim in the assertion shall not exceed 5 minutes (300 seconds) from the time of issuance. Any assertion with an exp value set beyond this limit must be rejected.	Yes
nbf	The time before which the token shall not be accepted for processing. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.5 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	No
aud	Identifier of the authorization server token endpoint where this authorization assertion is to be used. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.3 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	Yes
sub	Identifier of the **healthcare organization** that requests access. **URA nummer** is mandatory, *additionaly* other identifiers may be added. The codesystem (`issuing_system`) for the identifier is also mandatory. For the URA this is OID: 2.16.528.1.1007.3.3 5.1 | Vertrouwen: Identificatie (see page 62) Allowed format for this identifier is: • `http://fhir.nl/fhir/NamingSystem/ura|<URA>`	Yes

sub_role	Code of the type of the **organization** (healthcare supplier) that requests access. **RoleCodeNL** is mandatory. The codesystem (`issuing_system`) for the identifier is also mandatory. For the RoleCodeNL this is OID: 2.16.840.1.113883.2.4.15.1060 Sub role is required when the responding party needs to check the patient consent. For instance when a user does not have an authorization base when requesting patient information.	Conditional
user_id	Identifier of the **responsible user** (healthcare professional) who requests access. **Preferred: UZI nummer** Allowed formats for this identifier are: • `urn:oid:2.16.528.1.1007.3.1.<UZI>` (without leading zero of UZI) • `http://fhir.nl/fhir/NamingSystem/uzi-nr-pers|<UZI>` 5.1 | Vertrouwen: Identificatie (see page 62) **User or system** In some cases a system is allowed to access data without a specific user being involved. Whenever there is a request for patient information, the identifier of the responsible user MUST be communicated. The only known exception to this rule is the retrieval of the Workflow Task that is requested based on the Notification Task in the TTA Notified Pull.	Yes

user_role	Code of the role of the responsible user (healthcare professional) who requests access. **Preferred: UZI rolcode** Allowed formats for this code are: • `urn:oid:2.16.840.1.113883.2.4.15.111.<UZI rolcode` (without leading zero, both before and after the . within the UZI rolcode) • `http://fhir.nl/fhir/NamingSystem/uzi-rolcode|<UZI rolcode>` 5.1 | Vertrouwen: Identificatie (see page 62) User identification (user_id and user_role claims) is only required in the authorization assertion when access to patient data is requested. This implies that these claims are not required in authorization assertions used in access token requests for Notification endpoints.	Conditional
authorizer	Identifier of the **healthcare organization** that grants access. **URA nummer** is mandatory, *additionaly* other identifiers may be added. The codesystem (`issuing_system`) for the identifier is also mandatory. For URA this is OID: 2.16.528.1.1007.3.3 5.1 | Vertrouwen: Identificatie (see page 62) Allowed format for this identifier is: • `http://fhir.nl/fhir/NamingSystem/ura|<URA>`	Yes
authorization_base	See Authorization base	No

patient	Identifier of the patient for whom data is exchanged. 5.1 | Vertrouwen: Identificatie (see page 62)	Conditional

> Allowed format for this identifier is:
>
> - `urn:oid:2.16.840.1.113883.2.4.6.3.<BSN>` (without leading zero of BSN)

> Patient identification is only required when the Sending System requests access to the Notification endpoint of the Receiving System and the Sending System does not provide a Workflow Task that refers to a Patient resource containing the BSN of the patient. This way, the Receiving System is always able to identify a patient by BSN based on a Notification. The Receiving System must support receiving the BSN through the patient claim.

The Issuer of the authorization assertion may include additional claims in the authorization assertion, but the Issuer shall not require the authorization server to process these claims.

The exchange of the public key that corresponds to the private key that was used to sign the authorization assertion between the Assertion Issuer and the authorization server is beyond the scope of this normative specification. Therefore, system vendors have to make mutual agreements about the exchange of these public keys.

Authorization scope

The scope defines the requested access to the FHIR Server as specified in https://www.rfc-editor.org/rfc/rfc6749#section-3.3 . If a scope is provided in the access token request or access token response, it must be expressed in a string of space delimited scopes as defined in http://hl7.org/fhir/smart-app-launch/scopes-and-launch-context.html#scopes-for-requesting-clinical-data . The following additional requirements apply to the scope values:

- When requesting an access token for a Notification endpoint at the Receiving System, the scope value must be one of:
  - system/Task.c?code=http://fhir.twiin.nl/fhir/CodeSystem/TaskCode|pull-notification (create)
  - system/Task.u?code=http://fhir.twiin.nl/fhir/CodeSystem/TaskCode|pull-notification (update)
- When requesting an access token for a FHIR endpoint at the Sending System, the query parameters in the scopes must match (a subset of) the queries in the FHIR search requests listed in Task.input of the Notification Task (see Notification message (see page 217)).

The client must provide the requested scope in the access token request, except for cases where an authorization base is provided in the access token request as part of the authorization assertion.

The authorization server must provide the granted access scope in the access token response in accordance with https://www.rfc-editor.org/rfc/rfc6749#section-5.1 and the requirements mentioned above. The issued access token must grant access to the granted scope that the authorization server specifies in the access token response. The granted scope must be equal to or less than the scope that can be derived from the authorization base consent token.

Access token request

Based on the paragraphs above each access token request contains the parameters listed below:

Parameter	Value	Required
grant_type	"urn:ietf:params:oauth:grant-type:jwt-bearer"	Yes
assertion	JWT authorization assertion as specified in paragraph Authorization grant.	Yes
client_assertion_type	"urn:ietf:params:oauth:client-assertion-type:jwt-bearer"	Yes
client_assertion	JWT client assertion as specified in paragraph Request message.	Yes
client_id	ID of the resource client. This ID is issued by the authorization server. The value of the "client_id" parameter must identify the same client as is identified by the client assertion.	Yes
scope	Space separated list of requested scopes, see paragraph Authorization scope. The scope must not be encoded before the `x-www-form-urlencoded` encoding. e.g. before encoding it should look like: `patient/Observation.s?code=http://loinc.org|29463-7`	Conditional

Note that the access token request effectively contains two JWT assertions:

1. A client assertion that is used to authenticate the client. This assertion identifies and authenticates the **system** that is requesting access.

2. An authorization assertion that is used as an authorization grant. This assertion identifies both the **organization** and **user** that are requesting access.

Separating client authentication from client authorization in two separate assertions enables the client to select different Assertion Issuers for the two assertions. The targeted authorization server must register both Issuers as trusted Assertion Issuers for a specific client.

Access token requirements

The access token will be processed only by the party that issued the access token. Therefore, the form and contents of the token are determined by the authorization server (audience), so the access token is opaque to the resource client. The resource client should not take any dependency on the format or contents of an access token. The authorization server MAY issue certificate bound access tokens as specified in https://www.rfc-editor.org/rfc/rfc8705 , but this is not mandatory. To enable the server to issue certificate bound access tokens, the client MUST support mTLS for access token and resource requests as specified in section Network level security: mTLS 1.3.

The validity period of an OAuth 2.0 access token shall not exceed 15 minutes. Implementations must ensure that the exp (expiration) claim in the token is set accordingly, with a maximum lifetime of 900 seconds (15 minutes) from the time of issuance.

Clients should be designed to handle token expiration by obtaining a new access token as required.

Authorization base

When the Sending System receives a request from the Receiving System to access certain data, it is the primary responsibility of the Sending System to verify that the Receiving System is authorized to access that data. When a system receives an authorization base, it shall not use the UZI-rolcode to determine whether access should be granted. When publishing data on a resource server to be collected by the Receiving System, many Sending Systems register the authorization to access that data as an authorization base of some kind. To facilitate that authorization process, the Sending System may submit the authorization base (or a reference to it) to the Receiving System as part of the Notification (see section Notification message (see page 218)). If the Receiving System received an authorization base in the Notification, it must include that authorization base in the access token request to the Sending System (see section Authorization grant). This enables the authorization server of the Sending System to determine if the requested access can be granted based on the provided authorization base.

Since an authorization base is to be processed by the Sending System only, the form and contents of an authorization base are determined by the Sending System. The Receiving System should not take any dependency on the format or contents of an authorization base.

User authentication

Healthcare professionals are identified in their EHR system by logging in with their personal account. When a user of the Receiving System wants to request resources at the Sending System, the Sending System must be able to identify the user at the Receiving System as a legitimate healthcare professional who is working for the receiving organization before it can provide the requested data. Therefore, the Receiving System must implement the appropriate means to ensure the authenticity of the user.

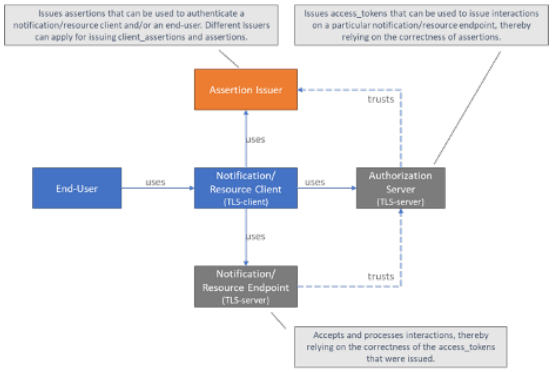
The Sending System can identify the healthcare professional at the receiving organization that is requesting patient data by the following claims in the authorization assertion of the access token request (see Authorization grant):

- **sub**: Identifier of the healthcare organization
- **user_id**: Identifier of the responsible user (healthcare professional)
- **user_role**: Code of the role of the responsible user (healthcare professional)

The type of identifiers used for organizations and users is beyond the scope of this TA. The same applies to the use of role codes.

Trust relationships

The picture below shows the different roles involved in the interactions, and clarifies the dependencies between these roles.



The Sending System hereby performs the following roles:

- Notification Client;
- Resource Server Endpoint.

The Receiving System performs the roles:

- Notification Server Endpoint;
- Resource Client.

Sending System and Receiving System both implement the role of Authorization Server.

The role of Assertion Issuer can be performed by a third-party, but can also be performed by the Sending System or by the Receiving System. Assertion Issuers producing client assertions do not necessarily have to produce authorization assertions as well. Different Issuers can be used for these types of assertions. Before issuing a client assertion or an authorization assertion, the Assertion Issuer has to make sure that applicable requirements regarding user authentication and other mutual security agreements between the Sending System and Receiver System have been met.

Trust and required level of user authentication between parties has to be arranged and agreed upon prior to performing the interaction.

Signature Algorithms

For verifying cryptographic tokens, we enforce the use of the following algorithms:

- **ES256** (Elliptic Curve P-256 with SHA-256)
- **ES512** (Elliptic Curve P-521 with SHA-512)
- ***PS256*** *(RSASSA-PSS with SHA-256) – Planned for future use*

Implementations must explicitly reject any other algorithms to ensure security and compliance with best practices.

For signing cryptographic tokens, one of the supported algorithms should be used.

Z1.4 | BgZ: Volume 3 - Content

Twiin gebruikt als content de BgZ zoals beschreven staat in de technische implementatie gids van Nictiz. De actuele versie is hieronder te vinden

> https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_2017_Technical_IG

Bijlagen

In het kader van de uitwisseling van de BgZ wordt veelal ook beschreven dat de relevante correspondentie ook uitgewisseld moet worden. Deze correspondentie wordt uitgewisseld aan de hand van de implementatiewijzer Correspondentie (see page 469).

Z1.4.1 | BgZ: FHIR Task reference codes (deprecated)

> This list is deprecated. And is hereby marked for removal for the next minor or major version of the Twiin afsprakenstelsel.
>
> See Z1.3.1 | Twiin-01 | Send BgZ Notification Task (see page 317) for the updated use of type codes in the Task input.

Every input reference in the FHIR Tasks for BgZ can be coded specific to the part. The codes of all HCIMs used in the BgZ are in the table below.

HCIM	Code	System
Patient MaritalStatus ContactPerson HealthProfessional	79191-3	http://loinc.org
Payer	48768-6	http://loinc.org
TreatmentDirective	11291000146105	http://snomed.info/sct
AdvanceDirective	11341000146107	http://snomed.info/sct
FunctionalOrMentalStatus	47420-5	http://loinc.org
Problem	11450-4	http://loinc.org
LivingSituation	365508006	http://snomed.info/sct
DrugUse	228366006	http://snomed.info/sct
AlcoholUse	228273003	http://snomed.info/sct
TobaccoUse	365980008	http://snomed.info/sct
NutritionAdvice	11816003	http://snomed.info/sct
Alert	75310-3	http://loinc.org
AllergyIntolerance	48765-2	http://loinc.org
MedicationAgreement	16076005	http://snomed.info/sct
AdministrationAgreement	422037009	http://snomed.info/sct
MedicationUse2	422979000	http://snomed.info/sct
MedicalDevice	46264-8	http://loinc.org

HCIM	Code	System
Vaccination	11369-6	http://loinc.org
BloodPressure	85354-9	http://loinc.org
BodyWeight	29463-7	http://loinc.org
BodyHeight	8302-2	http://loinc.org
LaboratoryTestResult	15220000	http://snomed.info/sct
Procedure	47519-4	http://loinc.org
Encounter	46240-8	http://loinc.org
PlannedCareActivityForTransfer	18776-5	http://loinc.org

Z1.4.2 | BgZ: FHIR Workflow Task implementation

The Sending System may choose to provide a Workflow Task resource that can be used to exchange status updates and other workflow related details related to the healthcare process that demands the data exchange. In the context of a BgZ-referral, the Sending System may choose to provide a Workflow Task resource that is used to exchange details about status updates or other workflow updates related to the referral (see Notification scope (see page 347)).

An example of a BgZ Workflow Task profile

Name	Card.	Type	Comments
definition	0..1	Reference (ActivityDefinition)	Reference to ActivityDefinition resources that defines the requested activity or service
status	1..1	code	requested | received | accepted | rejected | cancelled | completed
intent	1..1	code	“order”
priority	0..1	code	normal | urgent | asap | stat

Name	Card.	Type	Comments
code	1..1	CodeableConcept	
-- coding	1..1	Coding	
-- -- FhirProfile	1..1	Slice	
-- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- code	1..1	code	“3457005”
-- -- -- display	0..1	string	“verwijzen van patiënt”
-- text	1..1	string	“Verwijzing”
description	0..1	string	
focus	0..1	Reference(ReferralRequest | CarePlan)	
for	0..1	Reference(nl-core-patient)	Reference to referred patient
authoredOn	0..1	dateTime	Date of referral submission
requester	0..1	BackboneElement	
-- agent	1..1	Reference(nl-core-practitioner)	Reference to the practitioner who sent the referral
-- -- extension		Extension	
-- -- -- practitionerRole		Extension(Reference(nl-core-practitionerrole))	Extension to relate the Practitioner to an organization, Location, HealthcareService, role, specialism, etc.
-- onBehalfOf	0..1	Reference(nl-core-organization)	Reference to the Sending Organization

Name	Card.	Type	Comments
owner	0..1	Reference(nl-core-organization)	Reference to the Receiving Organization
restriction	0..1	BackboneElement	
-- period	0..1	Period	
-- -- start	0..1	dateTime	Earliest date to start requested treatment or service
-- -- end	0..1	dateTime	Latest date to start requested treatment or service
input	0..*	BackboneElement	
-- patientInformation	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://fhir.nl/fhir/StructureDefinition/nl-core-patient”
-- -- -- -- display	0..1	string	“HCIM Patient”
-- -- text	1..1	string	“Patient information”
-- -- valueString	1..1	string	“Patient?_include=Patient:general-practitioner”
-- paymentDetails	0..1	Slice	
-- -- type	1..1	CodeableConcept	

Name	Card.	Type	Comments
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-Payer”
-- -- -- -- display	0..1	string	“HCIM Payer”
-- -- text	1..1	string	“Insurance information”
-- -- valueString	1..1	string	“Coverage?_include=Coverage:payor:Patient&_include=Coverage:payor:Organization”
-- treatmentDirective	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-TreatmentDirective”
-- -- -- -- display	0..1	string	“HCIM TreatmentDirective”
-- -- text	1..1	string	“Known treatment directives”
-- -- valueString	1..1	string	“Consent?category=http://snomed.info/sct|11291000146105”
-- advanceDirective	0..1	Slice	

Name	Card.	Type	Comments
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-AdvanceDirective”
-- -- -- -- display	0..1	string	“HCIM AdvanceDirective”
-- -- text	1..1	string	“Known advance directives”
-- -- valueString	1..1	string	“Consent?category=http://snomed.info/sct|11341000146107”
-- functionalStatus	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-FunctionalOrMentalStatus”
-- -- -- -- display	0..1	string	“HCIM FunctionalOrgMentalStatus”
-- -- text	1..1	string	“Last known functional / mental status”
-- -- valueString	1..1	string	“Observation/$lastn?category=http://snomed.info/sct|118228005,http://snomed.info/sct|384821006”

Name	Card.	Type	Comments
-- problems	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-Problem”
-- -- -- -- display	0..1	string	“HCIM Problem”
-- -- text	1..1	string	“All known problems”
-- -- valueString	1..1	string	“Condition”
-- livingSituation	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-LivingSituation”
-- -- -- -- display	0..1	string	“HCIM LivingSituation”
-- -- text	1..1	string	“Current living situation”

Name	Card.	Type	Comments
-- -- valueString	1..1	string	"Observation/$lastn?code=http://snomed.info/sct|365508006"
-- drugUse	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	"http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile"
-- -- -- -- code	1..1	code	"http://nictiz.nl/fhir/StructureDefinition/zib-DrugUse"
-- -- -- -- display	0..1	string	"HCIM DrugUse"
-- -- text	1..1	string	"All known drug use"
-- -- valueString	1..1	string	"Observation?code=http://snomed.info/sct|228366006"
-- alcoholUse	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	"http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile"
-- -- -- -- code	1..1	code	"http://nictiz.nl/fhir/StructureDefinition/zib-AlcoholUse"
-- -- -- -- display	0..1	string	"HCIM AlcoholUse"

Name	Card.	Type	Comments
-- -- text	1..1	string	“All known alcohol use”
-- -- valueString	1..1	string	“Observation?code=http://snomed.info/sct|228273003”
-- tobaccoUse	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-TobaccoUse”
-- -- -- -- display	0..1	string	“HCIM TobaccoUse”
-- -- text	1..1	string	“All known tobacco use”
-- -- valueString	1..1	string	“Observation?code=http://snomed.info/sct|365980008”
-- nutritionAdvice	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-NutritionAdvice”

Name	Card.	Type	Comments
-- -- -- -- display	0..1	string	“HCIM NutritionAdvice”
-- -- text	1..1	string	“All known dietary recommendations”
-- -- valueString	1..1	string	“NutritionOrder”
-- alert	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-Alert”
-- -- -- -- display	0..1	string	“HCIM Alert”
-- -- text	1..1	string	“All known alerts”
-- -- valueString	1..1	string	“Flag”
-- allergyIntolerance	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-AllergyIntolerance”

Name	Card.	Type	Comments
-- -- -- -- display	0..1	string	“HCIM AllergyIntolerance”
-- -- text	1..1	string	“All known information regarding allergies”
-- -- valueString	1..1	string	“AllergyIntolerance”
-- medicationUse	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-MedicationUse”
-- -- -- -- display	0..1	string	“HCIM MedicationUse2”
-- -- text	1..1	string	“Known medication use”
-- -- valueString	1..1	string	“MedicationStatement?category=urn:oid:2.16.840.1.113883.2.4.3.11.60.20.77.5.3|6&_include=MedicationStatement:medication”
-- medicationAgreement	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”

Name	Card.	Type	Comments
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-MedicationAgreement”
-- -- -- -- display	0..1	string	“HCIM MedicationAgreement”
-- -- text	1..1	string	“Known medication agreements”
-- -- valueString	1..1	string	“MedicationRequest?category=http://snomed.info/sct|16076005&_include=MedicationRequest:medication”
-- administrationAgreement	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-AdministrationAgreement”
-- -- -- -- display	0..1	string	“HCIM AdministrationAgreement”
-- -- text	1..1	string	“Known administration agreements”
-- -- valueString	1..1	string	“MedicationDispense?category=http://snomed.info/sct|422037009&_include=MedicationDispense:medication”
-- medicalAids	0..1	Slice	
-- -- type	1..1	CodeableConcept	

Name	Card.	Type	Comments
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-MedicalDevice”
-- -- -- -- display	0..1	string	“HCIM MedicalDevice”
-- -- text	1..1	string	“Known medical aids”
-- -- valueString	1..1	string	“DeviceUseStatement?_include=DeviceUseStatement:device”
-- vaccinations	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-Vaccination”
-- -- -- -- display	0..1	string	“HCIM Vaccination”
-- -- text	1..1	string	“Known vaccinations”
-- -- valueString	1..1	string	“Immunization?status=completed”
-- bloodPressure	0..1	Slice	

Name	Card.	Type	Comments
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-BloodPressure”
-- -- -- -- display	0..1	string	“HCIM BloodPressure”
-- -- text	1..1	string	“Last known blood pressure”
-- -- valueString	1..1	string	“Observation/$lastn?code=http://FhirProfile.org|85354-9”
-- bodyWeight	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-BodyWeight”
-- -- -- -- display	0..1	string	“HCIM BodyWeight”
-- -- text	1..1	string	“Last known body weight”
-- -- valueString	1..1	string	“Observation/$lastn?code=http://FhirProfile.org|29463-7”

Name	Card.	Type	Comments
-- bodyHeight	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-BodyHeight”
-- -- -- -- display	0..1	string	“HCIM BodyHeight”
-- -- text	1..1	string	“Last known body height”
-- -- valueString	1..1	string	“Observation/$lastn?code=http://FhirProfile.org|8302-2,http://FhirProfile.org|8306-3,http://FhirProfile.org|8308-9”
-- results	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	“http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
-- -- -- -- code	1..1	code	“http://nictiz.nl/fhir/StructureDefinition/zib-LaboratoryTestResult-Observation”
-- -- -- -- display	0..1	string	“HCIM LaboratoryTestResult”
-- -- text	1..1	string	“Last known laboratory results per type”

Name	Card.	Type	Comments
-- -- valueString	1..1	string	"Observation/$lastn?category=http://snomed.info/sct|275711006&_include=Observation:related-target&_include=Observation:specimen"
-- procedures	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	"http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile"
-- -- -- -- code	1..1	code	"http://nictiz.nl/fhir/StructureDefinition/zib-Procedure"
-- -- -- -- display	0..1	string	"HCIM Procedure"
-- -- text	1..1	string	"Known surgical procedures"
-- -- valueString	1..1	string	"Procedure?category=http://snomed.info/sct|387713003"
-- encounters	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- FhirProfile	1..1	Slice	
-- -- -- -- system	1..1	string	"http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile"
-- -- -- -- code	1..1	code	"http://nictiz.nl/fhir/StructureDefinition/zib-Encounter"
-- -- -- -- display	0..1	string	"HCIM Encounter"

Name	Card.	Type	Comments
-- -- **text**	1..1	string	“Known hospital admissions (no outpatient contacts)”
-- -- **valueString**	1..1	string	“Encounter?class=http://hl7.org/fhir/v3/ActCode|IMP,http://hl7.org/fhir/v3/ActCode|ACUTE,http://hl7.org/fhir/v3/ActCode|NONAC

Z1.4.3 | BgZ: FHIR examples

1. Notification Task

1.1. New Notification Task


```
{
 "resourceType": "Task",
 "groupIdentifier": {
   "system": "http://example.com/fhir/NamingSystem/identifier",
   "value": "urn:uuid:484639e6-e647-464c-8722-6e8a73cda4e0"
 },
 "identifier": {
   "system": "http://example.com/fhir/NamingSystem/identifier",
   "value": "urn:uuid:6128cfe7-0e89-4d37-ba90-e4ca3b3fcbbe"
 },
 "status": "requested",
 "intent": "proposal",
 "code": {
   "coding": [
     {
       "system": "http://fhir.twiin.nl/fhir/CodeSystem/TaskCode",
       "code": "pull-notification"
     }
   ]
 },
 "restriction": {
   "period": {
     "end": "2023-10-14T15:36:05+02:00"
   }
 },
 "for": {
   "identifier": {
     "system": "http://fhir.nl/fhir/NamingSystem/bsn",
     "value": "172642863"
   }
 },
 "authoredOn": "2023-04-13T15:01:54+02:00",
 "requester": {
   "agent": {
     "identifier": {
       "system": "http://example.com/fhir/NamingSystem/dummy",
       "value": "sending-ehr-system-id"
     }
```

```
    },
    "onBehalfOf": {
      "identifier": {
        "system": "http://fhir.nl/fhir/NamingSystem/ura",
        "value": "sending-organization-id"
      }
    }
  },
  "owner": {
    "identifier": {
      "system": "http://fhir.nl/fhir/NamingSystem/ura",
      "value": "receiving-organization-id"
    }
  },
  "input": [
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/CodeSystem/TaskParameter",
            "code": "authorization-base"
          }
        ]
      },
      "valueString": "ZGFhNDFjY2MtZGFmMi00YjZkLThiNDYtN2JlZDk1MWEyYzk2"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-
LaboratoryTestResult-Observation",
            "display": "HCIM LaboratoryTestResult"
          }
        ]
      },
      "valueReference": {
        "reference": "Observation/123456"
      }
    },
    {
      "type": {
        "coding": [
          {
```

```
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/
IHE.MHD.Minimal.DocumentReference",
            "display": "Additional documentation"
          }
        ]
      },
      "valueString": "DocumentReference?status=current"
    }
  ]
}
```

1.2. Cancel Notification Task

```
{
 "resourceType": "Task",
 "identifier": {
   "system": "http://example.com/fhir/NamingSystem/identifier",
   "value": "urn:uuid:6128cfe7-0e89-4d37-ba90-e4ca3b3fcbbe"
 },
 "status": "cancelled",
 "intent": "proposal",
 "code": {
   "coding": [
     {
       "system": "http://fhir.twiin.nl/fhir/CodeSystem/TaskCode",
       "code": "pull-notification"
     }
   ]
 }
}
```

New Notification Task for BgZ including Additional documentation

```
{
 "resourceType": "Task",
 "groupIdentifier": {
   "system": "http://example.com/fhir/NamingSystem/identifier",
   "value": "urn:uuid:484639e6-e647-464c-8722-6e8a73cda4e0"
 },
 "identifier": {
   "system": "http://example.com/fhir/NamingSystem/identifier",
   "value": "urn:uuid:6128cfe7-0e89-4d37-ba90-e4ca3b3fcbbe"
 },
 "status": "requested",
 "intent": "proposal",
 "code": {
   "coding": [
     {
       "system": "http://fhir.twiin.nl/fhir/CodeSystem/TaskCode",
       "code": "pull-notification"
     }
   ]
 },
 "restriction": {
   "period": {
     "end": "2023-10-14T15:36:05+02:00"
   }
 },
 "for": {
   "identifier": {
     "system": "http://fhir.nl/fhir/NamingSystem/bsn",
     "value": "172642863"
   }
 },
 "authoredOn": "2023-04-13T15:01:54+02:00",
 "requester": {
   "agent": {
     "identifier": {
       "system": "http://example.com/fhir/NamingSystem/dummy",
       "value": "sending-ehr-system-id"
     }
   },
   "onBehalfOf": {
     "identifier": {
       "system": "http://fhir.nl/fhir/NamingSystem/ura",
       "value": "sending-organization-id"
     }
```

```
    }
  },
  "owner": {
    "identifier": {
      "system": "http://fhir.nl/fhir/NamingSystem/ura",
      "value": "receiving-organization-id"
    }
  },
  "input": [
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/CodeSystem/TaskCode",
            "code": "authorization-base"
          }
        ]
      },
      "value": "ZGFhNDFjY2MtZGFmMi00YjZkLThiNDYtN2JlZDk1MWEyYzk2"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://fhir.nl/fhir/StructureDefinition/nl-core-patient",
            "display": "HCIM Patient"
          }
        ]
      },
      "valueString": "Patient?_include=Patient:general-practitioner"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-Payer",
            "display": "HCIM Payer"
          }
        ]
      },
      "valueString": "Coverage?
_include=Coverage:payor:Organization&_include=Coverage:payor:Patient"
    },
```

```
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-
TreatmentDirective",
            "display": "HCIM TreatmentDirective"
          }
        ]
      },
      "valueString": "Consent?category=http://snomed.info/sct|11291000146105"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-AdvanceDirective",
            "display": "HCIM AdvanceDirective"
          }
        ]
      },
      "valueString": "Consent?category=http://snomed.info/sct|11341000146107"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-
FunctionalOrMentalStatus",
            "display": "HCIM FunctionalOrgMentalStatus"
          }
        ]
      },
      "valueString": "Observation/$lastn?category=http://snomed.info/sct|118228005, "
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-Problem",
            "display": "HCIM Problem"
```

```
        }
      ]
    },
    "valueString": "Condition"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
          "code": "http://nictiz.nl/fhir/StructureDefinition/zib-LivingSituation",
          "display": "HCIM LivingSituation"
        }
      ]
    },
    "valueString": "Observation/$lastn?code=http://snomed.info/sct|365508006"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
          "code": "http://nictiz.nl/fhir/StructureDefinition/zib-DrugUse",
          "display": "HCIM DrugUse"
        }
      ]
    },
    "valueString": "Observation?code=http://snomed.info/sct|228366006"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
          "code": "http://nictiz.nl/fhir/StructureDefinition/zib-AlcoholUse",
          "display": "HCIM AlcoholUse"
        }
      ]
    },
    "valueString": "Observation?code=http://snomed.info/sct|228273003"
  },
  {
    "type": {
      "coding": [
        {
```

```
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-TobaccoUse",
            "display": "HCIM TobaccoUse"
          }
        ]
      },
      "valueString": "Observation?code=http://snomed.info/sct|365980008"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-NutritionAdvice",
            "display": "HCIM NutritionAdvice"
          }
        ]
      },
      "valueString": "NutritionOrder"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-Alert",
            "display": "HCIM Alert"
          }
        ]
      },
      "valueString": "Flag"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-
AllergyIntolerance",
            "display": "HCIM AllergyIntolerance"
          }
        ]
      },
      "valueString": "AllergyIntolerance"
    },
```

```
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-MedicationUse",
            "display": "HCIM MedicationUse2"
          }
        ]
      },
      "valueString": "MedicationStatement?
category=urn:oid:2.16.840.1.113883.2.4.3.11.60.20.77.5.3|
6&_include=MedicationStatement:medication"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-
MedicationAgreement",
            "display": "HCIM MedicationAgreement"
          }
        ]
      },
      "valueString": "MedicationRequest?category=http://snomed.info/sct|
16076005&_include=MedicationRequest:medication"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-
AdministrationAgreement",
            "display": "HCIM AdministrationAgreement"
          }
        ]
      },
      "valueString": "MedicationDispense?category=http://snomed.info/sct|
422037009&_include=MedicationDispense:medication"
    },
    {
      "type": {
        "coding": [
```

```
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-MedicalDevice",
            "display": "HCIM MedicalDevice"
          }
        ]
      },
      "valueString": "DeviceUseStatement?_include=DeviceUseStatement:device"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-Vaccination",
            "display": "HCIM Vaccination"
          }
        ]
      },
      "valueString": "Immunization?status=completed"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-BloodPressure",
            "display": "HCIM BloodPressure"
          }
        ]
      },
      "valueString": "Observation/$lastn?code=http://loinc.org|85354-9"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-BodyWeight",
            "display": "HCIM BodyWeight"
          }
        ]
      },
      "valueString": "Observation/$lastn?code=http://loinc.org|29463-7"
    },
```

```
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-BodyHeight",
            "display": "HCIM BodyHeight"
          }
        ]
      },
      "valueString": "Observation/$lastn?code=http://loinc.org|8302-2,http://
loinc.org|8306-3,http://loinc.org|8308-9"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-
LaboratoryTestResult-Observation",
            "display": "HCIM LaboratoryTestResult"
          }
        ]
      },
      "valueString": "Observation/$lastn?category=http://snomed.info/sct|
275711006&_include=Observation:related-target&_include=Observation:specimen"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-Procedure",
            "display": "HCIM Procedure"
          }
        ]
      },
      "valueString": "Procedure?category=http://snomed.info/sct|387713003"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/zib-Encounter",
```

```
            "display": "HCIM Encounter"
          }
        ]
      },
      "valueString": "Encounter?class=http://hl7.org/fhir/v3/ActCode|IMP,http://
hl7.org/fhir/v3/ActCode|ACUTE,http://hl7.org/fhir/v3/ActCode|NONAC"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile",
            "code": "http://nictiz.nl/fhir/StructureDefinition/
IHE.MHD.Minimal.DocumentReference",
            "display": "Additional documentation"
          }
        ]
      },
      "valueString": "DocumentReference?status=current"
    }
  ]
}
```


Z1.4.4 | BgZ: Autorisatie

Voor de uitwisseling van de BgZ is door de zorgkoepels (voor het AORTA-domein) een autorisatierichtlijn[81] opgesteld. Aan de hand van deze autorisatierichtlijn wordt bepaald welk type zorgverleners de BgZ kunnen verzenden en opvragen en welke niet.

Deze autorisatie-afspraken gaan over de samenwerking tussen zorgprofessionals werkzaam voor:

- Ziekenhuizen
- Universitair medische centra
- Zelfstandige klinieken

Het gaat om gegevens uit het patiëntendossier van de zorgaanbieder die de gegevens beheert of onder zich heeft (brondossierhouder). Daarnaast worden afspraken vastgelegd over het beschikbaar stellen van niet-gestructureerde documenten, die logischerwijs bij onderhavige uitwisseling van de BgZ horen. Denk hierbij aan verslagen van eerder uitgevoerd onderzoek, een verwijsbrief of een verzoek om expertise. Het betreft dan de situatie waarin de patiënt wordt verwezen of overgedragen. Hiervoor geldt dezelfde autorisatie.

Op AORTA-specifieke afspraken na, ziet Twiin geen reden om af te wijken van de autorisatierichtlijn die de betrokken zorgkoepels hebben afgesproken. Onderstaande tabel is een samenvoeging van de autorisatiematrix uit paragraaf 3.5.3 van de autorisatierichtlijn met de arts-specialisaties (rolcode 01.*)

81. https://www.aorta-lsp.nl/over-aorta-lsp/autorisatierichtlijnen/autorisatierichtlijn-basisgegevensset-zorg-bgz

uit tabel uit paragraaf 3.4 van hetzelfde document. Dit betekent concreet dat alleen de volgende rollen de BgZ mogen versturen en/of raadplegen. Bij het opvragen van de BgZ kunnen niet-gestructureerde documenten worden meegezonden, waarvoor dezelfde autorisaties gelden.

Rol	UZI-rolcode
Arts	01.000
Medisch specialist	
Allergoloog	01.002
Anesthesioloog	01.003
Cardioloog	01.010
Cardiothoracaal chirurg	01.011
Dermatoloog	01.012
Arts v. maag-darm-leverziekten	01.013
Chirurg	01.014
Internist	01.016
Keel- neus en oorarts	01.018
Kinderarts	01.019
Arts klinische chemie	01.020
Klinisch geneticus	01.021
Klinisch geriater	01.022
Longarts	01.023
Arts microbioloog	01.024

Rol		UZI-rolcode
	Neurochirurg	01.025
	Neuroloog	01.026
	Nucleair geneeskundige	01.030
	Oogarts	01.031
	Orthopedisch chirurg	01.032
	Patholoog	01.033
	Plastisch chirurg	01.034
	Psychiater	01.035
	Radioloog	01.039
	Radiotherapeut	01.040
	Reumatoloog	01.041
	Revalidatiearts	01.042
	Uroloog	01.045
	Gynaecoloog	01.046
	Zenuwarts	01.050
	Internist-allergoloog	01.062
	Spoedeisende hulp arts	01.071
	Sportarts	01.074
Kaakchirurg		02.054

Rol	UZI-rolcode
Physician Assistant	81.000
Verpleegkundig specialist AGZ	30.076
Verpleegkundig specialist geestelijke gezondheidszorg	30.069

- Bij Pull: Wanneer de brondossierhouder geen grondslag (in de vorm van een authorization_base) heeft afgegeven dient de raadplegende gebruiker op basis van de rolcode geautoriseerd te worden. Dit geldt bijvoorbeeld bij een directe bevraging/direct pull. Deze codes dienen meegegeven te worden in autorization grant indien de raadplegende partij geen authorization base heeft: 10.4.2 | TTA FHIR - Authorization (see page 206)
- Bij Notified Pull: Wanneer het verzenden wordt gedaan via het notified pull communicatiepatroon dient de gebruiker die de notificatie verstuurt hiervoor geautoriseerd te zijn. Een brondossierhouder zal deze autorisatieregels dus moeten toepassen bij het verzenden van de BgZ. Als de raadplegende partij de grondslag (authorization base) gebruikt bij het aanvragen van een access token dan hoeft een bron alleen nog maar te toetsen of de grondslag daadwerkelijk is uitgegeven aan de raadplegende partij en hoeft er niet meer op basis van de rolcode geautoriseerd te worden.

