Twiin Afsprakenstelsel 1.3 voor consultatie

8 okt 2024 Dit is de 1.3 versie van het afsprakenstelsel voor consultatie

Het Twiin Afsprakenstelsel is publiek beschikbaar voor iedereen met interesse in landelijke beschikbaarheid en uitwisseling van gezondheidsgegevens.

Wat is Twiin?

Twiin is een samenwerkingsverband waarin zorgaanbieders, leveranciers en partners werken aan het Twiin Afsprakenstelsel.

Hoe meer zorgorganisaties gaan samenwerken in een keten of netwerk, hoe meer relaties er ontstaan. Nu is het vaak zo dat bij iedere uitwisseling van gezondheidsgegevens steeds opnieuw afspraken gemaakt worden. Dit gebeurt in Nederland meestal op lokaal of regionaal niveau waardoor onderling verschillende afspraken ontstaan. Om deze verschillen te beperken en landelijke opschaling mogelijk te maken, is een verbindend afsprakenstelsel nodig: het Twiin Afsprakenstelsel.

De meerwaarde van Twiin voor zorgaanbieders

- **Eén handtekening:**

Landelijk gezondheidsgegevens delen vraagt in de huidige situatie om afspraken met alle zorgaanbieders waarmee je wilt delen. Dit kan oplopen tot tientallen handtekeningen onder individuele samenwerkingsovereenkomsten. Aansluiten bij Twiin betekent één handtekening op één overeenkomst.

- **Veilig en betrouwbaar beschikbaar maken en delen van gegevens**:

Wanneer jij door Twiin bent gevalideerd voor een zorgtoepassing, kun je gegevens delen met alle andere gevalideerde Twiin Deelnemers voor die zorgtoepassing. Validatie zorgt ervoor dat je erop kunt vertrouwen dat alle deelnemers voldoen aan dezelfde afspraken.

- **Actief meedenken & passende ondersteuning:**

Twiin werkt graag samen met jou aan een actueel en praktisch toepasbaar afsprakenstelsel. Door mee te doen aan Twiin, oefen je invloed uit op de inhoud van het Twiin Afsprakenstelsel.

De meerwaarde van Twiin voor leveranciers

- **Technische afspraken:**

Samen met andere GtK Leveranciers werk je aan technische afspraken. Daarmee kunnen applicaties onderling veilig en betrouwbaar gegevens uitwisselen. Aansluiten bij Twiin betekent gezamenlijk werken aan generieke technische afspraken.

- **Innovatie:**

Door te testen en mee te denken help je ons verder innoveren. Zo laten we het Twiin Afsprakenstelsel in de praktijk werken. Klanten van GtK Leveranciers kunnen erop vertrouwen dat landelijke databeschikbaarheid wordt gerealiseerd.

- **Actief meedenken**

Twiin werkt graag samen met jou aan een actueel en praktisch toepasbaar afsprakenstelsel. Door mee te doen aan Twiin, oefen je invloed uit op de inhoud van het Twiin Afsprakenstelsel.

Wat is het Twiin Afsprakenstelsel?

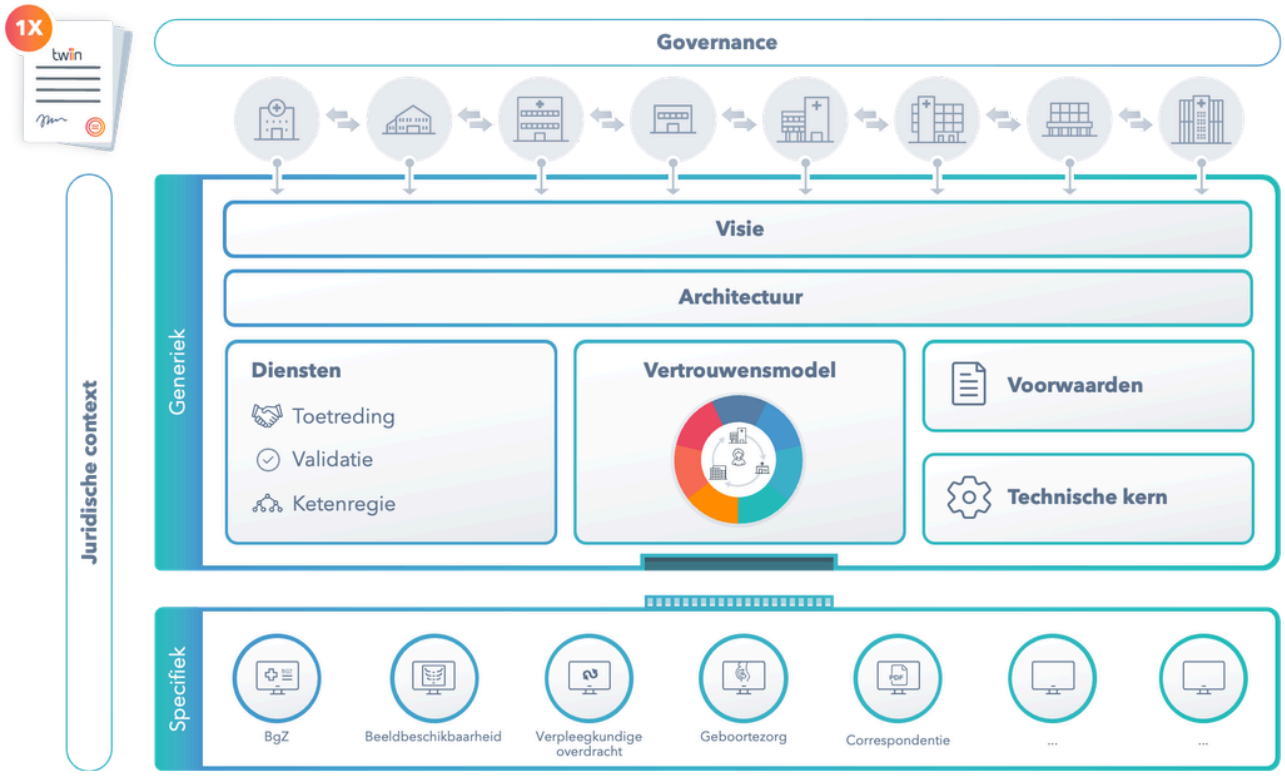
Het Twiin Afsprakenstelsel is een set samenwerkingsafspraken voor het delen en beschikbaar maken van gezondheidsgegevens; veilig en betrouwbaar, tussen zorgaanbieders, zorgnetwerken en voorzieningen, interoperabel op alle lagen en samen met zorgaanbieders en leveranciers.

Afspraken in samenhang

Het afsprakenstelsel bevat een generiek deel met daarin 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 patiënt 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 implementatie van zorgtoepassingen.

Generiek

Twiin heeft gekozen voor een generieke – en daardoor breed toepasbare - opzet. Standaardisatie en herbruikbaarheid zijn hierbij belangrijke uitgangspunten. Knooppunten en generieke functies, eventueel ingevuld door één of meerdere gemeenschappelijke voorzieningen, vormen de basis voor de verbindende architectuur van Twiin. Op deze manier kunnen verschillende communicatiepatronen toegepast worden.



Statement

Twiin volgt de ontwikkelen en NEN-normering 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

Leeswijzer

In de 1 | Leeswijzer vind je meer uitleg over de indeling van het Twiin Afsprakenstelsel en hoe je door het Afsprakenstelsel heen kunt navigeren.

Contact

Heb je vragen? Mail naar info@twiin.nl

Website van Twiin: www.twiin.nl

De afspraken in deze versie passen bij de huidige ontwikkelingen in het veld van digitale uitwisseling. Ontwikkelingen in wetgeving, ICT-innovaties, nieuwe inzichten en toetreders op de markt, houden we met onze samenwerkingspartners nauwlettend in de gaten en verwerken we in volgende versies. Het Twiin Afsprakenstelsel is een solide basis, waarop we samen verder groeien.

1 | Leeswijzer

Het Twiin Afsprakenstelsel kent een logische opbouw in menustructuur. Daarnaast is per doelgroep aangegeven welke onderdelen vooral relevant zijn. De wijzigingen ten opzichte van de vorige release zijn opgenomen in hoofdstuk 2 | Release informatie.

Menustructuur

- Twiin Afsprakenstelsel WIP
- Twiin Implementatiewijzer Zorgtoepassingen
- Twiin Ontwikkelsupplement

Klik op een onderdeel om direct naar het hoofdstuk te gaan.

Per doelgroep

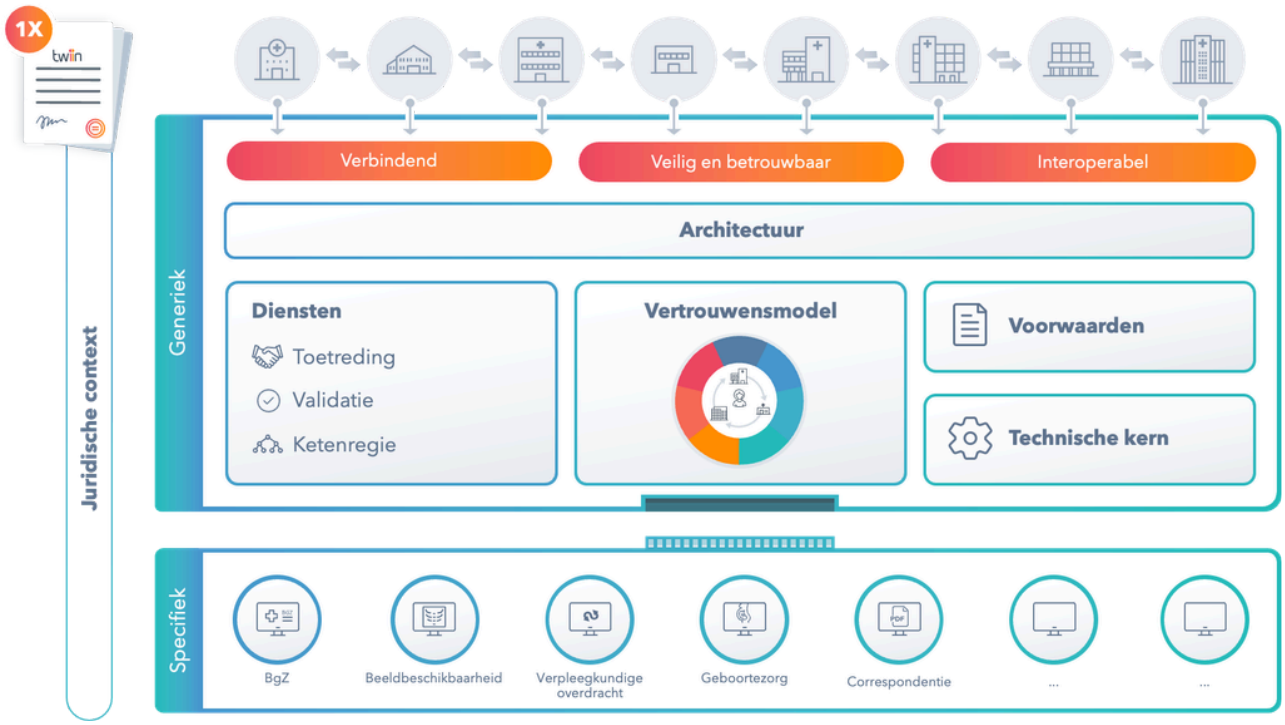
Per doelgroep een handreiking welke onderdelen van het afsprakenstelsel voor de doelgroep het meest relevant zijn: 1.1 | Doelgroepen

Begrippen

De begrippen die gebruikt worden in het Twiin Afsprakenstelsel staan op deze pagina toegelicht: 1.2 | Begrippen .

Samenhang Twiin Afsprakenstelsel

Onderstaand overzicht toont de samenhang tussen de verschillende onderdelen van het afsprakenstelsel.



1.1 | Doelgroepen

Voor wie is het Twiin Afsprakenstelsel?

Het Twiin Afsprakenstelsel is publiek beschikbaar voor iedereen met interesse in landelijke beschikbaarheid en uitwisseling van gezondheidsgegevens. Hieronder stippen we per doelgroep aan welke onderdelen relevant kunnen zijn.

Zorgaanbieders

Zorgaanbieders beslissen om als deelnemer aan te sluiten bij het Twiin Afsprakenstelsel. Relevante onderdelen zijn:

- Bestuurders: 3 | Visie , 6 | Governance , 5 | Vertrouwensmodel
- ICT Management: 3 | Visie 5 | Vertrouwensmodel 6 | Governance 9 | Voorwaarden 8 | Diensten 4 | Architectuur Twiin Implementatiewijzer 1.3 Zorgtoepassingen
- Juristen: 7 | Juridische context 6 | Governance 5 | Vertrouwensmodel 7 | Juridische context 9 | Voorwaarden
- Security & Privacy officers: 7 | Juridische context 5 | Vertrouwensmodel 7 | Juridische context 9 | Voorwaarden
- Projectleiders: 5 | Vertrouwensmodel 8 | Diensten Twiin Implementatiewijzer 1.3 Zorgtoepassingen
- Architecten, Leveranciers, Ontwerpers, Implementators, Beheerders; 10 | Technische kern Twiin Implementatiewijzer 1.3 Zorgtoepassingen 5 | Vertrouwensmodel Twiin Implementatiewijzer 1.3 Zorgtoepassingen 9 | Voorwaarden

Zorgverleners

Zorgverleners beslissen bij iedere behandeling of zij patiëntgegevens willen uitwisselen.

- Belangrijke onderdelen van het afsprakenstelsel: 3 | Visie 5 | Vertrouwensmodel

Patiënten

Dat voor het delen van gegevens de toestemming van de patiënt nodig is, staat beschreven in het 5 | Vertrouwensmodel van het Twiin Afsprakenstelsel. We voorzien ook dat patiënten inzicht krijgen in hun gegevens via hun persoonlijke gezondheidsomgeving (PGO). De ontsluiting hiervan is nog niet in deze versie van het afsprakenstelsel beschreven.

Leveranciers

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.

- Belangrijke onderdelen van het afsprakenstelsel: 10 | Technische kern Twiin Implementatiewijzer 1.3 Zorgtoepassingen 5 | Vertrouwensmodel Twiin Implementatiewijzer 1.3 Zorgtoepassingen 9 | Voorwaarden

Regio's

In verschillende regio's in Nederland werken zorgaanbieders samen om (elektronische) informatie-uitwisseling te bevorderen. Zij worden daarbij vaak ondersteund door een Regionale Samenwerkingsorganisatie (RSO). Een RSO is door de zorgaanbieders zelf opgericht en heeft daardoor een breed mandaat. RSO's kunnen de rol uitvoeren van Twiin Dienstverlener. Ook kunnen zij in opdracht van de deelnemer taken en verantwoordelijkheden van de GtK Beheerder op zich nemen.

- Belangrijke onderdelen van het afsprakenstelsel: 5 | Vertrouwensmodel 8 | Diensten 9 | Voorwaarden 10 | Technische kern Twiin Implementatiewijzer 1.3 Zorgtoepassingen

1.2 | Begrippen

Het Twiin Afsprakenstelsel sluit waar mogelijk aan bij begrippen uit wet- en regelgeving en de DIZRA.

Nictiz; Begrippen Duurzaam Informatiestelsel	Begrippen
Nictiz; Thesaurus Zorg en Welzijn	https://thesauruszorgenwelzijn.multites.net/
DIZRA; Begrippen Duurzaam Informatiestelsel Referentiearchitectuur	Begrippenlijst | DIZRA
NEN-normen en -begrippen	Begrippen bij NEN worden gedefinieerd in de context van de norm. Zie de begrippenlijst per NEN-norm.
iStandaarden; Begrippen iStandaarden in de Zorg en Ondersteuning van Zorg Instituut Nederland	Begrippenlijst
Begrippenlijst in de Handreiking voor het schrijven van de informatieparagraaf van een kwaliteitsstandaard	https://www.zorginzicht.nl/binaries/content/assets/zorginzicht/algemeen-ondersteuning/handreiking-voor-het-schrijven-van-de-informatieparagraaf-bij-een-kwaliteitsstandaard.pdf

In de Twiin-begrippenlijst beperken we ons tot de Twiin-specifieke begrippen.

1. Begrip: Beheerovereenkomst

Twiin Deelnemers die een GtK Beheerder inschakelen, sluiten een beheeroverkomst met de GtK Beheerder. De Twiin Organisatie stelt een model beheerovereenkomst beschikbaar die partijen kunnen gebruiken om passende afspraken met elkaar te maken.

2. Begrip: Deelnemersovereenkomst

De overeenkomst die Twiin Deelnemers sluiten om toe te treden tot het Twiin Afsprakenstelsel.

3. Begrip: Dienstverleningsovereenkomst

De overeenkomst die Twiin Deelnemers sluiten met een Twiin Dienstverlener.

De Twiin Dienstverlener voert regie op de implementatie, ontwikkeling en het beheer van één of meer zorgtoepassingen binnen een regio en/of binnen een categoraal netwerk. Daarnaast ondersteunt de Twiin Dienstverlener de Twiin Deelnemers bij het voldoen aan het Twiin Afsprakenstelsel.

4. Begrip: Geïdentificeerde patiënt

Een patiënt waarvan de identiteit is vastgesteld door de persoonsgegevens te verifiëren op basis van het BSN.

5. Begrip: Dossierhouder

Zorgaanbieder in het bezit van medische patiëntgegevens, die hij (via een uitwisselingssysteem) beschikbaar kan stellen aan een dossierraadpleger, of kan versturen naar een dossierontvanger.

6. Begrip: Dossierontvanger

Een natuurlijk persoon en/of organisatie die medische gegevens van een geïdentificeerde patiënt opgestuurd krijgt van een dossierhouder.

7. Begrip: Dossierraadpleger

Een natuurlijk persoon en/of organisatie die bevoegd is om medisch inhoudelijke gegevens in te zien van een geïdentificeerde patiënt.

8. Begrip: Gemeenschappelijke voorzieningen

Een product of dienst gericht op het ondersteunen van een generieke functie. (Bron: Datavoorgezondheid.nl)

9. 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.

10. Begrip: GtK

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. 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.

> Een GtK hoeft niet per se uit één uitwisselingssysteem of één (aparte) applicatie te bestaan. Een GtK kan gevormd worden door meerdere onderdelen. Deze onderdelen zijn dan allen benodigd om via het koppelvlak conform de Twiin afspraken te communiceren. Onderdelen kunnen bijvoorbeeld zijn: de broker, XIS, EPD of het uitwisselingssysteem. De eisen aan een GtK kunnen gezien worden als de koppelvlak-specificaties van het Twiin Afsprakenstelsel.

Meer uitleg en context over het begrip GtK onder het onderdeel architectuur 4 | Architectuur

11. Begrip: GtK Beheerder

Een organisatie die namens de Twiin Deelnemer invulling geeft aan het technisch beheer van het GtK.

12. Begrip: GtK Leverancier

Leverancier van een applicatie die een intentieverklaring heeft getekend om te komen tot validatie voor één of meer zorgtoepassingen, dan wel beschikt over een gevalideerde GtK.

13. Begrip: Regio

Een geografisch afgebakend deel van Nederland dat (idealiter) valt onder de verantwoordelijkheid van een regionale samenwerkingsorganisatie (RSO).

N.B. In Nederland zijn 12 RSO's, die lid zijn van RSO Nederland. Er zijn ook regio's die niet aangesloten zijn bij een RSO, maar waarbinnen wel een vorm van samenwerking op zorg-ICT bestaat en regio's waar dit nog geheel ontbreekt.

14. 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.

15. Begrip: Servicedesk Twiin Deelnemer

De eigen servicedesk die iedere Twiin Deelnemer zelf inricht inclusief contract met ondersteunende leveranciers of door een GtK Beheerder laat inrichten.

16. Begrip: Tijdlijn

Een tijdlijn is een integraal, plaats- en tijdonafhankelijk overzicht van statussen en resultaten, over de grenzen van de zorginstelling heen.

Het kent een samenhangende chronologische weergave, waardoor het benodigde inzicht en overzicht binnen de werkomgeving van de zorgverlener ontstaat en het biedt informatie waarvan de medische inhoudelijke integriteit, juistheid, tijdigheid, volledigheid, beschikbaarheid en performance geborgd is. Deze tijdlijn bevat alle voor de usecase relevante gegevens. Per usecase wordt bepaald of er een tijdlijn nodig is en welke gegevens de tijdlijn bevat.

17. Begrip: Twiin Bestuur

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. Op termijn wordt deze rol ingevuld door een eigenaarsraad met vertegenwoordigers van de twee overlegtafels die benoemd zijn in het reglement. Die eigenaarsraad zal dan worden ondergebracht bij een bestaande of nog op te richten rechtspersoon.

18. Begrip: Twiin Casemanager

Persoon werkzaam voor de Twiin Organisatie met inhoudelijke kennis voor het proces dat hij/zij begeleidt.

19. 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.

20. 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.

21. Begrip: Twiin Organisatie

Eindverantwoordelijke voor het Twiin Afsprakenstelsel met de rol van houder.

22. Begrip: Twiin Serviceportaal

Een communicatieplatform voor ketenregie met contactgegevens, versiebeheer en gemelde Incidenten (hierna: “Twiin Serviceportaal” (Supportal). De Twiin Organisatie zorgt voor de inrichting van het serviceportaal.

23. Begrip: Twiin Vertrouwensmodel

Het geheel van technische, organisatorische en juridische waarborgen voor het vertrouwen in de landelijke elektronische uitwisseling van medische gegevens.

24. Begrip: Twiin Voorwaarden

De voorwaarden waaraan Twiin Deelnemers zijn gehouden door ondertekening van de Twiin Deelnemersovereenkomst.

25. Begrip: Tijdlijn

Een tijdlijn is een integraal, plaats- en tijdonafhankelijk overzicht van statussen en resultaten, over de grenzen van de zorginstelling heen.

Het kent een samenhangende chronologische weergave, waardoor het benodigde inzicht en overzicht binnen de werkomgeving van de zorgverlener ontstaat en het biedt informatie waarvan de medische inhoudelijke integriteit, juistheid, tijdigheid, volledigheid, beschikbaarheid en performance geborgd is. Deze tijdlijn bevat alle voor de usecase relevante gegevens. Per usecase wordt bepaald of er een tijdlijn nodig is en welke gegevens de tijdlijn bevat.

26. Begrip: Zorgtoepassing

Een geautomatiseerde oplossing voor gegevensbeschikbaarheid die een specifiek zorgproces ondersteunt.

1.3 | Afsprakenstelsel in PDF

We publiceren het Twiin Afsprakenstelsel openbaar op het internet via Confluence. Hierdoor kan je makkelijk en overzichtelijk door de voor jou relevante onderdelen van het afsprakenstelsel heen klikken en heb je altijd de meest recente versie.

Toch liever een pdf van het Twiin Afsprakenstelsel?

Download hem hier.

2 | Release informatie

Het Twiin Afsprakenstelsel wordt continu doorontwikkeld: we zijn betrokken bij landelijke ontwikkelingen en leren van ervaringen tijdens beproevingen. Deze ervaringen gebruiken we om een volgende release aan te scherpen. Twiin werkt in een vastgestelde periode concrete onderwerpen uit, die we in opeenvolgende releases publiceren. In deze sectie bespreken we de meest actuele release van het Twiin Afsprakenstelsel en de wijzigingen ten opzichte van de vorige versie.

Heb je suggesties ter verbetering, neem dan contact met ons op via info@twiin.nl.

Onderstaande tabel toont de belangrijkste wijzigingen die zijn doorgevoerd met een verwijzing naar de desbetreffende pagina. Redactionele wijzigingen worden niet apart benoemd.