Z1.5 | BgZ: PvE

Validatie-eisen

In de tabel hieronder staan een aantal specifieke validatie-eisen voor de BgZ.

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-2a-AA-11	BgZ Authn en Authz	GtK verzender	GtK verzender borgt dat de autorisatierichtlijn BgZ is toegepast. Concreet betekent dit dat alleen de in de richtlijn geautoriseerde rollen een andere partij mogen notificeren voor het ophalen van de BgZ. De GtK verzender mag vervolgens vertrouwen op de interne autorisatieregels bij de GtK ontvanger (indien deze een valide authorization base heeft, zie ook BgZ-1-authz-03)	Access Policy: GtK verzender moet borgen dat alleen gebruikers met de in de autorisatiematrix opgesomde rollen BgZ notificaties mogen versturen: (TA141) Z1.4.4 | BgZ: Autorisatie#autorisatiematrix-BgZ (see page 375)
BgZ-2a-AA-15	BgZ Authn en Authz	GtK verzender	GtK verzender heeft het afgesproken access policy geïmplementeerd bij het verzenden van een notificatie	Access Policy: GtK verzender mag door gebruikers met de in de autorisatiematrix opgesomde rollen een BgZ laten verzenden: (TA141) Z1.4.4 | BgZ: Autorisatie#autorisatiematrix-BgZ (see page 375)
BgZ-3-1	content	GtK verzender	GtK verzender dient een Workflow-task aan te maken die voldoet aan de BgZ FHIR Workflow Task implementation.	Profiel: Z1.4.2 | BgZ: FHIR Workflow Task implementation (see page 347)

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-3-2	content	GtK ontvanger	GtK ontvanger dient een Workflow-Task die voldoet aan het BgZ Workflow Task Profile te kunnen interpreteren.	Profiel: Z1.4.2 | BgZ: FHIR Workflow Task implementation (see page 347)
BgZ-3-3	content	GtK verzender	GtK verzender dient een Notificatie-task aan te maken die voldoet aan het afgesproken profiel.	Profiel: (TA141) 10.5.1 | Twiin-01 | Send Notification Task#id-10.3.1| Twiin-01| SendNotificationTask-Request-message Referentiecodes: Z1.4.1 | BgZ: FHIR Task reference codes (deprecated) (see page 345)
BgZ-3-4	content	GtK ontvanger	GtK ontvanger dient een Notificatie-task die voldoet aan het afgesproken profiel te kunnen interpreteren.	Profiel: (TA141) 10.5.1 | Twiin-01 | Send Notification Task#id-10.3.1| Twiin-01| SendNotificationTask-Request-message Referentiecodes: Z1.4.1 | BgZ: FHIR Task reference codes (deprecated) (see page 345)
BgZ-3-5	content	GtK verzender	GtK verzender dient FHIR-resources conform de implementation guide van de informatiestandaard BgZ beschikbaar te kunnen stellen.	Profielen: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_2017_Technical_IG

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-3-6	content	GtK ontvanger	GtK ontvanger dient FHIR-resources conform de implementation guide van de informatiestandaard BgZ te kunnen interpreteren.	Profielen: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_2017_Technical_IG
BgZ-3-7	content	GtK verzender	GtK verzender dient correspondentie/ niet-discrete data conform Z3 | COR: Implementatiewijzer Correspondentie (see page 469) beschikbaar te kunnen stellen.	
BgZ-3-8	content	GtK ontvanger	GtK ontvanger dient correspondentie/ niet-discrete data conform Z3 | COR: Implementatiewijzer Correspondentie (see page 469) te kunnen interpreteren.	

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-3-9	content en autorisatie	GtK verzender	Het raadplegen van de gegevens mag alleen gebeuren binnen de geldigheidsduur van de verwijzing/ overdracht: 1 jaar. Dit is het laatste moment in de tijd waarop nog op basis van de veronderstelde toestemming de informatie mag worden opgevraagd. De geldigheidsduur moet worden opgenomen in de Task. Daarna is de *veronderstelde toestemming* niet meer geldig bij de verwijzende/ overdragende instelling en mag de informatie alleen op basis van de use case 'Opvraging BgZ bij eerdere behandelaar' en vooraf vastgelegde uitdrukkelijke patiënttoestemming worden opgevraagd via een elektronisch uitwisselingssystee m.	De geldigheidsduur van een verwijzing dan wel overdracht binnen de tweede lijn is gebaseerd op de geldigheidsduur die gehanteerd wordt tussen de eerste en tweedelijns verwijzingen, namelijk **één jaar**. Dit afgestemd met de volgende koepels FMS, NVZ, NFU en ZKN en wordt tot nader order gehanteerd als veldnorm.

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-3-10	routering	GtK verzender	Een GtK verzender dient, indien de beoogde GtK ontvanger dit vereist, de **definitionReference** in de **Send Notification** te vullen met de daardoor aangeleverde parameters	Deze parameters bieden de GtK ontvanger de mogelijkheid om een binnenkomende notificatie intern verder te routeren. Het is aan de Twiin-Deelnemer om deze lijsten te verspreiden onder de Twiin Deelnemers. Dit is een tijdelijke eis / oplossing totdat de TA routering is afgerond. Zie: 10.4.5 | TTA - Addressing (see page 210)
BgZ-3-11	beschikbaarheid	GtK verzender en ontvanger	Het GtK en systemen 'achter het GtK' dienen ieder een beschikbaarheid van minimaal 99,5% te hebben.	Dit percentage is gebaseerd op de vuistregel dat dit: • Betrouwbaar genoeg is voor deze toepassing. • De kosten beperkt houdt in vergelijking met hogere beschikbaarheidsniveaus (>99,9%), waarin deze exponentieel stijgen.

Aanvullende ketentest-eisen

De eisen in dit hoofdstuk zijn niet nodig zijn voor de Twiin-validatie van de zorgtoepassing. Deze eisen zijn wel nodig om te voldoen aan de ketentest, de informatiestandaard, de VIPP-eisen en eventuele andere functionele eisen.

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-1-FO-03	FO Nictiz	GtK verzender	GtK verzender maakt informatie beschikbaar conform de BgZ specificatie op basis van zibs versie 2017.	Specificatie: https://www.registratieaandebron.nl/pdf/BgZ_specificatie_obv_zibs_2017_v1.1.pdf
BgZ-1-FO-04	FO Nictiz	GtK ontvanger	GtK ontvanger kan informatie opvragen die voldoet aan de BgZ specificatie op basis van zibs versie 2017.	Specificatie: https://www.registratieaandebron.nl/pdf/BgZ_specificatie_obv_zibs_2017_v1.1.pdf
BgZ-1-FO-05	FO Nictiz	EPD verzender	Voor het vastleggend systeem 'achter' de GtK verzender geldt: Het EPD moet nieuwe gegevens, die vastgelegd worden als gevolg van een behandeling in de eigen instelling, vastleggen als zibs voor zover de gegevens onderdeel kunnen zijn van een later aan te maken BgZ.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-1-FO-06	FO Nictiz	EPD verzender	Voor het vastleggend systeem 'achter' de GtK verzender geldt: Het EPD moet nieuwe gegevens die vastgelegd worden als zibs voorzien van metagegevens.	Daarbij moet alle velden die gevuld zijn in de Metagegevens tabel[82] gevuld worden voor nieuwe zibs. Velden die leeg zijn in de metagegevens tabel mogen gevuld worden, maar dat hoeft niet. Vastleggen gebeurt zoveel mogelijk automatisch, bijvoorbeeld door huidige datumtijd te gebruiken. De datumtijd en zorgverlener kunnen onderdeel zijn van de zib (zo kent de zib Verrichting een Uitvoerder en een VerrichtingStartDatum). Waar dat niet het geval is, worden de BasisElementen gebruikt. In dat geval kan de ingelogde zorgverlener Auteur zijn en de huidige datumtijd gebruikt worden. Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen

82. https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1.0_Ontwerp_BgZ_MSZ#Metagegevens_tabel

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-1-FO-07	FO Nictiz	GtK verzender	GtK verzender moet een BgZ kunnen sturen bij verwijzing naar een andere zorginstelling of zorgverlener.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-08	FO (Nictiz)	GtK verzender	GtK verzender moet een verwijsbrief in document-formaat kunnen sturen bij verwijzing naar een andere zorginstelling of zorgverlener.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-09	FO Nictiz	Verwijzer	Een Verwijzer (zorgverlener) moet een andere zorginstelling kunnen kiezen om een BgZ mee te delen, met eventueel specialisme.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-10	FO Nictiz	GtK antwoorder	GtK antwoorder moet de mogelijkheid bieden om op een opvraging een BgZ beschikbaar te stellen.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-1-FO-11	FO Nictiz	EPD verzender	Voor het vastleggend systeem 'achter' de GtK verzender geldt: Een EPD moet metagegevens toevoegen aan een BgZ.	Voor zibs die aangemaakt zijn na implementatie van de informatiestandaard zijn dat minimaal alle velden die gevuld zijn in de Metagegevens tabel[83]. Voor historische zibs worden de metagegevens zo goed mogelijk gevuld. Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-12	FO Nictiz	GtK verzender, GtK ontvanger	GtK verzender en GtK ontvanger moeten beschrijven welke secties en welke zibs van de BgZ wel en niet ondersteund worden.	Deze documentatie moet beschikbaar zijn bij kwalificatie en voor ketenpartners. Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen

83. https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1.0_Ontwerp_BgZ_MSZ#Metagegevens_tabel

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-1-FO-13	FO Nictiz, meta gegevens	GtK verzender	GtK verzender dient, wanneer een gegevenselement van elders betrokken is en er zijn metagegevens op zib-niveau[84] opgeslagen, deze metagegevens mee te zenden.	Bijvoorbeeld: medicatie is opgehaald van het LSP en de identificaties van de LSP-bevraging zitten in het EPD, dan dienen deze meegezonden te worden. Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-14	FO Nictiz, meta gegevens	GtK verzender	GtK verzender: Wanneer een gegevenselement van elders betrokken is, en er zijn geen metagegevens opgeslagen, dan worden deze niet meegezonden.	Bijvoorbeeld: medicatie is overgenomen van een papieren AMO (Actueel Medicatie Overzicht). Op een AMO staan geen metagegevens op rij-niveau. Deze kunnen dus niet opgeslagen en meegestuurd worden. Er moet geen eigen identificatie aangemaakt worden wanneer het medicatievoorschrift elders is opgesteld. Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen

84. https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1.0_Ontwerp_BgZ_MSZ#Metagegevens_op_zib-niveau

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-1-FO-15	FO Nictiz, meta gegevens	GtK verzender	GtK verzender: Wanneer het gegevenselement niet van elders betrokken is, en het systeem kan persistente identificaties (die bij een volgende bevraging hetzelfde zijn) aanmaken, dan dienen deze meegezonden te worden.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-16	FO Nictiz, meta gegevens	GtK verzender	GtK verzender: Wanneer het gegevenselement niet van elders betrokken is, en het systeem kan geen persistente identificaties aanmaken, dan worden geen identificaties meegezonden.	Andere metagegevens mogen wel meegestuurd worden. Deze situatie is niet wenselijk en dient uitgefaseerd te worden, maar is zeker voor historische gegevens niet uit te sluiten. Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-17	FO Nictiz, meta gegevens	GtK verzender	GtK verzender: Wanneer het systeem geen onderscheid kan maken tussen eigen en van elders betrokken informatie, worden geen identificaties meegezonden.	Deze situatie is niet wenselijk en dient uitgefaseerd te worden. Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-1-FO-18	FO Nictiz	GtK ontvanger	GtK ontvanger moet de mogelijkheid bieden om een BgZ op te vragen bij een beschikbaarstellend EPD.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-19	FO Nictiz	Nieuwe behandelaar	Use case "Opvraging BgZ bij eerdere behandelaar": Een zorgverlener moet een te bevragen zorginstelling kunnen kiezen, ofwel een lijst tonen met alle beschikbare BgZ's in een repository.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-20	FO Nictiz	GtK ontvanger, EPD ontvanger	GtK ontvanger en de eventuele achterliggende systemen (zoals een EPD) moeten de mogelijkheid bieden om een BgZ te ontvangen.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-21	FO Nictiz	EPD ontvanger	Voor de systemen 'achter' GtK ontvanger geldt: Het EPD moet de betrokken afdelingen (administratief en/of specialisme) kunnen verwittigen van een ontvangen BgZ, waarna die BgZ ingezien kan worden.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-1-FO-22	FO Nictiz	EPD ontvanger	Voor de systemen 'achter' GtK ontvanger geldt: Een EPD moet alle informatie die via een BgZ ontvangen wordt kunnen tonen aan de zorgverlener.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-23	FO Nictiz	GtK ontvanger, EPD ontvanger	GtK ontvanger en de systemen 'achter' GtK ontvanger moeten beschrijven welke mogelijkheden ze wel en niet bieden betreffende hergebruik.	Deze documentatie moet beschikbaar zijn bij kwalificatie en voor ketenpartners. Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-24	FO Nictiz	EPD ontvanger	Voor de systemen 'achter' GtK ontvanger geldt: Een EPD moet alle informatie die via een BgZ ontvangen wordt, kunnen tonen aan de zorgverlener.	De informatie die getoond wordt, moet uit de gestructureerde zibs in de BgZ getoond worden waar deze aanwezig zijn. Het gaat niet om het inzien van een PDF of tekstuele secties uit een document. Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-1-FO-25	FO Nictiz	EPD ontvanger	Voor de systemen 'achter' GtK ontvanger geldt: Een EPD moet in staat zijn een ontvangen of geraadpleegde BgZ over te nemen wanneer dat medisch relevant is.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-26	FO Nictiz	EPD ontvanger	Voor de systemen 'achter' GtK ontvanger geldt: Een EPD moet in staat zijn een ontvangen of geraadpleegde verwijsbrief over te nemen wanneer dat medisch relevant is.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-27	FO Nictiz	EPD ontvanger	Voor de systemen 'achter' GtK ontvanger geldt: Een EPD dat gegevens overneemt neemt deze over als discrete zibs.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-28	FO Nictiz	EPD ontvanger	Voor de systemen 'achter' GtK ontvanger geldt: Een EPD dat zibs overneemt moet deze ook weer als zibs kunnen ontsluiten.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-29	FO Nictiz	EPD ontvanger	Voor de systemen 'achter' GtK ontvanger geldt: Een EPD moet metagegevens op document-niveau op kunnen slaan.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-1-FO-30	FO Nictiz	EPD ontvanger	Voor de systemen 'achter' GtK ontvanger geldt: Een EPD moet metagegevens op zib-niveau op kunnen slaan.	Wanneer deze aanwezig zijn, is opslaan van document-metagegevens optioneel. Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-FO-31	FO Nictiz	EPD ontvanger	Voor de systemen 'achter' GtK ontvanger geldt: Bij iedere overgenomen zib worden metagegevens opgeslagen.	Dit is minimaal: • de instelling vanwaar de gegevens betrokken zijn; • de gegevens die gevuld zijn in de Metagegevens tabel. Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-1-FO-32	FO Nictiz	EPD ontvanger	Voor de systemen 'achter' GtK ontvanger geldt: Daarnaast wordt de verantwoordelijke zorgverlener overgenomen wanneer deze in de zib of de metagegevens van de zib zit.	Bij historische of van oorspronkelijk elders betrokken gegevens kan deze zorgverlener niet altijd gevuld zijn. Daarnaast gaat het alleen om gegevens van de zorgverlener waar dit medisch relevant is. Bijvoorbeeld een voorschrijver van medicatie, steller van een diagnose of uitvoerder van een verrichting is relevant. Administratief personeel dat gegevens zoals contactpersonen invoert is dat niet. Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.1_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
BgZ-1-VIPP5-1	VIPP 5	GtK verzender	GtK verzender kan de BgZ en correspondentie verzenden naar andere instellingen van Medisch Specialistische Zorg.	Zie Handreiking VIPP 5 assessments[85], bijlage II, paragraaf 1.5, alinea module 3 Zie https://www.vipp-programma.nl/over-vipp/doelstellingen

85. https://www.norea.nl/uploads/bfile/367e3045-86fc-49cb-8f01-0ef470105695

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-1-VIPP5-2	VIPP 5	GtK ontvanger	GtK ontvanger kan de BgZ en correspondentie ontvangen vanuit een andere instelling van Medisch Specialistische Zorg.	Zie Handreiking VIPP 5 assessments[86], bijlage II, paragraaf 1.5, alinea module 3
BgZ-1-VIPP5-3	VIPP 5	GtK ontvanger, EPD ontvanger	GtK ontvanger en de systemen achter GtK ontvanger (bijvoorbeeld het EPD) kunnen aangewezen of gekozen secties van de BgZ ontvangen en hergebruiken vanuit een andere instelling van Medisch Specialistische Zorg.	Zie Handreiking VIPP 5 assessments[87], bijlage II, paragraaf 1.5, alinea module 3
BgZ-1-VIPP5-4	VIPP 5	Twiin deelnemer	De Twiin deelnemer (zorgorganisatie) heeft procedures rondom het uitwisselen van de BgZ en correspondentie met andere instellingen van Medisch Specialistische Zorg beschreven en geïmplementeerd.	Zie Handreiking VIPP 5 assessments[88], bijlage II, paragraaf 1.5, alinea module 3

86. https://www.norea.nl/uploads/bfile/367e3045-86fc-49cb-8f01-0ef470105695
87. https://www.norea.nl/uploads/bfile/367e3045-86fc-49cb-8f01-0ef470105695
88. https://www.norea.nl/uploads/bfile/367e3045-86fc-49cb-8f01-0ef470105695

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-1-AVG-01	TA NP	Nieuwe behandelaar	De nieuwe behandelaar mag alleen de gegevens opvragen die relevant zijn voor de uitvoering van de nieuwe behandelrelatie.	De nieuwe behandelaar (en de zorgorganisatie waarvan zij/hij deel uitmaakt) is ervoor verantwoordelijk om dataverzoeken proportioneel te houden.

Notified Pull-eisen

> Deze sectie is gelijk aan PvE | Notified Pull (see page 193)

BgZ-2a-TANP-01	Aanbieden notificatie-endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-ontvanger** dient een notificatie-endpoint aan te bieden aan de GtK-verzender. Een endpoint kan worden gedeeld door meerdere Twiin Deelnemers (bijv. een endpoint per GtK/ SaaS-dienst) of er kan sprake zijn van een endpoint per Twiin Deelnemer.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie o.a. Z1.2.1	TTA Exchanging BgZ - FHIR Notified Pull (see page 302)

BgZ-2a-TANP-02	Aanbieden resource-endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** dient een resource-endpoint aan te bieden aan GtK-ontvanger. Een endpoint kan worden gedeeld door meerdere Twiin Deelnemers (bijv. een endpoint per GtK/ SaaS-dienst) of er kan sprake zijn van een endpoint per Twiin Deelnemer.

BgZ-2a-TANP-02	Aanbieden resource-endpoint
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie o.a. Z1.2.1 | TTA Exchanging BgZ - FHIR Notified Pull (see page 302)

BgZ-2a-TANP-03	Aanbieden token-endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** en de **GtK-ontvanger** dienen een token-endpoint aan elkaar aan te bieden. Een endpoint kan worden gedeeld door meerdere Twiin Deelnemers (bijv. een endpoint per GtK/ SaaS-dienst) of er kan sprake zijn van een endpoint per Twiin Deelnemer.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie o.a. Z1.2.1 | TTA Exchanging BgZ - FHIR Notified Pull (see page 302)

BgZ-2a-AA-06	Aanmaken authorization_base
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** is in staat een digitale representatie van de in de context van een verwijzing veronderstelde toestemming aan te maken (`authorization_base`). Omdat de `authorization_base` alleen door GtK-verzender wordt verwerkt, worden de vorm en inhoud ervan bepaald door GtK-verzender. GtK-ontvanger mag niet afhankelijk zijn van het formaat of de inhoud van `authorization_base` . De vorm en inhoud van de `authorization_base` is (nog) niet gebonden aan normatieve eisen. Het bepalen van vorm en inhoud doet GtK-verzender bij voorkeur in afstemming met de gebruikte infrastructuur.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie (TA141) Z1.2.1.2 | BgZ: Authentication & Authorization#Authorization-base

BgZ-2a-AA-07 / BgZ-2a-AA-12	Aanmaken autorization_grant
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** en **GtK-ontvanger** zijn in staat een `authorization_grant` aan te maken die voldoet aan de specificaties
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Specificaties: (TA141) 10.4.2 | TTA FHIR - Authorization#id-10.2.5|TTAFHIR-Authentication&Authorization-Authorization-grant

BgZ-2a-AA-08	Aanmaken access token request voor notification-endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** is in staat conform de specificaties een access token request voor toegang tot het notificatie-endpoint aan te maken en aan GtK-ontvanger te versturen.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Specificaties: (TA141) Z1.2.1.2 | BgZ: Authentication & Authorization#Access-token-request Twiin-07 | Token Request (see page 270)

BgZ-2a-AA-09	Gelijke waardes in authentication_grant en access token request
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** en **GtK-ontvanger** dienen ervoor te zorgen dat het veld `sub` in de `authentication_grant` en het veld `client_id` in het access token request dezelfde waarde bevatten.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Specificaties: (TA141) Z1.2.1.2 | BgZ: Authentication & Authorization#Access-token-request Twiin-07 | Token Request (see page 270)

BgZ-2a-AA-10	Afhandelen access token request voor notification server endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-ontvanger** is in staat conform de specificaties een access token request van GtK-verzender voor toegang tot het notificatie server endpoint af te handelen
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Specificaties: (TA141) Z1.2.1.2 | BgZ: Authentication & Authorization#Access-token-request Twiin-07 | Token Request (see page 270)

BgZ-1-authz-03	Controleren autorization_base
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** dient te controleren of de grondslag (`authorization_base`) waarmee de GtK-ontvanger een verzoek doet daadwerkelijk is uitgegeven (aan de GtK-ontvanger). Wanneer de grondslag niet meekomt in de uitwisseling, is er geen sprake van het notified pull communicatiepatroon en dient de GtK-ontvanger op basis van de in de autorisatierichtlijn beschreven rollen het verzoek te autoriseren.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Autorisatiematrix: (TA141) Z1.4.4 | BgZ: Autorisatie#autorisatiematrix-BgZ (see page 375) Transacties: 10.5.4 | Twiin-04 | Search Resource(s) (see page 230) , 10.5.5 | Twiin-05 | Retrieve Resource (see page 232) Autorisatierichtlijn: https://www.aorta-lsp.nl/over-aorta-lsp/autorisatierichtlijnen/autorisatierichtlijn-basisgegevensset-zorg-bgz

BgZ-2b-trans-01	Aanmaken Workflow-Taks
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** is in staat een Workflow-Task aan te maken indien verzender geen Workflow-Task stuurt als payload van de Notification-Task.
Prescription Level/Type	Verplicht
Toetsing	Validatie

BgZ-2b-trans-01	Aanmaken Workflow-Taks
Transactie/verwijzing	Transactie 1 van Z1.2.1.1 | BgZ - data interactions (see page 306)

BgZ-2b-trans-02	Versturen notificatie-create-request
Omschrijving/Toelichting/ Uitleg/Implicaties	**GtK-verzender** is in staat een notificatie-create-request te versturen.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 2 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: (TA141) 10.5.1 | Twiin-01 | Send Notification Task#id-10.3.1| Twiin-01|SendNotificationTask-Request-message

BgZ-2b-trans-03	Afhandelen notificatie-create-request
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-ontvanger** is in staat een binnenkomend notificatie-create-request af te handelen en een passende response te versturen
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 3 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: (TA141) 10.5.1 | Twiin-01 | Send Notification Task#id-10.3.1| Twiin-01|SendNotificationTask-Response-message

BgZ-2b-trans-04	Versturen notificatie-create-request bij updates
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** is in staat een notificatie-create-request te versturen wanneer de dataset van de verwijzing is geüpdatet
Prescription Level/Type	Verplicht
Toetsing	Validatie

BgZ-2b-trans-04	Versturen notificatie-create-request bij updates
Transactie/verwijzing	Transactie 4 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie:(TA141) 10.5.1 | Twiin-01 | Send Notification Task#id-10.3.1|Twiin-01| SendNotificationTask-Request-message

BgZ-2b-trans-05	Afhandelen notificatie-create-request bij updates
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-ontvanger** is in staat een naar aanleiding van een geüpdatete dataset binnenkomend notificatie-create-request af te handelen en een passende response te versturen
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 5 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: (TA141) 10.5.1 | Twiin-01 | Send Notification Task#id-10.3.1| Twiin-01|SendNotificationTask-Response-message

BgZ-2b-trans-06	Versturen annulering
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** is in staat een notificatie-update-request te versturen wanneer GtK-verzender de notificatie wil annuleren of intrekken.
Prescription Level/Type	Optioneel
Toetsing	Validatie
Transactie/verwijzing	Transactie 6 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: (TA141) 10.5.2 | Twiin-02 | Cancel Notification Task#id-10.3.2| Twiin-02|CancelNotificationTask-Request-message

BgZ-2b-trans-07	Afhandeling annulering
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK-ontvanger is in staat een binnenkomend notificatie-update-request af te handelen en een passende response te versturen.
Prescription Level/Type	Verplicht

BgZ-2b-trans-07	Afhandeling annulering
Toetsing	Validatie
Transactie/verwijzing	Transactie 7 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: (TA141) 10.5.2 | Twiin-02 | Cancel Notification Task#id-10.3.2|Twiin-02|CancelNotificationTask-Notification-response

BgZ-2b-trans-08.read	Uitvoeren read-operaties
Omschrijving/Toelichting/Uitleg/Implicaties	De **GtK-ontvanger** is in staat read-operaties uit de notificatie-taak uit te voeren op het resource-endpoint van GtK-verzender.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 8 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.5 | Twiin-05 | Retrieve Resource (see page 232) De read-operaties zijn opgenomen in de notificatie-task onder Task.input:read-available-resources.

BgZ-2b-trans-09.read	Afhandelen read-requests
Omschrijving/Toelichting/Uitleg/Implicaties	GtK-verzender is in staat binnenkomende read-requests af te handelen en een passende response te versturen.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 9 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.5 | Twiin-05 | Retrieve Resource (see page 232)

BgZ-2b-trans-08.search	Uitvoeren search-operaties resource-endpoint
Omschrijving/Toelichting/Uitleg/Implicaties	GtK-ontvanger is in staat search-operaties uit de notificatie-taak uit te voeren op het resource-endpoint van GtK-verzender.

BgZ-2b-trans-08.search	Uitvoeren search-operaties resource-endpoint
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 8 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.4 | Twiin-04 | Search Resource(s) (see page 230) De search-operaties zijn opgenomen in de notificatie-task onder Task.input:query-available-resources.

BgZ-2b-trans-09.search	Afhandelen search-requests resource-endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK-verzender is in staat binnenkomende search-requests af te handelen en een passende response te versturen.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 9 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.4 | Twiin-04 | Search Resource(s) (see page 230)

BgZ-2b-trans-10	Uitvoeren read-operatie ophalen workflow-task
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-ontvanger** is in staat een read-operatie voor het ophalen van de Workflow-task uit te voeren op het resource-endpoint van GtK-verzender.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 10 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.3 | Twiin-03 | Get Workflow Task (see page 228) De indicator voor de aanwezigheid van een workflow-task is opgenomen in de notificatie-task onder Task.input:get-worflow-task.valueBoolean (waarde is `true`).

BgZ-2b-trans-11	Afhandelen read-operatie workflow-task
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-verzender** is in staat een binnenkomende read-request op de workflow-task af te handelen en een passende response te versturen.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 11 van Z1.2.1.1 | BgZ - data interactions (see page 306)

BgZ-2b-trans-12.read	Uitvoeren read-operatie uit workflow-task
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK-ontvanger is in staat read-operaties uit de workflow-taak uit te voeren op het resource-endpoint van GtK-verzender.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 12 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.5 | Twiin-05 | Retrieve Resource (see page 232) De read-operaties zijn opgenomen in de workflow-task onder `Task.input:read-available-resources`.

BgZ-2b-trans-13.read	Afhandelen read-request
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK-verzender is in staat binnenkomende read-requests af te handelen en een passende response te versturen.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 13 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.5 | Twiin-05 | Retrieve Resource (see page 232)

BgZ-2b-trans-12.search	Uitvoeren search-operaties op resource-endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK-ontvanger is in staat search-operaties uit de workflow-taak uit te voeren op het resource-endpoint van GtK-verzender.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 12 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.4 | Twiin-04 | Search Resource(s) (see page 230) De search-operaties zijn opgenomen in de workflow-task onder `Task.input:query-available-resources`.

BgZ-2b-trans-13.search	Afhandelen search-operaties op resource-endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK-verzender is in staat binnenkomende search-requests af te handelen en een passende response te versturen
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Transactie 13 van Z1.2.1.1 | BgZ - data interactions (see page 306) Specificatie: 10.5.4 | Twiin-04 | Search Resource(s) (see page 230)

Adresseringseisen

> Deze sectie is gelijk aan PvE | Adressering (see page 210)

BgZ-2a-TANP-04 / BgZ-2a-TANP-05	Publiceren adresinformatie endpoints
Omschrijving/Toelichting/ Uitleg/Implicaties	De GtK-ontvanger en GtK-verzender dienen de technische adressen van het resource-endpoint, het notificatie-endpoint en het token-endpoint kenbaar te maken aan de Twiin Beheerorganisatie. De wijze waarop technische adressen tussen GtK-verzender en GtK-ontvanger worden gecommuniceerd is (nog) niet gebonden aan normatieve eisen. De Twiin Beheerorganisatie publiceert de endpoints en technische adressen in ZORG-AB. Om de technische adressen van een andere partij te achterhalen kan er worden gekozen om ZORG-AB te raadplegen (10.6.5 | Addressing - ZORG-AB Transacties (see page 288)) maar dit is niet verplicht. GtK-verzender en GtK-ontvanger kunnen bijvoorbeeld ook onderling afspraken maken over de wijze waarop technische adressen worden gecommuniceerd.
Prescription Level/Type	Verplicht
Toetsing	n.v.t.
Transactie/verwijzing	De procedures hiervoor moeten nog worden opgesteld.

Identificatie en authenticatie-eisen

> Deze sectie is gelijk aan PvE \| Identificatie en authenticatie (see page 204)

Id-01	Zorgverleners dienen geïdentificeerd te worden op basis van een uniek ID
Omschrijving/Toelichting/ Uitleg/Implicaties	UZI of een ander uniek tot één persoon te herleiden nummer. Wanneer een eigen id wordt gebruikt moet dit een **unieke combinatie** van persoons-id en organisatie-id opleveren en dat dit **herleidbaar blijft** (ook na, bijvoorbeeld, vertrek van zorgverlener), uitgegeven op het op het juiste betrouwbaarheidsniveau
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	alle Twiin-transacties

Auth-01	Zorgverlener/gebruiker (van het GtK) dienen (lokaal) geauthentiseerd te worden op eIDAS-niveau hoog
Omschrijving/Toelichting/ Uitleg/Implicaties	Door de keten heen kan hier nog geen bewijs van worden meegeven zodat andere partijen de zorgverlener ook met zekerheid kunnen authenticeren.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	alle Twiin-transacties

BgZ-2a-AA-01 / BgZ-2a-AA-02	Opzoekbaar maken publieke sleutel gebruikt voor ondertekening
Omschrijving/Toelichting/ Uitleg/Implicaties	**GtK-verzender** en **GtK-ontvanger** dienen de publieke sleutel(s) die zij gebruiken voor de ondertekening van JWT's via `kid` opzoekbaar te maken voor GtK-ontvanger. De wijze waarop de uitwisseling van publieke sleutels tussen GtK-verzender en GtK-ontvanger plaatsvindt is (nog) niet gebonden aan normatieve eisen. GtK-verzender en GtK-ontvanger moeten daarom onderling en in afstemming met de gebruikte infrastructuur afspraken maken over de wijze van uitwisseling van publieke sleutels.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Z1.2.1.2 | BgZ: Authentication & Authorization (see page 310)

BgZ-2a-AA-03	Aanmaken client assertion
Omschrijving/Toelichting/ Uitleg/Implicaties	**GtK-verzender** is in staat een client assertion in de vorm van een `authentication_grant` aan te maken die voldoet aan de specificaties
Prescription Level/Type	Verplicht
Toetsing	Validatie

BgZ-2a-AA-03	Aanmaken client assertion
Transactie/verwijzing	Specificaties: 10.4.2 | TTA FHIR - Authorization | id 10.2.5 | TTA FHIR Authentication & Authorization Client authentication

BgZ-2a-AA-05	Identifiers GtK
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK-verzender en GtK-ontvanger dienen gebruik te maken van dezelfde identifiers voor de systemen die opereren als autorisatie-servers (authorization server token endpoints) Het toekennen en gebruiken van identifiers van systemen is (nog) niet gebonden aan landelijke normatieve eisen. GtK-verzender en GtK-ontvanger moeten daarom onderling en in afstemming met de gebruikte infrastructuur afspraken maken over de te gebruiken identifiers van systemen. Voor de BgZ is nu afgestemd dat de systeem identifiers zelf gekozen moeten zijn, maar de vorm van een FQDN of OID mogen hebben.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie `aud` -velden in Twiin-07 | Token Request (see page 270)

Autorization-eisen

> Deze sectie is gelijk aan PvE | Autorization (see page 206)

BgZ-2a-AA-04	Systeem identifiers autorisatie-clients
Omschrijving/Toelichting/ Uitleg/Implicaties	**GtK-verzender** en **GtK-ontvanger** dienen gebruik te maken van dezelfde identifiers voor de systemen die opereren als autorisatie-clients (OAuth clients). Het toekennen en gebruiken van identifiers van systemen is (nog) niet gebonden aan normatieve eisen. GtK-verzender en GtK-ontvanger moeten daarom onderling en in afstemming met de gebruikte infrastructuur afspraken maken over de te gebruiken identifiers van systemen.
Prescription Level/Type	Verplicht
Toetsing	Validatie

BgZ-2a-AA-04	Systeem identifiers autorisatie-clients
Transactie/verwijzing	Zie `iss` -velden in Z1.2.1.2 | BgZ: Authentication & Authorization (see page 310)

BgZ-2a-AA-04	Systeem identifiers autorisatie-servers
Omschrijving/Toelichting/ Uitleg/Implicaties	**GtK-verzender** en **GtK-ontvanger** dienen gebruik te maken van dezelfde identifiers voor de systemen die opereren als autorisatie-servers (authorization server token endpoints). Het toekennen en gebruiken van identifiers van systemen is (nog) niet gebonden aan landelijke normatieve eisen. GtK-verzender en GtK-ontvanger moeten daarom onderling en in afstemming met de gebruikte infrastructuur afspraken maken over de te gebruiken identifiers van systemen. Voor de BgZ is nu afgestemd dat de systeem identifiers zelf gekozen moeten zijn, maar de vorm van een FQDN of OID mogen hebben
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie `aud` -velden in Z1.2.1.2 | BgZ: Authentication & Authorization (see page 310)

BgZ-2a-AA-13	Aanmaken access token request voor resource endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	De **GtK-ontvanger** is in staat conform de specificaties een access token request voor toegang tot het resource-endpoint aan te maken en aan GtK-verzender te versturen. Eventueel inclusief een eerder van GtK-verzender ontvangen `authorization_grant` , welke de digitale representatie van de veronderstelde toestemming (`authorization_base`) bevat.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Specificaties: (TA141) Z1.2.1.2 | BgZ: Authentication & Authorization#Access-token-request (TA141) Twiin-07 | Token Request#Authorization-grant (TA141) Twiin-07 | Token Request#Authorization-base

BgZ-2a-AA-14	Aanmaken access token request voor resource endpoint
Omschrijving/Toelichting/ Uitleg/Implicaties	**GtK-verzender** is in staat conform de specificaties een access token request van GtK-ontvanger voor toegang tot het resource server endpoint af te handelen.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Specificaties: (TA141) Z1.2.1.2 | BgZ: Authentication & Authorization#Access-token-request

Netwerkbeveiligingseisen

> Deze sectie is gelijk aan PvE | Netwerkbeveiliging (see page 213)

5.010 / BgZ-2a-NS-02	Authenticeren met PKI
Omschrijving/Toelichting/ Uitleg/Implicaties	Om zich te kunnen authenticeren, kunnen alle systemen betrokken bij transacties in het kader van Twiin een geldig PKIo-certificaat overleggen. Gebruikte PKIo-certificaten dienen te zijn uitgegeven onder de CA “Staat der Nederlanden Private Services CA – G1”. Deze omvatten: • UZI-servercertificaat of • PKIoverheid Private Services CA – G1 certificate Het betreft de systemen in de rol van token-server en -client, notification-server en -client en resource-server en -client. Zie 10.4.7 | Network level security (see page 211)
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	

5.020	mTLS
Omschrijving/Toelichting/ Uitleg/Implicaties	Alle transacties in het kader van Twiin zijn beveiligd met Mutual Transport Layer Security[89] (mTLS).
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	

89. https://datatracker.ietf.org/doc/html/rfc8705

5.030 / BgZ-2a-NS-03	**Volgen TLS-richtlijnen NCSC**
Omschrijving/Toelichting/ Uitleg/Implicaties	**GtK-verzender** en **GtK-ontvanger** maken gebruik van TLS versies en -algoritmen die zijn geclassificeerd als beveiligingsniveau "goed" in de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS), 2025-5[90] van het NCSC: Verplicht gebruik van de volgende cryptografische algoritmes: • Certificate Verification: ECDSA, RSA en EdDSA* • Key exchange: ECDHE* is afgewaardeerd van goed naar voldoende. Met X25519MLKEM768, SecP256r1MLKEM768, SecP384r1MLKEM1024 zijn er alternatieven, maar deze algoritmes zijn (relatief) nieuw en maken nog geen deel uit van de TLS standaarden. ECDHE moet daarom nog gebruikt worden. • Bulk encryption: AES-256-GCM of ChaCha20-Poly1305 • Hash functions: SHA-512 of SHA-384 of SHA-256 Het is verplicht om *alle*** algoritmen aan te bieden die in de genoemde richtlijnen als "goed" zijn geclassificeerd. Hiermee wordt er voor gezorgd dat wanneer onverhoopt een algoritme in veiligheidsniveau daalt er andere alternatieven overblijven van niveau goed. *Deze algoritmen zijn afgewaardeerd naar beveiligingsniveau 'voldoende'. Maar zijn geen (beschikbare) varianten die geclassificeerd is met beveiligingsniveau 'goed'. Hierdoor is het noodzakelijk om ook deze algoritmen op het niveau 'voldoende' te gebruiken. **Er geldt een uitzondering voor ChaCha20-Poly1305. Voor bulk encryptie wordt door sommige partijen de keuze gemaakt voor AES-256-GCM en **niet** voor ondersteuning van ChaCha20-Poly1305. De laatste is namelijk niet compliant met de eisen (Federal Information Processing Standards) die het Amerikaanse NIST (National Institute of Standards and Technology) stelt. Het is voor een GtK-server niet verboden om ook andere algoritmen en TLS-versies te ondersteunen van een lager niveau dan goed. De rationale hierachter is dat hard- en software waar de GtK-server gebruik van maakt ook voor andere use cases buiten het Twiin Afsprakenstelsel ingezet kan worden. De GtK-verzender MOET in het kader van Twiin echter wel altijd de door Twiin beschreven algoritmen en TLS-versie bij de GtK-ontvanger aanbieden.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS), versie 2.1[91]

90. https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2025/juni/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2025-05/TLS-Richtlijnen-2025-05.pdf
91. https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1

5.040	Versleuteling volgens TLS
Omschrijving/Toelichting/ Uitleg/Implicaties	Transacties in het kader van Twiin worden versleuteld volgens TLS, zoals bedoeld in eis 5.020.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	

5.050 / BgZ-2a-NS-04	Controleren geldigheid TLS-certificaat
Omschrijving/Toelichting/ Uitleg/Implicaties	**GtK-verzender** en **GtK-ontvanger** controleren minimaal ieder uur door middel van CRL of OCSP de geldigheid van de certificaten van systemen waarmee transacties plaatsvinden.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	

5.060 / BgZ-2a-NS-05	CPS van het UZI-register
Omschrijving/Toelichting/ Uitleg/Implicaties	Systemen die de geldigheid van het UZI-servercertificaat van de andere Systemen dienen te controleren, voldoen aan de verplichting van het Certification Practice Statement (CPS) UZI-register.
Prescription Level/Type	Conditioneel Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie https://www.zorgcsp.nl/certification-practice-statement-cps , artikel 4.5.2 CRL's: https://www.zorgcsp.nl/certificate-revocation-lists-crl-s

BgZ-2a-NS-06	CPS van PKIo
Omschrijving/Toelichting/ Uitleg/Implicaties	Wanneer GtK-verzender en GtK-ontvanger de geldigheid van een PKIo-servercertficaat controleren, doen zij dit op basis van de afspraken in het Certification Practice Statement (CPS) PKIoverheid.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie https://cps.pkioverheid.nl/pkioverheid-cps-unified-v5.4.html , hoofdstuk 2

5.070	Gebruik CRL of OSCP
Omschrijving/Toelichting/ Uitleg/Implicaties	Systemen die de geldigheid van het PKIo-servercertificaat van de andere Systemen dienen te controleren, doen dit door middel van de meest recent gepubliceerde Certificaten Revocatie Lijst (CRL) of via het Online Certificate Status Protocol (OCSP), minimaal ieder uur.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	Zie https://cps.pkioverheid.nl/pkioverheid-cps-unified-v5.4.html , paragraaf 2.2.

5.080	Ondertekening volgens DNSSEC
Omschrijving/Toelichting/ Uitleg/Implicaties	GtK zijn in hun rol als DNS Server moet er voor zorgen dat de *name records* behorende bij de hostnames van GtK'en zijn ondertekend volgens DNSSEC. (proudly copied from MedMij (core.dns.300))[92]
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	

92. https://afsprakenstelsel.medmij.nl/asverplicht/mmverplicht/verantwoordelijkheden-core

5.090	Controleren ondertekenning DNSSEC
Omschrijving/Toelichting/ Uitleg/Implicaties	Elke GtK, in zijn rol als DNS resolver in het Domain Name System, controleert of de ontvangen name records zijn voorzien van ondertekening volgens DNSSEC en valideert deze volgens DNSSEC. Indien deze controle en validatie niet beide slagen, ziet hij af van verbinding met de betreffende hostname. Het gebruik van DNSSEC vermindert de kwetsbaarheid van het Domain Name System voor bijvoorbeeld DNS spoofing[93].
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	(proudly copied from MedMij (core.dns.301))[94]

Z2 | BB: Implementatiewijzer Beeldbeschikbaarheid - Trial

Inleiding

Deze implementatiewijzer is bedoeld voor leveranciers en zorgaanbieders. Leveranciers hebben een vooraanstaande rol om het landelijke dekkend netwerk te realiseren; zonder leveranciers geen uitwisseling. Twiin werkt daarom samen met leveranciers van zorginformatiesystemen. Bij de oplossingen die we samen bedenken, gaan we uit van de functionele behoeften van de eindgebruikers. Deelnemende zorgaanbieders geven hun leveranciers opdracht te voldoen aan de eisen van het Twiin Afsprakenstelsel, zodat zorgaanbieders gezondheidsgegevens kunnen uitwisselen.

In het afsprakenstelsel staan deze eisen helder beschreven. Leveranciers kunnen ook de rol van GtK Beheerder op zich nemen in opdracht van een deelnemer. Daarnaast kunnen ze hun applicaties laten valideren als GtK-applicatie.

- Belangrijke gerelateerde onderdelen van het afsprakenstelsel: Technische kern (see page 164), Twiin Implementatiewijzer Zorgtoepassingen (see page 294), Vertrouwensmodel (see page 56), Voorwaarden (see page 142),

De implementatiewijzer

Dit onderdeel beschrijft de technische implementatie voor de beschikbaarheid van data van de Twiin zorgtoepassing Beeldbeschikbaarheid.

De zorgtoepassing Beeldbeschikbaarheid beoogt het mogelijk te maken dat artsen kunnen beschikken over een tijdlijn - het overzicht van al het beschikbare beeldvormend onderzoek (beeld en verslag) van hun patiënten. Met één tijdlijn van onderzoeken van een patiënt krijgt de arts het benodigde inzicht en

93. https://datatracker.ietf.org/doc/html/rfc5452#section-3
94. https://afsprakenstelsel.medmij.nl/asverplicht/mmverplicht/verantwoordelijkheden-core

overzicht voor de processen van beeldacquisitie, -beoordeling, -bewerking en -opslag tot en met herbeoordelingen. Op basis van de tijdlijn kan een arts de achterliggende onderzoeksgegevens raadplegen en inzien.

Scope Beeldbeschikbaarheid

Door GtK's (Gevalideerde Twiin Knooppunten) te verbinden met elkaar helpt Twiin mee aan het realiseren van de Tijdlijn. Twiin schrijft voor welke transacties **tussen** de knooppunten verplicht zijn, inclusief de benodigde metadata, authenticatie, autorisatie en logging.

Achter een GtK is een Twiin Deelnemer vrij om een eigen architectuur te handhaven, zo lang het GtK waar hij/zij mee verbonden is de gevraagde data maar teruggeeft aan het opvragende GtK volgens de door Twiin omschreven standaard.

Dit zorgt voor standaardisatie tussen de GtK's, en maakt het uitwisselen van gegevens op landelijk niveau mogelijk.

Wat betekent dit voor de zorgverlener achter een GtK

Bij opvraag van gegevens zal het GtK van de raadplegende zorgverlener alle gekoppelde GtK's bevragen. Alle GtK's spreken dezelfde 'taal' omdat deze allemaal gevalideerd zijn tegen de door Twiin gestelde eisen. Hierdoor zullen alle GtK's een antwoord terugsturen dat door het opvragende GtK gebundeld kan worden teruggegeven aan de applicatie achter een GtK.

Inhoud

- Volume 1 geeft een functioneel overzicht voor de databeschikbaarheid van de zorgtoepassing Beeldbeschikbaarheid en de daarbij behorende eisen
- Volume 2 bevat de technische afspraken voor de uitwisseling van beelden en verslagen. Dit noemen we ook wel de Twiin Technische Afspraak (TTA)
- Volume 3: een verwijzing naar de informatiestandaard en de meta informatie

Z2.1 | BB: Volume 0 - Functioneel overzicht

Inhoud

Inleiding

In dit volume volgt:

- een beschrijving van het tijdlijn concept en de functionele usecase van de zorgtoepassing
- een overzicht van de communicatiepatronen die worden gebruikt voor deze zorgtoepassing
- een beschrijving of verwijzing naar de eisen die gesteld zijn door organisaties, programma's en/of informatiestandaarden.

In volume 2 volgen de de uitwerking van de transacties van de communicatiepatronen voor de zorgtoepassing beeldbeschikbaarheid (in het Engels).

Versie informatie

Versie Zorgtoepassing	Compatibel met Twiin Afsprakenstelsel release	Wijzingen
1.3.0	1.3.0 en alle opvolgende binnen de major release 1.x.x	

Functionele usecase

Tijdlijn

De medisch (beeldvormend) specialist wil een overzicht (tijdlijn) van alle beelden en verslagen die beschikbaar zijn op studieniveau. Via de tijdlijn verkrijgt hij/zij toegang tot een integraal, plaats- en tijdonafhankelijk chronologisch overzicht van een patiënt in de eigen werkomgeving van alle in Nederland uitgevoerde (radiologische) beeldvormende onderzoeken inclusief verslagen en beelden. Dit

is nodig voor een aantal zorgprocessen zoals het doorverwijzen van een patiënt of het intercollegiaal bespreken van patiënten tijdens bijvoorbeeld een MDO.

Usecases

In de NEN7541 (Beeldbeschikbaarheid) en de informatiestandaard Beeldbeschikbaarheid[95] zijn meerdere usecases voor het radiologie domein uitgewerkt.

De informatiestandaard Beeldbeschikbaarheid voorziet in het raadplegen van de tijdlijn, het opvragen van beelden en verslagen, en daarnaast ook hoe deze aangemeld dienen te worden (sinds release alpha2):

1. Radioloog stelt verslaggegevens beschikbaar t.b.v. tijdlijn (buiten scope van Twiin)
2. Radioloog stelt beeldgegevens beschikbaar t.b.v. tijdlijn (buiten scope van Twiin)
3. Radioloog/Behandelend arts raadpleegt tijdlijn data
4. Radioloog/Behandelend arts raadpleegt beelden
5. Radioloog/Behandelend arts raadpleegt verslagen

> Twiin beschrijft enkel het uitwisselen van gegevens tussen GtK's, hiermee vallen de usecases om gegevens aan te melden buiten scope van Zorgtoepassing Beeldbeschikbaarheid.
>
> Er wordt wel verwacht dat een GtK de juiste metadata teruggeeft bij een verzoek om gegevens, hierom adviseert Twiin wel deze twee usecases in acht te nemen voor het beschikbaar stellen van gegevens tbv de tijdlijn.

> Het versturen van beeld en verslag is voor nu geen onderdeel meer van de Informatiestandaard Beeldbeschikbaarheid. Hier wordt gewacht op de uitkomsten van de NEN7541 waar een opdracht is uitgezet om de push usecase uit te werken. Deze uitkomsten zullen opgenomen worden in de Informatiestandaard Beeldbeschikbaarheid.
>
> Zodra de Push usecases zijn toegevoegd aan de Informatiestandaard zal Twiin deze verwerken tot een TTA Push voor Zorgtoepassing Beeldbeschikbaarheid

> Twiin verwijst niet meer naar de Kwaliteitsstandaard en functionele eisen van de NVvR vanwege de eenvoudige reden dat Nictiz deze Kwaliteitsstandaard verwerkt in de Informatiestandaard.

Communicatiepatronen

Beeldbeschikbaarheid kan gerealiseerd worden met de volgende communicatiepatronen

95. https://informatiestandaarden.nictiz.nl/wiki/Bbs:V1_Ontwerp_Beeldbeschikbaarheid

10.1.2 | Communicatiepatroon: Indexed Pull (see page 172)

10.1.3 | Communicatiepatroon: Push (see page 175)

https://vzvz.atlassian.net/wiki/spaces/Twiin/pages/239305195

Z2.1.1 | BB: Raadplegen Tijdlijn Data

> Informatiestandaard alpha 2
>
> https://informatiestandaarden.nictiz.nl/wiki/Bbs:V1_alpha.2_Ontwerp_Beeldbeschikbaarheid
>
> Hoofdstuk 2.4 Usecase 3 Raadplegen Tijdlijn Data

Doel en Relevantie

Door de "tijdlijn radiologische onderzoeken" te raadplegen in de eigen werkomgeving krijgt de radioloog / behandelend arts inzicht in eerder uitgevoerde radiologische onderzoeken van de patiënt. Dit is essentieel voor het goed, veilig en verantwoord te laten verlopen van het radiologisch zorgproces. Beschikbaarheid van eerdere onderzoeken (beelden en verslagen) naast de meest actuele is relevant in elk zorgproces, waar beelden een rol spelen.

Indien dit gewenst is kunnen ook alleen radiologische onderzoeken die bij één zorginstelling van de patiënt beschikbaar zijn op de tijdlijn getoond worden (zie patient journey 2).

Voor het raadplegen van de tijdlijn is patiënttoestemming (vooraf of ad-hoc, im- of expliciet) verondersteld. In het geval dat de patiënt in een levensbedreigende situatie verkeert, niet aanspreekbaar is en er vooraf geen toestemming is vastgelegd dient een break-the-glass procedure te worden gevolgd.

Patient journey

1. Reguliere verwijzing (aangepast uit Kwaliteitsstandaard Beeldbeschikbaarheid)

Patiënt X met een bekende voorgeschiedenis meldt zich bij de huisarts met aanhoudende vermoeidheidsklachten. Op basis van haar anamnese en lichamelijk onderzoek besluit de huisarts een aantal bloedonderzoeken aan te vragen en een röntgenfoto van de longen van patiënt X in ziekenhuis A. De huisarts bespreekt de uitslagen van de onderzoeken met patiënt X. De bloedwaarden zijn normaal, maar in het verslag van de radioloog in ziekenhuis A staat dat er wat op de thoraxfoto is gezien, en dat nader onderzoek moet worden overwogen. De huisarts stelt een verwijzing voor naar de longarts. Gezien de wachttijden kiest patiënt X niet voor ziekenhuis A maar voor ziekenhuis B. Longarts B in ziekenhuis B ontvangt patiënt X op haar spreekuur. Ze luistert naar de klachten van de patiënt en leest de uitslagen van eerder uitgevoerde onderzoeken. Ook raadpleegt zij de tijdlijn radiologische onderzoeken.

2. Raadplegen onderzoeken van specifieke zorgaanbieder (aangepast uit Kwaliteitsstandaard Beeldbeschikbaarheid)

In 2018 valt patiënt Y van zijn fiets en gaat naar de SEH. Ademen doet veel pijn. SEH-arts A laat een foto van zijn borst maken in ziekenhuis A. Hij blijkt een aantal gekneusde ribben te hebben. In 2020 wordt patiënt Y door zijn huisarts verwezen naar ziekenhuis B, omdat hij aanhoudende hoestklachten heeft. Longarts B laat een foto van zijn longen maken. Radioloog B, die de beelden beoordeelt, ziet een wit vlekje op de long. Dit zou een tumor kunnen zijn maar ook een litteken. Eerder onderzoek kan meer uitsluitsel geven. Patiënt Y geeft aan dat hij eerder in ziekenhuis A is geweest. De radioloog raadpleegt de "tijdlijn radiologische onderzoeken" voor ziekenhuis A en ziet de borstfoto uit 2018. Radioloog B kan het witte vlekje op de long vergelijken met de foto in 2018 en rapporteert aan de longarts dat het hoogstwaarschijnlijk gaat om een litteken.

Proces en Context (pre- en postproces)

Preproces

- De radioloog / behandelend arts heeft een behandelrelatie met de patiënt.
- De radioloog / behandelend arts wil eerder uitgevoerde radiologische onderzoeken betrekken om tot een beter en vollediger oordeel, verslag en advies te komen, dan zonder het geval zou zijn.

Proces

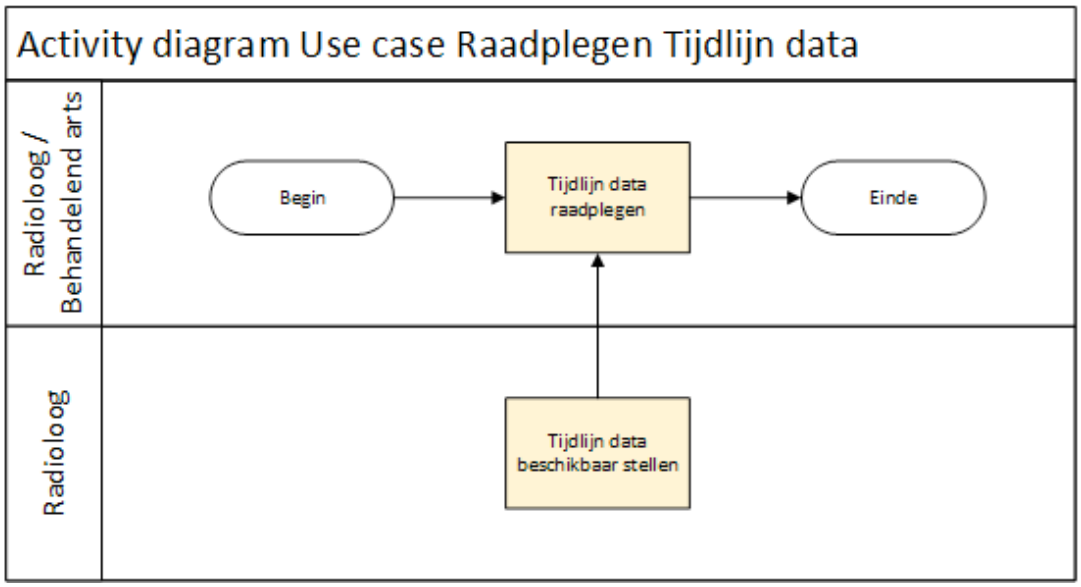
- De radioloog / behandelend arts raadpleegt de "tijdlijn radiologische onderzoeken"

Postproces

- De radioloog / behandelend arts krijgt de tijdlijn beschikbaar in zijn eigen werkomgeving als onderdeel van zijn workflow en geïntegreerd in het lokale patiëntendossier (EPD) én in het beeldendossier van de patiënt (PACS).
- De radioloog / behandelend arts ziet alle intern en extern (van één of meerdere zorgaanbieders) uitgevoerde radiologisch onderzoeken eenmalig in de tijdlijn.
- De radioloog / behandelend arts kan als volgende stap de beelden en verslagen van de getoonde onderzoeken raadplegen.

Bedrijfsrollen en UML activity diagram

Bedrijfsrol (actor)	Beschrijving bedrijfsrol
Radioloog	Stelt tijdlijn data beschikbaar
Radioloog / Behandelend arts	Raadpleegt tijdlijn data



Informatieoverdracht

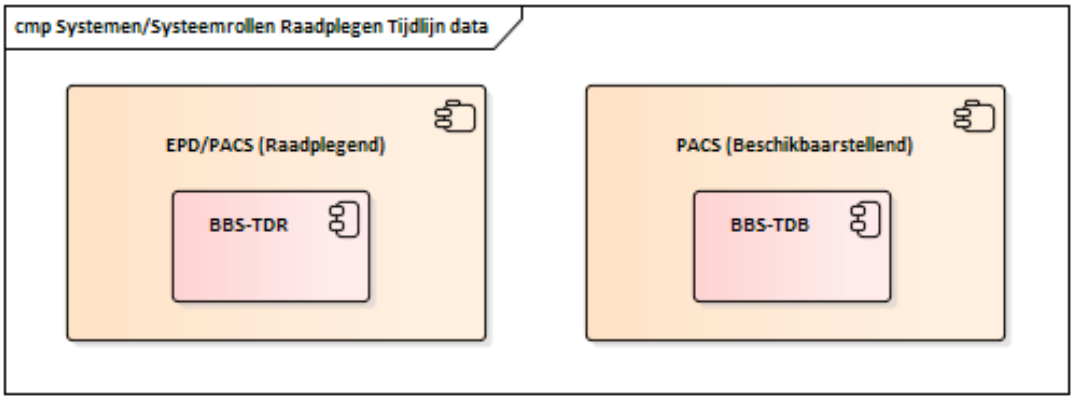
Systemen & Systeemrollen

Systemen:

- PACS/EPD van de raadplegende organisatie
- PACS van de beschikbaarstellende, producerende organisatie

Systeemrollen:

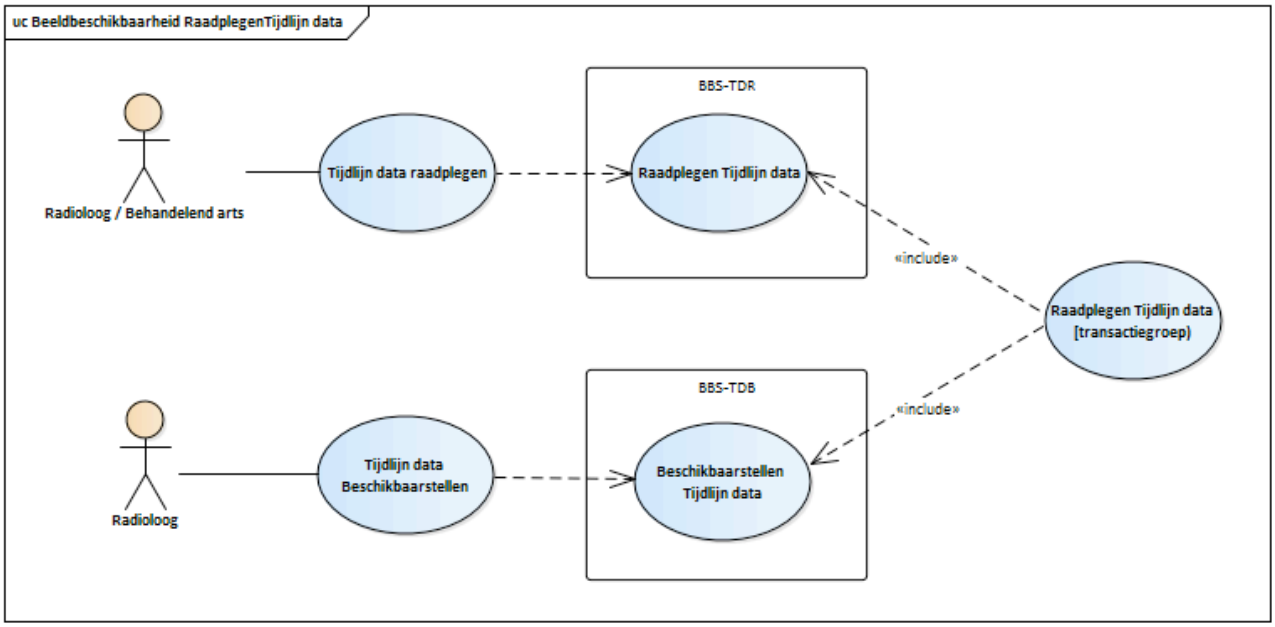
- Raadplegend Systeem EPD / PACS
  - TijdlijnDataRaadplegendSysteem (BBS-TDR)
- Beschikbaarstellend systeem PACS (producerende organisatie)
  - TijdlijnDataBeschikbaarstellendSysteem (BBS-TDB)



Transacties & Transactiegroepen

Het uitwisselen van gegevens tussen de verschillende systeemrollen gebeurt op basis van transacties, een verzameling van transacties (bijvoorbeeld een vraag- en antwoordbericht) vormt een zogeheten transactiegroep.

Samenhang bedrijfsrollen, activiteiten, transacties, systeemrollen en transactiegroepen



Transactiegroep	Transacties	Systeemrol	Systeem	Bedrijfsrol	Publicatie
Raadplegen tijdlijn data	Raadplegen tijdlijn data	BBS-TDR	PACS/EPD	Radioloog/ Behandelend arts	V1.0.0-alpha.2[96]
	Beschikbaarstellen tijdlijn data	BBS-TDB	PACS	Radioloog	V1.0.0-alpha.2[97]

96. https://decor.nictiz.nl/pub/bbs/bbs-html-20240208T092809/tr-2.16.840.1.113883.2.4.3.11.60.133.4.2-2022-06-13T000000.html
97. https://decor.nictiz.nl/pub/bbs/bbs-html-20240208T092809/tr-2.16.840.1.113883.2.4.3.11.60.133.4.2-2022-06-13T000000.html

Z2.1.2 | BB: Raadplegen Verslag

> Informatiestandaard alpha 2
>
> https://informatiestandaarden.nictiz.nl/wiki/Bbs:V1_alpha.2_Ontwerp_Beeldbeschikbaarheid
>
> Hoofstuk 2.5 Usecase 4 Raadplegen Verslag

Doel en Relevantie

De radioloog / behandelend arts raadpleegt relevante verslagen om tot een beter en vollediger oordeel, verslag en advies te komen, dan zonder het geval zou zijn. Dit is essentieel voor het goed, veilig en verantwoord laten verlopen van het radiologisch zorgproces. Beschikbaarheid van eerdere onderzoeken (beelden en verslagen) naast de meest actuele is relevant in elk zorgproces, waar beelden een rol spelen. De radioloog / behandelend arts raadpleegt het verslag via de tijdlijn radiologische onderzoeken. Voor het raadplegen van verslagen via de tijdlijn is patiënttoestemming (vooraf of ad-hoc, in- of expliciet) verondersteld.

Patient journey

Reguliere verwijzing vervolg op patient journey 3 uit usecase 3, (binnen Twiin ZT BB Z2.1.1 | BB: Raadplegen Tijdlijn Data (see page 418) journey 1)

Radioloog B in ziekenhuis B beoordeelt de CT thorax die van patiënt X is gemaakt, raadpleegt de tijdlijn radiologische onderzoeken, ziet dat in ziekenhuis A recent een thoraxfoto is gemaakt en dat haar analyse en conclusie in het verlengde liggen van wat radioloog A heeft opgenomen in het verslag. Ze maakt het verslag van de CT thorax met haar bevindingen voor longarts B. Op basis van al het aanvullend onderzoek stelt longarts B een diagnose en wordt besloten tot een behandeling met radiotherapeutische bestraling.

Proces en Context (pre- en postproces)

Preproces

Via tijdlijn:

- Usecase 3 Raadplegen tijdlijn data.
- De radioloog / behandelend arts ziet op de tijdlijn een eerder onderzoek waarvan hij een verslag wil raadplegen.

Buiten tijdlijn:

- De radioloog / behandelend arts is op de hoogte van een eerder onderzoek waarvan hij een verslag wil raadplegen.

Proces

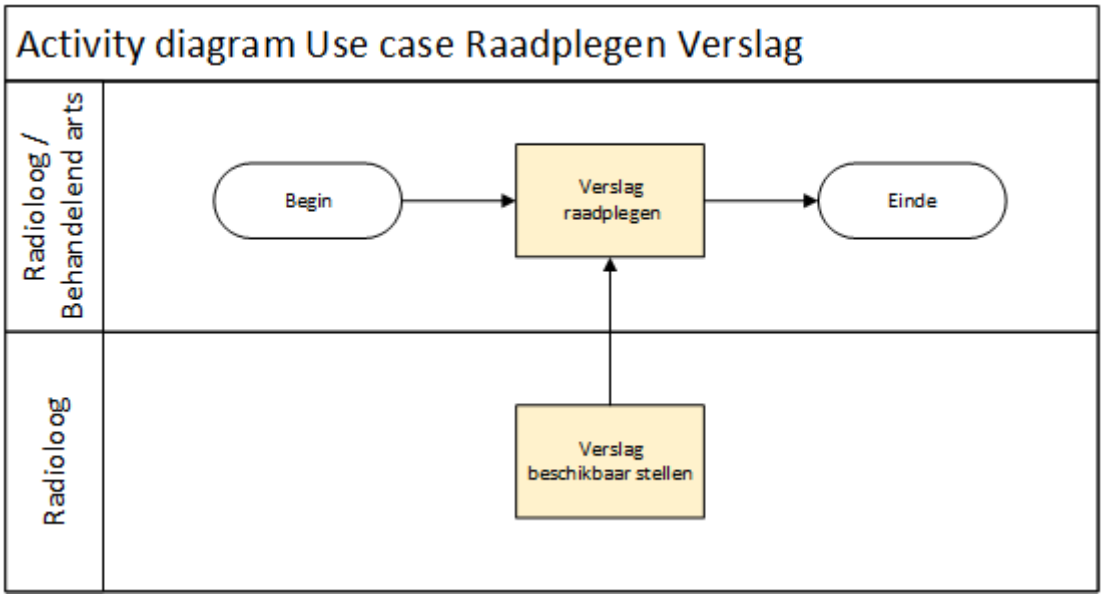
- De radioloog / behandelend arts raadpleegt het verslag via de tijdlijn radiologische onderzoeken.

Postproces

- De radioloog / behandelend arts ziet het geraadpleegde verslag in de eigen werkomgeving in eigen formaat.

Bedrijfsrollen en UML activity diagram

Bedrijfsrol (actor)	Beschrijving bedrijfsrol
Radioloog	Stelt verslag beschikbaar
Radioloog / Behandelend arts	Raadpleegt verslag



Informatieoverdracht

Systemen & Systeemrollen

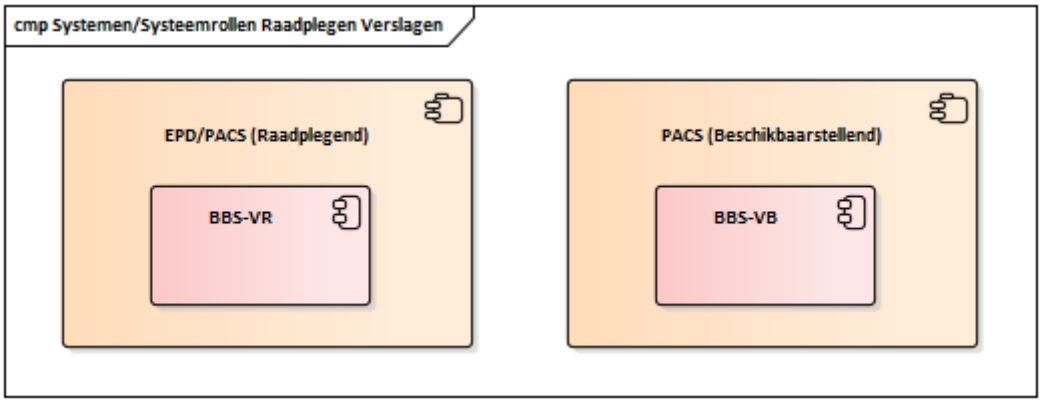
Systemen:

- PACS/EPD van de raadplegende organisatie
- PACS van de beschikbaarstellende, producerende organisatie

Systeemrollen:

- Raadplegend Systeem EPD / PACS
  - VerslagRaadplegendSysteem (BBS-VR)

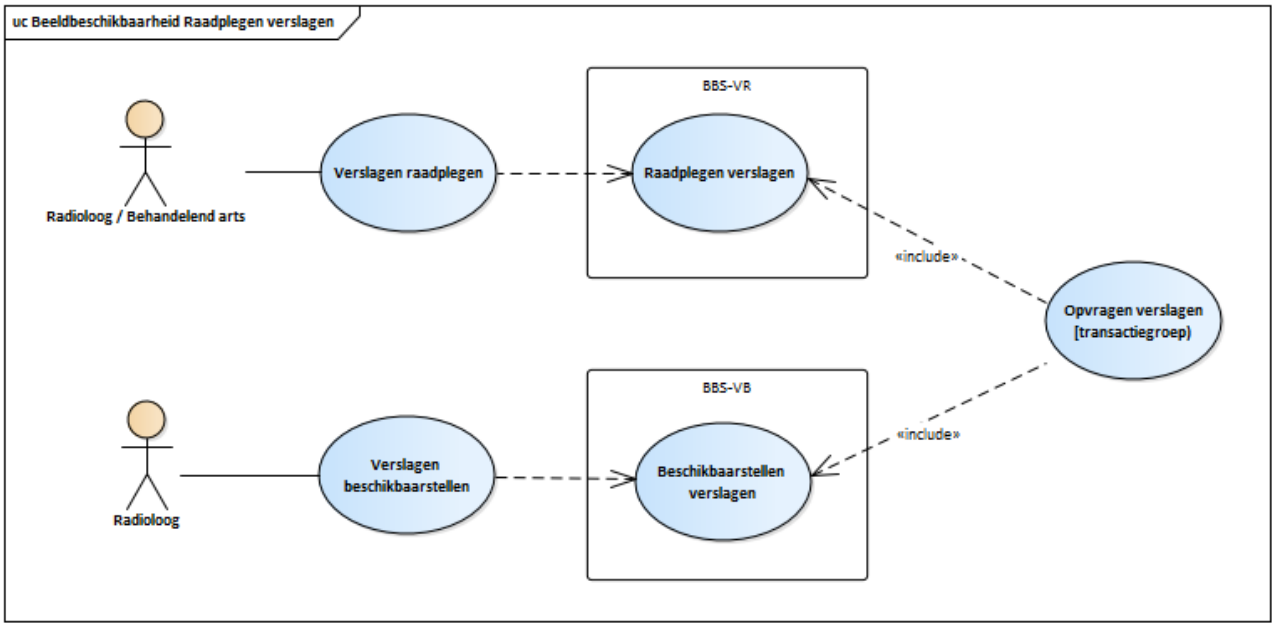
- Beschikbaarstellend systeem PACS (producerende organisatie)
  - VerslagBeschikbaarstellendSysteem (BBS-VB)



Transacties & Transactiegroepen

Het uitwisselen van gegevens tussen de verschillende systeemrollen gebeurt op basis van transacties, een verzameling van transacties (bijvoorbeeld een vraag- en antwoordbericht) vormt een zogeheten transactiegroep.