Release - Nr	Betreft	Verwijzing
	8 okt 2024 Minor Release 1.3 - voor consultatie	
1.3 - 24	De term GtK beheerder aangepast. De Twiindeelnemer is verantwoordelijk voor het beheer. De beheerder is uitvoerder (in opdracht van de Twiin deelnemer).	Begrip: GtK Beheerder
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 Routing in het Twiin Afsprakenstelsel is opgenomen.	10.2.8 | TTA - Addressing 10.3.1 | Twiin-01 | Send Notification Task 9.1 | Voorwaarden Twiin Deelnemer 5.19b Z1.5 | BgZ: PvE BgZ-3-10
1.3 - 22	Nieuwe begrippen toegevoegd aan de begrippenlijst: Begrip: Servicedesk Twiin Deelnemer, Begrip: Incident, Begrip: Twiin Serviceportaal	1.2 | Begrippen
1.3 - 21	Verwijzing naar eIDAS betrouwbaarheidsniveau's toegevoegd.	7 | Juridische context (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 Z1.5 | BgZ: PvE 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).	10.1.9 | Generieke functie - Logging Eisen logging

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
1.3 - 17	GZN-eisen voor verbindingen tussen de GTK's vervalt en zijn vervangen door neutrale eisen voor veilig-netwerk die volgen uit NEN7522. Zie specifiek de vijf punten in Voorwaarden GtK nr. 1.3. De Voorwaarden GtK Beheer zijn aangepast als volgt: • Voorwaarde nr. 2.1 is aangevuld. SLA moet ook zien op beschikbaarheid; • Voorwaarde nr. 5.1 is aangevuld. SLA moet ook zien op incidentafhandeling en beschikbaarheid (minimaal 99,5%); • Voorwaarde nr. 5.2 is daarmee komen te vervallen.	9.1 | Voorwaarden Twiin Deelnemer, 9.4 | Voorwaarden GtK, 9.3 | Voorwaarden GtK Beheer
1.3 - 16	Reglement geüpdatet op een aantal punten: inhoudelijke expertise leden overlegtafels, 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
1.3 - 15	Deelnemersovereenkomst aangepast op de volgende punten: • In artikel 1.a zijn de definities GtK en GtK Beheerder zijn 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
1.3 - 14	De bestaande Verklaring GtK Leverancier toegevoegd aan hoofdstuk goverance en een proces toegevoegd voor het verkrijgen van die verklaring.	6.4 | Verklaring GtK Leverancier 8.1.4 | Verkrijgen Verklaring GtK Leverancier

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 , 7 | Juridische context , 9.1 | Voorwaarden Twiin Deelnemer 10.1 | Kern Volume 1 - Communicatiepatroon Overview
1.3 - 12	Definitie van identificatie aangescherpt. Ook is aangepast dat het wetsvoorstel Diaz inmiddels in behandeling is.	5.1 | Vertrouwen: Identificatie , 5 | Vertrouwensmodel
1.3 - 11	Verhelderd dat veronderstelde toestemming alleen is toegestaan bij de use case verwijzen en dat WGBO-toestemming nodig is bij de use case opvragen dossier.	5.5 | Vertrouwen: Patiënttoestemming , 9.1 | Voorwaarden Twiin Deelnemer
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
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. De voorwaarden 5.12 en 5.13 samengevoegd in één nieuwe voorwaarden 5.12 ter verduidelijking dat de autorisatieafspraken worden gevolgd zoals beschikbaar voor de Zorgtoepassing en dat deze rolgebaseerd is. De verplichting om een MAP te gebruiken die gebaseerd is op UZI-rolcodes komt hiermee te vervallen.	9.1 | Voorwaarden Twiin Deelnemer
1.3 - 8	Update H3.1 Twiin in relearie tot Wegiz, NVS,LVS en LDN	3.1 Twiin in relatie tot EHDS, Wegiz, NVS, LVS en LDN
1.3 - 7	Autoristatieafspraken aangepast. De verzendende partij moet de autorisatierichtlijn BgZ toepassing (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 ; preconditie toegevoegd dat de behandelend arts geautoriseerd is; • Autorisatie BgZ Z1.4.4 | BgZ: Autorisatie : toelichting gegeven. • Eis BgZ-2a-AA-11 • User_ID is verplicht om altijd mee te sturen. User_role en subrole zijn conditioneel verplicht: 10.2.5 | TTA FHIR - Authentication & Authorization • Aanscherping vertrouwensmodel: 5.3 | Vertrouwen: Autorisatie	Z1.1.1 | Uitwisseling BgZ bij verwijzing of overdracht , Z1.4.4 | BgZ: Autorisatie , Z1.5 | BgZ: PvE , 10.1.6 | Generieke functie - Autorisatie , 10.2.5 | TTA FHIR - Authentication & Authorization , 5.3 | Vertrouwen: Autorisatie

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.	4 | Architectuur
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
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
1.3 - 3	Proces incidentmelding en proces handhaving toegevoegd ter uitwerking van de dienst ketenregie.	8.3.1 | Incidentmelding, 8.4 | Handhaving
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

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 1 - Functioneel overzicht

	2 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	4 | Architectuur, 3.1 Twiin in relatie tot EHDS, Wegiz, NVS, LVS en LDN

	voorzieningen. Daar stond ook een verwijzing naar landelijke ontwikkelingen wat een onnodige dubbeling was.	
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
1.2.1 - 23	Toepassen juiste terminologie (Resource Server → Responding GtK)	10.3.3 | Twiin-03 | Get workflow Task
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.]	10.2.3 | TTA FHIR - Notified pull
1.2.1 - 21	Toetreden deelnemer toegelicht in de zin dat deelnemer aangeeft welke Twiin Dienstverlener is betrokken.	8.1.1 | Toetreden Deelnemer
1.2.1 - 20	Releasebeleid toegelicht (vaststellen omvat ook release roadmap voor onderwerpen die nog in ontwikkeling zijn)	6.5 | Releasebeleid , 6.6 | Reglement
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: Patiënttoestemming
1.2.1 - 18	Aanscherping: Zorgverleners worden geïdentificeerd met een landelijk uniek nummer (die ook uniek blijft).	5.1 | Vertrouwen: Identificatie 9.1 | Voorwaarden Twiin Deelnemer
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 , 10.4.5 | IHE ITI-40 | Provide X-User Assertion , 10.2.5 | TTA FHIR - Authentication & Authorization
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.	4.1 | Twiin Principes
1.2.0 - 15	Implementatiewijzer Verpleegkundige overdracht bevat een informatieve toelichting.	Z4 | VO: implementatiewijzer Verpleegkundige overdracht - 1.2.0 Informative UNDEFINED
1.2.0 - 14	Implementatiewijzer Zorgtoepassing Geboortezorg bevat een informatieve toelichting.	Z5 | IGD: implementatiewijzer Geboortezorg 1.2.0 Informative UNDEFINED
1.2.0 - 13	Implementatiewijzer Zorgtoepassing Beeldbeschikbaarheid herschreven in 3 volumes voor beproeving (status trial) inclusief PvE.	Z2 | BB: Implementatiewijzer Beeldbeschikbaarheid 1.3.0 Trial
1.2.0 - 12	Implementatiewijzer Zorgtoepassing Correspondentie toegevoegd in 3 volumes voor beproeving (status trial) inclusief PvE.	Z3 | COR: implementatiewijzer Correspondentie 1.2.0 Trial

1.2.0 - 11	Implementatiewijzer Zorgtoepassing BgZ herschreven in 3 volumes voor beproeving (status trial) inclusief PvE.	Z1 | BgZ: Implementatiewijzer Basisgegevensset Zorg - 1.2.0 Trial
1.2.0 - 10	TA Notified Pull (Technical Agreement) Notified Pull opgenomen in het Twiin Afsprakenstelsel en zorgtoepassing BgZ.	10.2.3 | TTA FHIR - Notified pull Z1.2.1 | TTA Exchanging BgZ - FHIR Notified Pull
1.2.0 - 9	Zorgtoepassingen onderdeel afsprakenstelsel naast de " generieke kern" met eigen versienr.	Twiin Implementatiewijzer 1.3 Zorgtoepassingen
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
1.2.0 - 7	Diensten zijn geactualiseerd en herschreven. Processen zijn ondergebracht bij de bijbehorende diensten waardoor het onderdeel processen is vervallen.	8 | Diensten
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
1.2.0 - 5	Onderdeel Grondslag hernoemd naar Visie en volledig herschreven	3 | Visie
1.2.0 - 3	Begrip GtK verduidelijkt	Begrip: GtK
1.2.0 - 2	Voorwaarden (voorheen onderdeel van de aansluit- en implementatiewijzer) op het hoogste niveau gebracht en verbeterd, verduidelijkt, beknopter en concreter gemaakt Begrip en voorwaarden GtK-netwerk is vervallen en is opgenomen als eis aan het GtK.	9 | Voorwaarden
1.2.0 - 1	Releasebeleid toegevoegd	6.5 | Releasebeleid

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

Releasebeleid

Het releasebeleid is een onderdeel van de governance, zie 6.5 | Releasebeleid

Vorige versies

Klik hier om uit te vouwen...

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 en daaruit voortvloeiende aanpassing in validatieproces, voorwaarden 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

- Vertrouwensmodel geactualiseerd
- Generieke functies en gemeenschappelijke voorzieningen:
-
    - 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 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 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
- Algehele tekst en lees verbeterslag op alle onderdelen en een minder diep geneste menustructuur
- PDF download afsprakenstelsel
- Aanscherping begrippenlijst
- Verbeterde leeswijzer en leeswijzer per doelgroep

Inhoudelijk

- Governance Twiin op hoofdlijn
- Uitwerking Vertrouwensmodel
- Gehele revisie van het onderdeel Generieke functies en gemeenschappelijke voorzieningen (gewenste situatie obv vertrouwensmodel, de huidige situatie is geschetst en een mogelijk groeipad)
- Uitwerking dienstenmodel
    - Implementatiediensten; Toetreding en validatiediensten
    - Twiin afsprakenbeheer
    - Ketenregie

- Uitwerking processen
  - Proces Toetreden en validatie (Validatieloket)
  - Proces Ketenregie
- Aanscherping, nuancering en decompositie GtK Gevalideerd Twiin Knooppunt in GtK dienstverlener, GtK beheerder, GtK applicatie en GtK-netwerk
- Aanpassing Voorwaarden (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)
- Toegevoegd is een uitleg van hoe we omgaan met lokalisatie zolang nog niet iedereen is aangesloten op Mitz als gemeenschappelijke voorziening (Lokalisatie & toestemming)

3 | Visie

Hoe meer zorgorganisaties gaan samenwerken in een keten of netwerk, hoe meer relaties er ontstaan. Nu is het vaak zo dat bij iedere uitwisseling van gezondheidsgegevens steeds opnieuw afspraken gemaakt worden. Dit gebeurt in Nederland meestal op lokaal of regionaal niveau waardoor onderling verschillende afspraken ontstaan. Om deze verschillen te beperken en landelijke opschaling mogelijk te maken, is een verbindend afsprakenstelsel nodig: het Twiin Afsprakenstelsel.

Visie van Twiin

Laten we samen bijdragen aan betere zorg in Nederland door landelijke beschikbaarheid van gezondheidsgegevens te realiseren. Door heldere afspraken te maken, waarmee zorgaanbieders deze gegevens landelijk beschikbaar kunnen stellen en delen. Voor betere zorg voor de patiënt, om administratieve last van zorgaanbieders te verlichten en te voorkomen dat kostbare tijd van zorgverleners verloren gaat aan het zoeken naar de juiste gezondheidsgegevens. Daarom legt Twiin de afspraken samen met zorgaanbieders, leveranciers en partners vast in het Twiin Afsprakenstelsel.

Visie van Twiin

Doelstelling van Twiin

De doelstelling van Twiin is het:

Realiseren en in gebruik nemen van een **verbindend** afsprakenstelsel tussen zorgaanbieders, zorgnetwerken en voorzieningen voor beschikbaarheid van gezondheidsgegevens:

- veilig en betrouwbaar
- interoperabel op alle lagen
- samen met zorgaanbieders en leveranciers

Principes van Twiin

Om richting en structuur te geven aan het ontwerp van het Twiin Afsprakenstelsel hebben we de Twiin principes geformuleerd. De Twiin principes zijn fundamentele uitgangspunten, afgeleid van de visie, doelstelling en de overtuigingen van Twiin.

Klik voor een uitgebreide toelichting, rationale en implicatie van de principes

Twiin verbindt met knooppunten en generieke functies

Knooppunten en generieke functies, eventueel ingevuld door één of meerdere gemeenschappelijke voorzieningen, vormen de basis voor de verbindende architectuur van Twiin.

Een knooppunt in de context van het Twiin Afsprakenstelsel is een koppelvlak dat de verbinding met andere knooppunten vormt en uitwisseling mogelijk maakt. Het knooppunt kan bestaan uit een koppelvlak op een regionale infrastructuur, een landelijke infrastructuur maar ook op de omgeving van een zorgaanbieder.

Generieke functies zijn afspraken, standaarden of voorzieningen die landelijk nodig zijn om het vinden en beschikbaar maken van patiëntengegevens te realiseren. Vaak worden generieke functies (identificatie, authenticatie, autorisatie, lokalisatie, adressering, toestemming en logging) en gemeenschappelijke voorzieningen in één adem genoemd, maar ze zijn niet hetzelfde. Het is noodzakelijk om generieke functies in te vullen door middel van een oplossing. Dit kan op verschillende manieren plaatsvinden; onder andere door een gemeenschappelijke voorziening in te zetten.

Twiin volgt de landelijke afspraken over generieke functies en gemeenschappelijke voorzieningen en past daar het Twiin Afsprakenstelsel op aan. Wanneer er geen open stelsel is voor een generieke functie kiest Twiin voor beschikbare gemeenschappelijke voorzieningen om gegevensuitwisseling en databeschikbaarheid mogelijk te maken.

Twiin in relatie tot Wegiz, NVS, LVS en LDN

Lees meer over de relatie van Twiin met de Wegiz, Nationale Visie en Strategie (NVS), Landelijk Vertrouwensstelsel (LVS), Landelijk Dekkend Netwerk (LDN): 3.1 Twiin in relatie tot EHDS, Wegiz, NVS, LVS en LDN

3.1 Twiin in relatie tot EHDS, Wegiz, NVS, LVS en LDN

Twiin verbindt initiatieven

In het zorgveld zijn er verschillende initiatieven die bijdragen aan de beschikbaarheid van gezondheidsgegevens. De oplossingen hebben vaak een eigen set afspraken, ze verschillen in doelgroep, scope, uitgangspunten, tijdspad en aanpak. Vaak is er wel een overeenkomst in visie en doel. Twiin wil deze initiatieven verbinden. Dat vereist een gezamenlijke aanpak en duidelijke taakverdeling. Door te kiezen voor een samenhangend afsprakenstelsel kunnen de verschillende initiatieven naar elkaar toegroeien.

Statement

Twiin volgt de ontwikkelingen en NEN-normering als onderdeel van de Wegiz. Twiin sluit aan op de keuzes die op Europees en landelijk niveau worden gemaakt en neemt deze op in het Twiin Afsprakenstelsel.

Twiin en EHDS

Twiin brengt de Zorgtoepassingen waar mogelijk in lijn met de interoperabiliteitseisen die volgen uit de EHDS, zodra deze beschikbaar komen. Twiin verwijst nu in de implementatiewijzers naar de relevante toepasselijke informatiestandaard. Als die wordt geactualiseerd op basis van de EHDS, wijzigt daarmee ook de implementatiewijzer. Die blijft immers altijd verwijzen naar de meest actuele versie van die informatiestandaard.

De opzet van het Twiin Afsprakenstelsel sluit goed aan bij de opzet van de EHDS. De EHDS bepaalt dat leveranciers moeten zorgen voor een interoperabiliteitsmodule. Twiin Afsprakenstelsel stelt eisen aan een GtK. Deze twee begrippen sluiten goed op elkaar aan. Een GtK kan in de toekomst worden ingezet als een EHDS-interoperabiliteitsmodule.

Twiin, de Wegiz en (nieuwe) zorgtoepassingen

Het Twiin Afsprakenstelsel is zo generiek mogelijk van aard en daardoor toepasbaar voor meerdere zorgtoepassingen. De zorgtoepassingen ‘Beeldbeschikbaarheid’, uitwisseling van de ‘Basisgegevensset Zorg (BgZ)’ en ‘Correspondentie’ zijn opgenomen in deze release met als status ‘trial use’. De kandidaat zorgtoepassingen die in ontwikkeling zijn voor opname in het afsprakenstelsel zijn opgenomen in het ontwikkelsupplement. Voorbeelden hiervan zijn ‘Verpleegkundige overdracht’ en ‘Geboortezorg’. Twiin sluit aan bij de ontwikkeling van de aangewezen gegevensuitwisselingen onder de Wegiz. In samenwerking met deelnemers en leveranciers ontwikkelen we nieuwe zorgtoepassingen op het Twiin Afsprakenstelsel.

Twiin en de Nationale Visie en Strategie (NVS)

In 2023 werd de Nationale Visie & Strategie (NVS) aangeboden aan de Tweede Kamer. Op deze visie is positief gereageerd vanuit zowel de politiek als het zorgveld. Twiin maakt met het afsprakenstelsel mogelijk dat partners uitvoering geven aan plateau 1 van de NVS (interoperabiliteit georganiseerd). Daarmee leveren we een bijdrage aan het fundament van plateau 2 (Netwerk georganiseerd) en 3 (Integraal georganiseerd). Deze waarde van het Twiin Afsprakenstelsel wordt erkend door de betrokken partijen.

Twiin en het Landelijk Vertrouwensstelsel (LVS)

De ambitie van het Landelijk Vertrouwensstelsel (LVS) is het neerzetten van het geheel van technische, organisatorische en juridische afspraken voor het vertrouwen in de landelijke elektronische uitwisseling en beschikbaarheid van gezondheidsgegevens. Het project LVS richt zich allereerst op de geprioriteerde gegevensuitwisselingen onder de Wegiz en werkt daarnaast aan een groeipad richting plateau 2 en 3. Doel hierbij is het aanbrengen van samenhang en verbinding met betrekking tot vertrouwen tussen bestaande afsprakenstelsels (zoals Twiin, AORTA, Nuts, MedMij, etc). VWS heeft het Twiin Afsprakenstelsel gekozen als dé centrale plek voor de vastlegging van

geharmoniseerde en gestandaardiseerde vertrouwensafspraken in de zorg. Het geeft een kader voor alle technische, organisatorische en juridische afspraken die nodig zijn voor landelijke databeschikbaarheid.

Twiin en ‘Landelijk Dekkend Netwerk van infrastructuren voor gegevensuitwisseling in de zorg’ (LDN)

Om binnen de IZA-termijn te komen tot landelijke gegevensuitwisseling wordt door het programma LDN (landelijk dekkend netwerk zorgdata-infrastructuren) gewerkt aan het verbinden van bestaande infrastructuren om zo te komen tot een communicatienetwerk. Tegelijkertijd worden op het fundament van het communicatienetwerk de eerste stappen gezet om te komen tot een publiek data- en integratieplatform, om de stap te kunnen maken naar databeschikbaarheid, die nodig is om netwerkzorg te ondersteunen.

Twiin bouwt met het Twiin Afsprakenstelsel mee aan het landelijk dekkend netwerk van infrastructuren. Ook andere initiatieven zoals CumuluZ, Health-RI, Nuts en vele andere (regionale) infrastructuren bouwen mee aan het landelijk dekkend netwerk van infrastructuren. Om ook deze infrastructuren met elkaar te verbinden zijn voor landelijke databeschikbaarheid landelijke, uniforme afspraken voor vertrouwen noodzakelijk. Hiervoor is op initiatief van VWS het project Landelijk Vertrouwensstelsel (LVS) gestart.

Twiin draagt zorg voor de afspraken als het gaat om de uitwisseling en verbinding tussen bronnen (over verschillende infrastructuren) en generieke functies door middel van Gevalideerde Twiin Knooppunten (GtK’s). Het doel is om in de tijdsperiode van het Integraal Zorg Akkoord (IZA) en plateau 1 van de Nationale Visie en Strategie op het gezondheidsinformatiestelsel (NVS) de eerste stappen te zetten om bestaande netwerken te verbinden en om zo te komen tot interoperabiliteit voor primair gebruik: gegevensuitwisseling tussen zorgverleners.

> De visie van Twiin is dat het Twiin Afsprakenstelsel in samenwerking met CumuluZ, Health-RI, het Landelijk Vertrouwensstelsel en het Landelijk Dekkend Netwerk kan doorgroeien naar het landelijk afsprakenstelsel voor ontsluiting van bronnen en verbinding van infrastructuren, platformen en voorzieningen in het gezondheidsdomein.

4 | Architectuur

De architectuur van Twiin bevat de architectuurvisie, de principes van Twiin, de conceptuele architectuur met een toelichting op het begrip knooppunten (GtK's), generieke functies en gemeenschappelijke voorzieningen. Op desub pagina's staat een toelichting over databeschikbaarheid, communicatiepatronen, en de bedrijfs- en solutionarchitectuur van Twiin.

Inhoud

Architectuurvisie - Verbinden op alle lagen van interoperabiliteit

Twiin is een verbindend afsprakenstelsel

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 generieke functies en maken afspraken. De relaties die ontstaan zijn bestuurlijk, organisatorisch, juridisch, procesmatig, semantisch en technisch van aard; over alle lagen van het interoperabiliteitsmodel. Dit leidt tot een complexe situatie met vele zorgaanbieders, verschillende processen, informatiestromen, infrastructuren en koppelvlakken. Om deze complexiteit beheersbaar te houden, is een verbindend afsprakenstelsel nodig: dat is de essentie van het Twiin Afsprakenstelsel. Om verbinding tot stand te brengen, zijn er twee mogelijkheden: het maken van gezamenlijke afspraken en het overbruggen van verschillen.

Het maken van gezamenlijke afspraken doen we in het Twiin Afsprakenstelsel. Afspraken over doelstelling, principes, verantwoordelijkheden, governance, voorwaarden, wet- en regelgeving, adequate beveiliging, verkrijgen van vertrouwen en technische afspraken. Generiek, dus onafhankelijk van een zorgtoepassing. In het specifieke deel van het Afsprakenstelsel beschrijven we de implementatie van zorgtoepassingen, gebaseerd op het generieke deel.

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

➡️ Organisatie; door middel van het groeimodel *(kies keuze groeimodel*) en de deelnemersovereenkomst met samenwerkingsvoorwaarden

➡️ Twiin Dienstverlener; om zorgaanbieders te ondersteunen bij het voldoen aan het Twiin Afsprakenstelsel

➡️ Technische Translatie; het kan nodig zijn een technische translatie uit te voeren door het GtK voor het vertalen van verschillende standaarden.

Meer over technische translaties

Bij technische translaties valt onderscheid te maken in:

- Syntactische translaties (bv van FHIR STU3 naar FHIR R4)
- Semantische translaties (bv van BgZ2017 naar BgZ2020)
- Contenttransformatie: Omzetten van bijvoorbeeld de content van een CDA document in een XDS repository naar FHIR syntax en visa-versa

- Infrastructurele-integratie: gaat over alle aspecten van het op elkaar aansluiten van de security methodiek en de metadata die gebruikt worden binnen de twee infrastructuren (bijvoorbeeld: token migratie)
- Workflow-synchronisatie: gaat over het overbruggen van verschillende workflow mechanismen. Denk hierbij bijvoorbeeld aan het omzetten van een pull transactie van resources naar een document

Deze translaties kunnen op 2 manieren plaats vinden:

- Onder verantwoordelijkheid van de verzender of de ontvanger;
- Via een centrale dienst, die de translatie uitvoert.

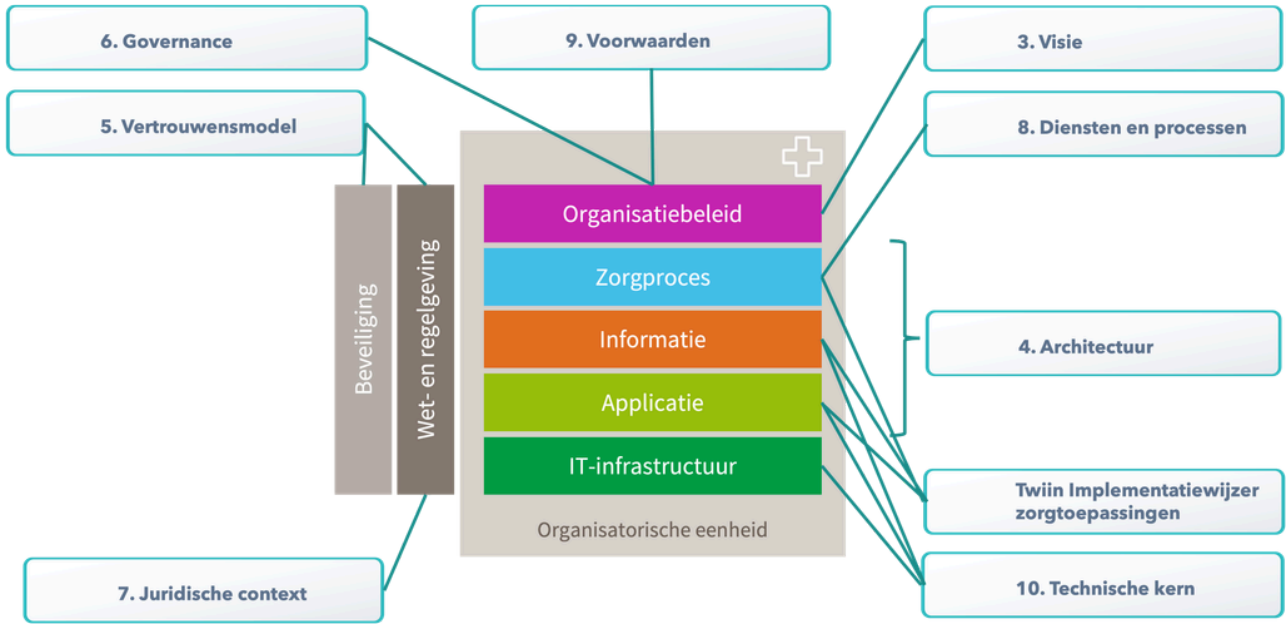
Waarbij we met betrekking tot verantwoordelijkheden een onderscheid kunnen maken tussen specificeren van de translatie en de operatie van de translaties.