Samenhang bedrijfsrollen, activiteiten, transacties, systeemrollen en transactiegroepen



Transactiegroep	Transacties	Systeemrol	Systeem	Bedrijfsrol	Publicatie
Raadplegen Verslagen	Raadplegen verslagen	BBS-VR	PACS/EPD	Radioloog/ Behandelend arts	V1.0.0-alpha.2[98]
	Beschikbaarstellen verslagen	BBS-VB	PACS	Radioloog	V1.0.0-alpha.2[99]

Z2.1.3 | BB: Raadplegen Beeld

Informatiestandaard alpha 2

> https://informatiestandaarden.nictiz.nl/wiki/Bbs:V1_alpha.2_Ontwerp_Beeldbeschikbaarheid
>
> Hoofdstuk 2.6 Usecase 5 Raadplegen Beeld

Doel en Relevantie

De radioloog / behandelend arts raadpleegt relevante beelden om tot een beter en vollediger oordeel, verslag en advies te komen, dan zonder het geval zou zijn. Dit is essentieel voor het goed, veilig en verantwoord te laten verlopen van het radiologisch zorgproces. Beschikbaarheid van eerdere onderzoeken (beelden en verslagen) naast de meest actuele is relevant in elk zorgproces, waar beelden een rol spelen. De radioloog / behandelend arts raadpleegt beelden via de tijdlijn radiologische onderzoeken. Voor het raadplegen van beelden via de tijdlijn is patiënttoestemming (vooraf of ad-hoc, in- of expliciet) verondersteld.

Patient journey

Reguliere verwijzing (vervolg op patient journey 1 uit usecase 3) (binnen Twiin ZT BB Z2.1.1 | BB: Raadplegen Tijdlijn Data (see page 418) journey 1)

Longarts B raadpleegt de tijdlijn radiologische onderzoeken en haalt het onderzoek uit ziekenhuis A op. Samen met de patiënt bekijkt ze de thoraxfoto uit ziekenhuis A en wat radioloog A daarop heeft gezien. Ze besluit tot het aanvragen van een CT thorax om beter te bepalen wat er in de longen zit, en wat kan worden uitgesloten.

98. https://decor.nictiz.nl/pub/bbs/bbs-html-20240208T092809/tr-2.16.840.1.113883.2.4.3.11.60.133.4.26-2022-06-14T000000.html
99. https://decor.nictiz.nl/pub/bbs/bbs-html-20240208T092809/tr-2.16.840.1.113883.2.4.3.11.60.133.4.27-2022-06-14T000000.html

Proces en Context (pre- en postproces)

Preproces

Via tijdlijn:

- Usecase 3 Raadplegen tijdlijn data.
- De radioloog / behandelend arts ziet op de tijdlijn een eerder onderzoek waarvan hij de beelden wil raadplegen.

Buiten tijdlijn:

- De radioloog / behandelend arts is op de hoogte van een eerder onderzoek waarvan hij de beelden wil raadplegen.

Proces

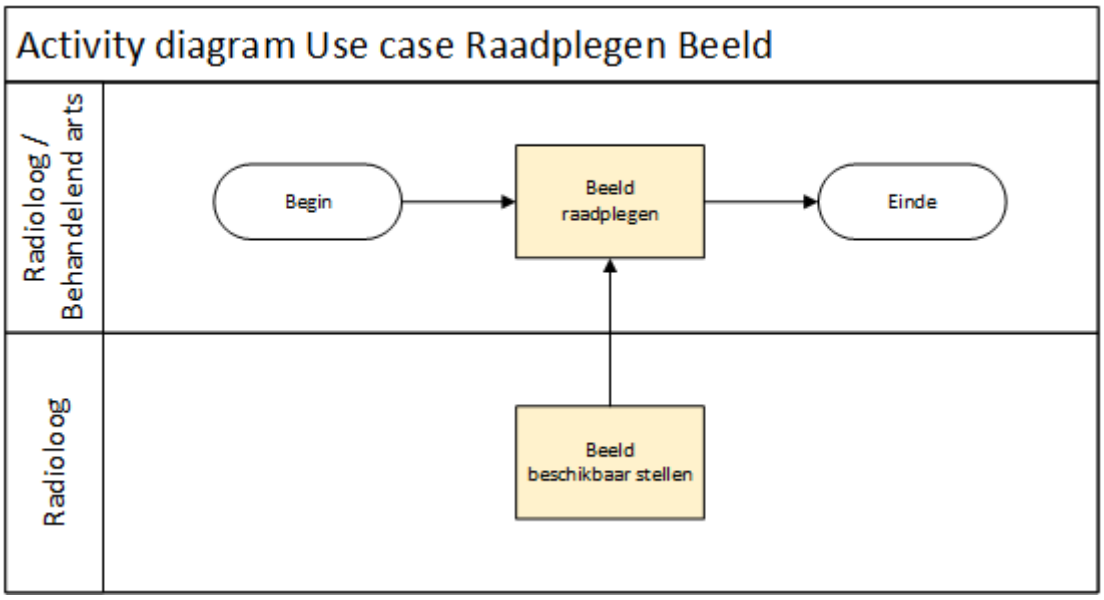
- De radioloog / behandelend arts raadpleegt de beelden via de tijdlijn radiologische onderzoeken.

Postproces

- De radioloog / behandelend arts ziet de opgehaalde beelden in zijn eigen werkomgeving.

Bedrijfsrollen en UML activity diagram

Bedrijfsrol (actor)	Beschrijving bedrijfsrol
Radioloog	Stelt beelden beschikbaar
Radioloog / Behandelend arts	Raadpleegt beelden



Informatieoverdracht

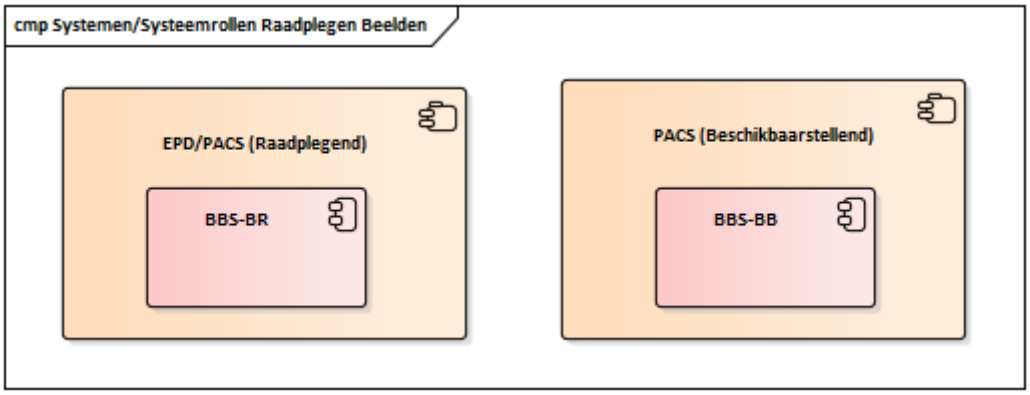
Systemen & Systeemrollen

Systemen:

- PACS/EPD van de raadplegende organisatie
- PACS van de beschikbaarstellende, producerende organisatie

Systeemrollen:

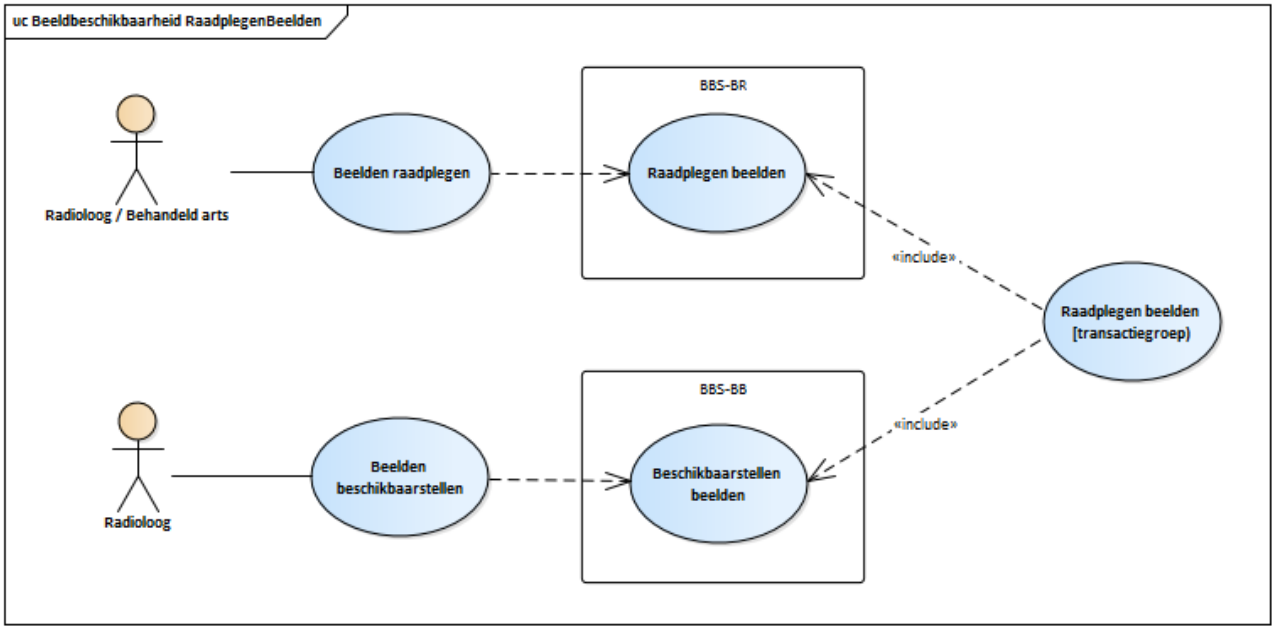
- Raadplegend Systeem EPD / PACS
  - BeeldRaadplegendSysteem (BBS-BR)
- Beschikbaarstellend systeem PACS (producerende organisatie)
  - BeeldBeschikbaarstellendSysteem (BBS-BB)



Transacties & Transactiegroepen

Het uitwisselen van gegevens tussen de verschillende systeemrollen gebeurt op basis van transacties, een verzameling van transacties (bijvoorbeeld een vraag- en antwoordbericht) vormt een zogeheten transactiegroep.

Samenhang bedrijfsrollen, activiteiten, transacties, systeemrollen en transactiegroepen



Transactiegroep	Transacties	Systeemrol	Systeem	Bedrijfsrol	Publicatie
Raadplegen Beelden	Raadplegen beelden	BBS-BR	PACS/EPD	Radioloog/ Behandelend arts	V1.0.0-alpha.2[100]
	Beschikbaarstellen beelden	BBS-BB	PACS	Radioloog	V1.0.0-alpha.2[101]

100. https://decor.nictiz.nl/pub/bbs/bbs-html-20240208T092809/tr-2.16.840.1.113883.2.4.3.11.60.133.4.14-2022-06-13T000000.html
101. https://decor.nictiz.nl/pub/bbs/bbs-html-20240208T092809/tr-2.16.840.1.113883.2.4.3.11.60.133.4.14-2022-06-13T000000.html

Z2.2 | BB Volume 1 - Twiin Technical Agreement

This volume describes the technical agreements and the needed transactions on how to exchange the information needed to support the Functional Usecases as described in Volume 1.

Currently there are five functional usecases described in Z2.1 | BB: Volume 0 - Functioneel overzicht (see page 416), these usecases biggest difference is they or use a 'push' to send information, or make use of a 'pull' to retrieve information.

Push

The following Functional Usecases are covered by Z2.2.2 | BB: Push (see page 433)

- https://vzvz.atlassian.net/wiki/spaces/Twiin/pages/291471732
- https://vzvz.atlassian.net/wiki/spaces/Twiin/pages/291995819

Pull

The following Functional Usecases are covered by Z2.2.1 | BB: Indexed Pull (see page 429)

- Z2.1.1 | BB: Raadplegen Tijdlijn Data (see page 418)
- Z2.1.2 | BB: Raadplegen Verslag (see page 422)
- Z2.1.1 | BB: Raadplegen beelden

Z2.2.1 | BB: Indexed Pull

> Original page can be found at 10.3.2 | TTA SOAP - Indexed Pull (IHE)

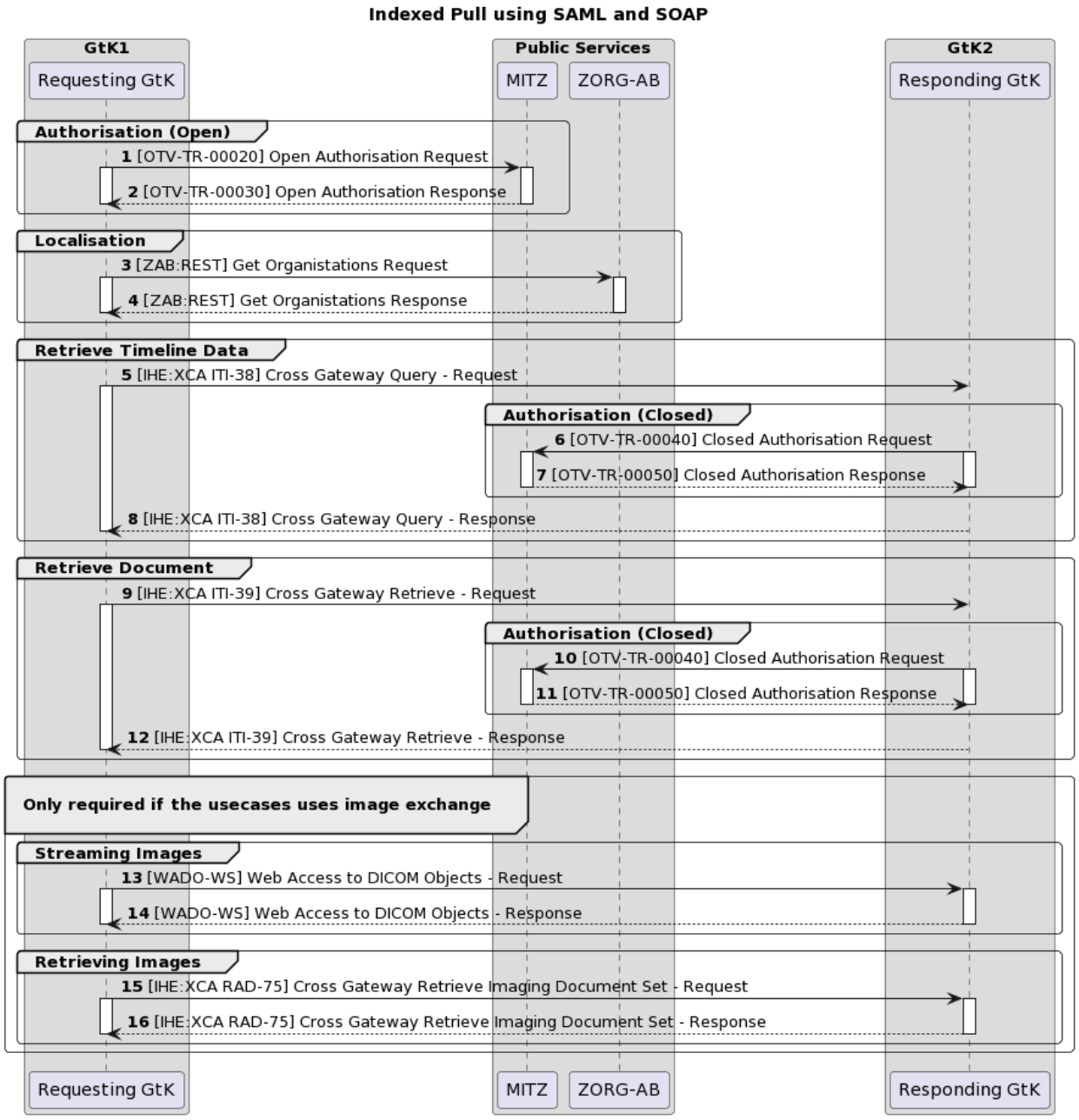
This Twiin Technical Agreement (TTA) describes and specifies technical responsibilities to which parties agree when connecting to exchange transactions to facilitate the Indexed Pull.

The Indexed Pull starts with several transactions required to locate where data is to be retrieved, aswell as the required endpoints where this data can be retrieved.

Sequence diagram

The sequence diagram below visualizes the full flow for the Indexed Pull interaction sequence.

Twiin describes the transaction between the GtK applications, applications behind these GtK applications can communicate with a GtK in any way they want, as long as the GtK uses the transactions as in this diagram


Indexed Pull using SAML and SOAP
GtK1
Requesting GtK
Public Services
MITZ
ZORG-AB
GtK2
Responding GtK
Authorisation (Open)
1 [OTV-TR-00020] Open Authorisation Request
2 [OTV-TR-00030] Open Authorisation Response
Localisation
3 [ZAB:REST] Get Organistations Request
4 [ZAB:REST] Get Organistations Response
Retrieve Timeline Data
5 [IHE:XCA ITI-38] Cross Gateway Query - Request
Authorisation (Closed)
6 [OTV-TR-00040] Closed Authorisation Request
7 [OTV-TR-00050] Closed Authorisation Response
8 [IHE:XCA ITI-38] Cross Gateway Query - Response
Retrieve Document
9 [IHE:XCA ITI-39] Cross Gateway Retrieve - Request
Authorisation (Closed)
10 [OTV-TR-00040] Closed Authorisation Request
11 [OTV-TR-00050] Closed Authorisation Response
12 [IHE:XCA ITI-39] Cross Gateway Retrieve - Response
Only required if the usecases uses image exchange
Streaming Images
13 [WADO-WS] Web Access to DICOM Objects - Request
14 [WADO-WS] Web Access to DICOM Objects - Response
Retrieving Images
15 [IHE:XCA RAD-75] Cross Gateway Retrieve Imaging Document Set - Request
16 [IHE:XCA RAD-75] Cross Gateway Retrieve Imaging Document Set - Response
Requesting GtK
MITZ
ZORG-AB
Responding GtK

Each section consists of several steps. The steps correspond to the numbers in the sequence diagram.

> For all IHE transactions it is required to include a SAML token. This is usually included in the request the XIS (source) sends to a GtK.
>
> As Twiin decribes the transactions between GtK's, the transaction between a XIS and a GtK can be however the implementators of these applications see fit, as long as the transactions between GtK's include the SAML token as Twiin decribes it to be.
>
> IHE ITI-40 | Provide X-User Assertion (see page 265)

Section	Step	Description
Authorisation (Open)	1	Before initiating the retrieval of the Timeline data, a XIS behind the Initiating GtK sends a request to this GtK. After this request is recieved the GtK first sends an 'open' authorisation request to the Public Service know as 'MITZ' 10.6.3 | Patient Consent - Mitz Transacties (see page 284) - OTV-TR-00020
	2	This request is replied to by MITZ, in this request, the GtK's where data is available, are given back to the Initiating GtK 10.6.3 | Patient Consent - Mitz Transacties (see page 284) - OTV-TR-00030
Localisation	3	After the GtK 'knows' where available data can be retrieved, the Initiating GtK then requests the endpoints at the Public Service know as ZORG-AB 10.6.5 | Addressing - ZORG-AB Transacties (see page 288)
	4	ZORG-AB replies to this request with the endpoints 10.6.5 | Addressing - ZORG-AB Transacties (see page 288)
Retrieve Timeline data	5	Using the endpoints the GtK uses this information to send the query. With this transaction a SAML token is included 10.5.7 | IHE ITI-38 | Cross Gateway Query (see page 237) (TA141) 10.5.7.1 | ITI-38 examples#ITI-38-request
	6	The responding GtK then checks if the patients permission is in check at MITZ 10.6.3 | Patient Consent - Mitz Transacties (see page 284) - OTV-TR-00040
	7	A response is sent back 10.6.3 | Patient Consent - Mitz Transacties (see page 284) - OTV-TR-00050

	8	After the 'closed authentication' transaction is done, the Responding GtK retrieves the metadata at the XIS(es) connected with the Responding Gtk and sends this back to the Initiating Gateway. 10.5.7 | IHE ITI-38 | Cross Gateway Query (see page 237) (TA141) 10.5.7.1 | ITI-38 examples#ITI-38-response The Initiating GtK bundles the replies of the one or more Responding GtK's and sends this back to the XIS application originally requesting the data from the Initiation Request. A Timeline can now be built using this data in the XIS
Retrieve Document	9	Using the Timeline data, a request for a document can now be done from within the XIS (Consumer, connected to the Initiating GtK). The XIS then sends this request to the Initiating GtK. The Initiating GtK then sends a request including a SAML token to the Responding GtK where the XIS (Source, connected to the Responding GtK) is behind and the requested document is available. 10.5.8 | IHE ITI-39 | Cross Gateway Retrieve (see page 249) (TA141) 10.5.8.1 | ITI-39 examples#ITI-39-request
	10	(see step 6) 10.6.3 | Patient Consent - Mitz Transacties (see page 284) - OTV-TR-00040
	11	(see step 7) 10.6.3 | Patient Consent - Mitz Transacties (see page 284) - OTV-TR-00050
	12	After the 'closed authentication' transaction is done, the Responding GtK retrieves the document from the XIS where this document is available and sends this back to the Initiating Gateway 10.5.8 | IHE ITI-39 | Cross Gateway Retrieve (see page 249) (TA141) 10.5.8.1 | ITI-39 examples#ITI-39-response The Initiating Gateway on its turn returns this document to the XIS from where the document is requested from.
Streaming Images	13	the WADO-WS transaction can be used by a Requesting GtK to retrieve DICOM images in a different format and resolution. 10.5.6 | Twiin-06 | WADO-WS (see page 234)
	14	The images are sent back in the requested format 10.5.6 | Twiin-06 | WADO-WS (see page 234)

Retrieving Images	15	It is also possible the request is done for images instead of documents. Prior to this transaction a KOS object is retrieved using steps 9-12. Using the information in the retrieved KOS object images can be requested. 10.5.9 | IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set (see page 256) (TA141) 10.5.9 | RAD-75 examples#RAD-75-request
	16	The images are sent back 10.5.9 | IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set (see page 256) (TA141) 10.5.9 | RAD-75 examples#RAD-75-response

10.3 | Kern Volume 1a - Technical Agreements - CP (see page 185)

10.3.1.1 Notified Pull - Data interactions (see page 190)

Z2.2.2 | BB: Push

Besides the Indexed Pull to build up a Timeline and retrieve documents and images it is also possible to directly push Radiology Studies to a consulting party.

The architecture used for pushing Radiology Studies is not (yet) an open architecture. A nationwide solution has been implemented to push images from one user to another.

The project to implement this solution is called Twiin Portaal. For more information see https://www.vzvz.nl/diensten/gemeenschappelijke-diensten/twiin-portaal

In a future release it is intended to create an open architecture.

Z2.3 | BB: Volume 2 - Transacties

In dit onderdeel worden de transacties voor uitwisseling binnen de zorgtoepassing Beeldbeschikbaarheid beschreven. Hierbij wordt zoveel mogelijk verwezen naar de transacties in de implementatie handleiding kern.

De uitwisseling vindt plaats op basis van SOAP transacties.

Inhoud

Transacties tussen GtK applicaties

Geïndexeerde bevraging[102]	IHE ITI-38 | Cross Gateway Query (see page 237) IHE ITI-39 | Cross Gateway Retrieve (see page 249) IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set (see page 256)

Tussen de GtK's is het van belang dat er gebruik gemaakt wordt van een SAML token en een beveiligde verbinding door gebruik te maken van mTLS. Binnen het kern document zijn deze transacties verder uitgewerkt:

IHE ITI-40 | Provide X-User Assertion (see page 265)

Network Level Security mTLS 1.3 (see page 211)

Transacties naar gemeenschappelijke voorzieningen

Voor de transacties naar de gemeenschappelijke voorzieningen volgt hieronder een verwijzing naar het generiek implementatie en aansluitwijzer kern

Transacties naar gemeenschappelijke voorzieningen (see page 264)

Voorbeeld Transacties tussen GtK applicaties en bronsysteem

Twiin schrijft in principe niet voor hoe de communicatie tussen de GtK-applicatie en het bronsysteem plaatsvindt.

Wel geven we vanuit Twiin een voorbeeld hoe dit ingericht zou kunnen worden voor deze twee communicatiepatronen:

Geïndexeerde bevraging[103]	[IHE:XDS ITI-18] Opvraag metadata bij een GtK-applicatie[104] [IHE:XDS ITI-43] Opvraag gegevens bij een andere GtK-applicatie[105] [IHE:XDS RAD-69] Opvraag beelden bij via een GtK-applicatie[106]
Push - Versturen[107]	[IHE:XDS ITI-41] Aanmelden documenten[108] [IHE:XDS ITI-42] Registreren metadata[109] [IHE:XDS RAD-68] Aanmelden Beelden[110]

102. https://confluence.vzvz.nl/pages/viewpage.action?pageId=50371337
103. https://confluence.vzvz.nl/pages/viewpage.action?pageId=50371337
104. https://confluence.vzvz.nl/display/Twiin/%5BIHE%3AXDS+ITI-18%5D+Opvraag+metadata+bij+een+GtK-applicatie?src=contextnavpagetreemode
105. https://confluence.vzvz.nl/display/Twiin/%5BIHE%3AXDS+ITI-43%5D+Opvraag+gegevens+bij+een+andere+GtK-applicatie?src=contextnavpagetreemode
106. https://confluence.vzvz.nl/display/Twiin/%5BIHE%3AXDS+RAD-69%5D+Opvraag+beelden+bij+via+een+GtK-applicatie?src=contextnavpagetreemode

NB. ten opzichte van de transacties die in de kern zijn beschreven, zijn er voor beeldbeschikbaarheid geen aanvullingen

{}

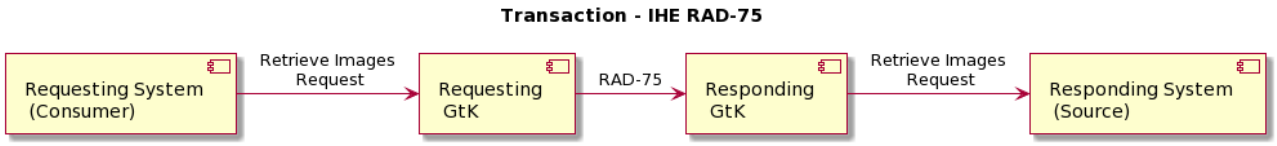
Z2.3.1 | BB: IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set

> This section is the same as the generic 10.5.9 | IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set (see page 256)

Scope

This transaction is used by the Requesting GtK to retrieve images from sources behind Responding GtK's. Prior to this transaction, the '10.5.7 | IHE ITI-38 | Cross Gateway Query (see page 237) is used for the necessary information (specifically the metadata of the KOS Objects and the KOS objects of the set of images to be requested)

Use Case Roles



> This transaction uses SOAP v1.2 and Synchronous Web Services.

Referenced standards

Implementers of this transaction shall comply with all requirements described in Web Services for IHE Transactions.[111]

ebRIM	OASIS/ebXML Registry Information Model v3.0

107. https://confluence.vzvz.nl/display/Twiin/Uitwisselconcept%3A++Push+-+Versturen?src=contextnavpagetreemode
108. https://confluence.vzvz.nl/display/Twiin/%5BIHE%3AXDS+ITI-41%5D+Aanmelden+documenten?src=contextnavpagetreemode
109. https://confluence.vzvz.nl/display/Twiin/%5BIHE%3AXDS+ITI-42%5D+Registreren+metadata?src=contextnavpagetreemode
110. https://confluence.vzvz.nl/display/Twiin/%5BIHE%3AXDS+ITI-41%5D+Aanmelden+documenten?src=contextnavpagetreemode
111. https://profiles.ihe.net/ITI/TF/Volume2/ch-V.html#Appendix%20V

ebRS	OASIS/ebXML Registry Services Specifications v3.0
ITI TF-3:4	Metadata in Document Sharing profiles
MTOM	SOAP Message Transmission Optimization Mechanism http://www.w3.org/TR/soap12-mtom/
XOP	XML-binary Optimized Packaging http://www.w3.org/TR/2005/REC-xop10-20050125/

Messages

Cross Gateway Retrieve Imaging Document Set

> For more technical specification, see the original document: https://www.ihe.net/uploadedFiles/Documents/Radiology/IHE_RAD_TF_Vol3.pdf

NB: This transaction is always performed in combination with the transaction ITI-40 where user data is added in a SAML token.
NB: All transactions are logged with an ITI-20 audit transaction, see IHE:ITI volume 2 for the correct implementation."

Z2.3.2 | BB: IHE ITI-38 | Cross Gateway Query

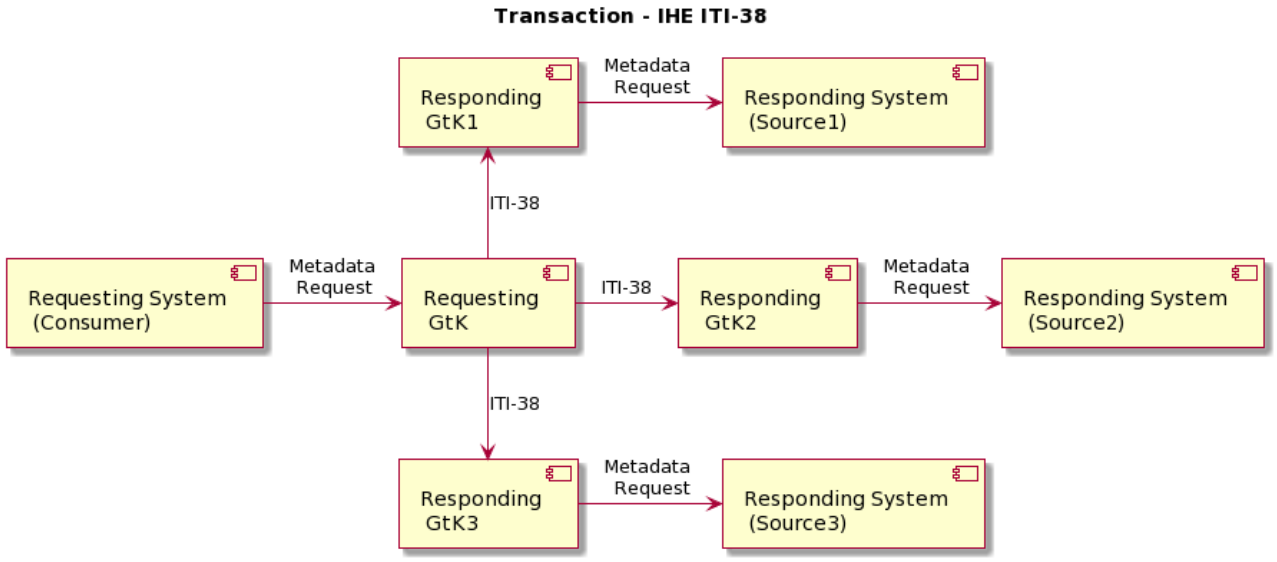
> This section is the same as the generic 10.5.7 | IHE ITI-38 | Cross Gateway Query (see page 237)

Scope

This transaction is used by the Requesting GtK to retrieve metadata. The Requesting GtK sends this request to all Responding GtK's where information is available. Prior to this transaction the Requesting GtK first needs to retrieve information about where metadata can be retrieved. This is needed to prevent excessive usage of the transaction to GtK's where no information is available.

> The Mitz open question specifications can be found on their website: Bijlage | Architectuurdocumenten

Use Case Roles



> This transaction uses SOAP v1.2 and Synchronous Web Services.

Referenced standards

Implementers of this transaction shall comply with all requirements described in Web Services for IHE Transactions.[112]

ebRIM	OASIS/ebXML Registry Information Model v3.0

112. https://profiles.ihe.net/ITI/TF/Volume2/ch-V.html#Appendix%20V

ebRS	OASIS/ebXML Registry Services Specifications v3.0
ITI TF-3:4	Metadata used in Document Sharing profiles

Messages

Cross Gateway Query

> For more technical specification, see the original document: https://profiles.ihe.net/ITI/TF/Volume2/ITI-38.html

NB: This transaction is always performed in combination with the transaction ITI-40 (see page 265) where user data is added in a SAML token.
NB: All transactions are logged with an ITI-20 audit transaction, see IHE:ITI volume 2 for the correct implementation."

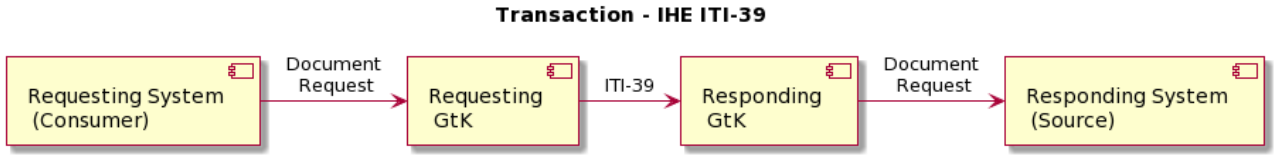
Z2.3.3 | BB: IHE ITI-39 | Cross Gateway Retrieve

> This section is the same as the generic 10.5.8 | IHE ITI-39 | Cross Gateway Retrieve (see page 249)

Scope

This transaction is used by the Requesting GtK to retrieve one of more documents from the Responding GtK.

Use Case Roles



> This transaction uses SOAP v1.2 and Synchronous Web Services.

Referenced standards

Implementers of this transaction shall comply with all requirements described in Web Services for IHE Transactions.[113]

ebRIM	OASIS/ebXML Registry Information Model v3.0
ebRS	OASIS/ebXML Registry Services Specifications v3.0
ITI TF-3:4	Metadata used in Document Sharing profiles
MTOM	SOAP Message Transmission Optimization Mechanism http://www.w3.org/TR/soap12-mtom/

Messages

Cross Gateway Retrieve

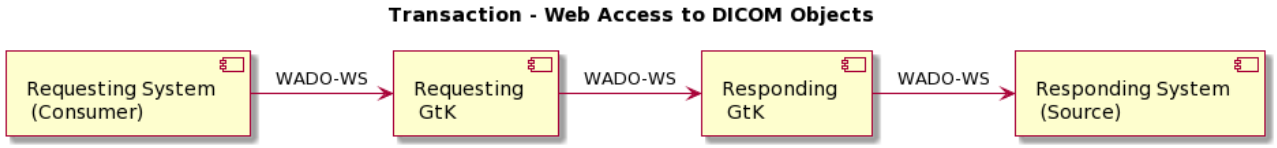
> For more technical specification, see the original document: https://profiles.ihe.net/ITI/TF/Volume2/ITI-39.html

NB: This transaction is always performed in combination with the transaction ITI-40 (see page 265) where user data is added in a SAML token.
NB: All transactions are logged with an ITI-20 audit transaction, see IHE:ITI volume 2 for the correct implementation."

Z2.3.4: WADO-WS

> In the Netherlands the WADO-WS transaction is used in the SOAP based exchange pattern Indexed Pull.
>
> Although this is a deprecated transaction it is still used by most consumers to 'stream' images. Which means, request images in other formats than the 'full DICOM' format. (for example JPEG in lower resolution)
>
> A Requesting GtK can choose to implement the WADO-WS transaction
>
> An Responding GtK should be able to receive the WADO-WS transaction

113. https://profiles.ihe.net/ITI/TF/Volume2/ch-V.html#Appendix%20V


Transaction - Web Access to DICOM Objects
Requesting System (Consumer)
WADO-WS
Requesting GtK
WADO-WS
Responding GtK
WADO-WS
Responding System (Source)

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- This wsdl file is for an XDS-I.b Imaging Document Source Actor
It can be used 'as is' to support Retrieve Imaging Document Set Transaction [RAD-69]
using Synchronous Web Services.-->
<definitions name="ImagingDocumentSource" targetNamespace="urn:ihe:rad:xdsi-b:2009"
xmlns="http://schemas.xmlsoap.org/wsdl/" xmlns:wsdl="http://schemas.xmlsoap.org/
wsdl/" xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/" xmlns:wsaw="http://
www.w3.org/2006/05/addressing/wsdl" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:tns="urn:ihe:rad:xdsi-b:2009" xmlns:wadows="urn:dicom:wado:ws:2011"
xmlns:deprecatedwadows="urn:dicom:ws:wado:2011" xmlns:ihe="urn:ihe:iti:xds-b:2007"
xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"> <documentation>IHE XDS-I.b
Imaging Document Source</documentation> <types>
<xsd:schema elementFormDefault="qualified">
<xsd:import namespace="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0" /> <xsd:import
namespace="urn:ihe:iti:xds-b:2007" />
<xsd:import namespace="urn:ihe:rad:xdsi-b:2009" />
</xsd:schema> </types>
<message name="RetrieveImagingDocumentSetRequest_Message"> <documentation>Retrieve
Imaging Document Set</documentation>
<part name="body" element="tns:RetrieveImagingDocumentSetRequest" />
</message>
<message name="RetrieveRenderedImagingDocumentSetRequest_Message">
<documentation>Retrieve Rendered Imaging Document Set</documentation>
<part name="body" element="wadows:RetrieveRenderedImagingDocumentSetRequest" /> </
message>
<message name="DeprecatedRetrieveRenderedImagingDocumentSetRequest_Message">
<documentation>Deprecated Retrieve Rendered Imaging Document Set</documentation>
<part name="body"
element="deprecatedwadows:RetrieveRenderedImagingDocumentSetRequest" /> </message>
<message name="RetrieveRenderedImagingDocumentSetResponse_Message">
<documentation>Retrieve Rendered Imaging Document Set Response</documentation>
<part name="body" element="wadows:RetrieveRenderedImagingDocumentSetResponse" /> </
message>
<message name="RetrieveDocumentSetResponse_Message">
<documentation>Retrieve Document Set Response</documentation>
<part name="body" element="ihe:RetrieveDocumentSetResponse" /> </message>
<portType name="ImagingDocumentSource_PortType">
<operation name="ImagingDocumentSource_RetrieveImagingDocumentSet"> <input
message="tns:RetrieveImagingDocumentSetRequest_Message"
wsaw:Action="urn:ihe:rad:2009:RetrieveImagingDocumentSet" /> <output
message="tns:RetrieveDocumentSetResponse_Message"
wsaw:Action="urn:ihe:iti:2007:RetrieveDocumentSetResponse" /> </operation>
```

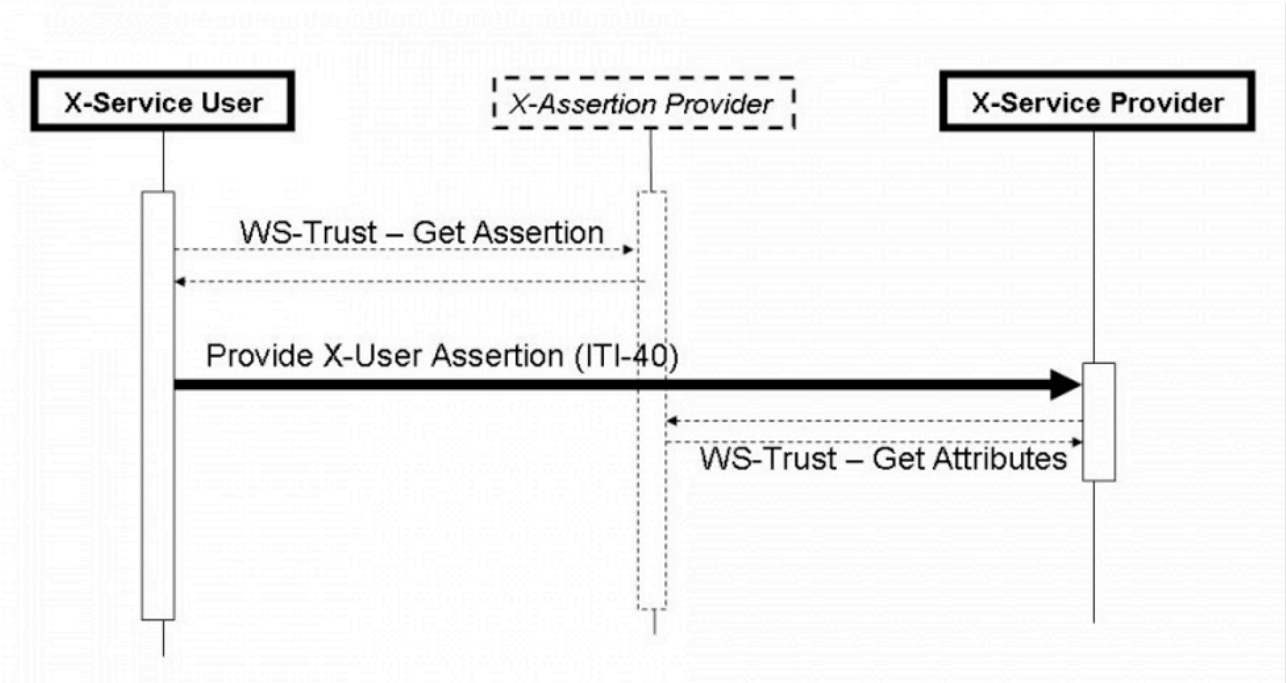
```
<operation name="ImagingDocumentSource_RetrieveRenderedImagingDocumentSet"> <input
message="tns:RetrieveRenderedImagingDocumentSetRequest_Message"
wsaw:Action="urn:dicom:wado:ws:2011:RetrieveRenderedImagingDocumentSet" /> <output
message="tns:RetrieveRenderedImagingDocumentSetResponse_Message"
wsaw:Action="urn:dicom:wado:ws:2011:RetrieveRenderedImagingDocumentSetResponse" />
</operation>
<operation
name="ImagingDocumentSource_DeprecatedRetrieveRenderedImagingDocumentSet"> <input
message="tns:DeprecatedRetrieveRenderedImagingDocumentSetRequest_Message"
wsaw:Action="urn:dicom:ws:wado:2011:RetrieveRenderedImagingDocumentSet" /> <output
message="tns:RetrieveDocumentSetResponse_Message"
wsaw:Action="urn:ihe:iti:2007:RetrieveDocumentSetResponse" /> </operation>
</portType>
<binding name="ImagingDocumentSource_Binding"
type="tns:ImagingDocumentSource_PortType">
<soap12:binding style="document" transport="http://schemas.xmlsoap.org/soap/http" />
<wsaw:UsingAddressing wsdl:required="true" />
<operation name="ImagingDocumentSource_RetrieveImagingDocumentSet">
<soap12:operation soapActionRequired="false" /> <input>
<soap12:body use="literal" />
</input> <output>
<soap12:body use="literal" /> </output>
</operation>
<operation name="ImagingDocumentSource_RetrieveRenderedImagingDocumentSet">
<soap12:operation soapActionRequired="false" /> <input>
<soap12:body use="literal" /> </input>
<output>
<soap12:body use="literal" />
</output>
</operation>
<operation
name="ImagingDocumentSource_DeprecatedRetrieveRenderedImagingDocumentSet">
<soap12:operation soapActionRequired="false" /> <input>
<soap12:body use="literal" /> </input>
<output>
<soap12:body use="literal" />
</output> </operation>
</binding>
<service name="ImagingDocumentSource_Service">
<port name="ImagingDocumentSource_Port_Soap12"
binding="tns:ImagingDocumentSource_Binding"> <soap12:address location="http://
servicelocation/ImagingDocumentSource_Service" />
</port> </service> </definitions>
```

Z2.3.5 | BB: IHE ITI-40 | Provide X-User Assertion

Scope

This transaction is used to add user attributes in the SOAP TTA transactions. The attributes are placed in a SAML-token in the security header of a, for example, ITI-75 transaction.

Use Case Roles



Referenced Standards

- OASIS http://www.oasis-open.org/committees/security/
- SAMLCore[114] SAML V2.0 Core standard
- WSS10[115] OASIS Standard, "OASIS Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)", March 2004.
- WSS11[116] OASIS Standard, "OASIS Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)", February 2006.
- WSS:SAMLTokenProfile1.0[117] OASIS Standard, “Web Services Security: SAML Token Profile”, December 2004

114. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
115. http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf
116. http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
117. http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0.pdf

- WSS:SAMLTokenProfile1.1[118] OASIS Standard, "Web Services Security: SAML Token Profile 1.1", February 2006
- XSPA-SAMLv1.0 OASIS Standard, "Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of the Security Assertion Markup Language (SAML) for Healthcare v1.0" , November 2009
- SAML 2.0 Profile For XACML 2.0 OASIS Standard, February 2005

Informative -- assist with understanding or implementing this transaction

- IHE Profiles
  - Personnel White Pages[119] Profile
  - Enterprise User Authentication[120] Profile
  - Basic Patient Privacy Consents[121] Profile
- OASIS
  - SAML V2.0 Standards http://www.oasis-open.org/committees/security/ .
  - SAML V2.0 Technical Overview
  - SAML Executive Overview
  - SAML Tutorial presentation by Eve Maler of Sun Microsystems
  - SAML Specifications
  - WS-Trust - OASIS Web Services Secure Exchange (WS-SX) TC
  - XSPA-XACMLv1.0 OASIS Standard, "Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare v1.0" , November 2009

Messages

Provide X-User Assertion

> For more technical specification, see the original document: https://profiles.ihe.net/ITI/TF/Volume2/ITI-40.html

Twiin implementation

The SAML token is only valid for 10 minutes. The SAML token has the following attributes (in addition to the required attributes from the SAML-standard)

Element	Opt.	DataType

118. http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf
119. https://profiles.ihe.net/ITI/TF/Volume1/ch-11.html
120. https://profiles.ihe.net/ITI/TF/Volume1/ch-4.html
121. https://profiles.ihe.net/ITI/TF/Volume1/ch-19.html

urn:nl:otv:names:tc:1.0:subject:mandated	C	HL7 V3 II
urn:ihe:iti:xua:2017:subject:provider-identifier	R	HL7 V3 II
urn:oasis:names:tc:xacml:2.0:subject:role	R	HL7 V3 CE
urn:ihe:iti:appc:2016:document-entry:event-code	O	HL7 V3 CV
urn:nl:otv:names:tc:1.0:subject:provider-institution	R	HL7 V3 II
urn:oasis:names:tc:xspa:1.0:subject:organization	O	String
urn:oasis:names:tc:xspa:1.0:subject:organization-id	O	anyURI
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	R	HL7 V3 CV

> The SAML token is only required in the transactions **between** GtK (external traffic).

Identification Raadpleger	
Name:	urn:nl:otv:names:tc:1.0:subject:mandated
Type:	urn:hl7-org:v3:II
Example:	`extension="123456789" root="2.16.528.1.1007.3.1" assigningAuthorityName="CIBG"`
Opt.:	**Conditional**, required if the person is mandated by the *verantwoordelijke-id.*

Identification Verantwoordelijke	
Name:	urn:ihe:iti:xua:2017:subject:provider-identifier

Type:	urn:hl7-org:v3:II
Example:	`extension="123456782" root="2.16.528.1.1007.3.1" assigningAuthorityName="CIBG"`
Opt.:	**Required,** UZI-nummer *verantwoordelijke.*

Rolcode verantwoordelijke healthcare provider	
Name:	urn:oasis:names:tc:xacml:2.0:subject:role
Type:	urn:hl7-org:v3:CE
Example:	`code="01.013" codeSystem="2.16.840.1.113883.2.4.15.111" codeSystemName="RoleCodeNL" displayName="Arts v. maag-darm-leverziekten"`
Opt.:	**Required,** UZI *rolcode*

Data category	
Name:	urn:ihe:iti:appc:2016:document-entry:event-code
Type:	urn:hl7-org:v3:CV
Example:	`code="GGC007" codeSystem="2.16.840.1.113883.2.4.3.111.5.10.1"`
Opt.:	**Optional**

Identification *verantwoordelijke* provider	
Name:	urn:nl:otv:names:tc:1.0:subject:provider-institution
Type:	urn:hl7-org:v3:II
Example:	`<AttributeValue DataType="urn:hl7-org:v3#II" ><InstanceIdentifier xmlns="urn:hl7-org:v3" extension="00014332" root="2.16.528.1.1007.3.3" /></AttributeValue>`
Opt.:	**Required, URA**

Alternative Identification *verantwoordelijke* provider	
Name:	urn:oasis:names:tc:xspa:1.0:subject:organization
Type:	String
Example:	`<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization"><saml:AttributeValue>Family Medical Clinic</saml:AttributeValue> </saml:Attribute>`
Opt.:	**Conditional, required if** urn:oasis:names:tc:xspa:1.0:subject:organization-id is not empty

Alternative Identification *verantwoordelijke* provider (id)	
Name:	urn:oasis:names:tc:xspa:1.0:subject:organization-id

Type:	AnyURI
Example:	`<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id"> <saml:AttributeValue>http://familymedicalclinic.org</ saml:AttributeValue> </saml:Attribute>`
Opt.:	**Conditional, required if** urn:oasis:names:tc:xspa:1.0:subject:organization is not empty

Purpose of use	
Name:	urn:oasis:names:tc:xspa:1.0:subject:purposeofuse
Type:	urn:hl7-org:v3#CV
Example:	<AttributeValue DataType=" urn:hl7-org:v3#CV"> <CodedValue xmlns="urn:hl7-org:v3" code="TREAT" codeSystem="2.16.840.1.113883.1.11.20448" displayName="treatment" /> </AttributeValue>
Opt.:	**Required**

Z2.3.6 | Network level security mTLS1.3

The network connections between GtK's must be secure. In a secure network, certificates play a crucial role by enabling the establishment of secure connections using TLS. They also ensure the authenticity and integrity of data in transit. Therefore mutual TLS shall be used between GtK's.

Both the Sending System and Receiving System expose endpoints that must be protected from unauthorized and malicious interactions. More specifically, access control measures must be applied to the following endpoints:

- Receiving System: Notification endpoint (FHIR Task endpoint)
- Sending System: Resource endpoint

Mutual TLS shall be used to protect these endpoints in the following ways:

- Authentication: The sending and receiving systems are mutually verifying each other's identity before establishing a secure connection. In this way only systems that are trusted are allowed to set up connections.

- Encryption: an mTLS connection is encrypted. This means that only the sending and receiving systems can read the exchanged data and no third, unauthorized party can 'listen in'.
- Integrity: mTLS assures that the data has not been modified by any unauthorized party during transmission. Any tampering attempts would alert the recipient.
- Protection against replay attacks: Each message sent over the connection includes a sequence number, and the recipient keeps track of the sequence numbers it has received. If a message with a previously received sequence number arrives, it is considered a replayed message and is rejected. This prevents attackers from intercepting and resending previously valid messages.

> There are endpoints where access control measures do not need to be enforced. For example, the endpoint where the JWKS is available. Mutual TLS does not need to be enforced there, because there is virtually no opportunity to do any real harm. On the other hand, in the technical core we do indeed also refer to those endpoints elsewhere—just not in the sense that they require extra attention from a network-level security perspective.

Terminology

- Certificate Authority (CA): A trusted entity responsible for issuing and managing certificates used in secure network connections.
- Certificate Revocation List (CRL): A list maintained by a Certificate Authority, containing revoked certificates to prevent the use of compromised or invalid certificates.
- Public Key Infrastructure overheid (PKIo): A PKI structure controlled by the Dutch government, governing the issuance and management of certificates in the Netherlands.
- Trusted Service Provider (TSP): A party authorized to issue PKIo certificates within the PKIo infrastructure, ensuring the integrity and security of the certificates they issue.

Network level security: mTLS 1.3

At the network level, mutual TLS (mTLS) must be applied. The TLS-implementation must comply with the security level "Good" as specified by the National Cyber Security Centre (NCSC). At the time of writing, the https://www.ncsc.nl/documenten/publicaties/2025/juni/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2025-05 (Security guidelines for Transport Layer Security 2025-05) require version 1.3 of the TLS standard for the security level "Good". In the case one or more of the cipher suites (Appendix B of the Security guidelines) are declassified by NCSC will this be described in a future version of the Twiin specification.

The exchange of a client certificate during the mTLS handshake does not only enable the server to authenticate the client on network level, but it also enables the server to issue certificate bound access tokens as specified in https://www.rfc-editor.org/rfc/rfc8705 as an additional security measure on application level. See section Resource server authorization: OAuth 2.0 (see page 211) for requirements on application level security using OAuth 2.0.

CRL / OCSP / CPS

The validity of a certificate shall be verified using a CRL, OCSP, or CPS check. A determined validity may be relied upon for a maximum of one hour, after which the verification must be performed again. If the validity of a certificate cannot be established, the connection shall be terminated, as it shall also be terminated if the certificate is found to be invalid.

PKIoverheid

Both the client and server certificates must be PKIo-certificates that are issued under the CA "Staat der Nederlanden Private Services CA – G1" (this includes UZI server certificates issued by UZI-registry (CIBG)). https://cert.pkioverheid.nl/

Note: the requirements specified in this chapter apply to Notification, FHIR, and token endpoints.

Z2.3.7 IHE ITI-20 | Record Audit Event

Scope

At every non-logging transaction an audit event is recorded and sent to the Audit Record Repository.

Use Case Roles

Referenced standards

RFC5424	The Syslog Protocol.
RFC5425	Transmission of Syslog Messages over TLS
RFC5426	Transmission of Syslog Messages over UDP
RFC7525	Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)
DICOM	DICOM PS3.15 Annex A.5 http://medical.nema.org/medical/dicom/current/output/chtml/part15/sect_A.5.html
ASTM E2147-01	Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems
NIST SP 800-92	Guide to Computer Security Log Management.
W3C XML 1.0	Extensible Markup Language (XML) 1.0

HL7 FHIR	*Release 4 http://hl7.org/fhir/R4/index.html*
RFC4627	*The application/json Media Type for JavaScript Object Notation (JSON)*

Messages

Send Audit Event – Syslog Interaction

> For more technical specification, see the original document: https://profiles.ihe.net/ITI/TF/Volume2/ITI-20.html

NB: This transaction is always performed in combination with the transaction ITI-40 (see page 265) where user data is added in a SAML token.
NB: All transactions are logged with an ITI-20 audit transaction, see IHE:ITI volume 2 for the correct implementation.

Send Audit Resource Rerquest Message - FHIR Feed Interaction

> This is part of the ITI TF Supplement: Add RESTful ATNA (Query and Feed) - Status: Trial Implementation

> For more technical specification, see the original document: paragraph 3.20.4.2 of https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RESTful-ATNA.pdf

Send Audit Bundle Request Message - FHIR Feed Interaction

> This is part of the ITI TF Supplement: Add RESTful ATNA (Query and Feed) - Status: Trial Implementation

> For more technical specification, see the original document: paragraph 3.20.4.3 of https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RESTful-ATNA.pdf

Z2.3.7 | BB: IHE ITI-1 | Maintain Time

Scope

This transaction is used to synchronize time among multiple systems.

Referenced Standards

NTP Network Time Protocol Version 3. RFC1305

SNTP Simple Network Time Protocol (SNTP) RFC4330

Messages

> For more technical specification, see the original document: https://profiles.ihe.net/ITI/TF/Volume2/ITI-1.html#3.1.1

Z2.4 | BB: Volume 3 - Content

Z2.4.1 | BB: Metadata

Documenten en beelden dienen wanneer ze opgeslagen worden een beschrijving mee te krijgen om ze vervolgens weer te kunnen vinden, gebruiken en hergebruiken in de toekomst. Hierom worden aan een beeld of document verschillende kenmerken (attributen) toegekend. Deze kenmerken noemt men metadata, dit is de data die een beeld of document zo beschrijft dat het gemakkelijk te vinden is, in het kort, metadata is data over data.

Bij het landelijk uitwisselen van documenten en beelden is het van belang dat de raadpleger weet wat voor vraag hij/zij kan stellen om zo relevante data terug te krijgen. Dit is de reden dat het binnen Twiin essentieel is een minimaal verplichte metadataset af te stemmen, waarmee de houder van de data deze kenbaar maakt voor de raadpleger.

Metadata

> Disclaimer
>
> Voor de vulling van metadata binnen BeeldBeschikbaarheid is gebruik gemaakt van de Nictiz Metadataset: XDS metadata - Nictiz[122]

122. https://nictiz.nl/standaarden/overzicht-van-standaarden/xds-metadata/

BB: Algemene metadata beschrijft metadata attributen die minimaal toegekend moeten worden aan een document. De ingevulde waarden zijn een voorbeeld en worden verder toegelicht waar nodig.

Mocht de metadataset niet toereikend zijn om beeld en verslag te kunnen onderscheiden van elkaar, dient dit onderbouwd aangegeven te worden, zodat Nictiz hierop een aanvulling kan doen.

1. Op de pagina BB: Metadata Radiologisch verslag zijn voor een radiologisch verslag specifieke waarden toegekend aan een aantal metadata attributen, deze specificatie definieert het radiologisch verslag.
2. Op de pagina BB: Metadata Beeldvormend onderzoek Radiologie (DICOM) is hetzelfde gedaan voor een beeldvormend onderzoek.

NB. Twiin beschrijft de transacties **tussen** GtK-applicaties om documenten en beelden te zoeken (query) en vervolgens op te halen. Twiin stelt geen verplichtingen over wat er achter een GtK-applicatie vereist is om een document of beeld aan te melden. Echter is metadata tenminste van belang voor het kunnen beantwoorden van een vraag tussen GtK-applicaties

Content

Naast de metadata is het ook van belang om af te spreken welke 'content' ofwel type verslag en beeldvormend onderzoek uitgewisseld zal worden, zodat de raadplegende partij dit formaat altijd kan verwerken.

Binnen Twiin wordt de volgende content voorgeschreven:

- Radiologisch verslag in PDF/A formaat
- Radiologisch verslag in CDA formaat
- Beelden in DICOM formaat

Z2.4.1.1 | BB: Metadata

Om beeld en verslag uit te kunnen wisselen wordt gebruik gemaakt van de 10.7.1 | Document/beeld gebaseerde Metadata (see page 290) zoals beschreven in de kern.

Voor Zorgtoepassing Beeldbeschikbaarheid worden voor beeld en verslag een aantal van deze velden verplichtingen ingevuld.

1.1.1. Invulling metadata voor Beeldbeschikbaarheid

- In het onderdeel Algemene metadata is het metadataveld 'referenceIdList' optioneel (O, Optional). Bij Beeldbeschikbaarheid is dit veld verplicht (R, Required) gesteld.
- Bij Zorgtoepassing Beeldbeschikbaarheid wordt momenteel enkel een Radiologisch verslag gedeeld als document. Voor de document gebaseerde metadata zijn hierom verplichte waarden vastgesteld. Zie hiervoor BB: Metadata Radiologisch verslag (see page 457)
- Bij Zorgtoepssing Beeldbeschikbaarheid worden momenteel enkel Radiologische beelden in het DICOM formaat uitgewisseld. Voor de beeld gebaseerde metadata zijn hierom verplichte waarden vastgesteld. Zie hiervoor BB: Metadata Beeldvormend onderzoek Radiologie (DICOM) (see page 458)

Metadata geïndexeerde bevraging

Disclaimer
Voor de vulling van metadata is gebruik gemaakt van de Nictiz Metadataset: XDS metadata - Nictiz[123]

De Nictiz metadata set is document gebaseerd en niet 1 op 1 van toepassing op b.v. resource gebaseerde uitwisseling.

APPLICATIE-LAAG

Het communicatiepatroon geïndexeerde bevraging (see page 172) maakt gebruik van metadata. De metadata wordt gebruikt binnen een use case om informatie te vinden bij verschillende zorgaanbieders.

Binnen Twiin passen we voor document gebaseerde bevragingen de volgende metadata-velden toe. De invulling van deze metadata-velden is vastgesteld binnen de use case.

Parameter	Opt	voorbeeld	beschrijving
Author	R	('Dr. Lewis Zimmerman')	Auteur van document
confidentialityCode	R	('N^^2.16.840.1.113883.5.25')	vertrouwelijkheidsniveau
creationTime	R	20100101230000	Tijd van aanmelden

123. https://nictiz.nl/standaarden/overzicht-van-standaarden/xds-metadata/

DocumentEntryStatus	R	('urn:oasis:names:tc:ebxml-regrep:StatusType:Approved')	De status van het document
patientId	R	'123456789^^^&2.16.840.1.113883.2.4.6.3&ISO'	BSN van cliënt
referenceIdList	O	642356235^^^&1.2.3.4.5.6&ISO^urn:ihe:iti:xds:2013:accession	Koppeling met ander document of beeld
repositoryUniqueId	R	1.1.4567332.1.1	Identificeert document Archief
serviceStartTime	R	20100101230000	Start van onderzoek
serviceStopTime	R	20100101230000	Stop van onderzoek
Document uniqueId	R	1.3.6.1.4.1.12559.11.13.2.1.231	Identificeert document
practiceSettingCode	R	('309964003^^2.16.840.1.113883.6.96')	Specialisme (in voorbeeld Radiology Department)
DocumentEntryType	R	urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1	Stable of On Demand
healthcareFacilityTypeCode	R	('V4^^ 2.16.840.1.113883.2.4.15.1060')	Type ZA (Zie nictiz metadata)
formatCode	R	('urn:ihe:rad:PDF^^1.3.6.1.4.1.19376.1.2.3')	Format van document
classCode	R	('9491000146107^^2.16.840.1.113883.6.96')	Imaging Documentation
typeCode	R	('722124004^^2.16.840.1.113883.6.96')	radiologisch verslag
mimeType	R	application/pdf	pdf

In het geval er DICOM beelden gedeeld worden is de volgende aanvullende metadata nodig.

Parameter	Opt	voorbeeld	beschrijving
StudyInstanceUID	R	Dicom tag (0020.000D)	Identificeert study

Parameter	Opt	voorbeeld	beschrijving
SeriesInstanceUID	R	Dicom tag (0020.000E)	Identificeert serie
eventCodeList	R	Dicom tag (0008,0060) (bijvoorbeeld MR) Anatomic Region	Geeft modaliteit aan Geeft lichaamsonderdeel aan

Toelichting algemene metadata

confidentialityCode

Code om het vertrouwelijkheidsniveau van het document te classificeren. De Nictiz metadata schrijft voor welke codes er gebruikt kunnen worden. Het is aan de bronhouder van de data om te bepalen welke documenten er als 'normal' geclassificeerd worden en of er documenten of beelden zijn die een hoger vertrouwelijkheidsniveau nodig hebben.

DocumentEntryStatus

Status van het document, kan de waarde 'Approved' of 'Deprecated' bevatten. Een deprecated document is een document dat vervangen is.

referenceIdList

De waarde in de referenceIdList wordt gebruikt om meerdere documenten aan elkaar te relateren. Meest praktische voorbeeld is het 'koppelen' van het verslag aan de beelden. IHE schrijft het volgende voor;

> The referenceIdList may be populated with the Accession Number and assigning authority.

Bron: *https://www.ihe.net/uploadedFiles/Documents/Radiology/IHE_RAD_TF_Vol2.pdf* table 4.68.4.1.2.3-1
Door bovenstaand te volgen zal er een unieke waarde zijn om toe te kennen aan de referenceIdList. Op deze waarde zal niet specifiek gezocht worden. Het is een manier voor de brondossierhouder om de data gestructureerd aan te bieden. De Nictiz metadataset schrijft hier de waarden voor die gebruikt moeten worden.

practiceSettingCode

Beschrijft het (zorg)specialisme. Een raadpleger kan een specifieke vraag (query) stellen om enkel data terug te krijgen over een specifiek specialisme, of alle binnengekomen data filteren op een specifiek specialisme.
De Nictiz metadataset schrijft hier de waarden voor die gebruikt moeten worden.

healthcareFacilityTypeCode

Beschrijft het zorgaanbiedertype. Een raadpleger kan een specifieke vraag (query) stellen om enkel data terug te krijgen over een specifiek zorgaanbiedertype, of alle binnengekomen data filteren op een specifiek zorgaanbiedertype.

De Nictiz metadataset schrijft hier de waarden voor die gebruikt moeten worden.

BB: Metadata Radiologisch verslag

> 1.1.1. Disclaimer
>
> Voor de vulling van metadata binnen BeeldBeschikbaarheid is gebruik gemaakt van de Nictiz Metadataset: XDS metadata – Nictiz[124]
>
> Mochten er toch verschillen zijn tussen wat binnen Twiin wordt voorgeschreven en wat Nictiz voorschrijft, dan prefereert Nictiz.

Onderstaande tabel geeft weer welke metadata gekoppeld is aan een Radiologisch verslag.

Parameter	opt	Verplichte waarde	Beschrijving
formatCode (optie a)	R	('urn:ihe:rad:PDF^^1.3.6.1.4.1.19376.1.2.3')	Format van document
formatCode (optie b)	R		Format van document
classCode	R	**('9491000146107^^** 2.16.840.1.113883.6.96 ')	Imaging Documentation
typeCode	R	**('722124004^^** 2.16.840.1.113883.6.96 ')	radiologisch verslag
mimeType (optie a)	R	application/pdf	pdf
mimeType (optie b)	R	text/xml	cda

2. Toelichting metadata radiologisch verslag

Alle gebruikte codes zijn gebaseerd op de Nictiz Metadataset.

2.1.1.1. formatCode

De formatCode geeft het format van het document aan. Een Radiologisch verslag mag of in CDA (text/xml) of PDF/A terug gegegeven worden door het Antwoordend GtK. Het Vragend GtK dient beide formaten te kunnen ontvangen.

---

124. https://nictiz.nl/standaarden/overzicht-van-standaarden/xds-metadata/

2.1.1.2. classCode

De classCode classificeert het document. Voor een radiologie verslag dient de class code **9491000146107** te zijn.

typeCode

De typeCode geeft het type document aan, het type document valt binnen de classificatie die eerder gedaan is. Voor een Radiologie verslag dient de typeCode **722124004** te zijn. *mimeType*

De mimeType geeft het mediatype van het document aan.

{}

BB: Metadata Beeldvormend onderzoek Radiologie (DICOM)

> Disclaimer
>
> Voor de vulling van metadata binnen BeeldBeschikbaarheid is gebruik gemaakt van de Nictiz Metadataset: XDS metadata - Nictiz[125]
>
> Mochten er toch verschillen zijn tussen wat binnen Twiin wordt voorgeschreven en wat Nictiz voorschrijft, dan prefereert Nictiz.

Onderstaande tabel geeft weer welke metadata gekoppeld is aan een beeldvormend onderzoek (DICOM).

Parameter	Opt.	Verplichte waarde	Beschrijving
formatCode	R	1.2.840.10008.5.1.4.1.1.88.59	Dicom SOP voor KOS
classCode	R	('**9491000146107**^^ 2.16.840.1.113883.6.96 ')	Imaging Documentation
typeCode	R	Dicom tag (0008,1032)	Voor RAD-68 (0008,1032)
mimeType	R	application/dicom	Type document
StudyInstanceUID	R	Dicom tag (0020.000D)	Identificeert study
SeriesInstanceUID	R	Dicom tag (0020.000E)	Identificeert serie

125. https://nictiz.nl/standaarden/overzicht-van-standaarden/xds-metadata/

eventCodeList	R	Dicom tag (0008,0060) (bijvoorbeeld MR) Anatomic Region	Geeft modaliteit aan Geeft lichaamsonderdeel aan

Toelichting metadata Beeldvormend onderzoek Radiologie (DICOM)

Alle gebruikte codes zijn gebaseerd op de Nictiz Metadataset.

formatCode

De format code geeft het format van het document aan. In het geval van beeldvormende onderzoeken schrijft Nictiz voor de SOP class UID van het KOS object toe te voegen. De SOP class UID van het KOS object is **1.2.840.10008.5.1.4.1.1.88.59**. De SOP class UID is terug te vinden in de DICOM metadata van het KOS object in DICOM tag **(0008,0016) SOP Class UID.**

classCode

De class code classificeert het document. Voor een beeldvormend onderzoek dient de class code **9491000146107** te zijn.

typeCode

De typecode geeft het type document aan, het type document valt binnen de classificatie die eerder gedaan is. In het geval van een beeldvormend onderzoek dient de typeCode ontleend te worden uit de metadata van het KOS object in DICOM tag (**0008,1032) Procedure Code Sequence.**

mimeType

De mimeType geeft het mediatype van het document aan. Voor een beeldvormend onderzoek zal dit **application/dicom** zijn.

StudyInstanceUID

Het StudyInstanceUID is het unieke nummer dat bij de studie van een beeldvormend onderzoek hoort. Het Study Instance UID is tijdens een RAD-75 (Cross Gateway Retrieve Imaging Document Set) request nodig om beelden te kunnen ophalen. Het Study Instance UID is terug te vinden in de DICOM metadata van het KOS object in DICOM tag **(0020.000D) StudyInstanceUID.**

SeriesInstanceUID

Het SeriesInstanceUID is het unieke nummer dat bij de serie (onderdeel van de studie) van een beeldvormend onderzoek hoort. Het Series Instance UID is tijdens een RAD-75 (Cross Gateway Retrieve Imaging Document Set) request nodig om beelden te kunnen ophalen. Het Series Instance UID is terug te vinden in de DICOM metadata van het KOS object in DICOM tag **(0020.000E) SeriesInstanceUID**.

eventCodeList

De eventcodelist beschrijft twee waarden,

- De modaliteit waarmee de beelden verkregen zijn. Nictiz schrijft hier vaste waarden voor. De modaliteit is terug te vinden in de DICOM metadata van het KOS object in DICOM tag **(0008,0060) Modality.**

In het geval een studie bestaat uit DICOM SOPS die verkregen zijn met meerdere modaliteiten zal de eventCodeList al deze modaliteiten hier weergeven.

bron https://www.ihe.net/uploadedFiles/Documents/Radiology/IHE_RAD_TF_Vol2.pdf

- Het deel van het lichaam (Anatomic Region) waarover het beeld gaat.

  Anatomic Region: the eventCodeList shall contain code(s) from the DICOM Content Mapping Resource (DICOM PS3.16) Context Group CID 4. Each anatomic region code's displayName shall be populted with the corresponding Code Meaning text from Context Group CID 4.

NB: In het Technisch Ontwerp Beeldbeschikbaarheid is inmiddels een kleinere selectie uit bovenstaande lijst gehaald en gepubliceerd. Twiin verwijst nog niet naar het Technisch Ontwerp omdat Nictiz zelf aangeeft dat het geheel nog in ontwerp is en niet gereed is voor implementatie.

onderstaande tabel is mogelijk hierom nog onderhevig aan wijziging.

Het goed kunnen terugsturen van de juiste metadata, is vooral bij lichaamsdeel sterk onderhevig aan het juist opslaan van deze codes bij de bron tijdens de acquisitie van het DICOM object. Het mappen naar onderstaande codes kan een uitdaging worden.

Twiin beschrijft communicatie tussen GtK's, echter het is zeer belangrijk dat zorginstellingen zich bewust zijn van een correcte vastlegging van gegevens en adviseert (naast alle andere metadata) onderstaande tabel ter harte te nemen om zo snel mogelijk DICOM metadata correct te vullen.

SNOMED CT Code	Code Meaning NL
63337009[126]	Structuur van onderste gedeelte van romp

126. http://snomed.info/id/63337009

SNOMED CT Code	Code Meaning NL
38266002[127]	Gehele lichaam in totaliteit
53120007[128]	Structuur van bovenste extremiteit
61685007[129]	Structuur van onderste extremiteit
67734004[130]	Structuur van bovenste deel van romp
774007[131]	Structuur van hoofd-halsregio
113257007[132]	Structuur van tractus circulatorius
80891009[133]	Structuur van hart
76752008[134]	Structuur van mamma
737561001[135]	Structuur van wervelkolom en/of ruggenmerg

- Bron: https://www.ihe.net/uploadedFiles/Documents/Radiology/IHE_RAD_TF_Vol2.pdf 4.68.4.1.2.3-1[136]
  Bron; http://dicom.nema.org/medical/dicom/current/output/html/part16.html#sect_CID_4[137]
  In de eventCodeList moet een code uit de DICOM Content Mapping Resource Context Group CID 4 aanwezig zijn.
  Bron: https://dicom.innolitics.com/ciods/nm-image/general-series/00180015
  Bron: https://dicom.innolitics.com/ciods/mr-image/mr-image/00082218

127. http://snomed.info/id/38266002
128. http://snomed.info/id/53120007
129. http://snomed.info/id/61685007
130. http://snomed.info/id/67734004
131. http://snomed.info/id/774007
132. http://snomed.info/id/113257007
133. http://snomed.info/id/80891009
134. http://snomed.info/id/76752008
135. http://snomed.info/id/737561001
136. https://www.ihe.net/uploadedFiles/Documents/Radiology/IHE_RAD_TF_Vol2.pdf%204.68.4.1.2.3-1
137. http://dicom.nema.org/medical/dicom/current/output/html/part16.html%22%20/l%20%22sect_CID_4

NB. Zodra de richtlijnen voor eventCodeList juist gevolgd wordt zal er een goede differentiatie gedaan kunnen worden tussen verschillende beeldvormende onderzoeken. Een query zou bijvoorbeeld kunnen zijn 'geef mij alle MR onderzoeken van patiënt X' of 'geef mij alle onderzoeken van patiënt X van de lumbaal regio'. Dit begint bij het juist vullen van DICOM tag (0008,2218) Anatomic Region Sequence.

{}

Z2.4.2 | BB: Autorisatierichtlijn en mappingtabel beeldbeschikbaarheid radiologie

Op dit moment is er nog geen eenduidige nationale autorisatierichtlijn beschikbaar die wij hier kunnen tonen.

Mocht er een initiatief zijn, anders dan Twiin, dat zich hiermee bezighoudt, dan horen wij dat graag.

Verdere uitwerking en implementatie volgen zodra de officiële richtlijnen beschikbaar zijn.

Z2.5 | BB: PvE

1. Validatie-eisen

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
TTA-BB-01	TTA BB	GtK Vrager	Om de tijdlijngegevens op te kunnen vragen dient de GtK Vrager de IHE: ITI-38 Cross Gateway Query inclusief SAML token uit te kunnen sturen volgens specificaties zoals beschreven in de Zorgtoepassing Beeldbeschikbaarheid.	Z2.3.2 | BB: IHE ITI-38 | Cross Gateway Query (see page 436) Z2.3.5 | BB: IHE ITI-40 | Provide X-User Assertion (see page 443)
TTA-BB-02	TTA BB	GtK Antwoorder	GtK Antwoorder zal eerst het meegestuurde token valideren dat door de GtK vrager is meegestuurd en vervolgens op de IHE: ITI-38 Cross Gateway Query antwoord geven in het juiste formaat en met de door Twiin beschreven specificaties met betrekking tot metadata.	Z2.3.2 | BB: IHE ITI-38 | Cross Gateway Query (see page 436) Z2.3.5 | BB: IHE ITI-40 | Provide X-User Assertion (see page 443) Z2.4.1.1 | BB: Metadata (see page 453)

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
TTA-BB-03	TTA BB	GtK Vrager	Om een of meerdere documenten op te kunnen vragen dient de GtK Vrager de IHE: ITI-39 Cross Gateway Retrieve inclusief SAML token uit te kunnen sturen volgens specificaties zoals beschreven in de Zorgtoepassing Beeldbeschikbaarheid.	Z2.3.3 | BB: IHE ITI-39 | Cross Gateway Retrieve (see page 438) Z2.3.5 | BB: IHE ITI-40 | Provide X-User Assertion (see page 443)
TTA-BB-04	TTA BB	GtK Antwoorder	GtK Antwoorder zal eerst het meegestuurde token valideren dat door de GtK vrager is meegestuurd en vervolgens op de IHE: ITI-39 Cross Gateway Retrieve antwoord geven in het juiste formaat en met de door Twiin beschreven specificaties met betrekking tot metadata.	Z2.3.3 | BB: IHE ITI-39 | Cross Gateway Retrieve (see page 438) Z2.3.5 | BB: IHE ITI-40 | Provide X-User Assertion (see page 443) BB: Metadata Radiologisch verslag (see page 457) BB: Metadata Beeldvormend onderzoek Radiologie (DICOM) (see page 458)
TTA-BB-05	TTA BB	GtK Vrager	Om een of meerdere beelden op te kunnen vragen dient de GtK Vrager de IHE: RAD-75 Cross Gateway Retrieve Imaging Document set inclusief SAML token uit te kunnen sturen volgens specificaties zoals beschreven in de Zorgtoepassing Beeldbeschikbaarheid.	Z2.3.1 | BB: IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set (see page 435) Z2.3.5 | BB: IHE ITI-40 | Provide X-User Assertion (see page 443)
TTA-BB-06	TTA BB	GtK Antwoorder	GtK Antwoorder zal eerst het meegestuurde token valideren dat door de GtK vrager is meegestuurd en vervolgens op de IHE: RAD-75 Cross Gateway Retrieve antwoord geven in het juiste formaat en met de door Twiin beschreven specificaties met betrekking tot metadata.	Z2.3.1 | BB: IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set (see page 435) Z2.3.5 | BB: IHE ITI-40 | Provide X-User Assertion (see page 443)
TTA-BB-07	TTA BB	GtK Vrager	De GtK Vrager zal bij ontvangst van een opgevraagd document de vastgestelde formats kunnen verwerken.	(TA141) Z2.4.1 | BB: Metadata#Content (see page 453)
TTA-BB-08	TTA BB	GtK Antwoorder	De GtK Antwoorder zal bij het opvragen van een document, het document terugsturen conform 1 van de vastgelegde formats.	(TA141) Z2.4.1 | BB: Metadata#Content (see page 453)

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie

2. Aanvullende ketentest eisen

De eisen in dit hoofdstuk zijn niet nodig zijn voor de Twiin validatie van de zorgtoepassing. Deze eisen zijn wel nodig om te voldoen aan de ketentest, de informatiestandaard en eventuele andere functionele eisen.

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BBV1-1	-			
BBV1-2	-	GtK antwoorder	Alle onderzoeken dienen binnen 1 tijdlijn gerangschikt te zijn: De GtK Antwoorder zal de gegevens (metadata) om de tijdlijn op te kunnen bouwen correct en volledig terug geven aan de GtK Vrager	• Alle gegevens zijn langs één tijdlijn gerangschikt zodat de relaties tussen verschillende typen gegevens bestudeerd kunnen worden.
BBV1-3	-	GtK vrager	Alle onderzoeken dienen binnen 1 tijdlijn gerangschikt te zijn: Er dient een logische tijdlijn gepresenteerd te worden	• Alle gegevens zijn langs één tijdlijn gerangschikt zodat de relaties tussen verschillende typen gegevens bestudeerd kunnen worden.
BBV1-4	-	GtK vrager	De onderzoeken dienen gefilterd te kunnen worden binnen de tijdlijn.	• Resultaten op de tijdlijn dienen gefilterd te kunnen worden op onder andere lichaamsregio en modaliteit. • Mogelijkheden voor filtering en sortering binnen de eigen werkomgeving van de tijdlijn van een patiënt werken voor interne en externe onderzoeken op de tijdlijn.

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BBV1-5	–	GtK vrager	Eenvoudig openen tijdlijn binnen de werkomgeving.	• Binnen de digitale werkomgeving van de zorgverlener geeft de tijdlijn een geïntegreerd overzicht van één patiënt inclusief alle in Nederland uitgevoerde onderzoeken met bijbehorende beelden en verslagen. • Er zijn daarvoor geen extra handelingen nodig door degene die in het zorgproces de tijdlijn nodig heeft en daartoe bevoegd is. • Viewer via SSO beschikbaar vanuit eigen werkomgeving
BBV1-6	–	GtK vrager	Bevoegdheid vloeit voort uit een behandelrelatie.	• Bevoegdheid vloeit voort uit een bestaande behandelrelatie met de patiënt of een behandelrelatie, die op dat moment wordt aangegaan met een (spoed)verwijzing, verzoek om een herbeoordeling of second opinion, bespreking in een MDO, e.d. • Aantoonbaar maken dat er een behandelrelatie is. Achteraf door goed te loggen, vooraf door met de juiste rol gegevens op te vragen, zodat de beschikbaar stellende instelling de autorisatie kan controleren.
BBV1-7	–	GtK vrager GtK antwoorder	Op basis van de rol kunnen meer of minder gegevens worden geraadpleegd.	• Op basis van de rol van elke zorgverlener en betrokkenheid bij de patiënt kunnen meer of minder (medisch inhoudelijke) gegevens op de tijdlijn worden geraadpleegd.
BBV1-8	–	GtK vrager GtK antwoorder	Performance tijdlijn: De tijdlijn is steeds compleet en actueel en met een snelheid beschikbaar, die past in het zorgproces en dit niet verstoort of vertraagt.	• Het samenstellen van de tijdlijn verstoort het ‘proces’ niet. • **Gaat hier om metadata,** niet om de beelden in diagnostische kwaliteit.
BBV1-9	–	GtK vrager	Radiologisch onderzoek is eenmalig zichtbaar binnen de tijdlijn: Elk uitgevoerd radiologisch onderzoek van een patiënt wordt eenmalig weergegeven in één landelijk dekkende tijdlijn.	• Onderzoeksdata die is gekopieerd/ geïmporteerd dient er niet toe te leiden dat in de tijdlijn dubbelingen worden weergegeven.

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BBV1-10	-	GtK vrager GtK antwoorder	Performance spoedverwijzing	Bij een spoedverwijzing zal rekening moeten worden gehouden met de tijd die het kost om beelden te maken in de producerende zorginstelling en deze te laten verschijnen in de tijdlijn van de gebruikende zorginstelling. Voor de maximale wachttijd bij spoed wordt aansluiting gezocht bij de het Kwaliteitskader Spoedzorgketen. Uit deze richtlijn kan voor de 2e lijns/ medisch specialistische zorg een maximale wachttijd van 90-95% binnen 15 minuten worden gedestilleerd en 100% binnen 30 minuten.
BBV1-11	-	GtK vrager GtK antwoorder	Toestemming patiënt: De patiënt dient expliciete of impliciete toestemming gegeven te hebben om de gegevens te tonen binnen de tijdlijn.	Aanvulling in kwaliteitsstandaard: Mocht de zorgverlener de tijdlijn willen raadplegen terwijl deze toestemming (nog) ontbreekt en/of impliciete toestemming (bijvoorbeeld op basis van een verwijzing) onvoldoende is voor een complete tijdlijn, dan moet de patiënt de gelegenheid krijgen alsnog expliciete toestemming te geven.
BBV1-12	-	GtK vrager GtK antwoorder	Breaking-the-glass toestemming patiënt	Met een breaking-the-glass procedure moet de tijdlijn ook in noodsituaties en/of in verband met de patiëntveiligheid beschikbaar zijn te maken wanneer toestemming van de patiënt (nog) ontbreekt.
BBV1-13	-			
BBV1-14	-	GtK antwoorder	Eisen Radiologisch verslag	Het verslag is een weerslag van alle informatie-elementen van het radiologisch zorgproces tot dat moment. Dit kan in volledig vrije vorm zijn of (deels) gestandaardiseerd en/of gestructureerd. Voor de tijdlijn radiologische onderzoeken is het verslag één geheel; het (tekst)document met de complete beoordeling van beelden door radioloog.

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BBV1–15	–	GtK vrager GtK antwoorder	Addendum eigen onderzoek	Addendum moet in de tijdlijn bij het oorspronkelijke verslag terug te zien zijn. In een addendum op het verslag wordt door de radioloog een aanvullende bevinding beschreven op het eigen onderzoek, die is gedaan nadat het verslag is geautoriseerd. Hierbij kan worden gedacht aan een extra bevinding als antwoord op een aanvullende vraag, na een aanvullende scan of analyse, na overleg in het MDO of de toevoeging dat op een later onderzoek een bevinding is gedaan die in retrospectie ook op dit eerdere onderzoek te zien was. Een addendum wordt gemaakt op het verslag van de eigen zorginstelling. Een verslag kan meerdere addenda hebben.
BBV1–16	–	GtK vrager GtK antwoorder	Rectificatie op eigen onderzoek	Wanneer na afronding van het onderzoek blijkt dat informatie in het verslag toch niet correct is, dan wordt door de radioloog een rectificatie gemaakt. Dit is een nieuw verslag bij een onderzoek van de eigen zorginstelling. De rectificatie vervangt het oorspronkelijke verslag, dat ook beschikbaar blijft.
BBV1–17	–	GtK vrager GtK antwoorder	Herbeoordeling onderzoek elders	Wanneer een radioloog wordt gevraagd om een radiologisch onderzoek van elders (beelden en verslag) nogmaals te beoordelen, dan is er sprake van een herbeoordeling. Dit gebeurt bijvoorbeeld bij een doorverwijzing voor specifieke expertise en behandeling en ter voorbereiding van een MDO. Een herbeoordeling wordt beschouwd als een nieuw radiologisch onderzoek op de tijdlijn. In het herbeoordelingsverslag wordt gerefereerd aan één of meer gebruikte voorgaande onderzoeken.