In lijn met het FHIR besluit (zie website NICTIZ en VWS) ondersteunt Twiin geen translaties tussen FHIR en CDA. We sluiten hierbij aan bij de uitgangspunten en besluiten binnen stelselregie.

In de visie van Twiin nemen knooppunten, generieke functies en gemeenschappelijke voorzieningen een essentiële plaats in. Om zorgaanbieders en bestaande zorgnetwerken met elkaar te verbinden op alle lagen van interoperabiliteit, maken we gebruik van knooppunten (in Twiin GtK's; Gevalideerde Twiin Knooppunt)

Relatie met het Interoperabiliteitsmodel

Het interoperabiliteitsmodel van Nictiz beschrijft verschillende lagen waarop het noodzakelijk is om afspraken te maken, zodat uitwisseling volledig interoperabel is. Ook Twiin onderschrijft dit model; in het afsprakenstelsel komen alle lagen van het interoperabiliteitsmodel aan bod. Het afsprakenstelsel hanteert een wat andere hoofdstukindeling. In onderstaande weergave is inzichtelijk gemaakt hoe de lagen van het Nictiz model en de indeling van het afsprakenstelsel samenhangen.



Architectuurprincipes

Om richting en structuur te geven aan het ontwerp van het Twiin Afsprakenstelsel hebben we de Twiin principes geformuleerd. De Twiin principes zijn fundamentele uitgangspunten, afgeleid van de visie, doelstelling en de overtuigingen van Twiin.

Klik voor een uitgebreide toelichting, rationale en implicatie van de principes

Conceptuele Architectuur Twiin

Dit onderdeel bevat een beschrijving op hoofdlijnen van Twiin op een functionele (niet technische gedetailleerde) wijze.

Gevalideerd Twiin Knooppunt (GtK)

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. 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.

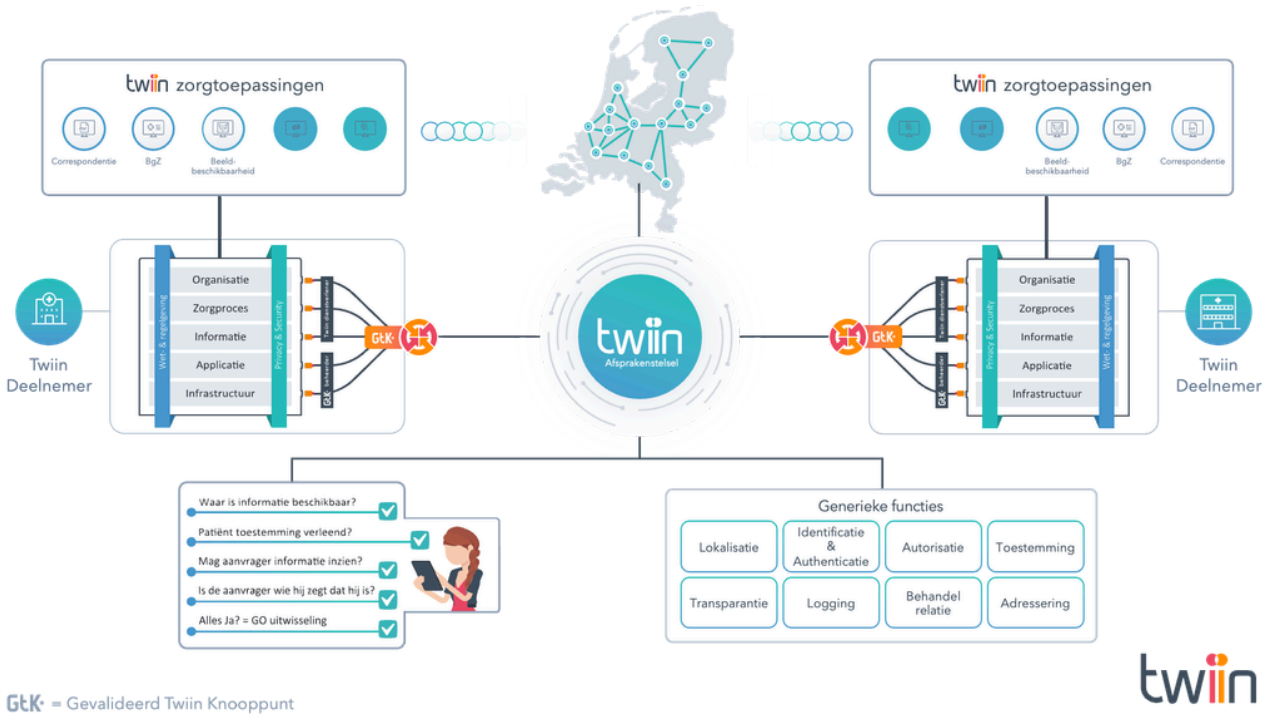
Een GtK hoeft niet per se uit één uitwisselingssysteem of één (aparte) applicatie te bestaan. Een GtK kan gevormd worden door meerdere onderdelen. Deze onderdelen zijn dan allen benodigd om via het koppelvlak conform de Twiin afspraken te communiceren. Onderdelen kunnen bijvoorbeeld zijn: de broker, XIS, EPD of het uitwisselingssysteem. De eisen aan een GtK kunnen gezien worden als de koppelvlak-specificaties van het Twiin Afsprakenstelsel.

De begrippen knooppunt en gemeenschappelijke voorzieningen zijn geïnspireerd op de visie op zorginfrastructuren (Mallie e.a. 2019), maar ook op oplossingen in het buitenland, zoals Carequality (2019) en TEFCA (2019) in de USA of ELGA (2017) in Oostenrijk. Door knooppunten en gemeenschappelijke voorzieningen te implementeren verbinden en hergebruiken we bestaande netwerken, voorzieningen en infrastructuren.

Knooppunten passen bij Nederland!

De Nederlandse zorg is organisatorisch sterk versnipperd. Vanuit de patiënt gezien is er enkel een relatie met een zorgaanbieder. Door de ontwikkeling van keten- en netwerkzorg, krijgen patiënten met meerdere zorgaanbieders te maken. De samenwerkingsverbanden die ontstaan, hebben behoefte aan beschikbaarheid van informatie over instellingsgrenzen heen. Professionals kunnen hierdoor beter hun werk doen en patiënten beter behandelen …en ook patiënten verwachten inzage in hun gezondheidsgegevens.. Door de jaren heen zijn vele lokale en regionale (deel)oplossingen ontstaan voor de beschikbaarheid van gegevens. Op nationaal niveau kunnen

instellingen echter niet of nauwelijks met elkaar uitwisselen. Twiin verbindt de deeloplossingen met het Twiin Afsprakenstelsel en de knooppunten. Hierdoor komen de idealen van 'continuity of care', beschikbaarheid van data en transparantie voor de patiënt dichterbij.



Figuur 1 laat zien dat Twiin zich richt op zorgtoepassingen voor landelijke beschikbaarheid van informatie. Bestaande regionale, landelijke, categorale zorgnetwerken brengen we met elkaar in verbinding via knooppunten door afspraken en gemeenschappelijke voorzieningen. Bij elke uitwisseling, of het beschikbaar stellen van gegevens, zijn controles ingebouwd die aansluiten bij de wet- en regelgeving.

Generieke functies en gemeenschappelijke voorzieningen

Generieke functies zijn afspraken, standaarden of voorzieningen die landelijk nodig zijn voor het vinden en beschikbaar maken van patiëntengegevens en om de waarborgen van het vertrouwensmodel goed in te kunnen richten. Vaak worden generieke functies (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 door de 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 gelden een aantal voorwaarden. Een keuze voor een bepaalde gemeenschappelijke voorziening kan ook weer vervallen als niet langer aan de voorwaarden wordt 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, dan 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 infrastructuur-onafhankelijk. De voorzieningen leggen alleen eisen op aan de koppelvlakken.
- Het proces voor onderhoud en beheer van de gemeenschappelijke voorziening is helder beschreven en duurzaam geborgd. Ook is er een autorisator aangewezen met een evenwichtige vertegenwoordiging van de belangen van de gebruikers in lijn met NEN7522.

Statement

Twiin volgt de ontwikkeling en NEN-normering 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.

Databeschikbaarheid en communicatiepatronen

Twiin onderschrijft de visie over databeschikbaarheid zoals verwoord in het Integraal Zorg Akkoord (IZA) en de Nationale Visie en Strategie (NVS). Twiin heeft bij de start in 2019 als uitgangspunt data- en beeldbeschikbaarheid gehanteerd. Twiin heeft een aantal generieke communicatiepatronen (technische use cases) onderkend en beschreven. Deze zijn ondersteunend bij de verandering van het uitwisselen van gegevens naar het realiseren van databeschikbaarheid. Het betreft push en pull patronen, die we hebben uitgewerkt in verschillende varianten: document en resource gebaseerd.

4.2 | Databeschikbaarheid en communicatiepatronen

Bedrijfsarchitectuur - Actoren

De Twiin architectuur kent organisaties en technische componenten als actoren. Dit deel bevat een beschrijving van de verschillende actoren. In de technische kern en de implementatiewijzer van de zorgtoepassingen van Twiin komen deze actoren terug in de uitwisselpatronen, transactie schema's en PvE's

4.3 | Bedrijfsarchitectuur - Actoren

Solutionarchitectuur - Technische kern

De technische uitwerking van de communicatiepatronen , de transactieschema's en de transacties hebben we ondergebracht in het onderdeel 10 | Technische kern van het afsprakenstelsel

4.1 | Twiin Principes

- P1. Landelijke beschikbaarheid en hergebruik van gezondheidsgegevens
- P2. Twiin is een vertrouwd netwerk van organisaties
- P3. Het Twiin Afsprakenstelsel leeft en blijft zich ontwikkelen
- P4. De functionele behoeften van zorgverleners, zorgaanbieders en patiënten zijn leidend
- P5. Deelname aan Twiin is vrijwillig maar niet vrijblijvend
- P6. Keuzevrijheid voor zorgaanbieders en leveranciers
- P7. Privacy en Security by design
- P8. Gebruik van internationale standaarden

De Twiin Principes zijn fundamentele uitgangspunten, afgeleid van de doelstelling, missie en visie van Twiin. Ze geven richting en structuur aan het ontwerp van het afsprakenstelsel en zijn gebaseerd op onze overtuigingen. De principes zijn voorzien van een rationale, waarin de belangrijkste ontwerpafwegingen 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
Algemeen				
1	**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. Burgers 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, bestuur, (vak)-verenigingen, informatie standaarden en infrastructuur op landelijk niveau in samenwerking met regionale en lokale organisaties. Twiin is schaalbaar en bruikbaar voor landelijke uitwisseling. Uitwisseling via knooppunten, gebruikmakend van (bestaande) gemeenschappelijke voorzieningen (conform visie samenhang op de zorginfrastructuren). Uit te breiden naar naar meerdere zorgtoepassingen. De architectuur van Twiin moet flexibel genoeg zijn om toekomstige (nieuwe) zorgtoepassingen te ondersteunen.
2	**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 (in het vertrouwensmodel) en deze te borgen door middel van validatie en technische maatregelen ontstaat er vertrouwen in elkaar.	Om problemen op te lossen die door een enkele organisatie moeizaam of helemaal niet kunnen worden gerealiseerd.	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
3	**P3. Het Twiin Afsprakenstelsel leeft en blijft zich ontwikkelen**	Het Twiin Afsprakenstelsel leeft. We groeien van ervaringen en verwerken deze in het afsprakenstelsel.	Om snel een eerste versie van het afsprakenstelsel te kunnen krijgen én te kunnen leren van tussentijdse ervaringen, volgt het afsprakenstelsel een groeimodel. 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	Het doel van Twiin is het faciliteren van meerdere zorgtoepassingen door het aanbieden van gemeenschappelijke voorzieningen en afspraken voor het landelijk beschikbaar maken en/of uitwisselen van gegevens. Twiin heeft als ambitie om zorgdomeinbreed te faciliteren.

			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.	Bij het oppakken van zorgtoepassingen zijn de reeds bestaande landelijke programma's in de lead.
4	**P4. De functionele behoeften van zorgverleners, zorgaanbieders en patiënten zijn leidend**	De functionele behoeften van zorgverleners, zorgaanbieders en patiënten zijn leidend voor het Twiin Afsprakenstelsel.	De voornaamste drijfveer van Twiin is om invulling te geven aan de functionele behoeften van zorgverleners en patiënten 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.	Voor de (door)ontwikkeling van Twiin, inclusief de gemeenschappelijke voorzieningen en afspraken, gelden de functionele behoeften als uitgangspunt.
5	**P5. Deelname aan Twiin is vrijwillig maar niet vrijblijvend**	*Vrijwillig* Een zorgaanbieder besluit zelf om wel of niet aan te sluiten ipv Twiin 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.	Mogelijk zal op termijn uitwisseling van gegevens in veldnormen worden opgenomen en via VWS worden verankerd in wetgeving. Door aansluiting op 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 meegedaan. Het afsprakenstelsel verplicht deelnemers niet om daadwerkelijk gegevens uit te wisselen. Dat is uiteindelijk aan de zorgaanbieder/patiënt. Zorgaanbieders die aansluiten hebben een inspanningsverplichting om gegevens beschikbaar te stellen.
6	**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 vrijheid hebben in de leverancierskeuze die het beste bij de bedrijfsprocessen past of economisch gezien het meest voordelig is. Zorgaanbieders moeten eenvoudig kunnen aansluiten met zo min mogelijk opgeworpen drempels. Leveranciers hebben gelijke kansen om deel te nemen.	De Twiin Dienstverleners moeten een brede kennis hebben van en relaties hebben met leveranciers. Twiin levert een overzicht van aansluitvoorwaarden voor zorgaanbieders, GtK Beheerders, Twiin Dienstverleners en GtK's en netwerk,
7	**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 ontwerpen van het Twiin Afsprakenstelsel en architectuur. Informatiebeveiliging en privacy zijn vanaf het begin meegenomen in het vertrouwensmodel en de technische uitwerking hiervan in de kern. Het heeft zijn 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
8	**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 informatiestandaarden.	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,	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

		Door NICTIZ en andere organisaties zijn al informatiestandaarden gedefinieerd.	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.	meerdere leveranciers. 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. 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) Nationale visie en strategie- gezondheidsinformatiestelsel
- In het Twiin Afsprakenstelsel hebben we de basisprincipes en afgeleide principes voor het informatiestelsel voor de zorg meegenomen. zoals beschreven in het Manifest van de DIZRA - Duurzaam Informatiestelsel Zorg Referentie Architectuur Start | DIZRA
- "Visie op samenhang in de zorginfrastructuren in Nederland" (Bus et al. 2019) evenals de aanvullingen op de principes van het informatiestelsel voor de zorg die daarin zijn beschreven. https://www.informatieberaadzorg.nl/binaries/informatieberaad-zorg/documenten/publicaties/2019/10/25/visie-op-samenhang-in-de-zorginfrastructuren-in-nederland/Visie+op+samenhang+in+zorginfrastructuren+30.pdf
- Trusted Exchange Framework and Common Agreement (TEFCA) - https://www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf
- MedMij (MM) - MedMij Afsprakenstelsels
- Zira - ZiRAonline.nl

4.2 | Databeschikbaarheid en communicatiepatronen

Twiin onderschrijft de visie over databeschikbaarheid zoals verwoord in het Integraal Zorg Akkoord (IZA) en de Nationale Visie en Strategie (NVS). Twiin heeft bij de start in 2019 als uitgangspunt data- en beeldbeschikbaarheid gehanteerd waarbij het idee daarachter is dat dat de vraag welke informatie wanneer nodig is en in welke zorgtoepassing losgekoppeld wordt van de onderste lagen van interoperabiliteit; een modulair ingerichte architectuur, of zoals de NVS stelt “data loskoppelen van functionaliteit”.

Twiin heeft in de startfase 4 conceptuele oplossingsrichtingen bepaald waarmee databeschikbaarheid bereikt kan worden. Ze zijn als bijlage opgenomen in het Twiin Afsprakenstelsel als informatieve toelichting en zijn gebruikt als richtinggevende oplossingen. Twiin-conceptuele oplossingsrichtingen.pdf

Onder databeschikbaarheid verstaan we de mate waarin data toegankelijk en beschikbaar zijn voor gebruikers wanneer ze die nodig hebben en daar recht op hebben. Het heeft betrekking op de mogelijkheid om gegevens op te vragen, te raadplegen, te wijzigen en te gebruiken. Als gezondheidsdata beschikbaar, bereikbaar en (her)bruikbaar zijn voor preventie, primair en secundair gebruik, kunnen we zorgproces- en usecase onafhankelijk voldoen aan de specifieke informatiebehoefte mét waarborgen voor patiëntveiligheid en privacy. Voor de burger zelf en voor alle betrokkenen in het zorgnetwerk die er recht op hebben.

- Databeschikbaarheid is van essentieel belang voor het nemen van beslissingen met betrekking tot preventie, gezondheid en onderzoek.
- Databeschikbaarheid helpt zorgaanbieders efficiënter om te gaan met gegevens en (financiële) middelen.
- Databeschikbaarheid voorkomt dubbeldiagnostiek en verkeerde diagnoses. Zorgverleners kunnen sneller de juiste behandeling bepalen.
- Databeschikbaarheid wordt gedragen door vertrouwen, want zonder vertrouwen wordt data niet gedeeld.

De voornaamste randvoorwaarden

- Beschikbaar stellen van data, gestandaardiseerd, bereikbaar en bruikbaar, ten behoeve van anderen in het zorgnetwerk wordt verplicht.
- Vertrouwen tussen de personen in het zorgnetwerk wordt geborgd. Dit doordat partijen voldoen aan normen, maar ook aan andere eisen die aan deelname tot het gezondheidsinformatiestelsel zijn gesteld. Denk bijvoorbeeld aan eisen op het gebied van verantwoordelijkheden, informatieveiligheid en kwaliteit.
- Alle betrokkenen in het netwerk (burger, mantelzorger, zorgverlener, sociale omgeving) beschikken over de informatie die nodig is voor het leveren van passende hybride zorg.
- Hergebruik van data moet mogelijk zijn: eenheid van taal.
- Uitwisseling van data moet mogelijk zijn: landelijk dekkend netwerk.

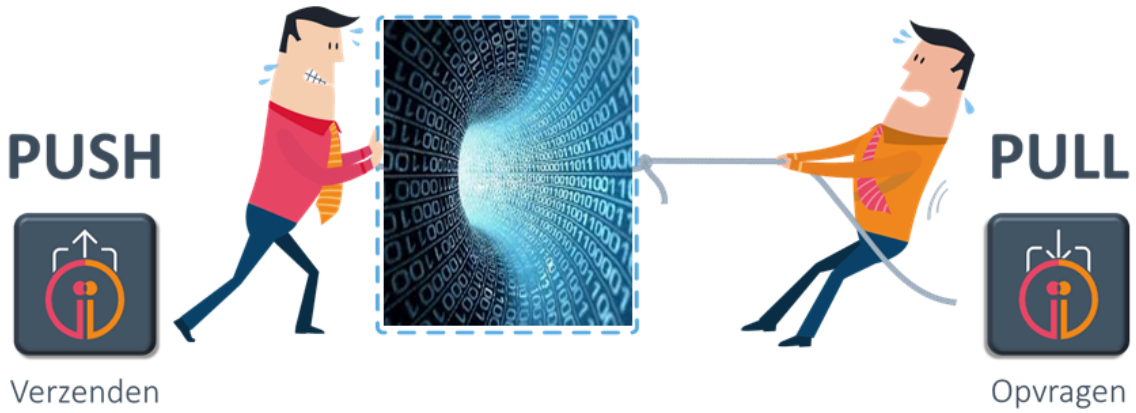
Databeschikbaarheid versus gegevensuitwisseling

Gegevensuitwisseling wordt vaak gezien als het versturen van gegevens van de ene zorgaanbieder naar een andere zorgaanbieder als onderdeel van een stap in het zorgproces. De ontvangende zorgverlener moet zijn werk doen met de (vaak onvoldoende en verouderde) gegevens die hij krijgt. Bovendien kan een zorgverlener die niet in deze gegevensuitwisseling is opgenomen, de gegevens niet inzien of hergebruiken. En dat is juist wél wenselijk als de gegevens relevant zijn voor een andere behandeling van dezelfde patiënt. Databeschikbaarheid gaat ervan uit dat de juiste informatie op het juiste moment éénduidig beschikbaar, bereikbaar en toegankelijk is (zonder dat de informatie (onnodig) wordt ‘rondgepompt’).

Twiin onderschrijft de visie op databeschikbaarheid zoals uitgewerkt in de NVS, maar realiseert zich dat de huidige praktijk anders is. Databeschikbaarheid vraagt anders denken en doen, en een gezamenlijk transitieplan. Twiin beoogt dat we vanuit de weerbarstige werkelijkheid toegroeien naar volledige databeschikbaarheid.

Generieke communicatiepatronen

Twiin heeft een aantal generieke communicatiepatronen (technische use cases) onderkend en beschreven. Deze zijn ondersteunend bij de verandering van het uitwisselen van gegevens naar het realiseren van databeschikbaarheid. Het betreft push en pull patronen, die we hebben uitgewerkt in verschillende varianten: document en resource gebaseerd.



Er zijn twee typen communicatiepatronen, die in de 10.1 | Kern Volume 1 - Communicatiepatroon Overview verder zijn uitgewerkt:

Communicatiepatroon	Naam van de technische afspraak	Type communicatiepatroon
Gericht verzenden	Push	Verzenden
Gericht beschikbaar stellen	Notified Pull	Verzenden
Gericht bevragen	Pull	Raadpleegbaar maken
Ongericht bevragen	Indexed Pull	Raadpleegbaar maken

Voor de uitwerking van deze communicatiepatronen zijn de meeste voorkomende functionele use casus leidend:

- Verwijzing/overdracht
- Consult/advies
- Ketenzorg/netwerkzorg
- Ad hoc dossier opvragen
- Uitbesteed onderzoek/behandeling

Deze functionele use casus zijn beknopt beschreven 10.1.1 | Functionele use cases databeschikbaarheid

Uitgebreide applicatie- en transactiediagrammen en bijbehorende Twiin Technische Afspraken (TTA's) zijn terug te vinden in de Technische kern voor databeschikbaarheid.

4.3 | Bedrijfsarchitectuur - Actoren

Binnen de architectuur van Twiin spelen verschillende actoren een rol.

- Twiin Deelnemer
- Twiin Dienstverlener
- GtK (Gevalideerd Twiin Knooppunt)
  - GtK verzender (sender) / zendend GtK
  - GtK ontvanger (receiver) / ontvangend GtK
  - GtK vrager (requester) / vragend GtK
  - GtK antwoorder (responder) / antwoordend GtK
- GtK Beheerder
- GtK Leverancier

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

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

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

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 (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. 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.

> Een GtK hoeft niet per se uit één uitwisselingssysteem of één (aparte) applicatie te bestaan. Een GtK kan gevormd worden door meerdere onderdelen. Deze onderdelen zijn dan allen benodigd om via het koppelvlak conform de Twiin afspraken te communiceren. Onderdelen kunnen bijvoorbeeld zijn: de broker, XIS, EPD of het uitwisselingssysteem. De eisen aan een GtK kunnen gezien worden als de koppelvlak-specificaties van het Twiin Afsprakenstelsel.

Voorbeelden van (onderdelen van) GtK's:

- XDS Gateway voor beeldduitwisseling en BgZ (via CDA)
- FHIR Gateway van AORTA
- Nuts Node voor eOverdracht
- FHIR koppelvlak voor BgZ
- Leveranciersplatformen

GtK's kunnen verschillende rollen aannemen. In de Technische kern worden de volgende GtK actoren onderscheiden:

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

GtK Beheerder

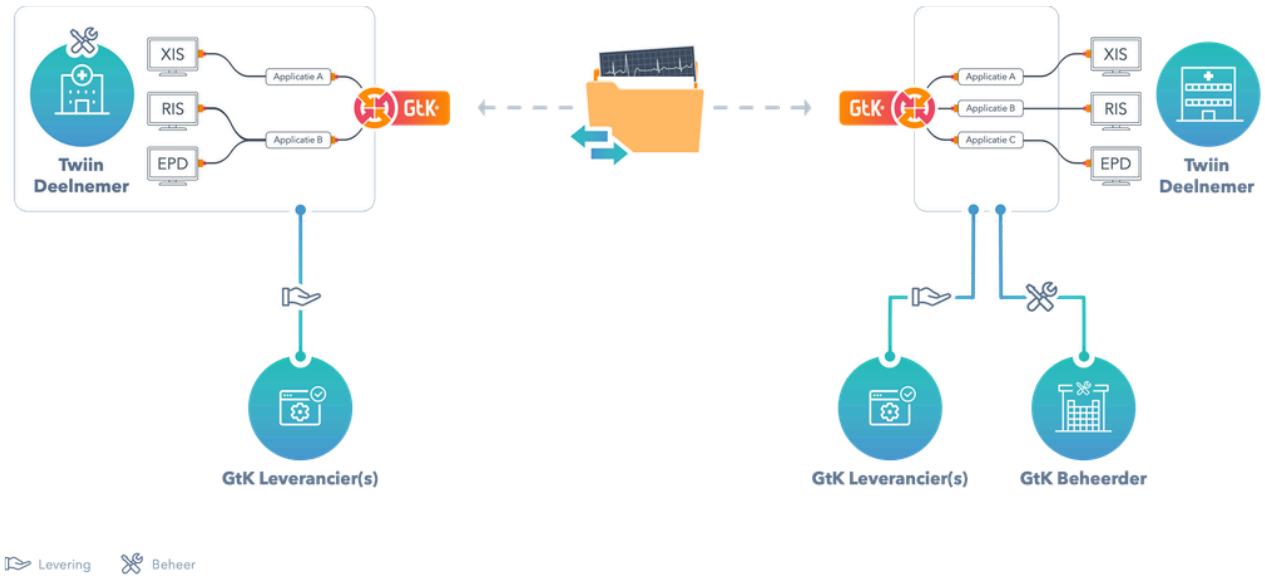
Een organisatie die namens de Twiin Deelnemer invulling geeft aan het technisch beheer van het GtK.

GtK Leverancier

Leverancier van een applicatie die een intentieverklaring heeft getekend om te komen tot validatie voor één of meer zorgtoepassingen, dan wel beschikt over een gevalideerde GtK.

In onderstaande figuur wordt weergegeven hoe de verschillende actoren zich tot elkaar kunnen verhouden en zijn verschillende actoren te zien:

- Twiin Deelnemer
- GtK Leverancier
- GtK
- GtK Beheerder



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 zelf GtK Beheerder is. Beide Twiin Deelnemers hebben ook te maken met leverancier(s) voor de onderdelen van de GtK's.

Bovenstaande situaties zijn voorbeelden, 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.

4.4 | Solution Architectuur - Technische kern

De technische uitwerking van de communicatiepatronen , de transactieschema's en de transacties hebben we ondergebracht in het onderdeel 10 | Technische kern van het afsprakenstelsel

5 | Vertrouwensmodel

Inhoud

Definitie en belang vertrouwensmodel

Het vertrouwensmodel is het geheel van technische, organisatorische en juridische waarborgen voor het vertrouwen in de landelijke elektronische uitwisseling van medische gegevens.

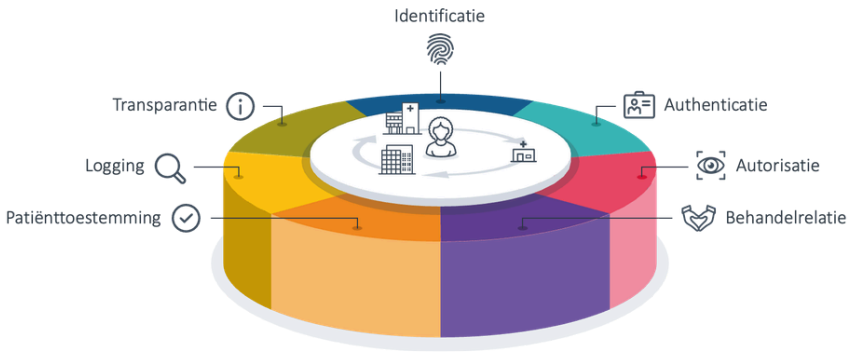
Het vertrouwensmodel ziet toe op het onderlinge vertrouwen tussen zorgaanbieders, zorgverleners en patiënten en borgt daarmee de vertrouwelijkheid van het medische dossier.

- De patiënt moet erop kunnen vertrouwen dat de zorgverleners en zorgaanbieders de vertrouwelijkheid van zijn dossier adequaat borgen, ook bij de uitwisseling van gegevens.
- Zorgverleners hebben een beroepsgeheim (op basis van de Wet BIG en WGBO). Het beroepsgeheim geldt voor alle informatie die zij in de uitoefening van hun beroep over een patiënt te weten komen. Dus ook het feit dat een patiënt onder behandeling is bij een zorgverlener valt hieronder. Anderen die beroepsmatig kennis krijgen van patiëntgegevens 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). Zorgaanbieders zijn verplicht om de beveiligingsnormen voor de zorg toe te passen en het vertrouwensmodel geeft invulling aan die normen (op basis van de Begz). Ook zijn zorgaanbieders verplicht de juiste randvoorwaarden te organiseren die zorgverleners in staat stellen goede zorg te verlenen (op basis van de Wkkgz). 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.

Onderdelen van het vertrouwensmodel

Het Twiin Afsprakenstelsel geeft invulling aan het vertrouwensmodel; in de onderliggende pagina's is voor elk onderdeel van het vertrouwensmodel beschreven welke afspraken gelden voor dat onderdeel en waar de Twiin Deelnemers zich aan verbinden. Omdat elke Twiin Deelnemer zich verbindt aan de afspraken, kunnen de Twiin Deelnemers elkaar vertrouwen. Het vertrouwensmodel bestaat uit de zeven onderdelen gevisualiseerd in onderstaand figuur.

Het vertrouwensmodel van Twiin correspondeert met de bovenste laag van het Uitwisselingskompas van VZVZ en geeft een invulling daaraan.



Bij elke elektronische uitwisseling geldt:

1. Identificatie: zorgaanbieders moeten erop kunnen vertrouwen dat de identiteit van een andere zorgaanbieder eenduidig wordt vastgesteld. Tevens moet de identiteit eenduidig worden vastgesteld van de patiënt over wie de uitgewisselde gegevens gaan;
2. Authenticatie: zorgaanbieders moeten zekerheid hebben over de identiteit van de andere zorgaanbieder en betrokken zorgverlener;
3. Autorisatie zorgaanbieders moeten zorgen dat alleen die gegevens uitgewisseld worden die nodig zijn voor de behandelingn de betrokken patiënt;
4. Behandelrelatie: zorgaanbieders moeten er op kunnen vertrouwen dat enkel toegang wordt verleend tot medische gegevens als sprake is van een behandelrelatie met de desbetreffende patiënt;
5. Patiënttoestemming: zorgaanbieders moeten erop kunnen vertrouwen dat de betrokken patiënt toestemming heeft gegeven die voldoet aan de voorwaarden;
6. Logging: zorgaanbieders moeten erop kunnen vertrouwen dat de andere aangesloten zorgaanbieders logging en de controle van de logging adequaat uitvoeren;
7. Transparantie: zorgaanbieders moeten erop kunnen vertrouwen dat de andere aangesloten zorgaanbieders de betrokken patiënt op begrijpelijke wijze hebben geïnformeerd over de uitwisseling van gegevens en de uitoefening van zijn rechten.

Bij de uitwisseling van gegevens tussen zorgaanbieders is een centrale vraag of een zorgaanbieder erop kan vertrouwen dat een andere zorgaanbieder voldoet aan alle vereisten voor het verlenen van toegang. Concreet: dat zorgaanbieders waarmee wordt uitgewisseld op de juiste wijze de zeven onderdelen van het vertrouwensmodel hebben ingericht. Het vertrouwensmodel kent daarom deze zeven onderdelen om de vertrouwelijkheid van het medische dossier te borgen. Deze onderdelen hangen samen; keuzes in het ene onderdeel zijn van invloed op keuzes in het andere onderdeel. Bij validatie toetst Twiin of de zorgaanbieder de waarborgen goed heeft ingericht voor de betreffende Zorgtoepassing.

In het vertrouwensmodel is onderscheid gemaakt tussen twee typen Communicatiepatronen : verzenden en raadpleegbaar maken. Ook gelden er verschillende eisen voor de twee typen in de Voorwaarden Twiin Deelnemer . Dit mede gelet op de eisen die gelden voor een elektronisch uitwisselingssysteem zoals bedoeld in de Wabvpz (zie Juridische Context).

Verwerkingsverantwoordelijkheid

Iedere zorgaanbieder is zelfstandig verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens in de eigen zorginformatiesystemen, waaronder het GtK. Daaruit volgt dat iedere zorgaanbieder als verwerkingsverantwoordelijke het aanspreekpunt is bij verzoeken van betrokkenen op basis van hun AVG-privacyrechten.

Iedere zorgaanbieder moet ervoor zorgen dat het eigen GtK voldoet aan de toepasselijke beveiligingsnormen, waaronder met name NEN 7510, NEN 7512 en NEN 7513. Dat maakt noodzakelijk dat zorgaanbieders vastleggen op welke manier zij invulling geven aan deze normen, zoals de vraag welke identificatiemiddelen zij gebruiken. De afspraken hierover zijn vastgelegd in het vertrouwensmodel van het Twiin Afsprakenstelsel.

Daarnaast is nodig dat zorgaanbieders afspreken waar de verantwoordelijkheid van de één begint en waar die eindigt. Dit is met name van belang bij gebruik van een elektronisch uitwisselingssysteem. Zo'n systeem maakt immers mogelijk dat een zorgverlener van een andere zorginstelling gegevens kan raadplegen in het zorginformatiesysteem. Zo moet een dossierraadpleger erop kunnen vertrouwen dat het GtK van de dossierhouder voldoet aan de toepasselijke beveiligingsnormen. Het is juist de verantwoordelijkheid van de dossierraadpleger dat enkel medewerkers met een behandelrelatie het dossier raadplegen bij de dossierhouder. Ook de toedeling van de verantwoordelijkheid bij uitwisseling is vastgelegd in het vertrouwensmodel van het Twiin Afsprakenstelsel.

Samenvatting invulling aspecten vertrouwensmodel Twiin

Aspect	Huidige invulling Twiin	Verwijzing uitwerking technische kern
Identificatie	Patiënt: BSN (gevalideerd / geverifieerd) Zorgaanbieder: URA Zorgverlener: UZI-nummer of een ander uniek tot één persoon te herleiden nummer op het juiste betrouwbaarheidsniveau	10.1.7 | Generieke functie - Identificatie en Authenticatie
Authenticatie	Zorgverlener: eIDAS hoog (breder dan UZI pas) Zorgaanbieder: UZI certificaat of vergelijkbaar PKI certificaten	10.1.7 | Generieke functie - Identificatie en Authenticatie
Autorisatie	Medisch Autorisatie Protocol (MAP)	10.1.6 | Generieke functie - Autorisatie
Behandelrelatie	De dossierraadpleger/-ontvanger moet een adequate autorisatiestructuur hebben ingericht en zorgdragen voor logging en adequate controle van de logging	NVT
Patiënttoestemming	Mitz bij raadpleegbaar maken	10.1.10 | Generieke functie - Toestemming
Logging	NEN 7513 formaat, NEN 7510 en NEN 7512 als procedure Uniforme rapportages inclusief procedures	10.1.9 | Generieke functie - Logging
Transparantie	De patiënt goed informeren over uitwisseling en over AVG-rechten en een procedure inrichten voor opvragen logging door de patiënt	NVT
Aspecten die samenhangen met het vertrouwensmodel:		
Adressering	Het aanleveren van adresgegevens voor opname in de gemeenschappelijke voorziening ZORG-AB zodat gevalideerde GtK's de adresgegevens kunnen controleren	10.7.8 | Generieke functie - Adressering
Lokalisatie	Mitz (bij raadplegen in de zin van Wabvpz)	10.1.11 | Generieke functie - Lokalisatie

Generieke functies worden uitgelegd in hoofdstuk 4 4 | Architectuur | Generieke functies en gemeenschappelijke voorzieningen

Statement

Het Twiin Afsprakenstelsel volgt de ontwikkeling van de NEN-normering van de generieke functies en sluit hierop aan.

Groeimodel ‘Groeien met Twiin’

Twiin realiseert zich dat niet alle Twiin Deelnemers al zover zijn om op dit beschreven niveau van het Twiin Vertrouwensmodel uit te kunnen wisselen. Daarom heeft Twiin een groeimodel gemaakt dat de Twiin Deelnemers helpt om te gaan voldoen aan het Twiin Afsprakenstelsel om te komen tot validatie. Het groeimodel is een leidraad in volwassenheidsniveaus om te gaan voldoen aan het Twiin Afsprakenstelsel en helpt om stapsgewijs invulling te geven aan het vertrouwensmodel. Twiin Deelnemers kunnen zelf keuzes maken – ondersteund vanuit Twiin.

Landelijk uitwisselen tussen GtK’s kan als wordt voldaan aan het Twiin Afsprakenstelsel en de Twiin Deelnemer is gevalideerd voor de betrokken zorgtoepassing. Zolang de Twiin Deelnemer nog niet is gevalideerd, kan de Twiin Deelnemer enkel uitwisselen in beperkt verband op basis van de Samenwerkingsvoorwaarden zoals omschreven in artikel 3 Deelnemersovereenkomst.

Klik hier om de Toolkit van Twiin te openen om de ‘Factsheet groeimodel’ te downloaden.

5.1 | Vertrouwen: Identificatie

ntificatie

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

Patiëntidentificatie

Om gegevens uit verschillende zorgaanbieders over dezelfde patiënt aan elkaar te relateren is het gebruik van het BSN verplicht gesteld (Zie Wabpvz).

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 patiënt 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 woonadres. Omdat Twiin nog niet heeft uitgewerkt hoe zorgaanbieders moeten omgaan met een niet aanwezig BSN, kunnen zorgaanbieders in die situatie voorlopig nog geen gegevens uitwisselen op basis van validatie door Twiin.

Zorgaanbieders

Om zorgaanbieders te kunnen identificeren, vereist de NEN7512 dat er een afspraak gemaakt dient te worden over het gebruik van een eenduidig identificatienummer. Als een patiënt 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 URA-nummer. Om zorgaanbieders te identificeren kiest Twiin voor het URA-nummer. Dit is een nummer dat alleen aan zorgaanbieders uitgegeven wordt en ook niet-declarerende zorgaanbieders kunnen een URA-nummer krijgen. Deze keuze ligt in lijn met de uitgangspunten zoals geformuleerd in het Informatieberaad.

Zorgverleners

Ook zorgverleners moeten identificeerbaar zijn door de partijen betrokken bij de gegevensuitwisseling (NEN7512). Op basis van bijvoorbeeld een medewerkersnummer van een andere organisatie kan niet bepaald worden wie de diagnose heeft gesteld, wie de persoon is die de medicatie voorschrijft, of toegang wenst tot het dossier. Twiin vindt het UZI-nummer hiervoor het meest geschikt. Het UZI-stelsel is het breedst bruikbare landelijke stelsel om zorgverleners en medewerkers te identificeren. Ook deze keuze ligt in lijn met de uitgangspunten zoals geformuleerd in het Informatieberaad.

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 authenticatiemiddelen beschikbaar komen, zullen die een plek krijgen in het Twiin Afsprakenstelsel.

Principe	Wie is verantwoordelijk Dossierhouder of dossierraadpleger/-ontvanger	Invulling Twiin	Toelichting
Patiënten worden geïdentificeerd met een landelijk uniek nummer; het BSN	Dossierhouder en dossierraadpleger/-ontvanger dienen patiënten op dezelfde manier te identificeren.	BSN	Twiin heeft nog niet uitgewerkt, hoe om te gaan met een niet aanwezig BSN en gaat vooralsnog uit van uitwisseling op basis van BSN. Als er geen BSN is kan er voorlopig dan ook niet uitgewisseld worden op basis van validatie door Twiin.
Zorgaanbieders worden geïdentificeerd met een landelijk uniek nummer	Dossierhouder en dossierraadpleger/-ontvanger dienen elkaar te kunnen identificeren.	URA (UZI-Register Abonneenummer)	Het URA-nummer is het breedst toepasbare landelijke stelsel om zorgaanbieders te identificeren. Het URA-nummer is verplicht maar daarnaast mogen ook andere identificatienummers gebruikt worden.
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 de raadplegende (verantwoordelijke) zorgverlener te kunnen identificeren. *Bij verzenden*:* De dossierhouder dient de verzendende zorgverlener te	UZI of een ander uniek tot één persoon te herleiden nummer op het juiste betrouwbaarheidsniveau.	UZI is 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. Om het UZI-nummer te verkrijgen is het nodig om ook een authenticatiemiddel af te nemen. De plannen zijn om deze koppeling los te maken.

	identificeren en het landelijke unieke nummer mee te sturen naar dossierontvanger.		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 NEN7518). Twiin stelt nu alleen de eis dat het nu 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 communicatiepatronen.

5.2 | Vertrouwen: Authenticatie

Authenticatie

Authenticatie is de verificatie van een beweerde identiteit. Met authenticatiemiddelen kan een persoon 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 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 niveau hoog, in lijn met de uitvoeringsverordening (EU) 2015/1502).

Betrouwbaarheid

De betrouwbaarheid van het authenticatiemiddel 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 zorginstellingen

Voor het authentiseren van zorginstellingen (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; voor authenticatie met een tweede factor is altijd een persoon nodig, wat het onwerkbaar maakt in geval van uitwisseling, met name bij de organisatie die informatie ontvangt en de organisatie die geraadpleegd wordt. Het is kortom niet mogelijk om zorginstellingen 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 authenticatiemiddel 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 authenticatiemiddelen beschikbaar komen, zullen die een plek krijgen in het Twiin Afsprakenstelsel.

Principe	**Wie is 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.
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 (NEN7510). De dossierhouder moet de identiteit kunnen controleren (d.m.v. een cryptografisch bewijs als een elekronische handtekening, volgens NEN7512). *Bij verzenden*:* De verzendende partij moet zijn eigen gebruiker identificeren en authenticeren (NEN7510). De dossierontvanger moet de identiteit kunnen controleren (d.m.v. een cryptografisch bewijs als een	*Bij raadpleegbaar maken:* De dossierraadpleger dient zijn eigen gebruikers te authenticeren op eIDAS hoog betrouwbaarheidsniveau. De authenticatie van 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).	NEN7512:2022 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.

	elekronische handtekening, volgens NEN7512).	*Bij verzenden:* De dossierhouder dient zijn eigen gebruikers te authenticeren op eIDAS hoog betrouwbaarheidsniveau. De authenticatie van 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 NEN7512 risicoklasse waar de betreffende gegevensuitwisseling onder valt. De dossierontvanger kan de externe gebruiker daarmee wel identificeren maar niet met zekerheid (authenticeren).	Ondertekening van het uitgewisselde is ook verplicht (NEN7512:2022): “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 medewerkere de indruk kan wekken dat een onjuiste uitwisseling eigenlijk een goede uitwisseling is.“ Ondertekening van gegevens is bedoelt voor de ontvanger. De ontvanger is gehouden op basis van NEN7512:2022 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.

* Verzenden en raadpleegbaar maken verwijzen naar de twee typen communicatiepatronen.

5.3 | Vertrouwen: Autorisatie

orisatie

Autorisatie bepaalt of een zorgmedewerker 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 patiënttoestemming van het vertrouwensmodel).

Proportionaliteit

Ook als een patiënt 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 moeten beleid en procedures vaststellen voor de gegevensuitwisseling, waaronder over het onderwerp autorisatiebeleid (NEN7512:2015, paragraaf 6.2.1, NEN7512:2022. paragraaf 6.1.1). De Gedragslijn toegangsbeveiliging digitale patiëntdossiers, d.d. 12 oktober 2020 bepaalt: "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] Dat kan door middel van de Twiin Deelnemersovereenkomst .

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 patiënt betrokken zorgverleners.[3]

Paragraaf 8.4.2 NEN7513:2018 bepaalt dat “zorginstellingen autorisatieprotocollen opstellen waarin de reguliere toegang tot bepaalde zorggegevens wordt gekoppeld aan een rol in het zorgproces (…). De logging moet kunnen worden gebruikt voor de verantwoording van bepaalde gebeurtenissen op een elektronisch dossier. Daarom moet in de logging verwijzingen worden opgenomen naar het autorisatieprotocol (…) Is er nog geen autorisatieprotocol (…) dan wordt het ontbreken ervan vermeld.” Deze werkwijze komt overeen met besluiten die zijn genomen binnen het Informatieberaad.

Ontwikkelingen

Daarnaast NEN is gestart met de ontwikkeling van een norm over autorisatie (NEN 7520) waarin de uitkomsten van programma Janus worden verwerkt. Twiin volgt de ontwikkelingen en zal aansluiten bij de uitkomsten.

Principe	Wie is 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 zorgt voor rolgebaseerde autorisatie.	*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 Deelnemers.	Twiin volgt de ontwikkeling van de landelijke afspraken over autorisatie in de NEN7520 en zal daarop aansluiten.

* Verzenden en raadpleegbaar maken verwijzen naar de twee typen communicatiepatronen.

Voetnoten

1. Er zijn echter nog maar een beperkt aantal informatiestandaarden beschikbaar, zoals voor de acute zorg en de geboortezorg (https://www.zorginzicht.nl/kwaliteitsinstrumenten). Ook autorisatierichtlijnen zijn nog maar beperkt beschikbaar (wel voor Huisartswaarneming en Medisch Generalistische Zorg) en Acute zorg; Het LSP kent een Medisch Autorisatie Protocol (MAP), er is een autorisatierichtlijn voor medicatieveiligheid (https://www.vzvz.nl/actueel/nieuwe-autorisatierichtlijn-medicatieveiligheid). In het kader van radiologisch onderzoek is binnen Twiin een concept autorisatierichtlijn opgesteld.
2. Te raadplegen op: https://nvz-ziekenhuizen.nl/toegangsbeveiliging-digitale-patientdossiers
3. Centraal Tuchtcollege, 29 januari 2021 (ECLI:NL:TGZCTG:2021:36) vindplaats.

5.4 | Vertrouwen: Behandelrelatie

andelrelatie

De verantwoordelijke gebruiker mag alleen toegang krijgen tot de patiëntgegevens, indien er een (actieve) behandelrelatie is tussen de patiënt en deze gebruiker én een actieve behandelingsovereenkomst met de zorgaanbieder.

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 patiënt '*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 patiënt geen inlichtingen over de patiënt verstrekken. Ze mogen anderen dan de patiënt ook geen inzage in of afschrift van de gegevens uit het dossier bieden, zonder toestemming van de patiënt. 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 patiënt.

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

Verzenden van gegevens

Bij het verzenden van gegevens verstuurt de dossierhouder zelf actief patiëntgegevens 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 patiënt 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 patiënt al bekend is. Het beroepsgeheim staat eraan in de weg dat de raadpleger gegevens opvraagt bij alle zorgaanbieders die zijn aangesloten bij het elektronisch uitwisselingssysteem. Op die manier zou de dossierraadpleger aan zorgaanbieders die de patiënt niet kennen, bekend maken dat hij een behandelingsovereenkomst heeft met de patiënt. Dat is onwenselijk. Immers valt ook het bestaan van de geneeskundige behandelingsovereenkomst 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 lokalisatie-voorziening is hiervoor een geschikte oplossing. De lokalisatie-voorziening zorgt ervoor dat alleen gegevens worden opgevraagd bij zorgaanbieders waar de patiënt 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 patiënt. De dossierhouder kan dit echter niet goed zelf controleren. De dossierhouder is vaak niet betrokken bij een opvolgend zorgtraject. Wanneer de huisarts de patiënt bijvoorbeeld doorverwijst naar het ziekenhuis, weet de huisarts niet altijd welk ziekenhuis de patiënt 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 patiënt heeft. Wenselijk is om aanvullend op de afspraak over controle van de logging te zorgen voor een notificatie van de raadpleging naar de patiënt. Twiin geeft hier nog geen invulling aan.

Behandelrelatie zorgverlener bij raadplegen van gegevens

Welke zorgverleners de patiënt 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 patiënt, 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 zoals Single-Sign-On.

Principe	**Wie is 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	De dossierraadpleger en -ontvanger moeten beide een autorisatiestru	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. Zo nodig moeten zorgaanbieders aanvullende logging en controle van logging inrichten.

	Bij raadpleegbaar maken:* Dossierraadpleger	ctuur hebben ingericht en zorgdragen voor logging en adequate controle van de logging. Twiin geeft nog geen invulling aan een inrichting voor notificatie van de raadpleging naar de patiënt. Ook geeft Twiin nog geen invulling aan controle van de behandelrelatie door middel van feitelijke omstandigheden zoals Single-Sign-On.		