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BBV1-18	-	GtK vrager GtK antwoorder	Eisen onderzoeksgegevens intern en extern	Voor alle onderzoeken, intern én extern, worden de volgende onderzoeksgegevens getoond: • Datum/tijd waarop het radiologisch onderzoek bij de patiënt is uitgevoerd cq waarop de beelden zijn gemaakt. • Omschrijving van de verrichting cq van het uitgevoerde onderzoek (bijv. CT thorax, MRI knie, echografie mamma, röntgenfoto voet). Hier kan ook de verrichting 'herbeoordeling' staan. Idealiter is er een landelijke tabel van verrichtingen. Zolang dit niet landelijk wordt gebruikt én voor de onderzoeken die van voor de ingebruikname zijn, worden onderzoeken omschreven aan de hand van modaliteit en anatomisch gebied. • Zorginstelling of organisatie waar het radiologisch onderzoek is uitgevoerd cq de producerende zorginstelling. • Het producerend specialisme, in dit geval "radiologie", is het verantwoordelijk medisch specialisme voor de uitvoering van het onderzoek. • Status van het onderzoek (gepland, opgeroepen, gereed, afgerond, gewijzigd), die volgt uit de verschillende processtappen van het radiologisch proces.
BBV1-19	-			
BBV1-21	-	GtK vrager GtK antwoorder	Eisen verslagen: het verslag als 1 geheel	Voor de tijdlijn en het gebruik in het zorgproces wordt het verslag als geheel beschouwd en niet een verzameling van losse informatie-elementen. De volledige tekst van een verslag (oud of nieuw, gestructureerd of niet) wordt weergegeven, bij voorkeur in de oorspronkelijke layout.

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BBV1-22	–	GtK vrager GtK antwoorder	Eisen verslagen: functionele gegevens	Het verslag heeft functionele gegevens die een zorgverlener wil weten over het verslag: • Datum/tijd waarop het verslag is geautoriseerd cq beschikbaar is gekomen. • Zorginstelling of organisatie waar het verslag van het radiologisch onderzoek is gemaakt. • Naam van de radioloog die het verslag heeft geautoriseerd en – indien anders – ook de naam van de radioloog die het verslag heeft gedicteerd. • Label van het verslag, waaraan is te zien of het verslag oorspronkelijk is of na autorisatie/ beschikbaar komen is aangepast (addendum of rectificatie).
BBV1-23	–	GtK vrager GtK antwoorder	Eisen verslagen: beschikbaar als document	Het verslag dient ook als document beschikbaar gesteld te worden.

Z3 | COR: Implementatiewijzer Correspondentie

Inleiding

Dit onderdeel beschrijft de technische implementatie voor de beschikbaarheid van bij andere zorgtoepassingen behorende correspondentie.

Deelname aan Twiin, de voorwaarden en het proces van validatie staat beschreven in het Twiin Afsprakenstelsel.

De correspondentie behorende bij de zorgtoepassingen van Twiin is veelal noodzakelijk voor de juiste interpretatie van de inhoud van de zorgtoepassing zelf. In lijn met de informatiestandaarden wordt bij de zorgtoepassingen alleen de uitwisseling van de bij de zorgtoepassing behorende zibs/resources beschreven. In deze implementatiewijzer bieden we ook ondersteuning voor de uitwisseling van bijbehorende correspondentie.

- Volume 1 geeft een functioneel overzicht voor de databeschikbaarheid van de correspondentie en de daarbij behorende eisen (see page 470)
- Volume 2a bevat de technische afspraken voor de uitwisseling van de correspondentie. Dit noemen we ook wel de Twiin Technische Afspraak (TTA) (see page 473)

- Volume 2b bevat de technische uitwerkingen van de transacties die gebruikt worden in de TTA (see page 483)
- Volume 3 een verwijzing naar de meta-informatie (see page 512)

Z3.1 | COR: Volume 0 - Functioneel overzicht

Inleiding

In dit volume is te vinden:

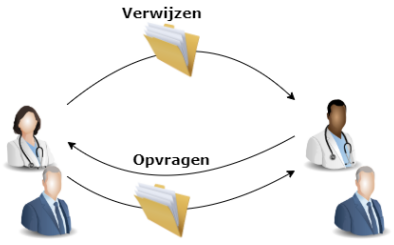
- een beschrijving van de functionele use-casus van de correspondentie
- een overzicht van de uitwisselpatronen die worden gebruikt voor de correspondentie
- een beschrijving van de invulling van het vertrouwensmodel met de daarbij behorende voorwaarden voor de correspondentie
- een beschrijving of verwijzing naar de eisen die gesteld zijn door organisaties, programma's en/of informatiestandaarden.

In volume 2 volgende de uitwerking van de transacties van de uitwisselpatronen voor de correspondentie (in het engels)

Functionele use-casus

Om de uitwisseling van gegevens in het kader van de zorgtoepassingen binnen Twiin beter te kunnen duiden is bijbehorende correspondentie belangrijk. Deze uitwisseling kan in 2 use cases uitgewerkt worden:

1. uitwisselen correspondentie behorende bij verwijzing of overdracht;
2. opvragen correspondentie behorende bij een eerdere behandeling



De meest gebruikte processen waar de uitwisseling van correspondentie in rol in speelt zijn:

- Verwijzing / overdracht
- Consult / advies

Vanuit deze processen zijn er 2 manieren om de correspondentie beschikbaar te stellen:

1. Uitwisseling correspondentie bij verwijzing of overdracht (versturen, functionele push)

2. Opvragen correspondentie bij eerdere behandelaar (opvragen, functionele pull)

Onderliggende pagina's

- Z3.1.1 | Uitwisseling correspondentie bij verwijzing of overdracht (see page 471)

Z3.1.1 | Uitwisseling correspondentie bij verwijzing of overdracht

Deze pagina beschrijft de uitwisseling in het geval van het versturen van de Correspondentie behorende bij een verwijzing of overdracht. De Z3.2.1 | COR TTA Exchanging correspondence – FHIR Notified Pull (see page 473) beschrijft de technische invulling van deze uitwisseling binnen Twiin.

> Gebaseerd op het functionele ontwerp Nictiz: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.0_BgZ_MSZ_Informatiestandaard#Use_case_1:_Uitwisseling_BgZ_bij_verwijzing_of_overdracht

Doel en relevantie

Bij het verzenden van bijbehorende correspondentie naar een andere instelling kan van verschillende varianten sprake zijn.

- Een arts verwijst naar een andere arts, of er is een overdracht van een patiënt naar die andere instelling en de eigen behandeling is daarmee afgelopen.
- Een tweede arts doet een deel van de behandeling zonder dat de eerdere arts de (eigen) behandeling beëindigt.

In al deze gevallen spreken we in deze informatiestandaard van verwijzing en/of overdracht. We maken geen strikt onderscheid tussen verwijzen en overdracht, en ook niet op de vraag of de verwijzende arts al dan niet bij de behandeling betrokken blijft. Dat kan per zorgproces nader bepaald worden. De essentie hier is dat de tweede arts een eigen, zelfstandige behandelovereenkomst met de patiënt aangaat.

Bedrijfsrollen

Rol	Toelichting
Verwijzer	De arts die een patiënt verwijst of overdraagt naar een andere arts bij een andere instelling en in het kader daarvan de correspondentie deelt.
Nieuwe behandelaar	De arts van de andere instelling die de correspondentie ontvangt en een behandelovereenkomst met de patiënt aangaat (of voortzet).

Proces en context

Patient journey

Een patiënt is onder behandeling bij een oncoloog in een regionaal ziekenhuis. De patiënt heeft een complexe aandoening, waarvoor de behandeling beter voortgezet kan worden in een nabij academisch ziekenhuis. De behandelend arts verwijst de patiënt door naar het academisch ziekenhuis, en verstrekt daarbij (alle of een deel van) de volgende documenten:

1. een verwijsbrief;
2. de benodigde dataset van de patiënt;
3. eventuele verdere bijlagen of verwijzingen.

De patiënt komt op een consult in het academisch ziekenhuis. De behandelend arts daar opent het eigen EPD en ziet de dataset en de overige informatie uit het regionale ziekenhuis in. Het academisch ziekenhuis zet de behandeling voort.

Precondities

- De patiënt is onder behandeling in een instelling.
- De behandelend arts besluit tot verwijzing of overdracht.
- De gegevens van de patiënt zijn vastgelegd in het EPD.
- Behandelend en ontvangend ziekenhuis kunnen digitaal de dataset en bijbehorende correspondentie uitwisselen.

Trigger event

Het besluit van een arts om een patiënt te verwijzen of over te dragen aan een andere instelling, waar de patiënt onder behandeling zal komen.

Proces

1. De behandelend arts kiest een instelling en specialisme (en mogelijk een zorgverlener binnen die instelling) waarnaar verwezen wordt.
2. De behandelend arts rondt de verwijzing af.
3. De dataset en bijbehorende correspondentie wordt verzonden.
4. Een arts in de ontvangende instelling ziet de dataset en bijbehorende correspondentie in, en neemt (indien gewenst) alle of een deel van de gegevens over.

Z3.3 | COR: Volume 1 - Twiin Technical Agreement

Twiin Technical Agreement

Exchanging FHIR Data using a generic Notified Pull mechanism

for trial implementation

Based on TA 0.99 - Implementation guide for Twiin participants

Table of contents

Z3.2.1 | COR TTA Exchanging correspondence - FHIR Notified Pull

For this use-case the exchange pattern Notified Pull with FHIR is used. Below you will find the description of this exchange pattern.

> Original page can be found at 10.3.1 | TTA FHIR - Notified pull (see page 185)

This Twiin Technical Agreement (TTA) describes and specifies the technical responsibilities to which parties agree when connecting to exchange transactions to facilitate the Notified Pull. This TTA is based on the TA Notified Pull[138], with the normative specifications remaining unchanged. The informative specifications, however, have been described using a specific implementation.

The possibility to exchange a client's medical record is for example required in case of a patient referral or transfer. When different healthcare organizations are involved in a client's treatment plan, attention should be paid to the required legal permission and the possible 'burden' for the receiving system when a medical record is transferred.

Relation to other documents

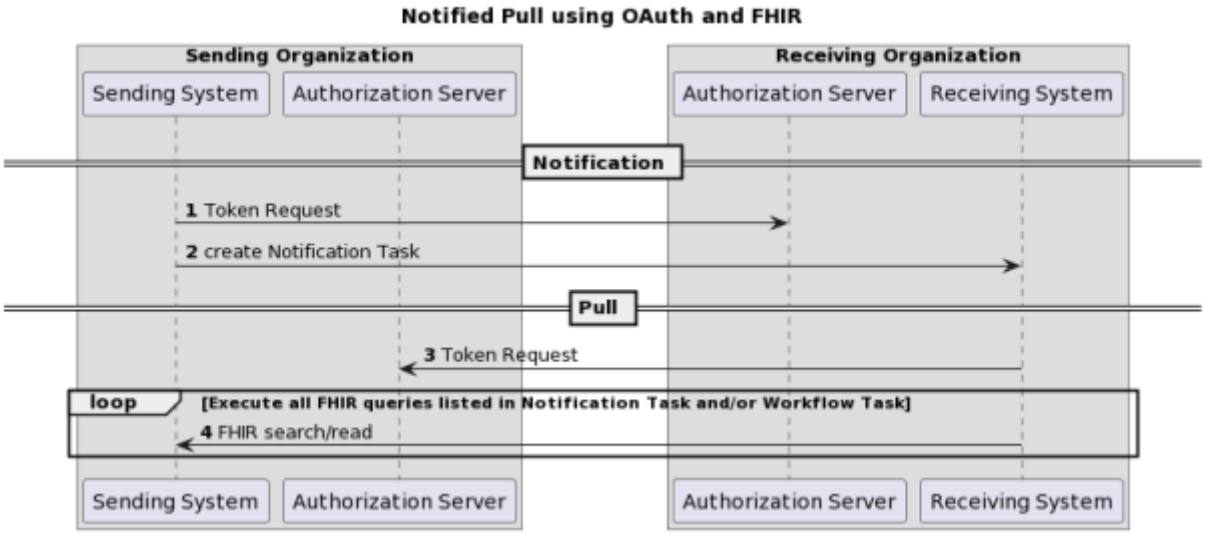
This document is written with the following documents as references:

- Nictiz - Informatiestandaard BgZ MSZ
- TA Notified Pull v1.x.x (latest version)[139]

138. https://www.twiin.nl/tanp
139. https://www.twiin.nl/tanp

Format

The format of this section follows the main interactions as presented below in the simplified sequence diagram of the Notified Pull sequence.



Interaction numbers 1 and 3 are described in the 10.4.2 | TTA FHIR – Authorization (see page 206). Interaction number 2 is described in10.3.1.1 Notified Pull – Data interactions (see page 190). A part of interaction number 4 is also described in 10.3.1.1 Notified Pull – Data interactions (see page 190). For specifics of the context of the Notified Pull, see Nictiz information standards.

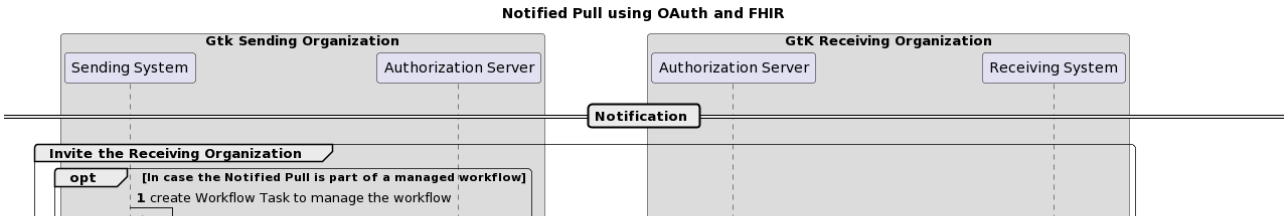
The sequence diagram below provides a complete overview that covers both the resource interactions and the authorization interactions of the complete Notified Pull interaction sequence.

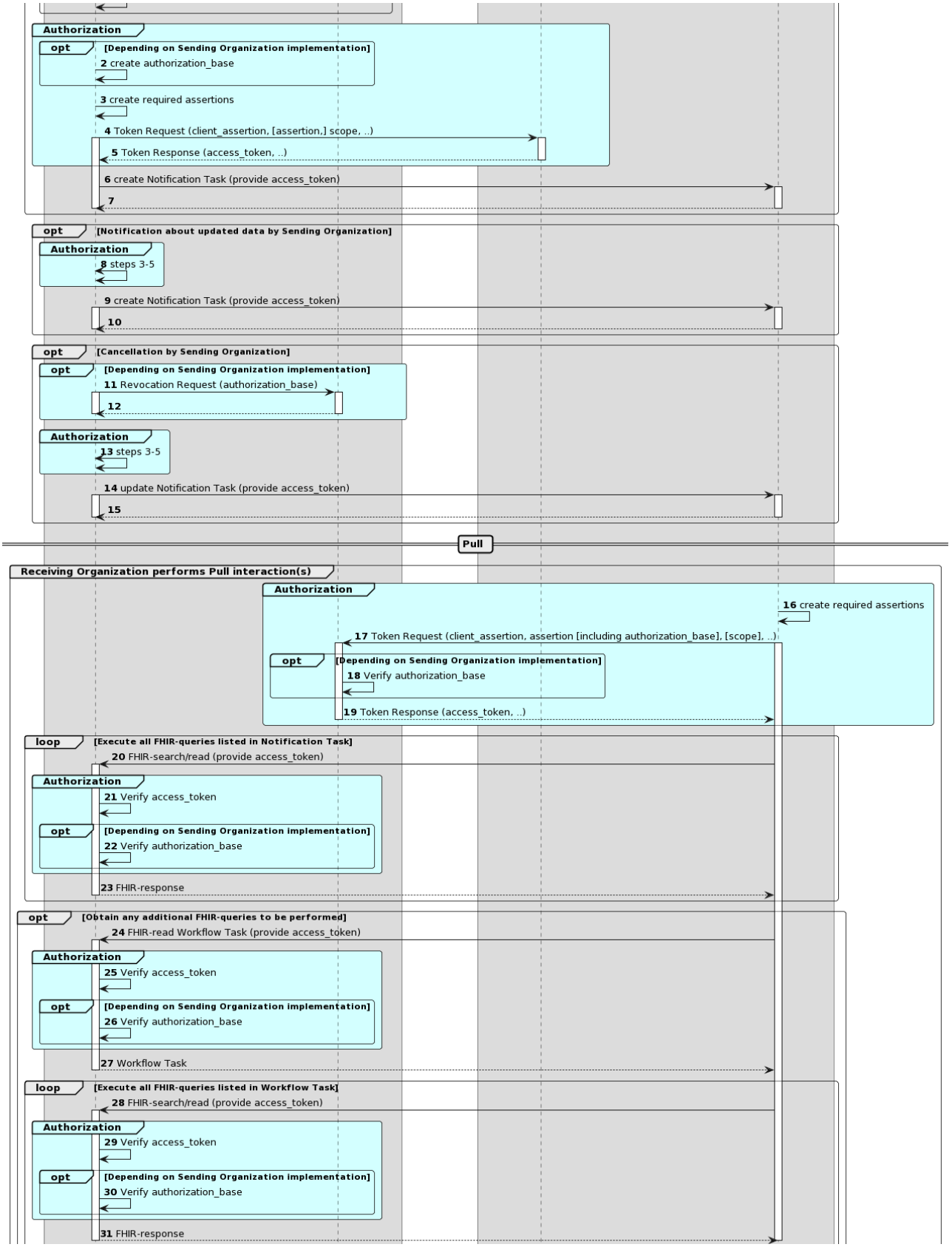
The Twiin specific solutions for identification and addressing can be found in 10.4.2 | TTA FHIR – Authorization (see page 206) and 10.4.5 | TTA – Addressing (see page 210) respectively.

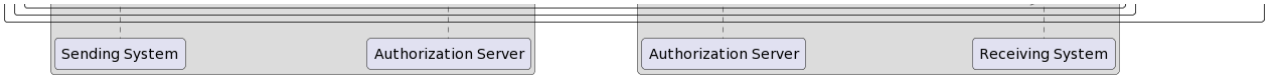
Sequence diagram

The sequence diagram below visualizes the full flow for the Notified Pull interaction sequence, including both interactions in the data layer using HL7 FHIR (described in 10.3.1.1 Notified Pull – Data interactions (see page 190)) and in authorization layer using OAuth 2.0 (marked cyan, described in 10.4.7 | Network level security (see page 211)).

Each section consists of several steps. The steps correspond to the numbers in the sequence diagram.




Authorization
opt
[Depending on Sending Organization implementation]
2 create authorization_base
3 create required assertions
4 Token Request (client_assertion, [assertion,] scope, ..)
5 Token Response (access_token, ..)
6 create Notification Task (provide access_token)
7
opt
[Notification about updated data by Sending Organization]
Authorization
8 steps 3-5
9 create Notification Task (provide access_token)
10
opt
[Cancellation by Sending Organization]
opt
[Depending on Sending Organization implementation]
11 Revocation Request (authorization_base)
12
Authorization
13 steps 3-5
14 update Notification Task (provide access_token)
15
Pull
Receiving Organization performs Pull interaction(s)
Authorization
16 create required assertions
17 Token Request (client_assertion, assertion [including authorization_base], [scope], ..)
opt
[Depending on Sending Organization implementation]
18 Verify authorization_base
19 Token Response (access_token, ..)
loop
[Execute all FHIR-queries listed in Notification Task]
20 FHIR-search/read (provide access_token)
Authorization
21 Verify access_token
opt
[Depending on Sending Organization implementation]
22 Verify authorization_base
23 FHIR-response
opt
[Obtain any additional FHIR-queries to be performed]
24 FHIR-read Workflow Task (provide access_token)
Authorization
25 Verify access_token
opt
[Depending on Sending Organization implementation]
26 Verify authorization_base
27 Workflow Task
loop
[Execute all FHIR-queries listed in Workflow Task]
28 FHIR-search/read (provide access_token)
Authorization
29 Verify access_token
opt
[Depending on Sending Organization implementation]
30 Verify authorization_base
31 FHIR-response



Section	Step	Description
Invite the Receiving Organization	1	If the Notified Pull is part of a managed workflow involving both the Sending Organization and the Receiving Organization, and this workflow specifies the creation of a FHIR Task (‘workflow task’) at the Sending System, then the flow starts with the creation of this task on the Sending System.
	2	The Sending System creates an authorization base, which is used later to communicate a presumed consent for the exchange of patient information. The Receiving System must treat the authorization base as an opaque element. The Receiving System should not depend on any information contained in the authorization base.
	3	The Sending System creates one or two assertions, which can be used to request an access token in the next step.
	4–5	The Sending System requests an access token which can be used in step 6. The Receiving System processes the token request and returns a token response containing, among other elements, an access token. The Sending System must treat the access token as opaque. The Sending System should not depend on any information contained in the access token.
	6–7	By invoking a create interaction regarding a FHIR Task ('notification task') on the Receiving System, the Sending System invites the Receiving System to perform one or more Pull interactions. The Receiving System processes the invitation and sends a technical response to complete the create interaction.
Notification about updated data by Sending Organization	8	The Sending System repeats steps 3–5.
	9–10	The Sending System updates the notification task on the Receiving System using the create interaction. The Receiving System returns a technical response message.

Cancellation by Sending Organization	11–12	The 'cancellation by Sending Organization' option provides a means for the Sending System to cancel/revoke an erroneously created notification. Depending on the implementation at the Sending Organization, the Sending System might have to start the cancellation by revoking the authorization base created in step 2, by sending a revocation request to the Sending Organization's authorization server. The authorization server processes the request and returns a response.
	13	The Sending System repeats steps 3–5.
	14–15	The Sending Organization informs the Receiving Organization by updating the Notification Task on the Receiving System (Task.status is set to "cancelled"). The Receiving System returns a technical response message.
Receiving Organization performs Pull interaction(s)	16	The Receiving System creates one or two assertions, which can be used to request an access token in the next step.
	17–19	The Receiving System requests an access token which can be used to perform the intended Pull interactions. The Sending Organization's authorization server processes the token request and returns a token response containing (among others) an access token. Depending on the Sending System implementation, the Sending System can choose to verify the consent before issuing an access token (preferred option). The Receiving System must treat the access token as an opaque element. The Receiving System should not depend on any information contained in the access token.
	20–23	The Receiving System initiates the intended interactions and processes the responses. The Sending System verifies the access token and can additionally decide to verify the authorization base at this point in the flow.
	24–27	In case the notification task indicates that a workflow task is available that contains (additional) Pull interactions to be performed, the Receiving System obtains this workflow task from the Sending System.
	28–31	The Receiving System initiates the (additional) Pull interactions listed in the workflow task, and processes the responses.

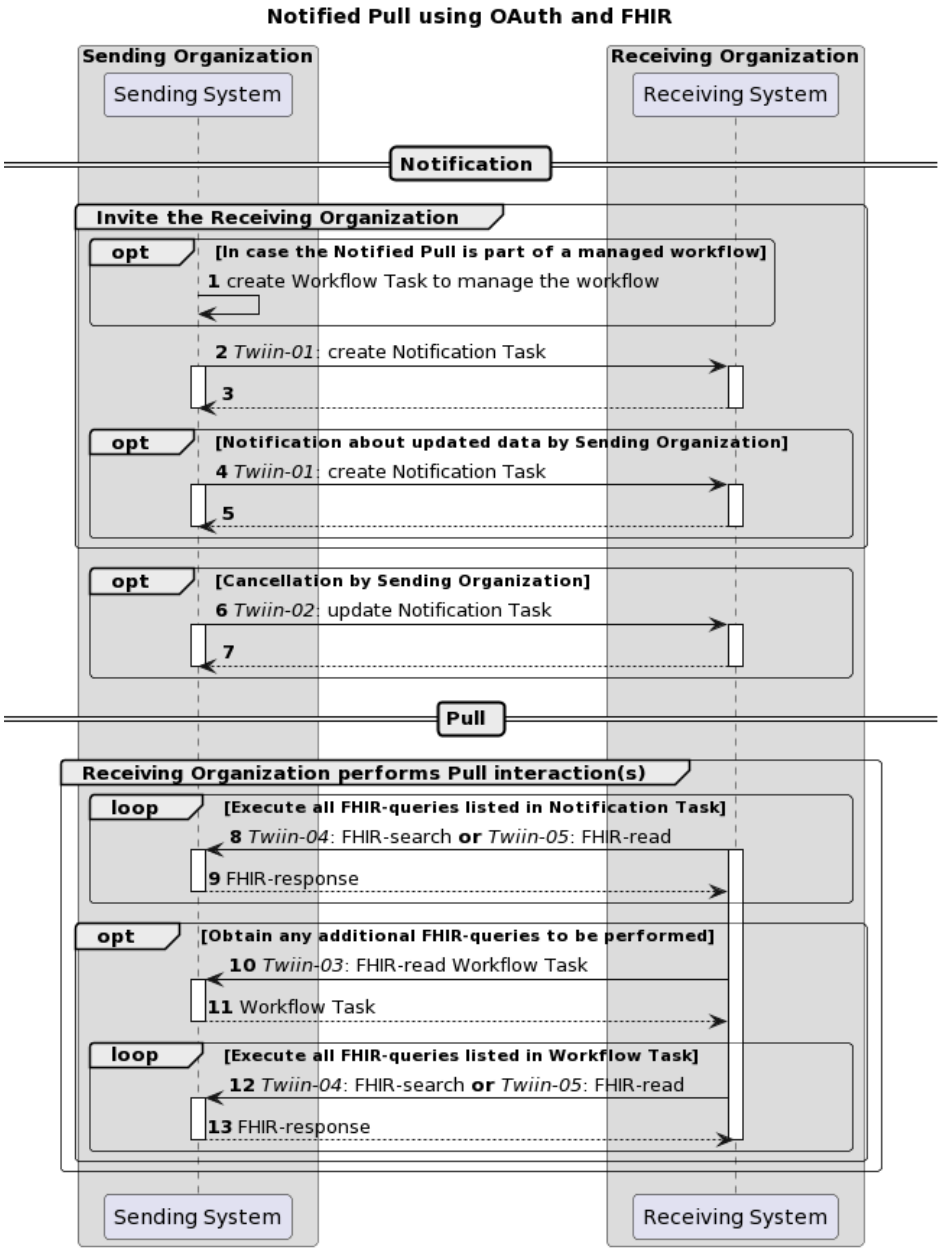
Z3.2.1.1 | COR – Data interactions

Original page can be found at: 10.3.1.1 Notified Pull – Data interactions (see page 190)

This chapter describes all relevant interactions for the Notified Pull interaction sequence on data level.

Notified Pull interaction sequence

All relevant interactions for the Notified Pull interaction sequence on data level are displayed in the sequence diagram below.



Description of the interactions in this sequence diagram:

Steps	Description
1	If the Notified Pull is part of a managed workflow involving both the Sending Organization and the Receiving Organization, and this workflow specifies the creation of a FHIR 'workflow task' at the sending system, then the flow starts with a creation of this task on the sending system. See Notification Task vs Workflow Task for additional details.
2-3	The sending system invites the receiving system to perform one or more Pull interactions (FHIR requests) by sending a FHIR task resource ('notification task') to the receiving system using a FHIR create interaction. The receiving system processes the invitation and sends a technical response to complete the create interaction. See 10.5.1 | Twiin-01 | Send Notification Task (see page 217) for a detailed description.
4-5	When the data set for which a notification message has been sent is updated in the sending system, the sending system must inform the receiving system about this update by sending a new notification message. The receiving system processes the invitation and sends a technical response to complete the create interaction. See 10.5.1 | Twiin-01 | Send Notification Task (see page 217) for a detailed description.
6-7	The 'cancellation by Sending Organization' option provides a means for the sending system to cancel or revoke an erroneously created notification. The sending system communicates the cancellation to the receiving system by sending an updated notification task to the receiving system using a FHIR conditional update interaction. The receiving system processes the interaction and sends a technical response to complete the conditional update interaction. See 10.5.2 | Twiin-02 | Cancel Notification Task (see page 225) for a detailed description.
8-9	The receiving system extracts the intended FHIR requests from the notification task listed in Task.input:read-available-resource and Task.input:query-available-resources. Subsequently, the receiving system initiates these FHIR requests and processes the responses. See 10.5.5 | Twiin-05 | Retrieve Resource (see page 232) for a detailed description for the retrieval of resources referenced in Task.input:read-available-resources. See 10.5.4 | Twiin-04 | Search Resource(s) (see page 230) for a detailed description for the retrieval of resources referenced in Task.input:query-available-resources.
10-11	In case that the notification task contains an indication that there is a workflow task at the sending system that contains additional FHIR requests (i.e. when Task.input:get-worflow-task.valueBoolean is true), the receiving system requests the workflow task at the sending system. See 10.5.3 | Twiin-03 | Get Workflow Task (see page 228)

12-13	The receiving system extracts the intended FHIR requests from the workflow task. Subsequently, the receiving system initiates these FHIR requests and processes the responses. See 10.5.5 | Twiin-05 | Retrieve Resource (see page 232) for a detailed description for the retrieval of resources referenced in Task.input:read-available-resources. See 10.5.4 | Twiin-04 | Search Resource(s) (see page 230) for a detailed description for the retrieval of resources referenced in Task.input:query-available-resources.

Notification task vs workflow task

The FHIR task resource used in the notification payload is not meant to track the status of a workflow or healthcare process that initiated the data exchange. When the data that is exchanged using the Notified Pull pattern serves for instance a patient referral or transfer, the status of that process should be tracked using a separate FHIR task resource that is maintained and hosted by the initiator of that process, i.e. the sending system. To keep a clear distinction between these two task resources, the task resource used as notification payload is referred to as the 'notification task', while the task resource that is used to track a healthcare process or workflow is referred to as a 'workflow task'. The notification task is sent from the sending system to the receiving system using a Push interaction (HTTP POST or PUT), while the workflow task is hosted at the sending system, and can be requested by the receiving system using a Pull interaction.

The use of a notification task as notification payload does not require the presence of a workflow task, but when a Notification task is sent in the context of a workflow that is maintained by the initiator of that workflow using a workflow task, the notification task MUST contain a reference to that workflow task.

Availability of BSN

For correct handling the BSN should be available as soon as possible, when this is legally required. The sending system has two possibilities:

- The BSN is sent in the authorization assertion (see page 206) used in the access token request before sending the notification task.
- The BSN is made available through the workflow task resource which is referenced in the basedOn attribute of the notification task resource. The workflow task resource must have a for reference with the identifier filled with the BSN.

The receiving system must support both. Since both variants are possible for the sending system to use, both must be supported by the receiving system, to be able to process from any sending system.

10.3.1 | TTA FHIR – Notified pull (see page 185)

10.4.7 | Network level security (see page 211)

Z3.2.1.2 | COR: Authentication & Authorization

> Original page can be found at: 10.4.2 | TTA FHIR - Authorization (see page 206)

> Attention! The specifications and requirements in this chapter are still a specific implementation for the Notified Pull communication pattern and have not yet been generalized to work for other communication patterns.

Resource server authorization: OAuth 2.0

On application level both the Notification endpoint of the Receiving System and the FHIR endpoint of Sending System are considered as resource endpoints that must be secured by https://www.rfc-editor.org/rfc/rfc6749. This implies that a client that wants to interact with a resource server (FHIR or Notification endpoint) must obtain an access token from an authorization server before it can interact with that resource server. The client must present this access token as bearer token in the HTTP Authorization header of each request to the resource server as specified in https://www.rfc-editor.org/rfc/rfc6750#section-2.1.

For further information on the transaction involved, please go to Twiin-07 | Token Request (see page 270)

Z3.2.2 | COR Correspondence implementation

The implementation for correspondence with Notified Pull is based on MedMij PDF/A. This appendix will provide a guideline on how to use the Notified Pull exchange pattern to transfer the correspondence between two healthcare organizations.

The Sending System may choose to provide a Workflow Task resource that can be used to exchange status updates and other workflow related details related to the healthcare process that demands the data exchange. In the context of a referral, the Sending System may choose to provide a Workflow Task resource that is used to exchange details about status updates or other workflow updates related to the referral (see Notification scope (see page 481)).

Although the following example only specifies the correspondence, in reality it will probably be part of another

Name	Card.	Type	Comments
definition	0..1	Reference (ActivityDefinition)	Reference to ActivityDefinition resources that defines the requested activity or service
status	1..1	code	requested | received | accepted | rejected | cancelled | completed

intent	1..1	code	“order”
priority	0..1	code	normal | urgent | asap | stat
code	1..1	CodeableConcept	
-- coding	1..1	Coding	
-- -- SNOMED	1..1	Slice	
-- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- code	1..1	code	“3457005”
-- -- -- display	0..1	string	“verwijzen van patiënt”
-- text	1..1	string	“Verwijzing”
description	0..1	string	
focus	0..1	Reference(ReferralRequest | CarePlan)	
for	0..1	Reference(nl-core-patient)	Reference to referred patient
authoredOn	0..1	dateTime	Date of referral submission
requester	0..1	BackboneElement	
-- agent	1..1	Reference(nl-core-practitioner)	Reference to the practitioner who sent the referral
-- -- extension		Extension	
-- -- -- practitionerRole		Extension(Reference(nl-core-practitionerrole))	Extension to relate the Practitioner to an organization, Location, HealthcareService, role, specialism, etc.
-- onBehalfOf	0..1	Reference(nl-core-organization)	Reference to the Sending Organization

owner	0..1	Reference(nl-core-organization)	Reference to the Receiving Organization
restriction	0..1	BackboneElement	
-- period	0..1	Period	
-- -- start	0..1	dateTime	Earliest date to start requested treatment or service
-- -- end	0..1	dateTime	Latest date to start requested treatment or service
input	0..*	BackboneElement	
-- correspondence	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- SNOMED	1..1	Slice	
-- -- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- -- code	1..1	code	“62591000146104”
-- -- -- -- display	0..1	string	“Correspondence”
-- -- text	1..1	string	“Correspondence”
-- -- valueString	1..1	string	“/Binary/<id>”

As described in the section Notified Pull interaction (see page 481) every reference can be coded specific to the part.

Z3.3 | COR Volume 2 - Transactions

The correspondence is communicated using the transactions described under this page.

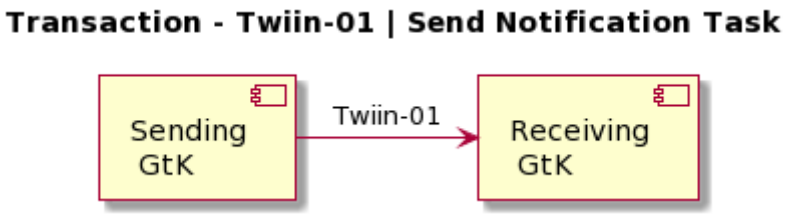
- Z3.3.1 | Twiin-01 | Send COR Notification Task (see page 484)

Z3.3.1 | Twiin-01 | Send COR Notification Task

> This section is the same as the generic 10.5.1 | Twiin-01 | Send Notification Task (see page 217)

This section describes the transaction needed for the notification.

Scope



This transaction delivers a notification from the Sending GtK to the Receiving GtK based on the specified referral.

Use Case Roles

Actor: Sending GtK

Role: Sends Notification Tasks on behalf of a referring user.

Actor: Receiving GtK

Role: Receives and processes Notification Tasks

Referenced Standards

- HL7® FHIR® standard STU3 https://hl7.org/fhir/stu3

Messages

Request message

The Notification message is sent by the Sending GtK when it needs to notify the Receiving GtK about one or more FHIR® resources that have been made available to the Receiving GtK.

The Notification that is sent to the Receiving GtK must be able to convey at least the following details:

- Identification of Sending GtK, Sending Organization and practitioner
- Identification of Receiving Organization
- References to individual FHIR® resources that have been made available at the Sending GtK
- FHIR® search or read queries that can be used to retrieve FHIR® resources that have been made available at the Sending GtK
- Authorization base (see (TA141) Twiin-07 | Token Request#Authorization-base)

The payload of this message consists of a https://hl7.org/fhir/stu3/task.html resource that contains at least the details mentioned above. This message is sent to communicate both a new and an updated data set to the Receiving GtK. The message results in a Task instance that will be referred to as the Notification Task.

> For the time being, the STU3 version of the FHIR® standard will be used because this TA will first be applied in the context of the BgZ (Basisgegevensset Zorg). Within that context, data is exchanged based on FHIR® STU3. As soon as data has to be exchanged using the Notified Pull pattern for newer FHIR® versions, it becomes opportune to provide or adopt a specification of the Notification for the corresponding FHIR® version.

The Sending GtK must initiate the Notification message using a create[140] interaction, i.e. sending an HTTP POST request to the Task endpoint of the Receiving GtK.

The media type of the HTTP body must be either *application/fhir+json* or *application/fhir+xml*.

When generating the Notification message, the Sending GtK must set the Task attributes as specified in the table below. For complete information on constructing a FHIR® Task Resource, see https://hl7.org/fhir/stu3/task.html .

Attribute	Card.	Description

140. https://hl7.org/fhir/STU3/http.html#create

definitionReference	0..1	This element will be used for routing purposes. The value could determine the organisational unit which will handle the notification. The display of this reference should be filled if no reference to a workflow Task exists and this value shall reference a valid ActivityDefinition resource. See also: 10.4.5 | TTA – Addressing (see page 210) Temporary agreement: We expect the activity definition reference to be in the same section as the references to the substantive resources: • In a thick notification, it will be referenced in the notification itself • In a thin notification, it will be referenced in the workflow task Until additional and more explicit agreements will be specified in the TA Routing, we will use this temporary agreement.
basedOn	0..*	Optional reference to a request–Type resource[141] that produced this event. If a workflow has been initiated and a Workflow Task is present, this must be referenced.
groupIdentifier	1..1	Unique identifier of the data set that is made available. An update to an existing data set at the Sending GtK triggers a new Notification Task, and thus a new Notification Task instance. Multiple Notifications Tasks on the same data set must share one unique identifier so that the Receiving GtK can identify them as relating to the same data set at the Sending GtK.
identifier	**1..1**	Business identifier of the task. This is a required field for traceability and cancellation of individual Notifications.

141. https://hl7.org/fhir/workflow.html#list

status	1..1	The state communicated by this event. Fixed value: • requested See also: https://hl7.org/fhir/stu3/valueset-request-status.html
intent	1..1	Indicates the "level" of actionability associated with the Task[2] (see page 217). Preferred value: • proposal See also: https://hl7.org/fhir/stu3/valueset-request-intent.html
code.coding	**1**..1	A code briefly describing what the task involves: • system = "http://fhir.twiin.nl/fhir/CodeSystem/TaskCode" • code = "pull-notification"
restriction.period	0..1	The period during which the data will be available for retrieval.
requester.agent.identifier	1..1	Identifier of the system that created this Notification. This could be the originating EHR System or the routing gateway system, dependent on which system created the Notification Task.
requester.onBehalfOf.identifier	**1**..1	Identifier of the Organization at which the data has been made available. The identifier shall be in the system “http://fhir.nl/fhir/NamingSystem/ura”
owner.identifier	**1**..1	Identifier of the Receiving Healthcare Organization. The identifier shall be in the system “http://fhir.nl/fhir/NamingSystem/ura”

input:authorization-base	**1..1**	The (TA141) Twiin-07 | Token Request#Authorization-base to be used when retrieving the data.
		Constraints:
		• type.coding
		  • system = "http://fhir.twiin.nl/fhir/CodeSystem/TaskParameter"
		  • code = "authorization-base".
		• valueString

input:get-workflow-task	0..1	An indicator to show whether or not all available resources are part of this Notification.
		Constraints:
		• type.coding
		  • system = "http://fhir.twiin.nl/fhir/CodeSystem/TaskParameter"
		  • code = “get-workflow-task”
		• valueBoolean
		Where valueBoolean:
		• true, the basedOn Workflow Task must be retrieved to get all available resources;
		• false (default), all available resources are available in the next (two) input slices.
		If this input slice is not added, the presumed value shall be false.

input: read-available-resource	0..*	The FHIR®-read interactions that can be performed to retrieve the data that was made available.
		Constraints:
		• type.coding (one or more of:)
		  • *Generic typing:*
		  • system = "http://hl7.org/fhir/restful-interaction"
		  • code = "read"
		  • *SNOMED CT typing **(deprecated)**:*
		  • system = “http://snomed.info/sct”
		  • code = a SNOMED CT code
		  • *LOINC typing **(deprecated)**:*
		  • system = “http://loinc.org”
		  • code = a LOINC code
		  • *FHIR profile typing **(prefered)**:*
		  • system = “http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile”
		  • code = a FHIR profile-id, e.g. "http://nictiz.nl/fhir/StructureDefinition/zib-DrugUse"
		• valueReference format
		  • [resourcetype]/[id]
		Where:
		• resourcetype denotes a FHIR® resourcetype;
		• id represents a logical id of a FHIR® resource instance.

input: query-available-resources	0..*	The FHIR®-search interactions that can be performed to retrieve the data that was made available.
		Constraints:
		• type.coding (one or more of:)
		  • *Generic typing:*
		  • system = "http://hl7.org/fhir/restful-interaction"
		  • code = "search-type"
		  • *SNOMED CT typing **(deprecated)**:*
		  • system = "http://snomed.info/sct"
		  • code = a SNOMED CT code
		  • LOINC typing ***(deprecated)***:
		  • system = "http://loinc.org"
		  • code = a LOINC code
		  • *FHIR profile typing **(prefered)***:
		  • system = "http://fhir.twiin.nl/fhir/NamingSystem/FhirProfile"
		  • code = a FHIR profile-id, e.g. "http://nictiz.nl/fhir/StructureDefinition/zib-DrugUse"
		• valueString format
		  • [resourcetype]{?[parameters]}
		Where:
		• Resourcetype denotes a FHIR® resourcetype;
		• parameters can be added to refine a FHIR®-search.

The Sending GtK MAY choose not to list the available FHIR® resources in Task.input. In that case, the Sending GtK MUST provide a reference to a Workflow Task resource in Task.basedOn. This Workflow Task MUST list the available FHIR® resources in Task.input, in the same format that is specified for the Notification Task. Additionally, in this case the Notification Task MUST have an entry in Task.input with the following values:

- Task.input.type.coding.system: "http://fhir.twiin.nl/fhir/CodeSystem/TaskParameter"
- Task.input.type.coding.value: "get-workflow-task"
- Task.input.valueBoolean: true

The Receiving GtK must accept both media types *application/fhir+json* and *application/fhir+xml*.

On receiving the submission, the Receiving GtK must validate the resource and respond with one of the HTTP codes defined in the (TA141) 10.5.1 | Twiin-01 | Send Notification Task .

The Notification should trigger an event in the Receiving GtK to facilitate the expected Pull.

Persistence of the Notification Task as a FHIR® resource is not required, whether it is necessary to persist is purely up to the receiving GtK and its internal implementation.

When the data set for which a Notification message has been sent is updated in the Sending GtK, the Sending GtK must inform the Receiving GtK about this update by sending a new Notification Message. In this case, Task.input:read-available-resource and Task.input:query-available-resources should only list the updated FHIR® resources. This way, the update can be communicated as a delta to the original data set. This relieves the Receiving GtK of determining which resources have changed in a larger set of resources. Note that the value of Task.identifier for the new Notification Task must differ from the value of Task.identifier Notification Task for the original data set, while the value of Task.groupIdentifier must be the same for all Notification Tasks on the same data set. This way, consecutive Notification Tasks on the same data set can be related to each other by the value of Task.groupIdentifier.

Response message

This message must be provided when a success or error condition needs to be communicated in response to an inbound request message. Success is only indicated once the Notification is received and completely processed.

To enable the Sending GtK to know the outcome of technical / syntactic processing of the Notification Task, the Receiving GtK must return either an empty body or an OperationOutcome resource. This body must be accompanied with the correct HTTP status code, e.g.:

- 200 OK – Notification received and not persisted.
- 201 Created – Notification received and persisted. In this case http-headers Location and Etag should be filled.
- 400 Bad Request – Notification could not be parsed or failed basic FHIR® validation rules.
- 404 Not Found – Resource type not supported, or wrong endpoint.
- 412 Precondition Failed – The processing of the Notification Task could not be finished, since the criteria were not selective enough.
- 422 Unprocessable Entity – The Notification Task resource violated applicable server business rules. This should be accompanied by an OperationOutcome resource providing additional detail.

Whether or not the resources referenced from any of the input elements can be retrieved shall not be a factor in the HTTP status.

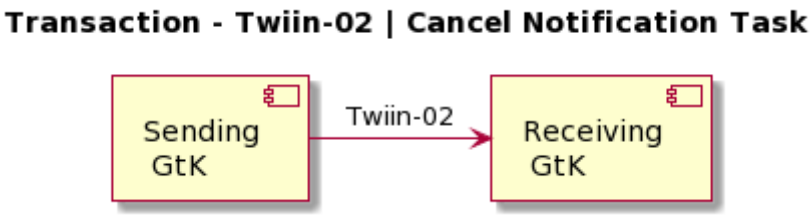
The Sending GtK processes the response according to application defined rules.

Z3.3.2 | Twiin-02 | Cancel COR Notification Task

> This page is the same as the generic 10.5.2 | Twiin-02 | Cancel Notification Task (see page 225)

This section describes the transaction needed for the cancellation of the notification.

Scope



This transaction delivers a cancellation notification from the Sending GtK to the Receiving GtK based on the specified referral. Twiin only requires that a GtK can receive this message, sending and processing the message is optional.

Actor	Sending Twiin-02	Receiving Twiin-02	Processing Twiin-02
Sending GtK	Optional	N/A	N/A
Receiving GtK	N/A	Mandatory	Optional

Use Case Roles

Actor: Sending GtK

Role: Sends Cancellation Notification Tasks on behalf of a referring user.

Actor: Receiving GtK

Role: Receives and processes Cancellation Notification Tasks

Referenced Standards

- HL7® FHIR® standard STU3 https://hl7.org/fhir/stu3

Messages

Request message

The Notification Cancellation request message is sent when the Sending GtK needs to send a cancellation of a previous Notification to the Receiving GtK. Just as the Notification message, the payload of this message consists of a FHIR® STU3 Task resource.

The Sending GtK can cancel a previous Notification using a conditional update[142] interaction on the Task that represents that previous Notification. This is done by sending an HTTP PUT request to the Task

endpoint of the Receiving GtK, where the value of Task.identifier of that previous Notification is included in the query parameters of the PUT request.

The media type of the HTTP body must be either *application/fhir+json* or *application/fhir+xml*.

When generating the Notification Cancellation message, the Sending GtK must set the Task attributes as specified in the table below. For complete information on constructing a FHIR® Task Resource, see https://hl7.org/fhir/stu3/task.html .

Attribute	Card.	Description
identifier	**1..1**	Business identifier of the Notification Task; the value of this identifier must be equal to the value of the identifier of the Notification Task that is to be cancelled.
status	1..1	The state communicated by this event. Fixed value: • cancelled
intent	1..1	Indicates the "level" of actionability associated with the Task[1] (see page 225). Preferred value: • proposal See also: https://hl7.org/fhir/stu3/valueset-request-intent.html
code.coding	**1..1**	A code briefly describing what the task involves: • system = "http://fhir.twiin.nl/fhir/CodeSystem/TaskCode" • code = "pull-notification"

In the absence of a reference to the patient (for example, within the Workflow Task), the token request for this cancellation SHALL include the patient's BSN within the assertion.

The Receiving GtK must accept both media types *application/fhir+json* and *application/fhir+xml*.

On receipt of the submission, the Receiving GtK must validate the resource and respond to the cancellation message according to the requirements specified in Notification response (see page 225).

The Notification SHOULD trigger an event in the Receiving GtK to cancel any intended Pull interaction.

Persistence of the Notification Task as a FHIR® resource is not necessary.

142. http://hl7.org/fhir/stu3/http.html#cond-update

Notification response

This message must be provided when a success or error condition needs to be communicated in response to an inbound Notification message. Success is only indicated once the Notification is received and completely processed.

To enable the Sending GtK to know the outcome of technical / syntactic processing of the Notification Task, the Receiving GtK must return either an empty body or an OperationOutcome resource. This body must be accompanied with the correct HTTP status code, e.g.:

- 200 OK – Notification received and not persisted.
- 201 Created – Notification received and persisted. In this case http-headers Location and Etag should be filled.
- 400 Bad Request – Notification could not be parsed or failed basic FHIR® validation rules.
- 404 Not Found – Resource type not supported, or wrong endpoint.
- 412 Precondition Failed – The processing of the Notification Task could not be finished, since the criteria were not selective enough.
- 422 Unprocessable Entity – The Notification Task resource violated applicable server business rules. This should be accompanied by an OperationOutcome resource providing additional detail.

The Sending GtK processes the response according to application defined rules.

Z3.3.3 | Twiin-03 | Get COR workflow Task

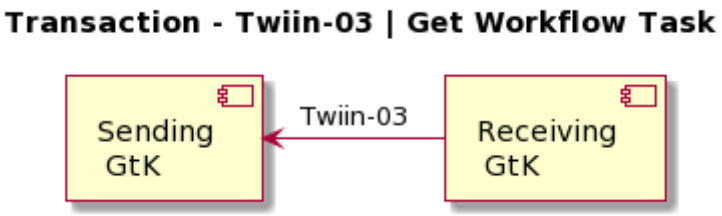
> This page is the same as the generic 10.5.3 | Twiin-03 | Get Workflow Task (see page 228)

This section describes the transaction of the retrieval of the Workflow Task.

> If a workflow Taks is used its definitionReference must be filled and shall reference a valid ActivityDefinition resource.

> Temporary agreement: We expect the activity definition reference to be in the same section as the references to the substantive resources:
>
> - In a thick notification, it will be referenced in the notification itself
> - In a thin notification, it will be referenced in the workflow task
>
> Until additional and more explicit agreements will be specified in the TA Routing, we will use this temporary agreement.

Scope



This transaction supports getting the Workflow Task by the Requesting System at the Resource Server.

Use Case Roles

Actor: Requesting GtK

Role: Requests the workflow Task on behalf of a requesting user.

Actor: Responding GtK

Role: Processes the request and responds with the requested resource.

Referenced Standards

- HL7® FHIR® standard STU3 https://hl7.org/fhir/stu3

Messages

Request message

The requesting system wants to obtain the workflow Task for information about a known workflow. The workflow Task is retrieved using a the FHIR® read interaction, i.e. executing an HTTP GET request to the Task endpoint of the resource server.