* Verzenden en raadpleegbaar maken verwijzen naar de twee typen communicatiepatronen.

5.5 | Vertrouwen: Patiënttoestemming

Patiënttoestemming

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

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 noodsituaties. Wel is vereist dat de patiënt 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 patiënt 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 patiënt 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 patiënt uitdrukkelijke toestemming heeft gegeven, voordat gegevens beschikbaar worden gemaakt voor raadplegen via een elektronisch uitwisselingssysteem. De brondossierhouder 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 patiënttoestemming/het bezwaar elders beleggen. Het gebruikte uitwisselingssysteem kan dit bijvoorbeeld namens de bron doen.

Ontwikkelingen

Er is een norm in ontwikkeling, NEN 7517, over toestemming. Daarnaast is er een consultatie geweest over het Wetsvoorstel opvraagbaarheid gegevens voor spoedeisende zorg waarop Twiin ook een reactie heeft ingediend. Twiin volgt de ontwikkelingen en sluit daarop aan

Principe	Wie is verantwoordelijk Dossierhouder of dossierraadpleger/-ontvanger	Invulling Twiin	Toelichting
De dossierhouder is verantwoordelijk voor de controle van de toestemming van de patiënt. *Bij verzenden*:* Veronderstelde toestemming is toegestaan als het gaat om de use case verwijzen. Bij opvragen dossier is WGBO-	Dossierhouder	Gebruik van Mitz bij raadpleegbaar maken	Twiin onderschrijft de wens van menig patiënt dat deze de toestemming voor de uitwisseling van gegevens via één

toestemming vereist. *Bij raadpleegbaar maken*:* Voorafgaande uitdrukkelijke toestemming is vereist.			kanaal kan regelen en dit niet per zorgaanbieder hoeft te doen. Deze mogelijkheid biedt Mitz. De patiënt kan binnen Mitz zijn eigen toestemmingskeuzes vastleggen. Daarnaast kan de zorgaanbieder namens de patiënt toestemmingskeuzes vastleggen in Mitz.

* Verzenden en raadpleegbaar maken verwijzen naar de twee typen communicatiepatronen.

5.6 | Vertrouwen: Logging

ging

Logging vindt zowel plaats bij de raadplegende/ontvangende partij als de dossierhouder. Hiermee wordt voldaan aan de NEN7513. Daarnaast biedt het de dossierhouder inzage in wie patiëntgegevens heeft uitgewisseld en onder welke autorisatie dit is gedaan.

Gestandaardiseerde logging

Uit zowel artikel 15e Wabvpz en NEN 7510, NEN 7512 en met name NEN 7513 volgt dat zorginstellingen patiënten inzage moeten kunnen geven in wie toegang heeft gehad tot het patiëntdossier. 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 zorginstelling) of landelijke communicatie, moet logging uit verschillende bronnen vergelijkbaar zijn. Hiertoe moet een export faciliteit aanwezig zijn. Hierbij moet syntax en semantiek van de export vastliggen volgens de eisen in de NEN-norm. Telkens wanneer patiëntgegevens worden uitgewisseld, dienen loggegevens bijgehouden te worden.

Patiëntinzage

Patiënten 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 worden getoond. Indien een patiënt twijfelt aan de rechtmatigheid van een raadpleging, of de juistheid van de gegevens in het log, kan hij zich wenden tot de betreffende zorgaanbieder.

Principe	Wie is 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 patiënten mogelijk is.	Dossierhouder en dossierraadpleger/-ontvanger	Deelnemers binden zich via de Voorwaarden Twiin Deelnemer aan het geven van inzage aan patiënten	Wenselijk is een gemeenschappelijke voorziening waarmee de patiënt inzage krijgt in de logging (van de uitwisselingen) van deelnemers van Twiin, maar deze is nog niet beschikbaar.
De communicerende partijen moeten afspraken maken over de interne inzage in en systematische controle van logging.	Dossierhouder en dossierraadpleger/-ontvanger	Deelnemers binden zich via de Voorwaarden Twiin Deelnemer aan het uitvoeren van de logging.	-
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	Deelnemers binden zich via de Voorwaarden Twiin Deelnemer aan het uitvoeren van de logging.	-

5.7 | Vertrouwen: Transparantie

nsparantie

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

Privacy statement

Artikel 12 van de AVG verplicht de zorgaanbieder als verwerkingsverantwoordelijke tot transparante verwerking van persoonsgegevens. De zorgaanbieder moet aan de patiënt 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;
- en, wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens.

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) gelden aanvullende eisen ten aanzien van transparantie. Artikel 15c Wabvpz verplicht de zorgaanbieder de patiënt 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 patiënt over deze wijziging, alsmede over de mogelijkheid om de gegeven toestemming aan te passen of in te trekken.

Patiëntinzage

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

Principe	Wie is verantwoordelijk Dossierhouder of dossierraadpleger/-ontvanger	Invulling Twiin	Toelichting
Zorgaanbieders moeten de patiënt 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 patiënt in de privacyverklaring goed informeren over uitwisseling en over zijn AVG-rechten en tevens moeten zij zorgdragen voor een procedure waarmee patiënten de logging kunnen opvragen.	Niet van toepassing

6 | Governance

Inhoud

Inleiding

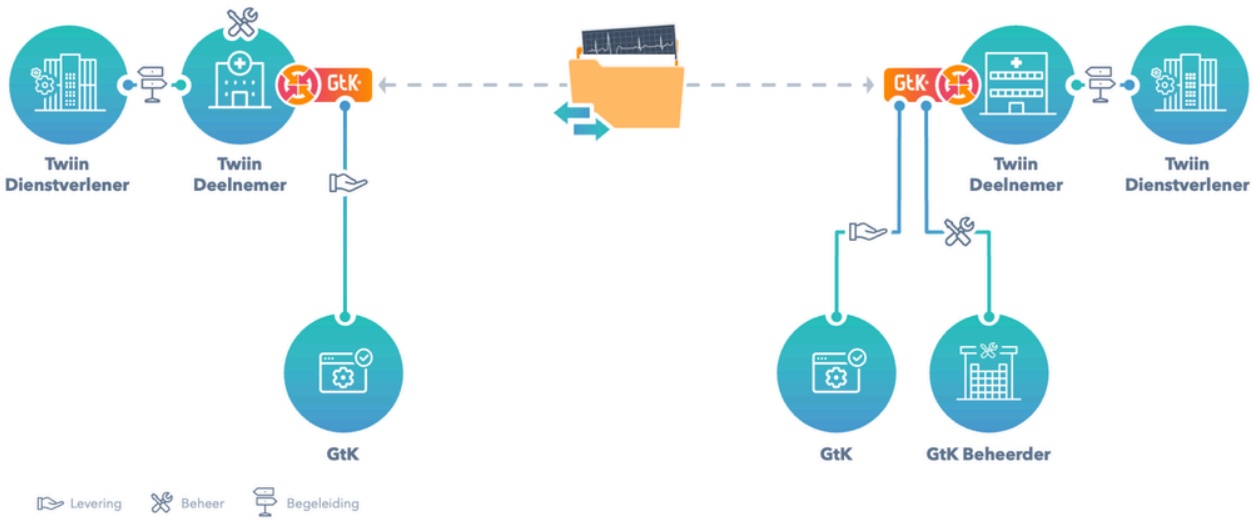
Onder governance verstaan we de inrichting van de rollen, taken, verantwoordelijkheden en spelregels die nodig zijn voor het beheer en de doorontwikkeling van het Twiin Afsprakenstelsel. In het Twiin Afsprakenstelsel is vastgelegd hoe de inspraak en de besluitvorming wordt georganiseerd, wie de betrokken 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 committeren aan het Twiin Afsprakenstelsel. Dan wordt uitgelegd hoe validatie is ingericht. Als laatste 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:

1. 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. 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. Op termijn wordt de rol van Twiin Bestuur ingevuld door een eigenaarsraad met vertegenwoordigers van de twee Overlegtafels die benoemd zijn in het reglement. Die eigenaarsraad zal dan worden ondergebracht bij een bestaande of een nog op te richten rechtspersoon.
2. De Twiin Deelnemer wisselt binnen de kaders van het Twiin Afsprakenstelsel gegevens uit met andere Twiin Deelnemers.
3. De Twiin Dienstverlener die diensten aanbiedt aan één of meer Twiin Deelnemers, waaronder het begeleiden van de Twiin Deelnemer bij de implementatie, beheer en ontwikkeling van één of meer Zorgtoepassingen binnen een regio en/of binnen een categoraal netwerk en het ondersteunen van de Twiin Deelnemer om te voldoen aan het Twiin Afsprakenstelsel.
4. De GtK Beheerder die beheertaken uitvoert ten aanzien van een GtK, waaronder het inrichten van een servicedesk.
5. De GtK Leverancier is de leverancier van een GtK.



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) tekent 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 Voorwaarden Twiin Deelnemer. 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 Voorwaarden Twiin Dienstverlener vervult, waaronder het beheer van de Samenwerkingsvoorwaarden voor Twiin Deelnemer. 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.

Twiin Deelnemer zorgt ervoor dat de voorwaarden Twiin Dienstverlener zijn belegd en ook de Voorwaarden GtK Beheer. Als de Twiin Deelnemer een externe partij inschakelt voor GtK beheer, maakt 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 Dienstverleningsovereenkomst en Beheerovereenkomst. Deze modelovereenkomsten zijn op te vragen via info@twiin.nl.

Verklaringen

Verklaring Twiin Dienstverlener

De Twiin Dienstverlener ondertekent de Verklaring Twiin Dienstverlener. Daarin verklaart deze partij dat hij de taken en verantwoordelijkheden op zich te neemt zoals die in het Twiin Afsprakenstelsel voor deze rol staan beschreven. De Twiin Organisatie onderschrijft met het ondertekenen 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 Verkrijgen verklaring Twiin Dienstverlener.

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 reglement, is vereist dat GtK Beheerder de Verklaring GtK Beheerder tekent met de Twiin Organisatie. Daarin verklaart de GtK Beheerder dat hij de taken en verantwoordelijkheden op zich te neemt zoals die in het Twiin Afsprakenstelsel voor zijn rol staan beschreven. De Twiin Organisatie onderschrijft met de verklaring dat de diensten die de GtK Beheerder aanbiedt, passend zijn om invulling te geven aan hun rol zoals omschreven in het Twiin Afsprakenstelsel.

Het proces voor het tekenen van een Verklaring GtK Beheer is beschreven onder het menu Verkrijgen verklaring GtK Beheerder.

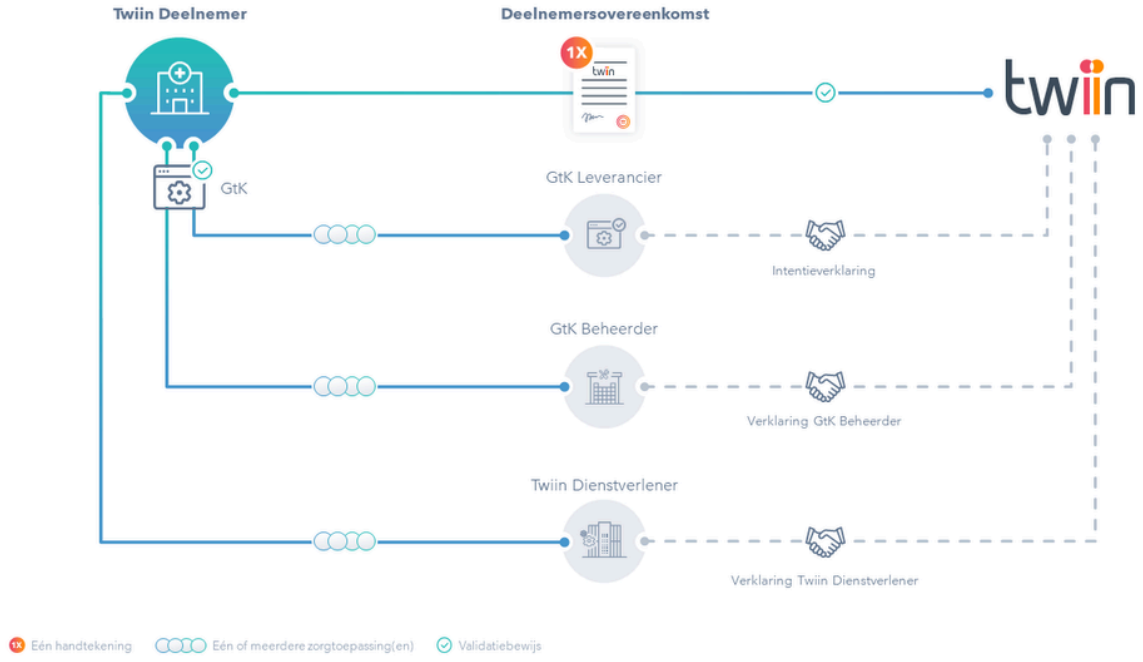
Intentieverklaring GtK Leverancier

Een leverancier die een applicatie of functionaliteit wil laten valideren als GtK, tekent eerst een Intentieverklaring met de Twiin Organisatie waarin is bepaald dat de leverancier zich inspant om zo goed mogelijk te voldoen aan het Twiin Afsprakenstelsel.

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 Validatie Twiin Deelnemer 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 Validatie GtK 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 Releasebeleid bepaalt hoe vaak wijzigingen door middel van een nieuwe release kunnen worden doorgevoerd en welke versies geldig zijn. Het Reglement beschrijft hoe de relevante stakeholders worden betrokken bij de ontwikkeling van het Twiin Afsprakenstelsel. 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 inbreng en 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;
x. Twiin Dienstverlener: een implementatie- en kennispartner die de regie voert op 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.

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 patiënten 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 en het beleid van het Twiin Afsprakenstelsel, alsmede de voor de Deelnemer relevante architectuur en technische specificaties; 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. De 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 de GtK en tussen de eigen GtK en die van andere Twiin Deelnemers.

b. Deelnemer is ervoor verantwoordelijk dat het beheer van de 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 haar ingeschakelde Twiin Dienstverlener(s) en stelt de Twiin Organisatie op de hoogte als sprake is van een wisseling.

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 en 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: Deed - Attribution-ShareAlike 4.0 International - Creative Commons .
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 patiënt.

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. Twiin is een programma van VZVZ, ZN en RSO-NL dat op korte termijn zal worden ondergebracht in de Twiin Organisatie, waarvoor VZVZ een aantal operationele beheertaken uitvoert.

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 Voorwaarden Twiin Dienstverlener 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 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. Twiin is een programma van VZVZ, ZN en RSO-NL dat op korte termijn zal worden ondergebracht in de Twiin Organisatie, waarvoor VZVZ een aantal operationele beheertaken uitvoert.

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 Voorwaarden GtK Beheer 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.

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 haar 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 offlinecommunicatie.

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: Functie: Datum, plaats: Handtekening:	Naam: Functie: Datum, plaats: Handtekening:

6.5 | Releasebeleid

Het Twiin Afsprakenstelsel ontwikkelt zich voortdurend. Ontwikkelingen binnen en rondom Twiin 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.

Release frequentie

- 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 post-fix

- Aan de onderdelen van de release kan een postfix worden toegevoegd om te duiden wat de status is:
  - **Zonder toevoeging:** Een versie met de status normatief;
  - **Review**: Een versie ter review;
  - **Trial**: Een versie voor beproeving.

- De onderdelen in het ontwikkelsupplement kunnen de volgende statussen hebben:
  - **Informative:** Een informatieve toelichting over wat Twiin voor dit onderdeel te bieden heeft (is onderdeel van het ontwikkelsupplement);
  - **Draft**: Een conceptuele beschrijving, vaak nog onvolledig (is onderdeel van het ontwikkelsupplement);
  - **Candidate:** Een kandidaat Zorgtoepassing die nog in ontwikkeling is.

Afhankelijkheid Release Twiin Afsprakenstelsel en de Twiin Zorgtoepassingen

- Het Twiin Afsprakenstelsel en de Zorgtoepassingen van het Twiin Afsprakenstelsel hebben beide eigen versienummers, maar zijn wel van elkaar afhankelijk.
- Zorgtoepassingen met hetzelfde majornummer zijn compatibel met het Twiin Afsprakenstelsel met hetzelfde majornummer. Bij verhoging van een majorrelease van het Twiin Afsprakenstelsel zal de Zorgtoepassing ook een nieuw majornummer release krijgen.
- Twiin spant zich ervoor in dat de Zorgtoepassingen zoveel mogelijk op elkaar aansluiten en in lijn zijn met de landelijke ontwikkelingen en Twiin houdt hier rekening mee bij de planning van nieuwe releases.

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.

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 besluitvorming over de verdere ontwikkeling van het Twiin Afsprakenstelsel, waaronder bij het vaststellen van nieuwe releases van het Twiin Afsprakenstelsel in overeenstemming met het releasebeleid.

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, te onderhandelen en te beslissen over de onderwerpen die op de agenda staan van het overleg en ter zake kundig 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, te onderhandelen en te beslissen 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.

Artikel 6. Taken

Iedere Overlegtafel heeft de volgende taken:

- Adviseren van het Twiin Bestuur over doorontwikkeling en toepassing van het Twiin Afsprakenstelsel.
- Adviseren van het Twiin Bestuur over implementatievraagstukken die impact hebben op 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. Besluiten

a. De besluiten van de beide Overlegtafels betreffen in ieder geval advies over vaststellen van een nieuwe major of minor release en advies over de onderwerpen voor een eerstvolgende release, de release roadmap. De Overlegtafels worden voorafgaand aan publicatie geïnformeerd over het uitbrengen van een patch release. De Twiin Organisatie kan bij het vaststellen van een nieuwe release alleen gemotiveerd afwijken van een advies van een Overlegtafel, behalve voor zover artikel 7.b en/of 7.c van toepassing is.

b. In geval van een negatief advies van een Overlegtafel dient de Twiin Organisatie een aangepast voorstel in waarin recht wordt gedaan aan de bezwaren zoals verwoord in het negatieve advies. Beide Overlegtafels krijgen vervolgens minimaal 30 dagen gelegenheid om nogmaals advies uit te brengen. In het geval één van beide Overlegtafels over het herziene voorstel een negatief advies afgeeft, roept de Twiin Organisatie beide Overlegtafels gezamenlijk bijeen om een oplossing te zoeken waarmee beide Overlegtafels akkoord gaan. In het geval er geen oplossing wordt gevonden die door beide Overlegtafels gedragen is, neemt het Twiin Bestuur zo nodig 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.

Artikel 8. Wijze van besluitvorming

a. Reguliere besluitvorming is bij voorkeur op basis van consensus. Wanneer dit niet mogelijk blijkt, worden reguliere besluiten genomen met meerderheid van stemmen. Negatieve adviezen over (een deel van) een nieuwe release worden genomen met minimaal tweederde van de stemmen en worden voorzien van een onderbouwing en - voor zover mogelijk - een alternatief voorstel.

b. Bij afwezigheid kan een lid van de Overlegtafel zijn standpunt ten aanzien van een of meerdere agendapunten of voorliggende besluiten voorafgaand schriftelijk kenbaar maken aan de voorzitter of secretaris, in welk geval de voorzitter dit mee zal nemen bij de stemming over de betreffende agendapunten. Een lid van een Overlegtafel kan zich tijdens een vergadering ook laten vertegenwoordigen door een van de andere leden van de desbetreffende Overlegtafel. Dit dient voorafgaand aan de vergadering per mail aan de secretaris te worden medegedeeld.

Artikel 9. Wijziging en aanvulling Reglement

a. De beide Overlegtafels evalueren jaarlijks de van 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 alle relevante 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 dit Twiin Afsprakenstelsel, kunnen Twiin Deelnemers gegevens uitwisselen via een GtK. Welke partij welke rol heeft binnen het Twiin Afsprakenstelsel is omschreven in de governance. Wat er van deze partijen wordt verwacht en welke eisen worden gesteld, moet passen binnen het wetgevend kader.

In dit hoofdstuk staat een overzicht van de wet- en regelgeving en de normen die van toepassing is 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

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 6 oktober 2024). Dit overzicht zal worden uitgebreid met de verordening betreffende de Europese ruimte voor gezondheidsgegevens (ook wel genoemd “EHDS”) als deze verordening is vastgesteld. In grote lijnen omschrijft het hoofdstuk Visie hoe het Twiin Afsprakenstelsel zich verhoudt tot de EHDS. Ook het wetsvoorstel identificatie en authenticatie in de zorg (Wet Diaz) zal worden opgenomen, zodra deze is vastgesteld.

Naam en vindplaats	Afkorting
Wet op de geneeskundige behandelingsovereenkomst https://wetten.overheid.nl/BWBR0005290/2021-07-01#Boek7_Titeldeel7_Afdeling5	WBGO
Wet beroepen individuele gezondheidszorg https://wetten.overheid.nl/BWBR0006251/2021-07-01	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/BWBR0037173/2021-07-01	Wkkgz
Algemene verordening gegevensbescherming Deze Europese verordening vervangt sinds 25 mei 2018 de Richtlijn bescherming persoonsgegevens en de Wet bescherming persoonsgegevens (Wbp) en bevat onder meer de meldplicht datalekken (voorheen de Wet meldplicht datalekken) https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex%3A32016R0679	AVG
Uitvoeringswet Algemene verordening gegevensbescherming Implementatiewetgeving die de normen in de AVG voor Nederland nader invult https://wetten.overheid.nl/BWBR0040940/2020-01-01	UAVG
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/BWBR0023864/2020-07-01	Wabvpz
Besluit elektronische gegevensverwerking door zorgaanbieders Dit besluit van 10 november 2017, beschrijft nadere regels over functionele, technische en organisatorische maatregelen bij elektronische gegevensverwerking door en tussen zorgaanbieders https://wetten.overheid.nl/BWBR0040238/2020-10-01	Begz
Wet elektronische gegevensuitwisseling in de zorg wetten.nl - Regeling - Wet elektronische gegevensuitwisseling in de zorg - BWBR0048095 (overheid.nl)	Wegiz
Besluit elektronische gegevensuitwisseling in de zorg wetten.nl - Regeling - Besluit elektronische gegevensuitwisseling in de zorg - BWBR0048096 (overheid.nl)	Begiz

Verordening betreffende elektronische identificatie en vertrouwensdiensten Deze verordening maakt wederzijdse erkenning van nationale inlogmiddelen mogelijk en vervangt de eerdere Richtlijn 1999/93/EG. Voor Twiin is eIDAS relevant nu de NEN7510 naar deze wet verwijst voor de betrouwbaarheidsniveaus voor authenticatiemiddelen EUR-Lex - 32014R0910 - EN - EUR-Lex (europa.eu) Betrouwbaarheidsniveaus van stelsels voor elektronische identificatie (artikel 8)	eIDAS

Tabel 2.1: De belangrijkste wetten op het gebied van zorginformatie-uitwisseling

Wet op de geneeskundige behandelingsovereenkomst (WGBO)

De WGBO bevat onder andere het recht van de patiënt:

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

Deze wet verplicht de zorgverlener onder andere:

- zich te houden aan de professionele standaard en de kwaliteitsstandaarden;
- te voldoen aan de informatieplicht richting de patiënt;
- te voldoen aan de dossierplicht.

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

De zorgverlener is op basis van deze wet gebonden aan het medische beroepsgeheim. Hij mag dus niet zonder toestemming van de patiënt aan anderen dan de patiënt inlichtingen over de patiënt 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 patiënt wél inzien zonder toestemming van de patiënt, mits noodzakelijk voor het uitvoeren van hun werkzaamheden.

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.

Wet beroepen individuele gezondheidszorg (Wet BIG)

De Wet BIG heeft als doel om de kwaliteit van de beroepsuitoefening te bevorderen en te bewaken en de patiënt 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. Verder voorziet de Wet BIG de beroepsbeoefenaren in tuchtrechtspraak. Dit is een bijzondere vorm van rechtspraak die erop gericht is de kwaliteit van de beroepsuitoefening te bevorderen en bewaken.

Beroepsbeoefenaren

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.

Registers

Voor elk van de genoemde beroepen stelt de rijksoverheid registers in. Het gaat hier om een zogeheten constitutieve registratie. Die komt erop neer dat alleen geregistreerde personen de beroepstitel mogen voeren en dat alleen zij vallen onder het tuchtrecht. 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)

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 patiënten een klacht hebben over de zorg. Op basis van de Wkkgz kunnen patiënten 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 tekenen, totdat anders wordt besloten conform de besluitvormingsprocedure die in het reglement 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 en de GtK Beheerder zoals uitgewerkt in de governance.

Algemene verordening gegevensbescherming (AVG)

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: 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 zijn 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 is 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

Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)

De UAVG geeft een nadere invulling voor de toepassing van 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).

De UAVG wijst de Autoriteit Persoonsgegevens aan als de toezichthouder voor de AVG die handhavend kan optreden.

Toepassing op het Twiin Afsprakenstelsel

Iedere Twiin Deelnemer is zelfstandig verwerkingsverantwoordelijke voor de verwerking van persoonsgegegevens in de eigen zorginformatiesystemen waaronder de GtK. Daaruit volgen een aantal 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.
- De Twiin Deelnemer moet voldoen aan de toepasselijke beveiligingsnormen, waaronder met name NEN 7510, NEN 7512 en 7513. Het vertrouwensmodel legt op een aantal onderdelen vast op welke wijze zorgaanbieders invulling geven aan deze normen. Tevens is het onderdeel transparantie van het vertrouwensmodel een invulling van het recht van de betrokkene op transparantie. Het onderdeel patiënttoestemming van het vertrouwensmodel is een invulling van de AVG-grondslag toestemming.
- De Twiin Deelnemer is ervoor verantwoordelijk dat hun eigen GtK voldoen aan de toepasselijke beveiligingsnormen, waaronder met name NEN 7510, NEN 7512 en 7513. Met het proces validatie GtK toetst de Twiin Organisatie de naleving van deze normen.
- 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. Deelnemer is verplicht om een (sub)verwerkersovereenkomst te (laten) sluiten met alle verwerkers zoals uitgewerkt in de Voorwaarden Twiin Deelnemer.
- De Twiin Deelnemer is gehouden om zelf een gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren als het gaat om verwerkingsactiviteit met een hoog privacyrisico zoals ook vastgesteld in de Voorwaarden Twiin Deelnemer.

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 hoeven ook niet door de Twiin-organisatie te worden ontwikkeld en/of beheerd. De Twiin-organisatie heeft zodoende geen rol van eigenaar, verwerkingsverantwoordelijke of (sub)verwerker ten aanzien van deze gemeenschappelijke voorzieningen.

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. De belangrijkste rechten van de patiënt 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 betrokken op basis van de AVG.

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

- De plicht de patiënt 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 zijn patiënt uitdrukkelijke toestemming te vragen voor het beschikbaar stellen van de patiëntgegevens via een elektronisch uitwisselingssysteem;
- De patiënt te informeren als nieuwe categorieën zorgverleners aansluiten bij het elektronisch uitwisselingssysteem.

Toepassing op het Twiin Afsprakenstelsel

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

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

In het onderdeel patiënttoestemming van het vertrouwensmodel is vastgelegd hoe Twiin Deelnemers de de uitdrukkelijke toestemming van de patiënt registreren zoals vereist in de Wabvpz. In het onderdeel transparantie van het vertrouwensmodel is nadere invulling gegeven aan de wijze waarop Twiin Deelnemers de patiënt informeren zoals vereist in de Wabvpz.

Het gebruik van het BSN

De Wabvpz bevat verplichtingen over het gebruik van het BSN. Om patiënten 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 patiënten. 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 Berichten Voorziening in de Zorg) die zorgen voor de ontsluiting van het BSN-register en het Registratie Niet-ingezetenen.
- BSN-validatie
  Zodra de nieuwe patiënt voor het eerst in het ziekenhuis 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 twijfels zijn 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 patiënt wel bekend is binnen een ziekenhuis-informatiesysteem, maar dat deze nog niet is gevalideerd. Bijvoorbeeld als een patiënt zich nog niet heeft geïdentificeerd met een identiteitsbewijs.

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 patiënt mag delen met een andere zorgaanbieder, moet de brondossierhouder een gevalideerd BSN van de patiënt hebben. Dat wil dus zeggen dat de patiënt fysiek in de zorginstelling is geweest en dat de identiteit van de patiënt is vastgesteld aan de hand van een wettig identiteitsdocument. (NB dit staat los van het feit dat de patiënt daarnaast toestemming moet hebben gegeven voor het delen van zijn gegevens).
- Voor het raadplegen van gedeelde patiëntgegevens van een andere zorgaanbieder, is het voldoende dat de patiënt in de eigen organisatie bekend is met een geverifieerd BSN. De patiënt 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 patiënt nog niet bekend is in de zorginstelling die gegevens raadpleegt. Uitgangspunt is in deze gevallen dat men erop kan vertrouwen dat de zorginstelling die de medische gegevens heeft vastgelegd en aangemeld voor delen buiten de zorginstelling, het BSN heeft geverifieerd. Het proces van validatie van het BSN in de raadplegende zorginstelling blijft bestaan. De eerste keer dat een patiënt daar fysiek aanwezig is, geldt de reguliere validatieprocedure.

Toepassing op het Twiin Afsprakenstelsel

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

Besluit elektronische gegevensverwerking door zorgaanbieders (Begz)

De 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.

De 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 de 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) dat de logging ten minste 5 jaar bewaard vanaf het moment dat de logregel wordt geschreven.

Overigens is de 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 NEN7510.

Toepassing op het Twiin Afsprakenstelsel

De Voorwaarden Twiin Deelnemer 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)

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 patiëntgegevens 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' 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)

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

Normen voor informatiebeveiliging – NEN 7510, 7512, 7513

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. Voor de zorgsector is een aangepaste versie van deze norm opgesteld. De reden hiervoor is dat er zorg-specifieke 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 7510:2017)

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.

Ondertekening van het uitgewisselde is ook verplicht. 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 patiëntdossier.

Toepassing op het Twiin Afsprakenstelsel

De Voorwaarden Twiin Deelnemer 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. De normen zijn toegepast in het vertrouwensmodel en dan met name in de onderdelen authenticatie, autorisatie en logging en ook in de uitwerking van die functies in de technische kern.

Normen voor generieke functies – NEN 7517, 7518, 7519, 7520

De normen voor generieke functies zijn nog in ontwikkeling. Het gaat om toestemming (NEN 7517), identificatie en authenticatie (NEN7518), lokalisatie (NEN7519) 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.

Normen voor specifieke gegevensuitwisselingen – NEN 7503, NEN 7540, NEN 7541

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.

NEN 7540, Basisgegevensset Zorg (NEN 7540:2024)

NEN 7540 specifieert twee usecases voor de uitwisseling van de BgZ tussen instellingen voor medisch specialistische zorg. De twee usecases zijn: uitwisseling BgZ bij verwijzing of overdracht en opvraging BgZ bij eerdere behandelaar. NEN 7540 formuleert eisen voor voor zorgaanbieders om hiervoor de gecertificeerde zorginformatiesystemen en elektronische uitwisselingssystemen zorgvuldig in te zetten en te beheren.

NEN 7541, Beeldbeschikbaarheid

De norm voor beeldbeschikbaarheid is nog in ontwikkeling. Twiin volgt de ontwikkeling van de NEN-normering en zal de Implementatiewijzer Beeldbeschibaarheid 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 erxpertise.

Toepassing op het Twiin Afsprakenstelsel

Twiin heeft een implementatiewijzer opgesteld voor de Implementatiewijzer Basisgegevensset Zorg.

8 | Diensten

Twiin biedt diensten aan voor toetreding en validatie. De processen die bij deze diensten horen zijn per dienst uitgewerkt.

Uitgangspunten

Processen worden onder begeleiding van een Twiin Casemanager doorlopen.

Diensten zijn ingericht op basis van de volgende uitgangspunten:

- We gebruiken zo veel als mogelijk bestaande organisaties, diensten en structuren.
- We organiseren het beheer zo dicht mogelijk bij de bron: lokaal dan wel regionaal. Hierdoor ontstaan efficiënt ingerichte beheerprocessen en dienstverlening. Regie vindt plaats op landelijk niveau.
- Alleen neutrale en onafhankelijke organisaties kunnen/mogen de diensten van Twiin aanbieden; zakelijke belangen mogen geen invloed hebben op het beheer van Twiin.

Onderliggende pagina’s

8.1 | Toetreden

In dit hoofdstuk is omschreven hoe de verschillende partijen toetreden tot het Twiin Afsprakenstelsel. Per rol is omschreven hoe partijen zich verbinden aan dit afsprakenstelsel. Na het doorlopen van de bijbehorende processen, zijn de rollen, taken en verantwoordelijkheden van elke partij duidelijk voor betrokkenen.

8.1.1 | Toetreden Deelnemer

Begrip: Twiin Deelnemer geeft aan welke Begrip: Twiin Dienstverlener is ingeschakeld, tekent vervolgens de 6.1 | Deelnemers overeenkomst en treedt daarmee toe tot het Twiin Afsprakenstelsel.

De Twiin Organisatie beheert de getekende Deelnemersovereenkomst.

8.1.2 | Verkrijgen Verklaring Twiin Dienstverlener

Omschrijving van het proces

Binnen deze dienst doorloopt een Twiin Dienstverlener samen met een Twiin Casemanager de taken en verantwoordelijkheden. Deze taken en verantwoordelijkheden volgen uit de Voorwaarden Twiin Dienstverlener die bij de rol Twiin Dienstverlener horen.

Na het doorlopen van de taken en verantwoordelijkheden geeft Twiin een Verklaring Twiin Dienstverlener af. Twiin zal een overzicht van Twiin Dienstverleners publiceren.

Toegevoegde waarde

Door de verklaring te ondertekenen geeft de Twiin Dienstverlener aan bereid te zijn om 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 Organisatie en de Twiin Deelnemers duidelijk welke partijen ze kunnen benaderen voor ondersteuning bij hun deelname aan Twiin.

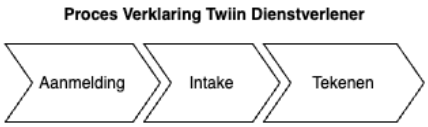
Doelstelling

De doelstelling van het Proces Verklaring Twiin Dienstverlener is dat een partij die de rol Twiin Dienstverlener zou willen invullen op de hoogte wordt gebracht van wat de bijbehorende taken en verantwoordelijkheden zijn. Deze taken en verantwoordelijkheden volgen uit de Voorwaarden Twiin Dienstverlener. De Twiin Organisatie houdt een lijst bij met Twiin Dienstverleners zodat het voor een Twiin Deelnemer makkelijker is om een Twiin Dienstverlener te vinden.

Verantwoordelijkheden

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

Toelichting processtappen Verkrijgen Verklaring Twiin Dienstverlener



1. Aanmelden	
Input	Aanmelding van een Twiin Dienstverlener
Activiteit	Een nieuwe Twiin Dienstverlener meldt zich bij de Twiin Organisatie.
Output	Informatie over de nieuwe 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 Twiin Dienstverlener samen met de Twiin Organisatie of deze organisatie deze rol kan vervullen. De Twiin Organisatie en de Twiin Dienstverlener tekenen vervolgens de Verklaring Twiin Dienstverlener.
Output	Verklaring Twiin Dienstverlener
Wie?	• Twiin Casemanager • Twiin Organisatie • Twiin Dienstverlener

8.1.3 | Verkrijgen Verklaring GtK Beheerder

Omschrijving van het proces

Binnen deze dienst doorloopt een GtK Beheerder samen met een Twiin Casemanager de taken en verantwoordelijkheden. Deze taken en verantwoordelijkheden volgen uit de Voorwaarden GtK Beheer die bij de rol GtK beheerder horen.

Na het doorlopen van de taken en verantwoordelijkheden geeft Twiin een Verklaring GtK Beheerder af. Twiin zal een overzicht publiceren van GtK Beheerders.

Toegevoegde waarde

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

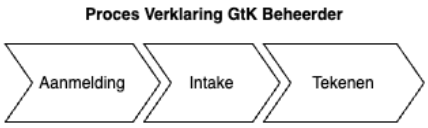
Doelstelling

Het doel van het Proces Verkrijgen Verklaring GtK Beheerder is dat een partij die de rol van GtK Beheerder zou willen vervullen op de hoogte wordt gebracht van wat de bijbehorende taken en verantwoordelijkheden zijn. Deze taken en verantwoordelijkheden volgen uit de Voorwaarden GtK Beheer. De Twiin Organisatie houdt een lijst bij met GtK Beheerders, zodat het voor een Twiin Deelnemer makkelijker is om een GtK Beheerder te vinden.

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 Verkrijgen Verklaring GtK Beheerder



1. Aanmelden	
Input	Aanmelding van een GtK Beheerder
Activiteit	Een nieuwe GtK Beheerder meldt zich bij de Twiin Organisatie.
Output	Informatie over de nieuwe GtK Beheerder
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 Casemanager • Twiin Organisatie • GtK Beheerder

8.1.4 | Verkrijgen Verklaring GtK Leverancier

Omschrijving van het proces

Binnen deze dienst doorloopt een GtK Leverancier samen met een Twiin Casemanager de Voorwaarden GtK om na te gaan of het mogelijk is om een GtK van de GtK Leverancier te laten valideren voor één of meer Zorgtoepassing.

Na het doorlopen van de Voorwaarden GtK, kan de Verklaring GtK Leverancier getekend worden. De Twiin Organisatie zal een overzicht publiceren van GtK's.

Toegevoegde waarde

Door de verklaring te ondertekenen geeft de GtK Leverancier aan bereid te zijn om te 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 voor welke Zorgtoepassing(en).

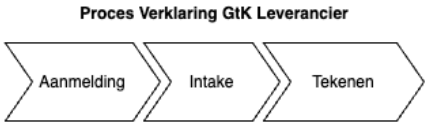
Doelstelling

De doelstelling van het Proces Ondertekenen Verklaring GtK Leverancier is dat een partij die de rol GtK Leverancier zou willen invullen op de hoogte wordt gebracht van wat de Voorwaarden GtK zijn. De Twiin Organisatie houdt een lijst bij met GtK Leveranciers zodat het voor een Twiin Deelnemer makkelijker is om een GtK te vinden.

Verantwoordelijkheden

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

Toelichting processtappen Verkrijgen Verklaring GtK Leverancier



1. Aanmelden	
Input	Aanmelding van een GtK Leverancier
Activiteit	Een nieuwe GtK Leverancier meldt zich bij de Twiin Organisatie.
Output	Informatie over de nieuwe GtK Leverancier
Wie?	• Twiin Casemanager • GtK Leverancier

2. Intake	
Input	Lijst Voorwaarden GtK
Activiteit	Een Twiin Casemanager doorloopt samen met de GtK Leverancier de Voorwaarden GtK voor één of meer zorgtoepassingen.

Output	Ingevuld intakeformulier
Wie?	• Twiin Casemanager • GtK Leverancier

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

8.2 | Valideren

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

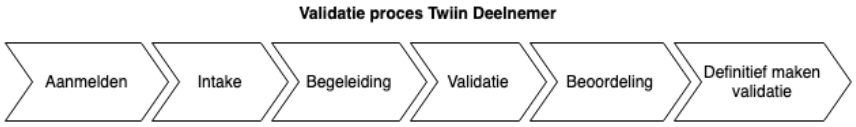
In de onderliggende pagina's staat een korte omschrijving van de dienst en de toegevoegde waarde.

8.2.1 | Validatie Twiin Deelnemer

Omschrijving van de dienst

Het valideren van een Twiin Deelnemer per zorgtoepassing. Twiin doorloopt met de Twiin Deelnemer het Proces Validatie Twiin Deelnemer.

Proces Validatie Twiin Deelnemer



Doelstelling

De doelstelling van het Proces Validatie Twiin Deelnemer is om op een zorgvuldige en beheerste wijze deelnemers te valideren om aan te tonen dat een Twiin Deelnemer voldoet aan alle voorwaarden van het Twiin Afsprakenstelsel om landelijk gegevens uit te wisselen voor een Twiin Zorgtoepassing. Dit met als achterliggend doel om het vertrouwen te borgen tussen Twiin Deelnemers dat aan alle voorwaarden is voldaan om landelijke gegevens uit te wisselen voor die Twiin Zorgtoepassing. Een Twiin Deelnemer dient aan de 9.1 | Voorwaarden Twi in Deelnemer te voldoen om gevalideerd te worden. Een Twiin Deelnemer is verplicht een Twiin Dienstverlener aan te dragen bij het tekenen van de Twiin Deelnemersovereenkomst, een Twiin Deelnemer kan deze rol ook zelf vervullen. De Twiin Dienstverlener ondersteunt de Twiin Deelnemer tijdens het validatietraject.

Verantwoordelijkheden

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

- De Twiin Deelnemer is verantwoordelijk voor het implementeren van de voorwaarden die het Twiin Afsprakenstelsel stelt. Tijdens de validatie moet de Twiin Deelnemer hiervoor documentatie aanleveren.
- De Twiin Dienstverlener ondersteunt de Twiin Deelnemer gedurende het Proces Validatie en kan de relevante documentatie namens de Twiin Deelnemer aanleveren.
- De Twiin Casemanager voert de volgende taken uit bij het Proces Validatie Twiin Deelnemer:
  - Administratie van het dossier validatie en controle op de volledigheid ervan.
  - Controleren of deelnemer voldoet aan de voorwaarden.
  - Opstellen van het advies.
- 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 het Proces Validatie vindt plaats:

- Tijdig voor het verlopen van de geldigheid van de validatie. De geldigheid wordt meegegeven in het Bewijs van Validatie Twiin Deelnemer.
- Bij grote wijzigingen in de voorwaarden die worden gesteld aan Twiin Deelnemers.
- Op basis van het proces handhaving.

Toelichting processtappen validatie Twiin Deelnemer

Twiin neemt het verzoek van een deelnemer in behandeling. Na het doorlopen van het Proces Validatie, voldoet de Twiin Deelnemer aan de Voorwaarden Twiin Deelnemer van het Twiin Afsprakenstelsel om landelijk gegevens uit te wisselen.

1. Aanmelden	
Input	Aanmelden Twiin Deelnemer voor validatie voor een Zorgtoepassing
Activiteit	Een Twiin Deelnemer meldt zich bij Twiin met een verzoek tot validatie voor één of meer Zorgtoepassingen.
Output	Informatie over de Twiin Deelnemer.
Wie?	• Twiin Deelnemer

2. Intake	
Input	Intake van een deelnemer voor validatie van een nieuwe Zorgtoepassing
Activiteit	Een Twiin Casemanager houdt een intake en informeert de deelnemer over procedure en vereisten. Hierbij zal ook kenbaar gemaakt worden waar een deelnemer gedurende het proces met zijn vragen terecht kan.
Output	Samenvatting van intake en plan voor vervolg
Wie?	• Twiin Casemanager • Twiin Deelnemer

3. Begeleiding van de zorgaanbieder en doorlopen voorwaarden	
Input	Twiin voorwaarden en status zorgaanbieder
Activiteit	De deelnemer wordt begeleid in het voldoen aan de voorwaarden en wat daarvoor moet gebeuren. • Inrichting van processen en afspraken • Ondersteuning bij inrichting bij processen en afspraken
Output	De Twiin Deelnemer kan alle stukken aanleveren die nodig zijn voor validatie.
Wie?	• Twiin Dienstverlener • Twiin Deelnemer

4. Validatie	
Input	Dossier validatie Twiin Deelnemer
Activiteit	Controle van het dossier door Twiin Casemanager
Output	Beoordeling van dossier met advies voor validatie
Wie?	• Twiin Casemanager

5. Beoordeling advies

Input	Beoordeling van de validatie
Activiteit	Bestuur van Twiin beoordeelt de validatie o.b.v. het advies van de Twiin Casemanager.
Output	Advies en besluit, positief of negatief, over validatie van één of meer Zorgtoepassingen van deelnemer, inclusief een periode dat de validatie van kracht blijft.
Wie?	Twiin Bestuur

6. Definitief maken validatie	
Input	Positief besluit validatie Twiin Deelnemer door Twiin Bestuur
Activiteit	Twiin Deelnemer ontvangt een Bewijs van Validatie Twiin Deelnemer
Output	Bewijs van Validatie Twiin Deelnemer voor één of meer Zorgtoepassingen
Wie?	• Twiin Deelnemer • Twiin Bestuur

8.2.2 | Validatie GtK

Omschrijving van de dienst

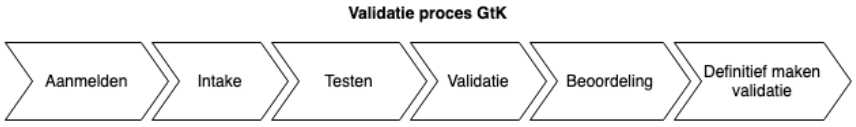
Een leverancier van een Begrip: GtK dient deze per zorgtoepassing te laten valideren door Twiin. Door testen en controle op eisen die het Twiin Afsprakenstelsel stelt aan de applicatie voor de betreffende Zorgtoepassing, toetst de Twiin Organisatie of het GtK aan alle eisen voldoet. Als dit het geval is, ontvangt het GtK een Bewijs van Validatie GtK.

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.

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

Proces Valideren GtK



Doelstelling

De doelstelling van het Proces 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 genoemd in het Twiin Afsprakenstelsel om dit vertrouwen te kunnen waarborgen.

Verantwoordelijkheden

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

- De GtK Leverancier is verantwoordelijk voor het implementeren van de eisen 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:
    - Administratie van het validatie dossier en controle op de volledigheid ervan.
    - Controleren of er voldaan wordt aan de vereisten.
    - Opstellen van het advies.
- Het Twiin Bestuur beoordeelt de validatie o.b.v. het advies van de Twiin Casemanager en geeft een Bewijs van Validatie GtK uit.

Validatie GtK

De GtK Leverancier van een GtK doorloopt het validatietraject. Wanneer het validatieproces succesvol is doorlopen, ontvangt hij voor de gevalideerde applicatie een Bewijs van Validatie GtK. Het Bewijs van Validatie GtK is enkel van toepassing op de gevalideerde versie van een de applicatie.

Validatie van een GtK is noodzakelijk als een leverancier een GtK wil inzetten binnen Twiin. De GtK Leverancier kan de GtK laten valideren voor één of meer Zorgtoepassingen.

Twiin valideert GtK's tegen een testomgeving, waarbij het GtK wordt geaccepteerd.

Hervalideren

Het opnieuw doorlopen van het Proces Validatie vindt plaats als:

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

Toelichting processtappen Validatie GtK

Na het doorlopen van het validatieproces voor GtK's, is getoetst dat de applicatie voldoet aan de eisen van het Twiin Afsprakenstelsel voor een bepaalde Zorgtoepassing.

1. Aanmelden	
Input	Aanmelden van een nieuwe leverancier of een nieuwe Zorgtoepassing van een (bestaande) leverancier
Activiteit	Een huidige of nieuwe leverancier van een GtK meldt zich bij Twiin met een verzoek tot (uitbreiding) validatie.
Output	Informatie over de nieuwe leverancier, GtK en Zorgtoepassing
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 vereisten. Bij de intake zal een intentieverklaring worden getekend door de GtK Leverancier. 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 • Getekende intentieverklaring
Wie?	• Twiin Casemanager • GtK Leverancier

3. Testen door leverancier	
Input	GtK inclusief testscript en testomgeving van Twiin

Activiteit	• Leverancier koppelt zijn GtK aan de desbetreffende testomgeving. • Leverancier doorloopt de testscenario's van de desbetreffende Zorgtoepassing. De volgende testfases worden doorlopen: • Testen van de inhoud van berichten • Testen van de gehele keten, zoals beschreven in de implementatiehandleiding van de desbetreffende Zorgtoepassing, tegen de testomgeving
Output	• Beide testfases zijn met succes doorlopen en de validatie kan starten;
Wie?	• Twiin Casemanager • GtK Leverancier

4. Validatie	
Input	GtK van de leverancier inclusief testscript en testomgeving van Twiin
Activiteit	Gedurende de validatie zullen de testen 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 testen met een advies voor validatie
Wie?	• Twiin Casemanager • GtK Leverancier

5. Beoordeling advies	
Input	Beoordeling van de validatie
Activiteit	Bestuur van Twiin beoordeelt de validatie o.b.v. het advies van de Twiin Casemanager.
Output	Advies en besluit, positief of negatief, over validatie GtK door Twiin, inclusief een periode dat de validatie van kracht blijft en een hervalidatie
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 voert de uiteindelijke regie en zorgt voor de inrichting van een communicatieplatform voor ketenregie met contactgegevens, versiebeheer en gemelde Incidenten (hierna: Twiin Serviceportaal (Supportal).
- De Twiin Deelnemer zorgt voor één aanspreekpunt van de eigen organisatie voor vermelding in het Twiin Serviceportaal en voor contact met de eigen GtK voor zover nodig.
- Twiin Deelnemers en hun GtK Beheerders hebben zelf de regie over de contactgegevens van 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 Servicedesk Twiin Deelnemer 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 het Proces Handhaving.

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. 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 verstoringen, onderhoud en repeterend onderhoud)
- Contactgegevens Servicedesk Twiin Deelnemers
- Contactgegevens GtK Beheerder van Twiin Deelnemer (indien van toepassing)
- Email notificaties
- Zoeken op Servicedesk Twiin Deelnemer.