```
GET [base]/Task/[id]
```

The requesting system may provide the HTTP Accept header. Valid values for this header are *application/fhir+json* or *application/fhir+xml*. If none is set, the resource server will use its default.

Response message

The resource server returns the workflow Task that is requested.

The payload of this message consists of a https://hl7.org/fhir/stu3/task.html resource that contains relevant information to the workflow. This message is returned to the Receiving System.

The media type of the HTTP body must be either *application/fhir+json* or *application/fhir+xml*, based on the Accept header or default response content type.

At this time there is no generic specification of the contents of the workflow Task more specific than the FHIR® specification.

Persistence of the Workflow Task as a FHIR® resource is not necessary.

When an error occurs an OperationOutcome resource must be returned with more details on the reason.

The HTTP response must be accompanied with the correct HTTP status code, e.g.:

- `200` OK – The request is accepted and responded
- `401` Not Authorized - Authorization is required for the interaction that was attempted
- `404` Not Found – The request could not be processed, i.e. the resource with that id doesn't exist.
- `410` Gone – The request could not be processed, because the resource does not exist anymore.

The requesting system processes the response according to application defined rules.

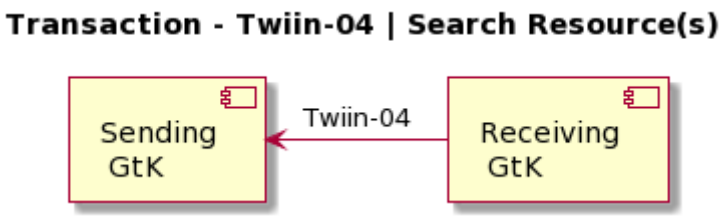
Z3.3.4 | Twiin-04 | Search COR Resource(s)

> This page is the same as the generic 10.5.4 | Twiin-04 | Search Resource(s) (see page 230)

This section describes the transaction of the retrieval of the FHIR® resources.

> In the communication pattern notified pull these resources are referenced in the input field of the Notification or Workflow Task.
> These input fields contain valueString in the input slice: query-available-resources.

1. Scope



This transaction supports the request of resources by the Requesting GtK to the Resource Server.

2. Use Case Roles

Actor: Requesting GtK

Role: Sends a request for resources on behalf of a retrieving user.

> In the communication pattern notified pull, this is the Receiving GtK.

Actor: Responding GtK

Role: Processes the request and responds with the requested resources.

> Note: In the communication pattern notified pull, this is the Sending GtK.

3. Referenced Standards

- HL7® FHIR® standard STU3 https://hl7.org/fhir/stu3

4. Messages

4.1. Request message

The requesting GtK wants to obtain the resources that were referenced in the Task. These resources are retrieved using a FHIR® search interaction, i.e. executing an HTTP GET request to the resource servers FHIR® endpoint. If there is a relative path, the input valueString must be appended to the FHIR® base-url.

```
GET [base]/<ResourceType>?parameter=value
```

> **Percent-encoding of query parameters**
>
> When constructing URLs that include query parameters (e.g., code=...), it is important to percent-encode any reserved characters that could cause syntactic ambiguity, in accordance with https://datatracker.ietf.org/doc/html/rfc3986.
>
> **Exception**
> The slash character (/) may appear unencoded in query parameter values, as it is explicitly allowed in the query component of a URI per RFC 3986 (see Appendix A), and is commonly accepted by web servers and FHIR implementations.

The requesting GtK may provide the HTTP Accept header. Valid values for this header are *application/fhir+json* or *application/fhir+xml*. If none is set, the resource server will use its default.

4.2. Response message

The responding GtK returns the resource(s) that are requested.

The payload of this message consists of a FHIR® Bundle resource that contains the requested resource(s). This message is returned to the Receiving GtK.

The media type of the HTTP body must be either *application/fhir+json* or *application/fhir+xml*, based on the Accept header or default response content type.

When an error occurs an OperationOutcome resource must be returned with more details on the reason.

The HTTP response must be accompanied with the correct HTTP status code, e.g.:

- `200` OK – The search was processed and a valid response was returned
- `400` Bad Request – The search could not be processed or failed basic FHIR® validation rules
- `401` Not Authorized – Authorization is required for the interaction that was attempted
- `404` Not Found – The resource type not supported

The requesting GtK processes the response according to application defined rules.

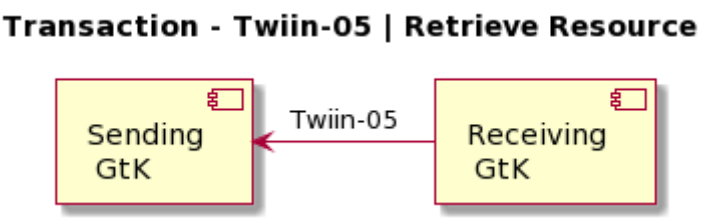
Z3.3.5 | Twiin-05 | Retrieve COR Resource

> This page is the same as the generic 10.5.5 | Twiin-05 | Retrieve Resource (see page 232)

This page describes the transaction of the retrieval of the FHIR® resources.

> In the communication pattern notified pull these resources are referenced in the input field of the Notification or Workflow Task.
> These input fields contain valueReference in the input slice: read-available-resource.

Scope



This transaction supports the request of resources by the Requesting System to the Resource Server.

Use Case Roles

Actor: Requesting GtK

Role: Sends a request for a specific resource on behalf of a retrieving user.

> In the communication pattern notified pull, this is the Receiving GtK.

Actor: Responding GtK

Role: Processes the request and responds with the requested resource.

> Note: In the communication pattern notified pull, this is the Sending GtK.

Referenced Standards

- HL7® FHIR® standard STU3 https://hl7.org/fhir/stu3

Messages

Request message

The requesting GtK wants to obtain the resources that were referenced in the Task. These resources are retrieved using a FHIR® read interaction, i.e. executing an HTTP GET request to the resource servers FHIR® endpoint. If there is a relative path, the input valueReference must be appended to the FHIR® base-url.