8.3.1 | Incidentmelding

- Twiin Deelnemers zorgen voor goede afspraken met hun eigen GtK Leverancier en eventuele GtK Beheerder 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.
  - Meldingen worden gedaan in Supportal 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 waarbij bekend is welke specifieke andere partijen zijn betrokken, kunnen worden gericht aan die andere partijen (Twiin Deelnemers en hun GtK Beheerders) via de contactgegevens die te vinden zijn in Supportal.
- 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.
- Twiin Deelnemers zorgen dat hun eigen Servicedesk Twiin Deelnemer beschikbaar is conform de werkafspraken van 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 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 te starten.

8.4 | Handhaving

Het proces 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 van één of meer Incidenten.
3. Bij het constateren van niet-naleving in het kader van het doorlopen van het proces Valideren Twiin Deelnemer en/of Valideren GtK.

Het proces 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 van Twiin Deelnemer/GtK 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.
4. **Formele ingebrekestelling.** De formele ingebrekestelling is de laatste aanmaning om te voldoen aan de niet-naleving en gebeurt schriftelijk;
5. **Formele beëindiging Twiin Deelnemersovereenkomst.** 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 Intentieverklaring GtK 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 daarentegen openbaar.

De ingebrekestelling is een schriftelijke aanmaning waarin een partij door de Twiin Organisatie wordt opgedragen 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, GtK Dienstverlener en/of GtK krijgt om de niet-naleving op te heffen. Als de gestelde termijn wordt overschreden is de Twiin Deelnemer GtK Beheerder, Twiin Dienstverlener en/of GtK in verzuim en kan de overeenkomst door de Twiin Organisatie worden ontbonden.

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 de 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.

Onderliggende pagina’s

- 9.1 | Voorwaarden Twiin Deelnemer
- 9.2 | Voorwaarden Twiin Dienstverlener
- 9.3 | Voorwaarden GtK Beheer
- 9.4 | Voorwaarden GtK

9.1 | Voorwaarden Twiin Deelnemer

Zodra een Twiin Deelnemer de Deelnemersovereenkomst heeft ondertekend, is de Twiin Deelnemer gebonden aan de voorwaarden die in het schema hieronder verplicht zijn gesteld. Vanaf validatie moet de Twiin Deelnemer voldoen aan alle Twiin Voorwaarden zoals in het schema hieronder weergegeven. Na validatie ontvangt Twiin Deelnemer een bewijs van validatie waarmee Twiin Deelnemer landelijk gegevens kan uitwisselen.

Tot aan validatie gelden de Samenwerkingsvoorwaarden. Deze 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 Twiin Deelnemer.

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

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	Deelnemer heeft de Twiin Deelnemersovereenkomst ondertekend.	Ja	Ja		
1.2		Deelnemer heeft een (sub)verwerkersovereenkomst getekend met verwerker(s) die toegang heeft/hebben tot persoonsgegevens ter zake van de (kandidaat) GtK die 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	Deelnemer is gevalideerd voor de desbetreffende Zorgtoepassing.	Nee	Ja	In te vullen	In te vullen

2.2	Twiin Dienstverlener	Deelnemer is verplicht een Twiin Dienstverlener in te schakelen. Voor iedere zorgtoepassing kan de Twiin Deelnemer maar één Twiin Dienstverlener inschakelen. Deelnemer zorgt dat de Voorwaarden Twiin Dienstverlener worden vervuld. Deelnemer kan ook zelf de rol van Twiin Dienstverlener vervullen voor zichzelf en voor andere Twiin Deelnemers. In dat geval, is Deelnemer zelf gehouden om de voorwaarden van de Twiin Dienstverlener te vervullen.	Ja	Ja		
2.3	GtK Beheerder	Deelnemer zorgt dat de voorwaarden GtK beheer worden vervuld. Deelnemer kan deze verplichtingen nakomen door een GtK Beheerder in te schakelen.	Ja	Ja		
2.4	Beveiliging	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. Deelnemer beschikt over een auditverklaring voor NEN7510 of een vergelijkbare andere verklaring. * Door deel te nemen aan het Twiin Afsprakenstelsel geeft Deelnemer invulling aan NEN 7512.	Ja, waarbij de verklaring nog geen vereiste is	Ja		In te vullen vanaf wanneer audit-verklaring beschikbaar is
2.5	Privacy	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. 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 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. Deelnemer zal samenwerken met de andere Twiin Deelnemers om: i) het datalek zo nodig te melden aan de Autoriteit	Ja	Ja		

		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.				
2.6	Rechten van patiënten	Deelnemer zorgt voor een adequaat proces waarmee de patiënt te allen tijde zijn wettelijke rechten ter bescherming van zijn persoonsgegevens kan uitoefenen. Als Deelnemer een verzoek ontvangt, terwijl een andere Twiin Deelnemer voor dat verzoek verantwoordelijk is, dan zal Deelnemer die het verzoek ontvangt de andere Twiin Deelnemer hierover onverwijld informeren en de patiënt naar de juiste Twiin Deelnemer verwijzen. Deelnemer stelt de andere Twiin Deelnemers die persoonsgegevens van een patiënt 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. Deelnemer verstrekt de patiënt informatie over deze ontvangende Twiin Deelnemers indien de patiënt hierom	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	Deelnemer moet controleren op de behandelrelatie tussen zorgverlener en patiënt. Deelnemer zorgt voor een autorisatiestructuur die zo goed mogelijk borgt dat een zorgverlener enkel met een behandelrelatie toegang krijgt tot gegevens van de patiënt.	Ja	Ja		

4. Informatie

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
#	Onderwerp	Omschrijving	Verplicht vanaf ondertekening Deelnemersovereenkomst	Verplicht vanaf validatie	Eventuele afwijking	Toelichting afwijking incl. tijdpad
4.1	Algemeen	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		Deelnemer zorgt ervoor dat ter beschikking gestelde gegevens voldoen aan semantiek, formaat en structuur	Nee	Ja	In te vullen	In te vullen

		conform het Twiin Afsprakenstelsel en gebruikte Nictiz informatiestandaarden, zoals vastgelegd in de Aansluit- en implementatiewijzer.				
4.3	Metadata	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		Deelnemer maakt alleen gebruik van gevalideerde Twiin knooppunten (GtK's).	Nee	Ja	In te vullen	In te vullen
5.2		Deelnemer is verantwoordelijk voor implementatie van de GtK conform het Twiin Afsprakenstelsel.	Nee	Ja	In te vullen	In te vullen
5.3		Deelnemer volgt het releasebeleid van Twiin.	Ja	Ja		
5.4	Testmanagement	Deelnemer beschikt, naast de productieomgeving, over een test-/acceptatieomgeving zoals beschreven in de NEN7510-2.	Ja	Ja		
5.5		Deelnemer doorloopt een ketentest.	Nee	Ja	In te vullen	In te vullen
5.6		Deelnemer gebruikt een set testpatiënten met een geldig fictief BSN.	Nee	Ja	In te vullen	In te vullen
5.7	Identificatie	Deelnemer gebruikt geverifieerde en gevalideerde Burgerservicenummers (BSN) van patiënten.	Ja	Ja		
5.8		Deelnemer zorgt voor het eenduidig identificeren van zorgverleners en zorgaanbieders bij gebruik van de GtK.	Ja	Ja		
5.9		Deelnemer zorgt voor identificatie van zorgaanbieders op basis van het UZI-Register Abonneenummer (URA). 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).	Nee	Ja	In te vullen	In te vullen
5.10	Authenticatie	Deelnemer is verantwoordelijk voor de authenticatie van gebruikers van het GtK.	Ja	Ja		

5.11		Deelnemer gebruikt een authenticatiemiddel dat voldoet aan eIDAS-hoog.	Nee	Ja	In te vullen	In te vullen
5.12	Autorisatie	Deelnemer gebruikt een rolgebaseerd autorisatieprotocol zoals afgesproken voor de Zorgtoepassing.	Ja	Ja		
5.13	Toestemming	Deelnemer draagt zorgt voor het (laten) uitvragen, vastleggen en toepassen van de toestemming van de patiënt (voor de use case verwijzen is vastleggen van de toestemming geen vereiste).	Ja	Ja		
5.14		Deelnemer maakt gebruik van Mitz als toestemmingsvoorziening voor zover nodig voor de zorgtoepassing (bij communicatiepatronen 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	Deelnemer maakt gebruik van een lokalisatievoorziening wanneer de zorgtoepassing dit vereist (bij communicatiepatronen raadpleegbaar maken).	Ja	Ja		
5.16		Deelnemer maakt gebruik van de lokalisatievoorziening van Mitz wanneer de zorgtoepassing dit vereist (bij communicatiepatronen raadpleegbaar maken).	Nee	Ja	In te vullen	In te vullen
5.17	Adressering	Deelnemer zorgt dat de adresinformatie op betrouwbare wijze wordt verkregen.	Ja	Ja		
5.18		Deelnemer levert zijn eigen adresgegevens aan bij Twiin beheerorganisatie voor publicatie in Zorg-AB. Als Deelnemer routering wil realiseren, deelt de Deelnemer de gegevens voor interne routering met andere Deelnemers.	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	Deelnemer is verantwoordelijk voor het loggen van transacties met gebruik van het GtK.	Ja	Ja		
5.20		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	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 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 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.	Ja	Ja		

		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.				

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	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 Deelnemer(s) en hun GtK Beheerder(s) bij de logging van transacties tussen Twiin Deelnemer(s) en gemeenschappelijke voorzieningen conform het Twiin	Nee	Ja	In te vullen	In te vullen

		Afsprakenstelsel.				

4. Applicatie

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
#	**Onderwerp**	**Omschrijving**	**Verplicht vanaf onderteKening Deelnemersovereenkomst**	**Verplicht vanaf vadidatie**	**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 heeft ondertekend, is 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	Ja	Ja		

		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 beveiligingsmaat regelen adequaat zijn conform de eisen zoals opgenomen in NEN 7510.				

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 voor het GtK.	Ja	Ja		
2.2		Aansluiten op de supportorganisatie 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 kwetsbaarheden ten aanzien van het GtK en beschikbaarheid.	Ja	Ja		
2.4		Zo nodig voeren van overleg met derden,	Ja	Ja		

		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.				

3. Informatie

Twiin Voorwaarden					*Samenwerkingsvoorwaarden*	
#	**Onderwerp**	**Omschrijving**	**Verplicht vanaf ondertekening Deelnemersovereenkomst**	**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 Deelnemersovereenkomst	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	In te vullen	In te vullen
4.3	Logging	Beheer van logging faciliteiten voor het GtK	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 Deelnemersovereenkomst	Verplicht vanaf validatie	Eventuele afwijking	Toelichting afwijking incl. tijdpad
5.1	Beveiliging	Zorgen voor een beveiligde en stabiele verbinding tussen de zorginformatiesystemen van Twiin Deelnemer en het GtK met goede SLA-afspraken over incidentafhandeling en beschikbaarheid	Ja	Ja		

		van het systeem (minimaal 99,5%).				

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 Twiin gevalideerd is.

#	Onderwerp	Omschrijving
1.1	Releasebeleid	Een GtK dient door middel van het installeren van updates, upgrades en patches aan het Twiin 6.5 | Releasebeleid te voldoen.
1.2	Vertrouwensmodel	Het GtK ondersteunt het Twiin 5 | Vertrouwensmodel en het gebruik van de generieke functies en gemeenschappelijke voorzieningen zoals omschreven in de implementatiewijzer per zorgtoepassing.
1.3	Netwerk	De GtK's moeten onderling verbonden kunnen worden via een veilig netwerk op basis van de volgende eisen: 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. 3. Inlog op het GtK voor doeleinden van beheer is uitsluitend toegestaan met partijen waarvan 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 NEN7510 certificering (of ISO 27001). 5. Het GtK moet worden beheerd door een GtK Beheerder die in bezit is van een geldige NEN 7510-certificering (of ISO27001).

#	Onderwerp	Voorwaarden
2.1	Beeldbeschikbaarheid	Voor de Zorgtoepassing Beeldbeschikbaarheid dient het GtK te voldoen aan de eisen zoals beschreven in de Implementatiewijzer voor beeldbeschikbaarheid.
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.

10 | Technische kern

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

- Volume 1 bevat een overzicht 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. Er zijn vier typen communicatiepatronen die een technische invulling zijn van verzenden of raadpleegbaar maken. Het type communicatiepatroon heeft effect op de invulling van het vertrouwensmodel. Afhankelijk van het type communicatiepatroon gelden andere voorwaarden voor validatie.
- Volume 2 bevat de Twiin Technical Agreements (de Twiin Technische Afspraken) afgekort TTA. Dit zijn gedetailleerde technische beschrijvingen van de communicatiepatronen. Dit volume is bestemd voor ontwerpers en solution architecten voor een internationale doelgroep en daarom geschreven in het Engels.
- Volume 3 bevat de content, zoals bijvoorbeeld metadata, die overkoepelend voor de zorgtoepassingen geldt.

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 en NEN-normering 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

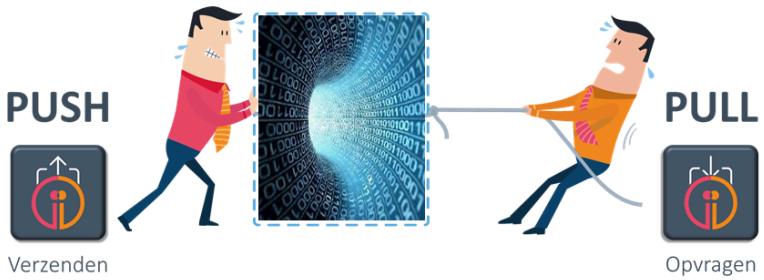
Inhoud

10.1 | Kern Volume 1 - Communicatiepatroon Overview

Voor het delen en uitwisselen (beschikbaar stellen) van data hebben we een viertal communicatiepatronen uitgewerkt. Dit betreft twee push en twee pull communicatiepatronen in twee varianten, namelijk SOAP(XD*) gebaseerd en RESTful(FHIR) gebaseerd.

In dit volume een overzicht 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.

De communicatiepatronen zijn er in twee typen: verzenden en raadpleegbaar maken. In de verschillende onderdelen van het vertrouwensmodel en in de Voorwaarden Twiin Deelnemer is uitgewerkt op welke manier de eisen verschillen, afhankelijk van het type communicatiepatroon. Dit gelet op het feit bijzondere eisen gelden voor een elektronisch uitwisselingssysteem zoals bedoeld in de Wabvpz (zie juridische context).



Versturen van data van zorgaanbieder A naar één of meerdere zorgaanbieders (documenten en resources). Deze twee communicatiepatronen zijn van het type verzenden.

- Push: data versturen
- Notified pull : verstuur notificatie en ontvanger haalt data op

Ontvangen van data door zorgaanbieder van één of meerdere zorgaanbieders (documenten en resources). Deze twee communicatiepatronen zijn van het type raadpleegbaar maken.

- Gerichte bevraging: zorgaanbieder A vraagt data op bij zorgaanbieder B
- Geïndexeerde bevragingen: zorgaanbieder A bevraagt alleen de zorgaanbieders die data voor de patiënt beschikbaar hebben

Functionele use casus

Voor de uitwerking van deze uitwisselpatronen zijn de meeste voorkomende functionele use casus leidend:

- Verwijzing/overdracht
- Consult/advies
- Ketenzorg/netwerkzorg
- Ad hoc dossier opvragen
- Uitbesteed onderzoek/behandeling

Deze functionele use casus zijn beknopt beschreven Functionele use cases databeschikbaarheid

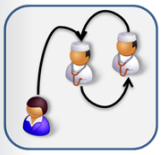
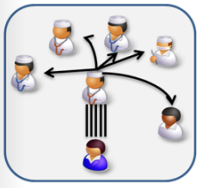
Overzicht uitwisselpatronen

10.1.1 | Functionele use cases databeschikbaarheid

Verwijzing / overdracht

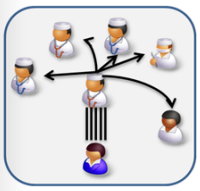
	De zorg wordt overgedragen van ontvanger naar verzender. Het dossier wordt gesloten bij de verzender en de behandeling inclusief dossiervoering en declaratie wordt overgenomen door de ontvanger (na acceptatie).
Type	Geplande zorg
Initiatief	Verzender
Hoofdbehandelaar	Ontvanger (na ontvangst)
Duur	Permanent
Relevante informatie o.a:	• BgZ • Relevante correspondentie • Beelden, verslagen en onderzoeken • Medicatiegegevens
Voorbeelden	• Verwijzing naar andere zorgaanbieder/verlener’ • Second opinion op initiatief patiënt

Consult / advies

 of 	Zorgverlener vraagt andere zorgverlener in consult. Verzender stelt gegevens beschikbaar aan ontvanger (inzage / sturen) en de ontvanger geeft advies over de behandeling. Zorg blijft onder de verantwoording van de verzender, inclusief dossiervoering en financiële verantwoording. Voor consult / advies kan de patiënt (eenmalig) worden gezien door de ontvangende zorgverlener. Eventueel kan de patiënt worden verwezen na uitvoeren van het consult.
Type	Geplande zorg
Initiatief	Verzender

Hoofdbehandelaar	Verzender
Duur	Tijdelijk
Relevante informatie	• BgZ • Relevante correspondentie • Beelden, verslagen en onderzoeken • Medicatiegegevens
Benodigde gemeenschappelijke voorzieningen	• Adressering • Makelaar (zorgaanbod / capaciteitsmanagement) • N.t.b.

Ketenzorg / netwerkzorg

 of 	Een (regionale) organisatie heeft de verantwoordelijkheid voor de zorg van een patiëntengroep, zoals CVA-, diabetes- en/of CVRM-patiënten. De zorg wordt geleverd door meerdere zorginstellingen, waarbij afspraken zijn gemaakt over de zorgverlening, logistiek, kwaliteit en financiële afhandeling. Er zijn 2 vormen van verantwoordelijkheid: • Alle zorgaanbieders hebben gezamenlijke verantwoordelijkheid, of • Eén zorgaanbieder heeft de verantwoordelijkheid voor de behandeling
Type	Geplande zorg
Initiatief	Verzender of ontvanger
Hoofdbehandelaar	Verzender en ontvanger
Duur	Permanent
Relevante informatie	• BgZ • Relevante correspondentie • Beelden, verslagen en onderzoeken • Medicatiegegevens
	Bij de use case "Ketenzorg" staat dat het initiatief bij de verzender ligt. Het initiatief kan ook bij de ontvanger liggen. Wanneer de verzender het initiatief heeft, zal het een trigger betreffen: verwachting dat de ontvanger er wat mee gaat doen. Als het om informatieoverdracht gaat, is het beter dat het initiatief bij de ontvanger ligt, kan deze de informatie ophalen op het moment dat deze de informatie nodig heeft. Dan heeft de ontvanger ook de meest actuele informatie. In geval van verzenden door de verzender kan de informatie al weer verouderd zijn op het moment dat de ontvanger er iets mee gaat doen.

Ad hoc dossier opvragen

	In sommige gevallen is directe inzage in dossier nodig op initiatief van de ontvanger, zoals opname op de HAP en SEH. Of in het geval dat de zorg wordt overgenomen en de ontvangende zorgverlener aanvullende informatie nodig die vooraf niet beschikbaar is gesteld.
Type	Ongepland zorg (of geplande zorg waarbij niet alle benodigde informatie beschikbaar is)
Initiatief	Ontvanger
Hoofdbehandelaar	Ontvanger
Duur	Tijdelijk
Relevante informatie	• BgZ • Relevante correspondentie • Beelden, verslagen en onderzoeken
Voorbeelden	• Tijdlijn voorziening raadplegen om volledig beeld van de patiënt te bekijken (Historisch dossier opvragen bij verwijzing) • Spoed zorg, zoals inzage op HAP en SEH • eLab voor apothekers, waarbij de apotheker de labwaarden controleert bij terhandstelling

Vorm van data	• Databeschikbaarheid
	  ◦ Gestructureerd
	  ▪ Losse ZIB's (HL7 CDA of HL7 FHIR)
	  ▪ Gegevensset o.b.v. ZIB's
	  ▪ Overige datasets (XML, HL7v2 of HL7v3)
	  ◦ Ongestructureerd
	  ▪ PDF
	  ▪ N.t.b.
	• Beeldbeschikbaarheid
	  ◦ DICOM
	  ◦ Non-DICOM (ecg, MP4)

Uitbesteed onderzoek / behandeling

	Een gedeelte van de zorg wordt uitgevoerd door een andere zorgaanbieder op verzoek van de verzender (onderlinge dienstverlening). De verzender en ontvanger hebben vooraf afspraken gemaakt over de zorginhoudelijk, logistieke en financiële afhandeling van het onderzoek / de behandeling.
Type	Geplande zorg
Initiatief	Verzender
Hoofdbehandelaar	Verzender (tijdelijke dossiervoering door ontvanger, met verslag of uitslag als terugkoppeling)
Duur	Tijdelijk
Relevante informatie	• Order / vraagstelling • BgZ • Relevante correspondentie • Beelden, verslagen en onderzoeken
Voorbeelden	• Extern onderzoek (laboratorium of beeldonderzoek) • Gezamenlijke (oncologie) behandeling met bijvoorbeeld radiotherapie of operatie in ander zorginstelling

10.1.2 | Communicatiepatroon : Indexed Pull

1. Use case

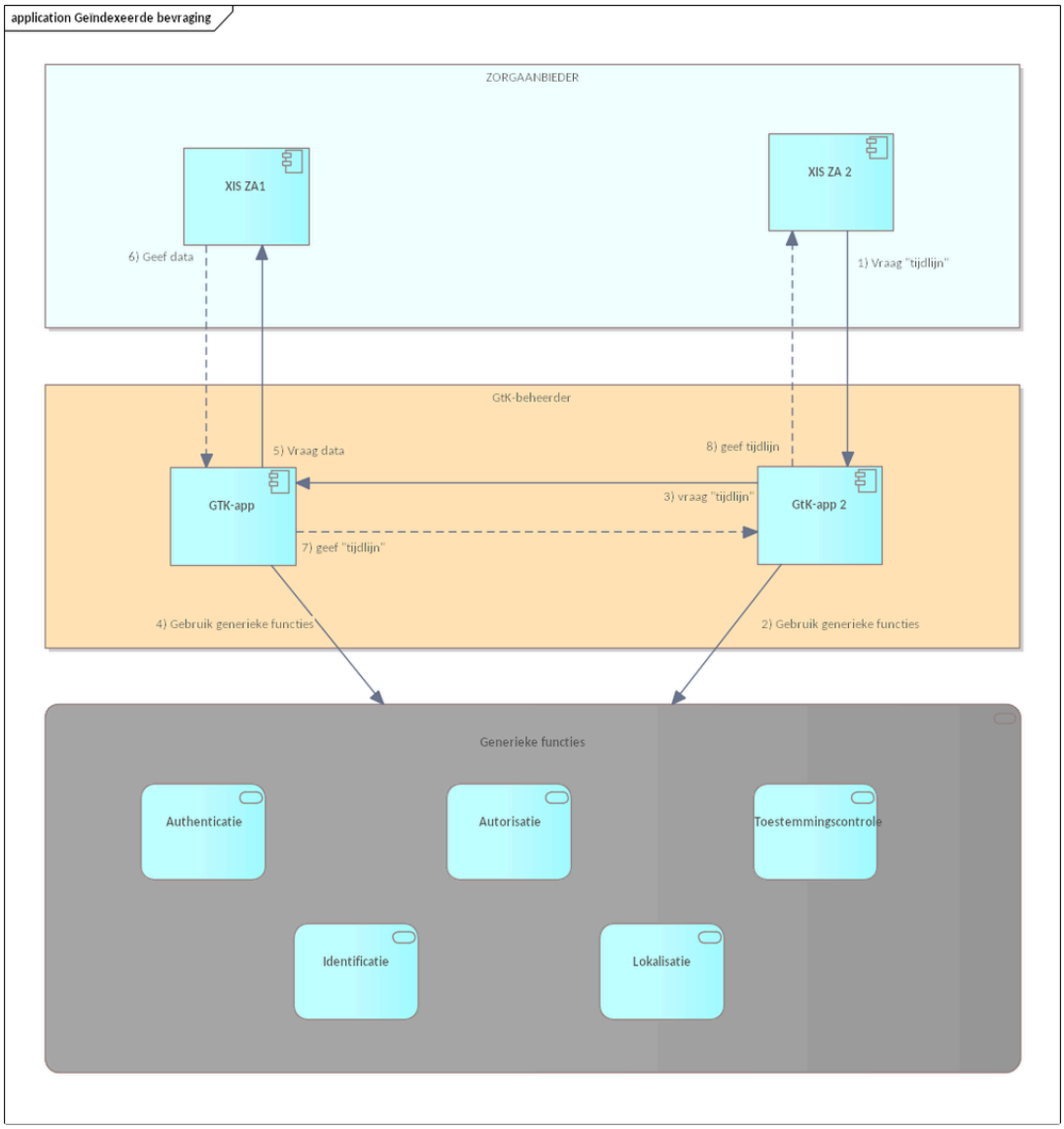
Vanuit Twiin zijn verschillende use cases beschreven voor gegevensuitwisseling. Hieronder staat een use case beschreven, waarin van dit communicatiepatroon gebruik kan worden gemaakt. Dit is een invulling van verzenden.