```
GET [base]/<ResourceType>/<id>
```

> The requesting GtK may provide the HTTP Accept header. Valid values for this header are *application/fhir+json* or *application/fhir+xml*. If none is set, the resource server will use its default.

Response message

The responding GtK returns the resource that is requested.

The payload of this message is the requested FHIR® resource. This message is returned to the requesting GtK.

The media type of the HTTP body must be either *application/fhir+json* or *application/fhir+xml*, based on the Accept header or default response content type.

When an error occurs an OperationOutcome resource must be returned with more details on the reason.

The HTTP response must be accompanied with the correct HTTP status code, e.g.:

- `200` OK – The search was processed and a valid response was returned
- `401` Not Authorized – Authorization is required for the interaction that was attempted
- `404` Not Found – The resource could not be found
- `410` Gone – The resource was deleted

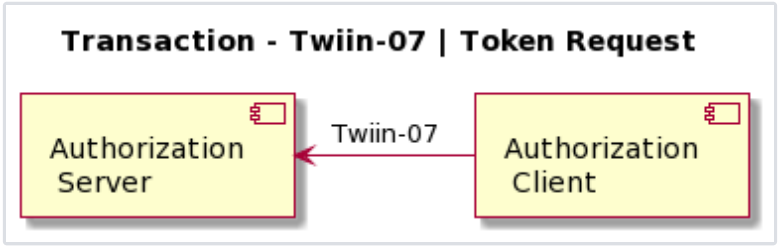
The requesting GtK processes the response according to application defined rules.

Z3.3.7 | Twiin-07 | Token Request

> This page is the same as the generic 10.3.7 | Twiin – 07 | Token Request (see page 270)

This page describes the transaction of the retrieval of the OAuth tokens

Scope



This transaction supports the request of an authentication token by the Requesting System to the Resource Server.

Use Case Roles

Actor: Authorization Client

Role: Client requesting an access token to authorize RESTful transactions.

Actor: Authorization Server

Role: Server that grants access tokens

Relevant Standards

- *OAuth 2.1*: The OAuth 2.1 Authorization Framework, published as draft-ietf-oauth-v2-1-01, 1 February 2021.
- *JWT Access Token*: JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens, published as draft-ietf-oauth-access-token-jwt-10, September 2020.
- *RFC4648*: The Base16, Base32, and Base64 Data Encodings, October 2006
- RFC6749: The OAuth 2.0 Authorization Framework, October 2012.
- *RFC7519*: JSON Web Token (JWT), May 2015.
- *RFC7522*: Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants, May 2015.
- *RFC7523*: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants, May 2015.
- *RFC7515*: JSON Web Signature (JWS), May 2015.
- *RFC7518*: JSON Web Algorithms (JWA), May 2015.
- *RFC8705*: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens, February 2020.

Messages

Request message

The resource server must be able to authenticate the client as a trusted client. The client is specified as the **system** that submits the access token request (not to be confused with the **organization** for which that system is acting). The OAuth specs leave room for different authentication methods for client authentication. The authentication methods that are proposed in the OAuth 2.0 core specifications (https://www.rfc-editor.org/rfc/rfc6749.html#section-2.3) all rely on the exchange of shared secrets. The use of shared secrets is considered as a security risk since they are prone to leakage. The use of an authentication method that relies on digital signatures using asymmetric cryptography offers better security. Therefore, the client must authenticate itself by providing a client assertion by means of a signed JWT as specified in https://www.rfc-editor.org/rfc/rfc7523#section-2.2.

The client assertion is a JWS Compact Serialized JWT that consists of a header, a payload, and a signature. The signature is created using a key pair belonging to the initiating system or to a third party trusted by the initiating system.

The header carries the claims listed below:

Claim	Description	Required

typ	Token type, must be “JWT”	Yes
alg	Cryptographic algorithm used to sign the client assertion. See https://www.rfc-editor.org/rfc/rfc7518#section-3.1 . All algorithms are described at (TA141) Twiin-07 | Token Request.	Yes
kid	Identifier of the key pair used to sign this JWT. See https://www.rfc-editor.org/rfc/rfc7515#section-4.1.4.	Yes

The payload contains a set of claims listed below:

Claim	Description	Required
jti	Unique identifier of the client assertion. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.7. The jti (JWT ID) is a unique identifier for a token and must not be reused. An assertion containing a duplicate jti (i.e., one that has been previously processed) shall be rejected to prevent replay attacks. Implementations should maintain a mechanism to track used jti values for the duration of their validity period.	Yes
iss	Identifier of the system that issued the client assertion. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.1 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	Yes
iat	The time at which the client assertion was issued. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.6. If there is an agreed age of a client assertion.	Conditional

exp	The expiration time on or after which the client assertion shall not be accepted for processing. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.4 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3. > The expiration time (exp) claim in the assertion shall not exceed 5 minutes (300 seconds) from the time of issuance. Any assertion with an exp value set beyond this limit must be rejected.	Yes
nbf	The time before which the token shall not be accepted for processing. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.5 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	No
aud	Identifier of the authorization server token endpoint where this client assertion is to be used. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.3 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	Yes
sub	Identifier of the OAuth client that requests access. This claim must match the value of the client_id parameter in the access token request. Note that the client is specified as the system that submits the access token request.	Yes

The Issuer of the client assertion may include additional claims in the assertion, but the Issuer shall not require the authorization server to process these claims.

The exchange of the public key that corresponds to the private key that was used to sign the client assertion between the Assertion Issuer and the authorization server is beyond the scope of this normative specification. This is the added value of Twiin. Twiin unambiguously describes the agreements that system providers typically need to make with each other.Note that the authorization server can authenticate the client on network level by the client certificate that the client must present during the mTLS handshake (see section Network level security (see page 206)). In theory, this could be used by the authorization server to authenticate the client on application level. However, this may cause problems since it introduces additional and potentially unwanted requirements on TLS termination and related matters. Therefore, a client must always provide a client assertion in the access token request.

Authorization grant

OAuth 2.0 requires the use of an authorization grant to request an access token. As specified in https://www.rfc-editor.org/rfc/rfc6749#section-1.3 “an authorization grant is a credential representing the resource owner's authorization (to access its protected resources) used by the client to obtain an access token.” OAuth 2.0 specifies several different authorization grants. Additionally, there are several RFC’s that specify extension grants, e.g. https://www.rfc-editor.org/rfc/rfc6749#section-4.5. Because this TA applies to situations where a resource client is acting on behalf of a user (health professional) that works

for an organization (healthcare provider), the use of the JWT Bearer Assertion authorization grant as specified in https://www.rfc-editor.org/rfc/rfc7523#section-2.1 is the most suitable authorization grant. This means that the resource client must provide an authorization assertion in each access token request to identify the acting user, organization, and authorization base to prove that it is authorized to access the requested data. This authorization assertion acts as the authorization grant that the client can present to prove that it is authorized to access the protected resources.

The authorization assertion is a JWS Compact Serialized JWT that consists of a header, a payload, and a signature. The signature is created using a key pair belonging to the initiating organization or to a third party trusted by the initiating organization.

The header carries the claims listed below:

Claim	Description	Required
typ	Token type, must be "JWT"	Yes
alg	Cryptographic algorithm used to sign the authorization assertion. See https://www.rfc-editor.org/rfc/rfc7518#section-3.1 . All algorithms are described at (TA141) Twiin-07 | Token Request.	Yes
kid	Identifier of the key pair used to sign this JWT. See https://www.rfc-editor.org/rfc/rfc7515#section-4.1.4.	Yes

The payload contains a set of claims that carry information required by NEN 7512 and NEN 7513.

Claim	Description	Required
jti	Unique identifier of the authorization assertion. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.7. > The jti (JWT ID) is a unique identifier for a token and must not be reused. An assertion containing a duplicate jti (i.e., one that has been previously processed) shall be rejected to prevent replay attacks. Implementations should maintain a mechanism to track used jti values for the duration of their validity period.	Yes
iss	Identifier of the system that issued the authorization assertion. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.1 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	Yes

iat	The time at which the authorization assertion was issued. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.6. This is only required if there is an agreed age of an authorization assertion.	Conditional
exp	The expiration time on or after which the authorization assertion shall not be accepted for processing. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.4 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3. The expiration time (exp) claim in the assertion shall not exceed 5 minutes (300 seconds) from the time of issuance. Any assertion with an exp value set beyond this limit must be rejected.	Yes
nbf	The time before which the token shall not be accepted for processing. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.5 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	No
aud	Identifier of the authorization server token endpoint where this authorization assertion is to be used. See https://www.rfc-editor.org/rfc/rfc7519#section-4.1.3 and https://www.rfc-editor.org/rfc/rfc7523.html#section-3.	Yes
sub	Identifier of the **healthcare organization** that requests access. **URA nummer** is mandatory, *additionaly* other identifiers may be added. The codesystem (`issuing_system`) for the identifier is also mandatory. For the URA this is OID: 2.16.528.1.1007.3.3 5.1 | Vertrouwen: Identificatie (see page 62) Allowed format for this identifier is: • `http://fhir.nl/fhir/NamingSystem/ura|<URA>`	Yes

sub_role	Code of the type of the **organization** (healthcare supplier) that requests access. **RoleCodeNL** is mandatory. The codesystem (`issuing_system`) for the identifier is also mandatory. For the RoleCodeNL this is OID: 2.16.840.1.113883.2.4.15.1060 Sub role is required when the responding party needs to check the patient consent. For instance when a user does not have an authorization base when requesting patient information.	Conditional
user_id	Identifier of the **responsible user** (healthcare professional) who requests access. **Preferred: UZI nummer** Allowed formats for this identifier are: • `urn:oid:2.16.528.1.1007.3.1.<UZI>` (without leading zero of UZI) • `http://fhir.nl/fhir/NamingSystem/uzi-nr-pers|<UZI>` 5.1 | Vertrouwen: Identificatie (see page 62) **User or system** In some cases a system is allowed to access data without a specific user being involved. Whenever there is a request for patient information, the identifier of the responsible user MUST be communicated. The only known exception to this rule is the retrieval of the Workflow Task that is requested based on the Notification Task in the TTA Notified Pull.	Yes

user_role	Code of the role of the responsible user (healthcare professional) who requests access. **Preferred: UZI rolcode** Allowed formats for this code are: • `urn:oid:2.16.840.1.113883.2.4.15.111.<UZI rolcode` (without leading zero, both before and after the . within the UZI rolcode) • `http://fhir.nl/fhir/NamingSystem/uzi-rolcode|<UZI rolcode>` 5.1 | Vertrouwen: Identificatie (see page 62) User identification (user_id and user_role claims) is only required in the authorization assertion when access to patient data is requested. This implies that these claims are not required in authorization assertions used in access token requests for Notification endpoints.	Conditional
authorizer	Identifier of the **healthcare organization** that grants access. **URA nummer** is mandatory, *additionaly* other identifiers may be added. The codesystem (`issuing_system`) for the identifier is also mandatory. For URA this is OID: 2.16.528.1.1007.3.3 5.1 | Vertrouwen: Identificatie (see page 62) Allowed format for this identifier is: • `http://fhir.nl/fhir/NamingSystem/ura|<URA>`	Yes
authorization_base	See Authorization base	No

patient	Identifier of the patient for whom data is exchanged. 5.1 | Vertrouwen: Identificatie (see page 62)	Conditional

> Allowed format for this identifier is:
>
> - `urn:oid:2.16.840.1.113883.2.4.6.3.<BSN>` (without leading zero of BSN)

> Patient identification is only required when the Sending System requests access to the Notification endpoint of the Receiving System and the Sending System does not provide a Workflow Task that refers to a Patient resource containing the BSN of the patient. This way, the Receiving System is always able to identify a patient by BSN based on a Notification. The Receiving System must support receiving the BSN through the patient claim.

The Issuer of the authorization assertion may include additional claims in the authorization assertion, but the Issuer shall not require the authorization server to process these claims.

The exchange of the public key that corresponds to the private key that was used to sign the authorization assertion between the Assertion Issuer and the authorization server is beyond the scope of this normative specification. Therefore, system vendors have to make mutual agreements about the exchange of these public keys.

Authorization scope

The scope defines the requested access to the FHIR Server as specified in https://www.rfc-editor.org/rfc/rfc6749#section-3.3 . If a scope is provided in the access token request or access token response, it must be expressed in a string of space delimited scopes as defined in http://hl7.org/fhir/smart-app-launch/scopes-and-launch-context.html#scopes-for-requesting-clinical-data . The following additional requirements apply to the scope values:

- When requesting an access token for a Notification endpoint at the Receiving System, the scope value must be one of:
  - system/Task.c?code=http://fhir.twiin.nl/fhir/CodeSystem/TaskCode|pull-notification (create)
  - system/Task.u?code=http://fhir.twiin.nl/fhir/CodeSystem/TaskCode|pull-notification (update)
- When requesting an access token for a FHIR endpoint at the Sending System, the query parameters in the scopes must match (a subset of) the queries in the FHIR search requests listed in Task.input of the Notification Task (see Notification message (see page 217)).

The client must provide the requested scope in the access token request, except for cases where an authorization base is provided in the access token request as part of the authorization assertion.

The authorization server must provide the granted access scope in the access token response in accordance with https://www.rfc-editor.org/rfc/rfc6749#section-5.1 and the requirements mentioned above. The issued access token must grant access to the granted scope that the authorization server specifies in the access token response. The granted scope must be equal to or less than the scope that can be derived from the authorization base consent token.

Access token request

Based on the paragraphs above each access token request contains the parameters listed below:

Parameter	Value	Required
grant_type	"urn:ietf:params:oauth:grant-type:jwt-bearer"	Yes
assertion	JWT authorization assertion as specified in paragraph Authorization grant.	Yes
client_assertion_type	"urn:ietf:params:oauth:client-assertion-type:jwt-bearer"	Yes
client_assertion	JWT client assertion as specified in paragraph Request message.	Yes
client_id	ID of the resource client. This ID is issued by the authorization server. The value of the "client_id" parameter must identify the same client as is identified by the client assertion.	Yes
scope	Space separated list of requested scopes, see paragraph Authorization scope.	Conditional

> The scope must not be encoded before the `x-www-form-urlencoded` encoding. e.g. before encoding it should look like:
>
> ```
> patient/Observation.s?code=http://loinc.org|29463-7
> ```

Note that the access token request effectively contains two JWT assertions:

1. A client assertion that is used to authenticate the client. This assertion identifies and authenticates the **system** that is requesting access.

2. An authorization assertion that is used as an authorization grant. This assertion identifies both the **organization** and **user** that are requesting access.

Separating client authentication from client authorization in two separate assertions enables the client to select different Assertion Issuers for the two assertions. The targeted authorization server must register both Issuers as trusted Assertion Issuers for a specific client.

Access token requirements

The access token will be processed only by the party that issued the access token. Therefore, the form and contents of the token are determined by the authorization server (audience), so the access token is opaque to the resource client. The resource client should not take any dependency on the format or contents of an access token. The authorization server MAY issue certificate bound access tokens as specified in https://www.rfc-editor.org/rfc/rfc8705 , but this is not mandatory. To enable the server to issue certificate bound access tokens, the client MUST support mTLS for access token and resource requests as specified in section Network level security: mTLS 1.3.

The validity period of an OAuth 2.0 access token shall not exceed 15 minutes. Implementations must ensure that the exp (expiration) claim in the token is set accordingly, with a maximum lifetime of 900 seconds (15 minutes) from the time of issuance.

Clients should be designed to handle token expiration by obtaining a new access token as required.

Authorization base

When the Sending System receives a request from the Receiving System to access certain data, it is the primary responsibility of the Sending System to verify that the Receiving System is authorized to access that data. When a system receives an authorization base, it shall not use the UZI-rolcode to determine whether access should be granted. When publishing data on a resource server to be collected by the Receiving System, many Sending Systems register the authorization to access that data as an authorization base of some kind. To facilitate that authorization process, the Sending System may submit the authorization base (or a reference to it) to the Receiving System as part of the Notification (see section Notification message (see page 218)). If the Receiving System received an authorization base in the Notification, it must include that authorization base in the access token request to the Sending System (see section Authorization grant). This enables the authorization server of the Sending System to determine if the requested access can be granted based on the provided authorization base.

Since an authorization base is to be processed by the Sending System only, the form and contents of an authorization base are determined by the Sending System. The Receiving System should not take any dependency on the format or contents of an authorization base.

User authentication

Healthcare professionals are identified in their EHR system by logging in with their personal account. When a user of the Receiving System wants to request resources at the Sending System, the Sending System must be able to identify the user at the Receiving System as a legitimate healthcare professional who is working for the receiving organization before it can provide the requested data. Therefore, the Receiving System must implement the appropriate means to ensure the authenticity of the user.

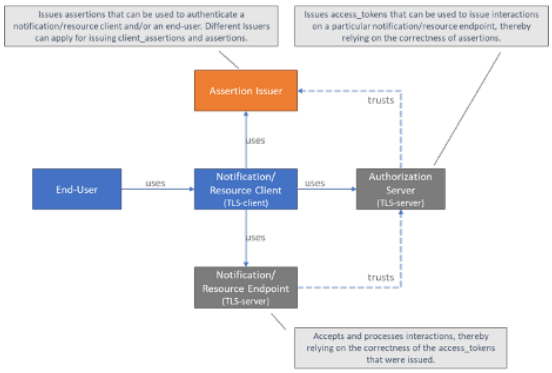
The Sending System can identify the healthcare professional at the receiving organization that is requesting patient data by the following claims in the authorization assertion of the access token request (see Authorization grant):

- **sub**: Identifier of the healthcare organization
- **user_id**: Identifier of the responsible user (healthcare professional)
- **user_role**: Code of the role of the responsible user (healthcare professional)

The type of identifiers used for organizations and users is beyond the scope of this TA. The same applies to the use of role codes.

Trust relationships

The picture below shows the different roles involved in the interactions, and clarifies the dependencies between these roles.



The Sending System hereby performs the following roles:

- Notification Client;
- Resource Server Endpoint.

The Receiving System performs the roles:

- Notification Server Endpoint;
- Resource Client.

Sending System and Receiving System both implement the role of Authorization Server.

The role of Assertion Issuer can be performed by a third-party, but can also be performed by the Sending System or by the Receiving System. Assertion Issuers producing client assertions do not necessarily have to produce authorization assertions as well. Different Issuers can be used for these types of assertions. Before issuing a client assertion or an authorization assertion, the Assertion Issuer has to make sure that applicable requirements regarding user authentication and other mutual security agreements between the Sending System and Receiver System have been met.

Trust and required level of user authentication between parties has to be arranged and agreed upon prior to performing the interaction.

Signature Algorithms

For verifying cryptographic tokens, we enforce the use of the following algorithms:

- **ES256** (Elliptic Curve P-256 with SHA-256)
- **ES512** (Elliptic Curve P-521 with SHA-512)
- ***PS256*** *(RSASSA-PSS with SHA-256) – Planned for future use*

Implementations must explicitly reject any other algorithms to ensure security and compliance with best practices.

For signing cryptographic tokens, one of the supported algorithms should be used.

Z3.4 | COR: Volume 3 - Content

Inhoudsopgave

Inhoud

Dit betreft de bijlagen van de andere zorgtoepassingen als pdf(/a) document.

Metadata

{}

COR: Samenvatting PvE

1. Validatie eisen

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
COR-1-authz-03	Autorisatierichtlijn	GtK ontvanger	De GtK ontvanger dient te controleren of de grondslag (authorization base) daadwerkelijk is uitgegeven aan de GtK verzender.	Wanneer de grondslag niet meekomt in de uitwisseling, is er geen sprake van het notified pull uitwisselpatroon en dient de GtK ontvanger op basis van de in de autorisatierichtlijn beschreven rollen het verzoek te autoriseren. Transacties: 10.5.5 | Twiin-05 | Retrieve Resource (see page 232) De autorisatierichtlijn van de primaire zorgtoepassing is van toepassing.
COR-2a-TANP-01	TANP	GtK ontvanger	GtK ontvanger dient een notificatie-endpoint aan te bieden aan GtK verzender.	Een endpoint kan worden gedeeld door meerdere Twiin Deelnemers (bijv. een endpoint per GtK/ SaaS-dienst) of er kan sprake zijn van een endpoint per Twiin Deelnemer. Zie o.a. Z3.2.1 | COR TTA Exchanging correspondence - FHIR Notified Pull (see page 473)
COR-2a-TANP-02	TANP	GtK verzender	GtK verzender dient een resource-endpoint aan te bieden aan GtK ontvanger.	Een endpoint kan worden gedeeld door meerdere Twiin Deelnemers (bijv. een endpoint per GtK/ SaaS-dienst) of er kan sprake zijn van een endpoint per Twiin Deelnemer. Zie o.a. Z3.2.1 | COR TTA Exchanging correspondence - FHIR Notified Pull (see page 473)
COR-2a-TANP-03	TANP	GtK verzender, GtK ontvanger	GtK verzender en GtK ontvanger dienen een token-endpoint aan elkaar aan te bieden.	Een endpoint kan worden gedeeld door meerdere Twiin Deelnemers (bijv. een endpoint per GtK/ SaaS-dienst) of er kan sprake zijn van een endpoint per Twiin Deelnemer. Zie o.a. Z3.2.1 | COR TTA Exchanging correspondence - FHIR Notified Pull (see page 473)

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
COR-2a-TANP-04	TANP	GtK verzender,	GtK verzender dient de technische adressen van het resource-endpoint en het token-endpoint kenbaar te maken aan de Twiin beheerorganisatie.	De wijze waarop technische adressen tussen GtK verzender en GtK ontvanger worden gecommuniceerd is (nog) niet gebonden aan normatieve eisen. De Twiin beheerorganisatie publiceert de endpoints en technische adressen in ZORG-AB. Om de technische adressen van een andere partij te achterhalen kan er worden gekozen om ZORG-AB te raadplegen (10.6.5 | Addressing - ZORG-AB Transacties (see page 288)) maar dit is niet verplicht. GtK verzender en GtK ontvanger kunnen bijvoorbeeld ook onderling afspraken maken over de wijze waarop technische adressen worden gecommuniceerd. Zie o.a. Z3.2.1 | COR TTA Exchanging correspondence - FHIR Notified Pull (see page 473)
COR-2a-TANP-05	TANP	GtK ontvanger	GtK ontvanger dient de technische adressen van het notificatie-endpoint en het token-endpoint kenbaar te maken aan de Twiin beheerorganisatie.	De wijze waarop technische adressen tussen GtK verzender en GtK ontvanger worden gecommuniceerd is (nog) niet gebonden aan normatieve eisen. De Twiin beheerorganisatie publiceert de endpoints en technische adressen in ZORG-AB. Om de technische adressen van een andere partij te achterhalen kan er worden gekozen om ZORG-AB te raadplegen (10.6.5 | Addressing - ZORG-AB Transacties (see page 288)) maar dit is niet verplicht. GtK verzender en GtK ontvanger kunnen bijvoorbeeld ook onderling afspraken maken over de wijze waarop technische adressen worden gecommuniceerd. Zie o.a. Z3.2.1 | COR TTA Exchanging correspondence - FHIR Notified Pull (see page 473)

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
COR-2a-AA-01	BgZ Authn en Authz	GtK verzender	GtK verzender dient de publieke steutel(s) die zij gebruikt voor de ondertekening van JWT's via `kid` opzoekbaar te maken voor GtK ontvanger.	De wijze waarop de uitwisseling van publieke sleutels tussen GtK verzender en GtK ontvanger plaatsvindt is (nog) niet gebonden aan normatieve eisen. GtK verzender en GtK ontvanger moeten daarom onderling en in afstemming met de gebruikte infrastructuur afspraken maken over de wijze van uitwisseling van publieke sleutels. Zie Z3.2.1.2 | COR: Authentication & Authorization (see page 481)
COR-2a-AA-02	BgZ Authn en Authz	GtK ontvanger	GtK ontvanger dient de publieke steutel(s) die zij gebruikt voor de ondertekening van JWT's via `kid` opzoekbaar te maken voor GtK verzender.	De wijze waarop de uitwisseling van publieke sleutels tussen GtK verzender en GtK ontvanger plaatsvindt is (nog) niet gebonden aan normatieve eisen. GtK verzender en GtK ontvanger moeten daarom onderling en in afstemming met de gebruikte infrastructuur afspraken maken over de wijze van uitwisseling van publieke sleutels. Zie Z3.2.1.2 | COR: Authentication & Authorization (see page 481)
COR-2a-AA-03	BgZ Authn en Authz	GtK verzender	GtK verzender is in staat een client assertion in de vorm van een `authentication_grant` aan te maken die voldoet aan de specificaties	Specificaties: (TA141) 10.4.2 | TTA FHIR - Authorization#Client-authentication
COR-2a-AA-04	BgZ Authn en Authz	GtK verzender, GtK ontvanger	GtK verzender en GtK ontvanger dienen gebruik te maken van dezelfde identifiers voor de systemen die opereren als autorisatie-clients (OAuth clients).	Het toekennen en gebruiken van identifiers van systemen is (nog) niet gebonden aan normatieve eisen. GtK verzender en GtK ontvanger moeten daarom onderling en in afstemming met de gebruikte infrastructuur afspraken maken over de te gebruiken identifiers van systemen. Zie `iss`-velden in Z3.2.1.2 | COR: Authentication & Authorization (see page 481)

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
COR-2a-AA-05	BgZ Authn en Authz	GtK verzender, GtK ontvanger	GtK verzender en GtK ontvanger dienen gebruik te maken van dezelfde identifiers voor de systemen die opereren als autorisatie-servers (authorization server token endpoints).	Het toekennen en gebruiken van identifiers van systemen is (nog) niet gebonden aan normatieve eisen. GtK verzender en GtK ontvanger moeten daarom onderling en in afstemming met de gebruikte infrastructuur afspraken maken over de te gebruiken identifiers van systemen. Zie `aud`-velden in Z3.2.1.2 | COR: Authentication & Authorization (see page 481)
COR-2a-AA-06	BgZ Authn en Authz	GtK verzender	GtK verzender is in staat een digitale representatie van de in de context van een verwijzing veronderstelde toestemming aan te maken (`authorization_base`).	Omdat de `authorization_base` alleen door GtK verzender wordt verwerkt, worden de vorm en inhoud ervan bepaald door GtK verzender. GtK ontvanger mag niet afhankelijk zijn van het formaat of de inhoud van `authorization_base`. De vorm en inhoud van de `authorization_base` is (nog) niet gebonden aan normatieve eisen. Het bepalen van vorm en inhoud doet GtK verzender bij voorkeur in afstemming met de gebruikte infrastructuur. Zie (TA141) Z3.2.1.2 | COR: Authentication & Authorization#Authorization-base
COR-2a-AA-07	BgZ Authn en Authz	GtK verzender	GtK verzender is in staat een `authorization_grant` aan te maken die voldoet aan de specificaties	Specificaties: (TA141) 10.4.2 | TTA FHIR - Authorization#Authorization-grant
COR-2a-AA-08	BgZ Authn en Authz	GtK verzender	GtK verzender is in staat conform de specificaties een acces token request voor toegang tot het notificatie-endpoint aan te maken en aan GtK ontvanger te versturen.	Specificaties: (TA141) Z3.2.1.2 | COR: Authentication & Authorization#Access-token-request

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
COR-2a-AA-09	BgZ Authn en Authz	GtK verzender, GtK ontvanger	GtK verzender en GtK ontvanger dienen ervoor te zorgen dat het veld `sub` in de `authentication_grant` en het veld `client_id` in het access token request dezelfde waarde bevatten.	Specificaties: (TA141) Z3.2.1.2 | COR: Authentication & Authorization#Client-authentication , (TA141) Z3.2.1.2 | COR: Authentication & Authorization#Access-token-request
COR-2a-AA-10	BgZ Authn en Authz	GtK ontvanger	GtK ontvanger is in staat conform de specificaties een acces token request van GtK verzender voor toegang tot het notificatie server endpoint af te handelen.	Specificaties: (TA141) Z3.2.1.2 | COR: Authentication & Authorization#Access-token-request
COR-2a-AA-12	BgZ Authn en Authz	GtK ontvanger	GtK ontvanger is in staat een client assertion in de vorm van een `authentication_grant` aan te maken die voldoet aan de specificaties.	Specificaties: (TA141) 10.4.2 | TTA FHIR - Authorization#Client-authentication
COR-2a-AA-13	BgZ Authn en Authz	GtK ontvanger	GtK ontvanger is in staat conform de specificaties een acces token request voor toegang tot het resource-endpoint aan te maken en aan GtK verzender te versturen.	Inclusief eerder van GtK verzender ontvangen `authorization_grant`, welke de digitale representatie van de veronderstelde toestemming (`authorization_base`) bevat. Specificaties: (TA141) Z3.2.1.2 | COR: Authentication & Authorization#Access-token-request
COR-2a-AA-14	BgZ Authn en Authz	GtK verzender	GtK verzender is in staat conform de specificaties een acces token request van GtK ontvanger voor toegang tot het resource server endpoint af te handelen.	Specificaties: (TA141) Z3.2.1.2 | COR: Authentication & Authorization#Access-token-request

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
COR-2a-NS-01	network security	GtK verzender, GtK ontvanger	GtK verzender en GtK ontvanger maken gebruik van mutual TLS (mTLS) versie 1.3.	Zie 10.4.7 | Network level security (see page 211)
COR-2a-NS-02	network security	GtK verzender, GtK ontvanger	GtK verzender en GtK ontvanger maken gebruik van de juiste PKIo-certificaten.	Gebruikte PKIo-certificaten dienen te zijn uitgegeven onder de CA "Staat der Nederlanden Private Services CA – G1". Deze omvatten: • UZI-servercertificaat; of • PKIoverheid Private Services CA – G1 certificate Het betreft de systemen in de rol van token-server en -client, notification-server en -client en resource-server en -client. Zie 10.4.7 | Network level security (see page 211)
COR-2a-NS-03	network security	GtK verzender, GtK ontvanger	GtK verzender en GtK ontvanger maken gebruik van de juiste cryptografische algoritmes.	Verplicht gebruik van de volgende cryptografische algoritmes: • Certificate Verification: ECDSA of RSA • Key exchange: ECDHE • Bulk encryption: AES-256-GCM of ChaCha20-Poly1305 of AES-128-GCM • Hash functions: SHA-512 of SHA-384 of SHA-256 Zie https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1
COR-2a-NS-04	network security	GtK verzender, GtK ontvanger	GtK verzender en GtK ontvanger controleren minimaal ieder uur door middel van CRL of OCSP de geldigheid van de certificaten van systemen waarmee transacties plaatsvinden.	Zie 10.4.7 | Network level security (see page 211)

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
COR-2a-NS-05	network security	GtK verzender, GtK ontvanger	Wanneer GtK verzender en GtK ontvanger de geldigheid van een UZI-servercertficaat controleren, doen zij dit op basis van de afspraken in het Certification Practice Statement (CPS) UZI-register.	Zie Certification Practice Statement (CPS) | Zorg CSP[143], artikel 4.5.2 CRL's: https://www.zorgcsp.nl/certificate-revocation-lists-crl-s
COR-2a-NS-06	network security	GtK verzender, GtK ontvanger	Wanneer GtK verzender en GtK ontvanger de geldigheid van een PKIo-servercertficaat controleren, doen zij dit op basis van de afspraken in het Certification Practice Statement (CPS) PKIoverheid.	Zie https://cps.pkioverheid.nl/cps_unified-v5_0-en.htm, hoofdstuk 2
COR-2b-trans-01	Transactions - BgZ interactions	GtK verzender	GtK verzender is in staat een Workflow-Task aan te maken	Transactie 1 van Z3.2.1.1 | COR - Data interactions (see page 477)
COR-2b-trans-02	Transactions - BgZ interactions	GtK verzender	GtK verzender is in staat een notificatie-create-request te versturen	Transactie 2 van Z3.2.1.1 | COR - Data interactions (see page 477) Specificatie: (TA141) 10.5.1 | Twiin-01 | Send Notification Task#Request-message

143. https://www.zorgcsp.nl/certification-practice-statement-cps

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
COR-2b-trans-03	Transactions - BgZ interactions	GtK ontvanger	GtK ontvanger is in staat een binnenkomend notificatie-create-request af te handelen en een passende response te versturen	Transactie 3 van Z3.2.1.1 | COR - Data interactions (see page 477) Specificatie: (TA141) 10.5.1 | Twiin-01 | Send Notification Task#Response-message
COR-2b-trans-04	Transactions - BgZ interactions	GtK verzender	GtK verzender is in staat een notificatie-create-request te versturen wanneer de dataset van de verwijzing is geüpdatet	Transactie 4 van Z3.2.1.1 | COR - Data interactions (see page 477) Specificatie:(TA141) 10.5.1 | Twiin-01 | Send Notification Task#Request-message
COR-2b-trans-05	Transactions - BgZ interactions	GtK ontvanger	GtK ontvanger is in staat een naar aanleiding van een geüpdatete dataset binnenkomend notificatie-create-request af te handelen en een passende response te versturen	Transactie 5 van Z3.2.1.1 | COR - Data interactions (see page 477) Specificatie: (TA141) 10.5.1 | Twiin-01 | Send Notification Task#Response-message
COR-2b-trans-06	Transactions - BgZ interactions	GtK verzender	GtK verzender is in staat een notificatie-update-request te versturen wanneer GtK verzender de notificatie wil annuleren of intrekken.	Transactie 6 van Z3.2.1.1 | COR - Data interactions (see page 477) Specificatie: (TA141) 10.5.2 | Twiin-02 | Cancel Notification Task#Request-message

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
COR-2b-trans-07	Transactions - BgZ interactions	GtK ontvanger	GtK ontvanger is in staat een binnenkomend notificatie-update-request af te handelen en een passende response te versturen.	Transactie 7 van Z3.2.1.1 | COR - Data interactions (see page 477) Specificatie: (TA141) 10.5.2 | Twiin-02 | Cancel Notification Task#Notification-response
COR-2b-trans-08.read	Transactions - BgZ interactions	GtK ontvanger	GtK ontvanger is in staat read-operaties uit de notificatie-taak uit te voeren op het resource-endpoint van GtK verzender.	Transactie 8 van Z3.2.1.1 | COR - Data interactions (see page 477) Specificatie: 10.5.5 | Twiin-05 | Retrieve Resource (see page 232) De read-operaties zijn opgenomen in de notificatie-task onder Task.input:read-available-resources.
COR-2b-trans-09.read	Transactions - BgZ interactions	GtK verzender	GtK verzender is in staat binnenkomende read-requests af te handelen en een passende response te versturen.	Transactie 9 van Z3.2.1.1 | COR - Data interactions (see page 477) Specificatie: 10.5.5 | Twiin-05 | Retrieve Resource (see page 232)
COR-2b-trans-08.search	Transactions - BgZ interactions	GtK ontvanger	GtK ontvanger is in staat search-operaties uit de notificatie-taak uit te voeren op het resource-endpoint van GtK verzender.	Transactie 8 van Z3.2.1.1 | COR - Data interactions (see page 477) Specificatie: 10.5.4 | Twiin-04 | Search Resource(s) (see page 230) De search-operaties zijn opgenomen in de notificatie-task onder Task.input:query-available-resources.

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
COR-2b-trans-09.search	Transactions - Bg Z interactions	GtK verzender	GtK verzender is in staat binnenkomende search-requests af te handelen en een passende response te versturen.	Transactie 9 van Z3.2.1.1 | COR - Data interactions (see page 477) Specificatie: 10.5.4 | Twiin-04 | Search Resource(s) (see page 230)
COR-2b-trans-10	Transactions - Bg Z interactions	GtK ontvanger	GtK ontvanger is in staat een read-operatie voor het ophalen van de Workflow-task uit te voeren op het resource-endpoint van GtK verzender.	Transactie 10 van Z3.2.1.1 | COR - Data interactions (see page 477) Specificatie: 10.5.3 | Twiin-03 | Get Workflow Task (see page 228) De indicator voor de aanwezigheid van een workflow-task is opgenomen in de notificatie-task onder Task.input:get-worflow-task.valueBoolean (waarde is `true`).
COR-2b-trans-11	Transactions - Bg Z interactions	GtK verzender	GtK verzender is in staat een binnenkomende read-request op de workflow-task af te handelen en een passende response te versturen.	Transactie 11 van Z3.2.1.1 | COR - Data interactions (see page 477)
COR-2b-trans-12.read	Transactions - Bg Z interactions	GtK ontvanger	GtK ontvanger is in staat read-operaties uit de workflow-taak uit te voeren op het resource-endpoint van GtK verzender.	Transactie 12 van Z3.2.1.1 | COR - Data interactions (see page 477) Specificatie: 10.5.5 | Twiin-05 | Retrieve Resource (see page 232) De read-operaties zijn opgenomen in de workflow-task onder `Task.input:read-available-resources`.

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
COR-2b-trans-13.read	Transactions - BgZ interactions	GtK verzender	GtK verzender is in staat binnenkomende read-requests af te handelen en een passende response te versturen.	Transactie 13 van Z3.2.1.1 | COR - Data interactions (see page 477) Specificatie: 10.5.5 | Twiin-05 | Retrieve Resource (see page 232)
COR-2b-trans-12.search	Transactions - BgZ interactions	GtK ontvanger	GtK ontvanger is in staat search-operaties uit de workflow-taak uit te voeren op het resource-endpoint van GtK verzender.	Transactie 12 van Z3.2.1.1 | COR - Data interactions (see page 477) Specificatie: 10.5.4 | Twiin-04 | Search Resource(s) (see page 230) De search-operaties zijn opgenomen in de workflow-task onder `Task.input:query-available-resources`.
COR-2b-trans-13.search	Transactions - BgZ interactions	GtK verzender	GtK verzender is in staat binnenkomende search-requests af te handelen en een passende response te versturen	Transactie 13 van Z3.2.1.1 | COR - Data interactions (see page 477) Specificatie: 10.5.4 | Twiin-04 | Search Resource(s) (see page 230)

2. Aanvullende ketentest eisen

De eisen in dit hoofdstuk zijn niet nodig zijn voor de Twiin validatie van de zorgtoepassing. Deze eisen zijn wel nodig om te voldoen aan de ketentest, de informatiestandaard, de VIPP-eisen en eventuele andere functionele eisen.

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
COR-1-FO-08	FO (Nictiz)	GtK verzender	GtK verzender moet een verwijsbrief in document-formaat kunnen sturen bij verwijzing naar een andere zorginstelling of zorgverlener.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.0_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
COR-1-FO-26	FO Nictiz	EPD ontvanger	Voor de systemen 'achter' GtK ontvanger geldt: Een EPD moet in staat zijn een ontvangen of geraadpleegde verwijsbrief over te nemen wanneer dat medisch relevant is.	Specificatie: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.0_BgZ_MSZ_Informatiestandaard#Systemen_en_systeemrollen
COR-1-VIPP5-1	VIP P 5	GtK verzender	GtK verzender kan de correspondentie verzenden naar andere instellingen van Medisch Specialistische Zorg.	Zie Handreiking VIPP5 assessments[144], bijlage II, paragraaf 1.5, alinea module 3 Zie https://www.vipp-programma.nl/over-vipp/doelstellingen
COR-1-VIPP5-2	VIP P 5	GtK ontvanger	GtK ontvanger kan de correspondentie ontvangen vanuit een andere instelling van Medisch Specialistische Zorg.	Zie Handreiking VIPP5 assessments[145], bijlage II, paragraaf 1.5, alinea module 3 Zie https://www.vipp-programma.nl/over-vipp/doelstellingen
COR-1-VIPP5-4	VIP P 5	Twiin deelnemer	De Twiin deelnemer (zorgorganisatie) heeft procedures rondom het uitwisselen van de correspondentie met andere instellingen van Medisch Specialistische Zorg beschreven en geïmplementeerd.	Zie Handreiking VIPP5 assessments[146], bijlage II, paragraaf 1.5, alinea module 3 Zie https://www.vipp-programma.nl/over-vipp/doelstellingen
COR-1-AVG-01	TA NP	Nieuwe behandelaar	De nieuwe behandelaar mag alleen de gegevens opvragen die relevant zijn voor de uitvoering van de nieuwe behandelrelatie.	De nieuwe behandelaar (en de zorgorganisatie waarvan zij/hij deel uitmaakt) is ervoor verantwoordelijk om dataverzoeken proportioneel te houden.

144. https://www.norea.nl/uploads/bfile/367e3045-86fc-49cb-8f01-0ef470105695
145. https://www.norea.nl/uploads/bfile/367e3045-86fc-49cb-8f01-0ef470105695
146. https://www.norea.nl/uploads/bfile/367e3045-86fc-49cb-8f01-0ef470105695