> 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.

1) De eerste stap is nodig om een tijdlijn inzichtelijk te maken aan de zorgverlener. Deze tijdlijn bestaat uit verschillende metadata elementen, zoals en niet gelimiteerd tot; patiëntnaam, patiëntnummer, type gegeven en de vindplaats van de data zelf. De tijdlijn kan samengesteld worden vanuit de informatie uit verschillende zorgsystemen. Delen van deze tijdlijn worden beschikbaar gesteld via één of meerdere GtK's. Om overvraging te voorkomen wordt gebruik gemaakt van een lokalisatie service. Hieronder wordt deze eerste stap in een diagram weergegeven.
2) Aan de hand van de tijdlijn kan de data opgehaald worden bij/via een GtK.



In bovenstaande applicatiediagram is globaal beschreven 'wat' in de basis de bedoeling is, voor de eerste stap. Verder in dit hoofdstuk worden verschillende technieken beschreven in sequence transactie diagrammen om aan te geven 'hoe' je tot een daadwerkelijke uitwisseling van data kunt komen.

1) Vanuit een XIS wordt de vraag "geef tijdlijn" aan het GtK gesteld.

2) De GtK stelt een lokalisatievraag aan een lokalisatievoorziening (vooralsnog kiest Twiin voor MITZ bij gebrek aan een landelijke voorziening) om te achterhalen bij welke zorginstellingen gegevens van de patiënt bekend zijn. Vervolgens worden de technische adressen opgehaald via ZORG-AB.

3) De vraag ‘geef tijdlijn' 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 patiënt toestemming bij de toestemmingsvoorziening Mitz.

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

6) Het bevraagde XIS stuurt de tijdlijngegevens 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.

- 10.1.7 | Generieke functie - Identificatie en Authenticatie
- 10.1.6 | Generieke functie - Autorisatie
- 10.1.10 | Generieke functie - Toestemming
- 10.1.11 | Generieke functie - Lokalisatie
- 10.7.8 | Generieke functie - Adressering

10.1.3 | Communicatiepatroon : Push

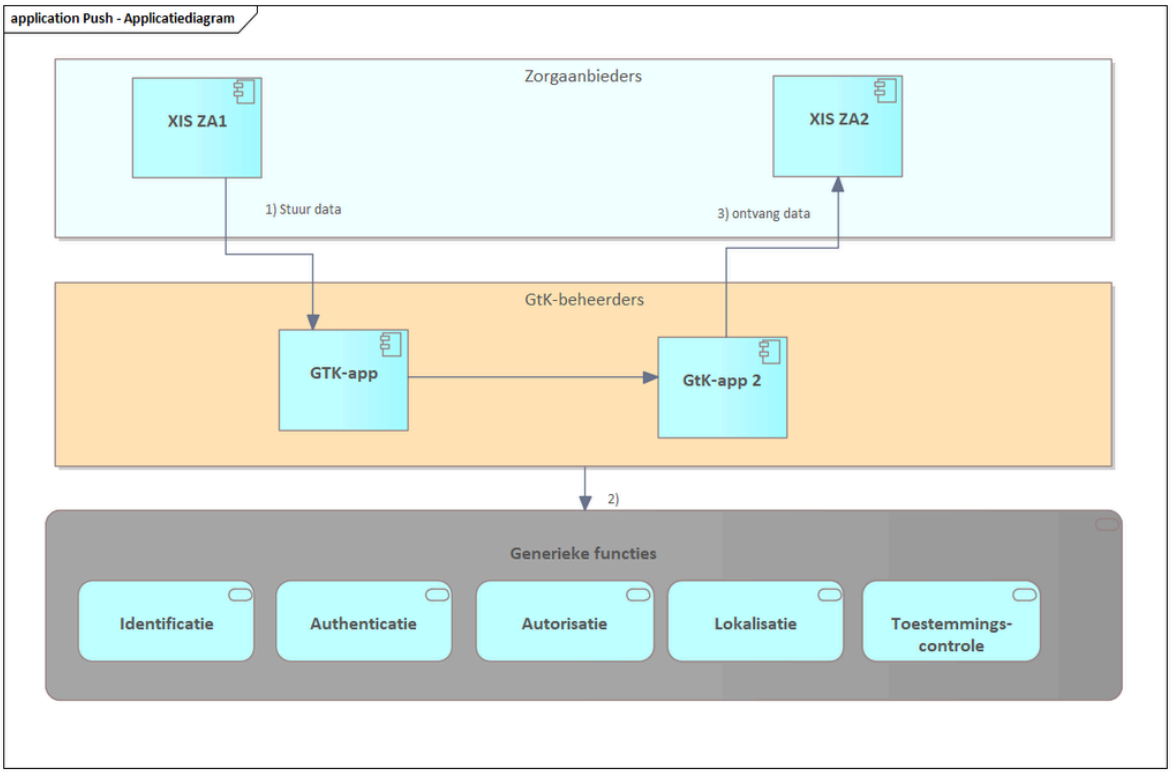
1. Use case

Vanuit Twiin zijn verschillende functionele use cases beschreven voor gegevensuitwisseling, hieronder staat een use case beschreven die van communicatiepatroon ‘Push - Versturen’ gebruik zou kunnen maken.

> *Een zorgverlener besluit de patiënt 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.

Voor het communicatiepatroon 'Push -Versturen’ zijn de volgende functies nodig:

- 10.1.7 | Generieke functie - Identificatie en Authenticatie
- 10.7.8 | Generieke functie - Adressering

10.1.4 | Communicatiepatroon : Notified Pull

1. Use case

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

> *Een patiënt 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.*

De "Notified Pull" biedt een oplossing voor de "juridische Push", waarbij gegevens van de ene organisatie naar de andere worden overgedragen. De Notified Pull-transactie verwacht dat bij een patiëntverwijzing de Ontvangende Organisatie zorgvuldig wordt geselecteerd door de Verzendende Organisatie. Deze actie bevestigt de behandelingsrelatie tussen de patiënt en de toekomstige zorgverlener en kan worden gezien als een "veronderstelde toestemming". De patiënt is op de hoogte van de verwijzing en begrijpt daarom dat zijn medische gegevens zullen worden overgedragen.

De "Notified Pull" zal een Ontvangende Organisatie op de hoogte stellen van medische dossiers die klaar zijn om te worden opgehaald (inclusief de vereiste toestemming van de patiënt). 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.

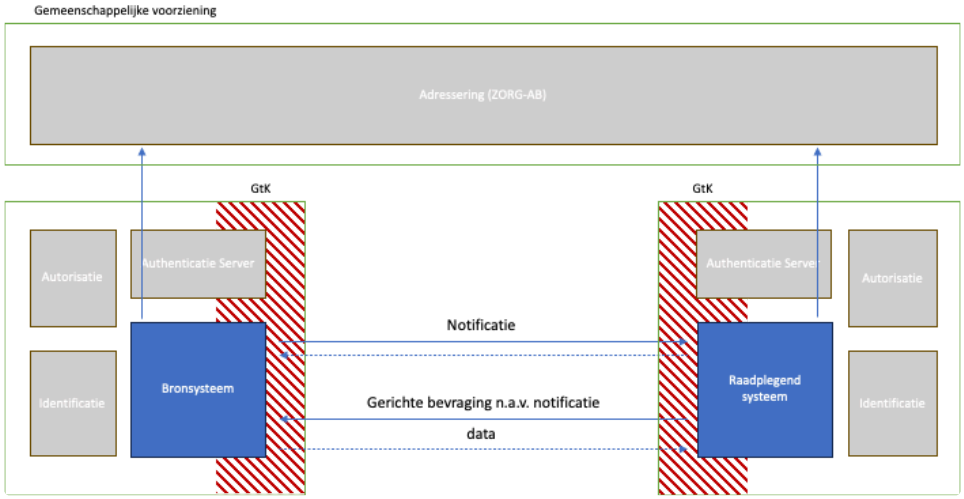
2. Applicatiediagram

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	Zendend GtK	Bronsysteem
Ontvangende Organisatie	Ontvangend GtK	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.

1. Het zendend GtK gebruikt generieke functies (grijze blokken) om de zorgverlener die de notificatie verstuurt (en dus verantwoordelijk is voor de verwijzing of overdracht) te identificeren en te authenticeren.
2. (Optioneel) Het zendend GtK gebruikt de gemeenschappelijke voorziening om het adres van het ontvangend GtK op te zoeken.
3. Het zendend GtK stuurt een notificatie naar het ontvangend GtK. Het ontvangend GtK stuurt een bevestiging van ontvangst.
4. Het ontvangend GtK maakt gebruik van de generieke functie Autorisatie om te bepalen of de zorgverlener de notificatie mag aanbieden.
5. Op basis van de ontvangen notificatie zal het ontvangend GtK het adres opzoeken van het bronsysteem.
6. De Zorgverlener die het ontvangend GtK gebruikt wordt geïdentificeerd en geauthenticeerd door gebruik te maken van de generieke functies (grijze blokken).
7. Daarna zal deze een gerichte bevraging uitsturen naar het zendend GtK om de data op te halen.
8. Het zendend GtK maakt gebruik van de generieke functie Autorisatie om te bepalen of de zorgverlener toegang krijgt tot de opgevraagde data.
9. Het zendend GtK stuurt de gevraagde data terug als antwoord op de vraag.

Voor de Notified Pull zijn de volgende functies nodig.

- 10.1.7 | Generieke functie - Identificatie en Authenticatie
- 10.1.6 | Generieke functie - Autorisatie
- 10.7.8 | Generieke functie - Adressering

10.1.5 | Communicatiepatroon : Pull

1. Use case

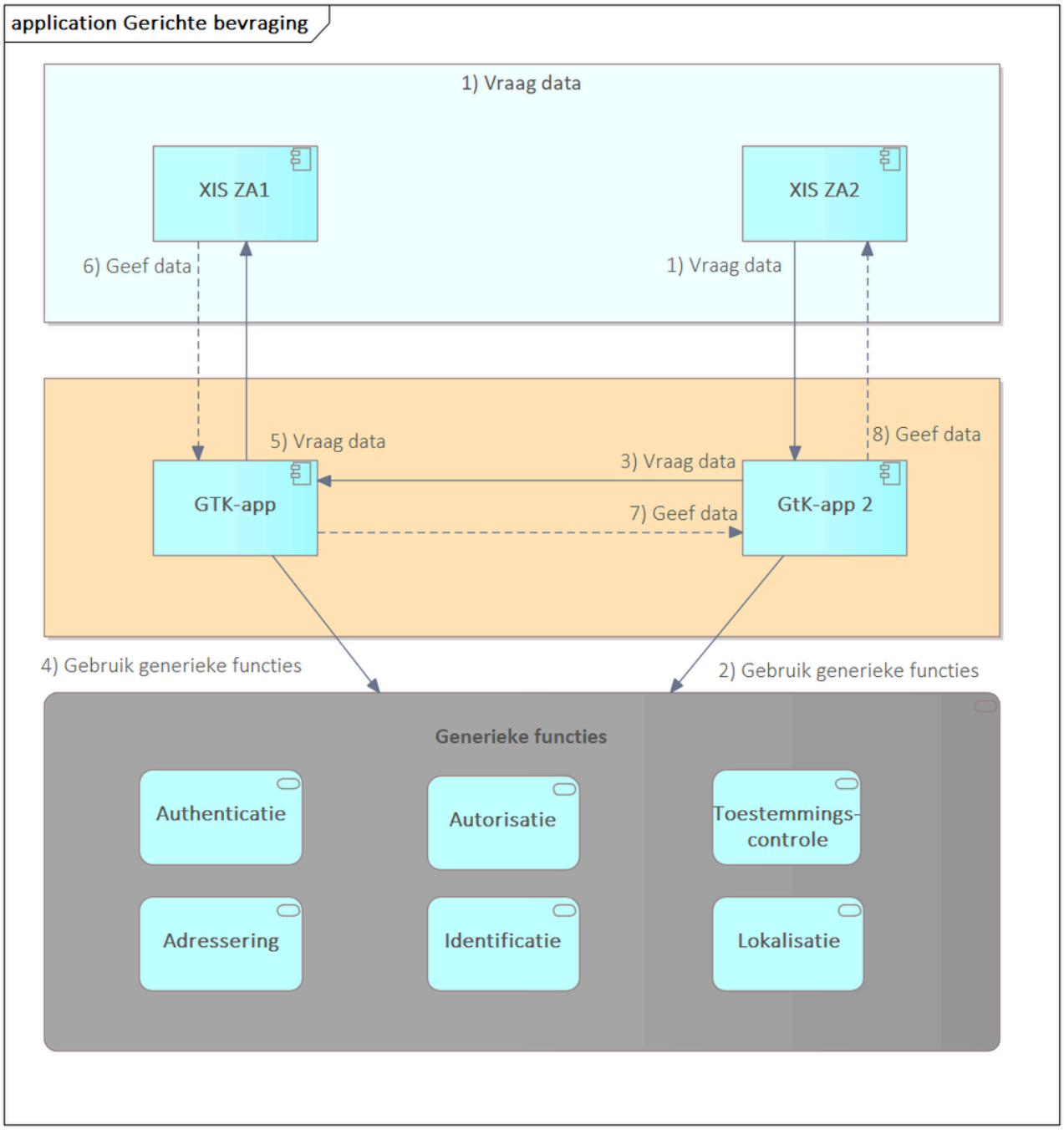
Vanuit Twiin zijn verschillende use cases beschreven voor gegevensuitwisseling, hieronder staat een use case beschreven die van dit communicatiepatroon gebruik zou kunnen maken.

> *Een patiënt 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 patiënt voor is gegeven.

2. Applicatiediagram

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



In bovenstaande applicatie diagram is globaal beschreven 'wat' in de basis de bedoeling is. Het is een vereenvoudigde weergave van de conceptuele Twiin oplossingsrichting A. Verder in dit hoofdstuk worden verschillende technieken beschreven in sequence transactie diagrammen om aan te geven 'hoe' er tot een daadwerkelijke uitwisseling van data gekomen kan worden.

Vanuit een XIS wordt via een GtK een vraag gesteld (1). De GtK zal de vraag afhandelen en hiervoor gebruik maken van een aantal gemeenschappelijke voorzieningen (2) om de vraag op de juiste manier te kunnen stellen (4). De bevraagde GtK zal op zijn beurt gebruik maken van een aantal gemeenschappelijke voorzieningen (3) om de vraag op de juiste manier af te kunnen handelen (5 en 6).

1. Vanuit een raadplegend XIS wordt aan de raadplegende GtK waarop hij aangesloten is een vraag gesteld.
2. De raadplegende GtK gebruikt de gemeenschappelijke voorzieningen om het vervolg te bepalen.
3. De raadplegende GtK stuurt de vraag door naar de bron GtK.
4. De bron GtK controleert de medische autorisatie en de patiënttoestemming bij de gemeenschappelijke voorzieningen.
5. De bron GtK stuurt de vraag door aan het bron XIS.

6. Het bron XIS geeft de gevraagde data terug aan de bron GtK
7. De bron GtK stuurt het antwoord door aan de raadplegende GtK.
8. De raadplegende GtK geeft het antwoord terug aan het raadplegende XIS.

De generieke functies die benodigd zijn voor de Gerichte Bevraging zijn;

- 10.1.7 | Generieke functie - Identificatie en Authenticatie
- 10.1.6 | Generieke functie - Autorisatie
- 10.1.10 | Generieke functie - Toestemming
- 10.7.8 | Generieke functie - Adressering

10.1.6 | Generieke functie - Autorisatie

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

In een zorgtoepassing moet er een rol gebaseerde autorisatieafspraak gemaakt zijn. Hier zal ieder GtK zich aan moeten houden, maar kan ook betekenen dat de autorisatieregels van de eigen zorgaanbieder(s) overruled worden. Dit kan betekenen dat een gebruiker mogelijk meer of minder mag doen dan (initieel) intern was afgesproken.

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.

10.1.7 | 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 geauthentiseerd 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.

GtK

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

Eisen Identificatie en authenticatie

Id-01	**Zorgverleners dienen geïdentificeerd te worden op basis van een uniek ID**
Omschrijving/Toelichting/Uitleg/Implicaties	Waar mogelijk is dit het UZI-nummer, maar ook een lokaal-id i.c.m. het URA mag gebruikt worden.
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

10.7.8 | Generieke functie - Adressering

De GtK’s dienen elkaars elektronische diensten te kunnen vinden. Hiervoor publiceert de Twiin beheerorganisatie de elektronische adressen van alle GtK-diensten in ZORG-AB, waardoor deze voor alle partijen vindbaar worden. ZORG-AB is een kandidaat bouwsteen in het duurzaam informatiestelsel van de Zorg. De 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 met ZORG-AB te gebeuren. Als een domein hier een andere oplossing voor bedenkt mag dat ook (b.v. onderlinge afspraken tussen GtKs). Hiermee worden deelnemers niet verplicht om functionaliteit voor de ZORG-AB-interfaces in te bouwen.

Optioneel: De technische beschrijving van het gebruik van ZORG-AB door een GtK staat in Volume II beschreven.

10.1.9 | Generieke functie - Logging

Wat is logging?

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

Logging is dit een verplichting voor zorginstellingen zich tegenover hun cliënten, collega’s, toezichthouders en anderen, te verantwoorden over de zorgvuldigheid waarmee zij met de persoonsgegevens omgaan volgens de wetgeving (i.e. AVG, WAVBPZ).

Log types

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

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 **burgers, 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 interactie uitwisseling. Interacties zijn gebeurtenissen waarbij acties plaatsvinden die betrekking hebben op inloggen, inzien van gegevens, wijzigen van gegevens, 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 verantwoordelijke gebruiker voor de toegang, dossierdeel, resultaat, rol en naam gebruiker, autorisatieprotocol, toestemmingsprofiel noodknopprocedure ja/nee.

Afhankelijk van de gebeurtenistypes, 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 NEN7513.

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 NEN7513 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 zorginstellingen en andere beheerders van persoonlijke gezondheidsinformatie over het verstrekken van informatie over wie toegang heeft gehad tot haar of zijn elektronisch patiëntdossier.

Voor een betrouwbare logging moeten niet alleen operationele gebeurtenissen worden gelogd, maar ook gebeurtenissen die de toegangsregeling betreffen, zoals structuur instellingen, 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 patiënt (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 staat een handreiking voor (dienstverleners en beheerders van) zorgaanbieders die te maken hebben met loggen en rapporteren.

In de NEN7513:2024* is er een nieuwe tabel opgesteld die expliciet voor de gebeurtenis gegevensuitwisseling geldt. Vanuit de NEN7513 werkgroep komt nog een implementatierichtlijn. Dit is de reden dat we hier vanuit Twiin niet op vooruit willen lopen en bijvoorbeeld het uitwisselingsformaat van de logging verplicht willen voorschrijven.

*bij de publicatie van consultatieversie van Twiin Afsprakenstelsel, is deze nieuwe versie van de norm nog niet publiekelijk beschikbaar. De verwachting is dat dit wel het geval is wanneer het Twiin Afsprakenstelsel v1.3 definitief gepubliceerd wordt.

Eisen 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 NEN7513:2024, tabel 21.
Prescription Level/Type	Verplicht
Toetsing	Validatie
Transactie/verwijzing	alle Twiin transacties

Log-02	**Het GtK moeten loggegevens over uitwisselingen met andere GtKs kunnen aanleveren aan die GtKs.**
Omschrijving/Toelichting/Uitleg/Implicaties	Dit kan bijvoorbeeld via door een ATNA interface aan te bieden.
Prescription Level/Type	Verplicht
Toetsing	Eis aan deelnemer
Transactie/verwijzing	

10.1.10 | Generieke functie - Toestemming

Wanneer er voor een uitwisseling een medisch dossier voor raadpleging beschikbaar worden gemaakt zonder dat men al weet wie, wanneer welke gegevens gaat raadplegen is uitdrukkelijke toestemming van de patiënt vereist.

Het brondossier is verantwoordelijk voor de controle op de toestemming. Deze patiënttoestemmingen worden tot op heden geregistreerd in het EPD van de zorgaanbieder en zijn vaak specifiek voor een uitwisselingsysteem. Het registreren hiervan is een administratieve last van de zorgaanbieder. Daarnaast is het soms voor de patiënt niet duidelijk / overzichtelijk waar en waarvoor toestemming is gegeven. Mede hierom is de voorziening Mitz ontwikkeld. Mitz biedt de functionaliteit voor het vastleggen van toestemmingen aan de zorgaanbieder, maakt het mogelijk dat deze voor meerdere elektronische uitwisselingssystemen te gebruiken is. Daarnaast biedt Mitz de patiënt functionaliteit om een overzicht te hebben van de alle zorgaanbieders waar een behandeling is (geweest) en om toestemmingen te beheren.

Het Informatieberaad heeft Mitz in 2022 opgenomen als onomstreden bouwsteen in het informatiestelsel in de zorg. Dit besluit geldt in ieder geval nog tot 2027 en wordt dan geëvalueerd. Dit betekent dat er voor Mitz een pas-toe-of-leg-uit-principe geldt. Voor de gegevensuitwisselingen die in Twiin worden ondersteund en waarvoor een uitdrukkelijke patiënttoestemming noodzakelijk is, verplicht Twiin het gebruik van Mitz.

10.1.10.1 | Eisen toestemming

Toestemming-01	**Een GtK dient een aansluiting op Mitz te hebben**
Omschrijving/Toelichting/Uitleg/Implicaties	Een GtK die uitwisselingen ondersteund waar uitdrukkelijke toestemming voor nodig is dient een Mitz Connector Aansluiting te ondersteunen
Prescription Level/Type	Conditioneel verplicht
Toetsing	
Transactie/verwijzing	Bijlage | Architectuurdocumenten

10.1.11 | Generieke functie - Lokalisatie

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

Raadplegende zorgaanbieders mogen gegevens alleen opvragen waar de patiënt al bekend is. Ook het enkele feit dat een patiënt wel of niet onder behandeling is bij een zorgaanbieder, valt namelijk onder het beroepsgeheim.

De toestemmingsvoorziening Mitz -waar nodig verplicht door Twiin- biedt een rudimentaire vorm van lokalisatie. Mitz biedt een dienst waaraan een zorgaanbieder kan vragen bij welke andere zorgaanbieders (potentiëel) gegevens van een bepaalde patiënt 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.

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.

10.1.12 | Generieke functie - netwerkbeveiliging

Eisen Netwerkbeveiliging

#	Omschrijving	Domein	Opmerking
5.010	Om zich te kunnen authentiseren, kunnen alle systemen betrokken bij transacties in het kader van Twiin een geldig PKI-certificaat overleggen.		Een geldig PKI-certificaat is een UZI-servercertifcaat of een PKIoverheid-certficaat.
5.020	Alle transacties in het kader van Twiin zijn beveiligd met Mutual Transport Layer Security (mTLS).		
5.030	Er wordt enkel gebruik gemaakt van TLS-versies en -algoritmen die zijn geclassificeerd als "goed" of “voldoende“ in de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS), versie 2.1 van het NCSC.		Een systeem biedt alleen TLS 1.3 aan als deze ook TLS 1.2 aanbiedt. Het is niet verplicht om *alle* algoritmen aan te bieden die in de genoemde richtlijnen als "goed" zijn geclassificeerd.
5.040	Transacties in het kader van Twiin worden versleuteld volgens TLS, zoals bedoeld in eis 5.020.		
5.050	Voordat daadwerkelijk transport plaats vindt, controleren de Nodes de geldigheid van elkaars certificaten door middel van CRL of OCSP.		
5.060	Systemen die de geldigheid van het UZI-servercertficaat van de andere Systemen dienen te controleren, voldoen aan de verplichting van het Certification Practice Statement (CPS) UZI-register		Zie Certification Practice Statement (CPS) | Zorg CSP , artikel 4.5.2
5.070	Systemen die de geldigheid van het PKIo-servercertficaat 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.		Zie https://cps.pkioverheid.nl/CPS_PA_PKIoverheid_G2_G3_Root_v4.3.pdf, paragraaf 2.2.

10.2 | Kern Volume 2a - Twiin Technical Agreements

The goal of this volume is to describe the Twiin generic re-useable exchange patterns (NL Twiin uitwisselpatronen) 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., PDF for correspondence)
- Transaction specifications based on:
  - Documents: IHE XDS/XCA
  - Resources: Based on FHIR

10.2.1 | TTA SOAP - Indexed Pull

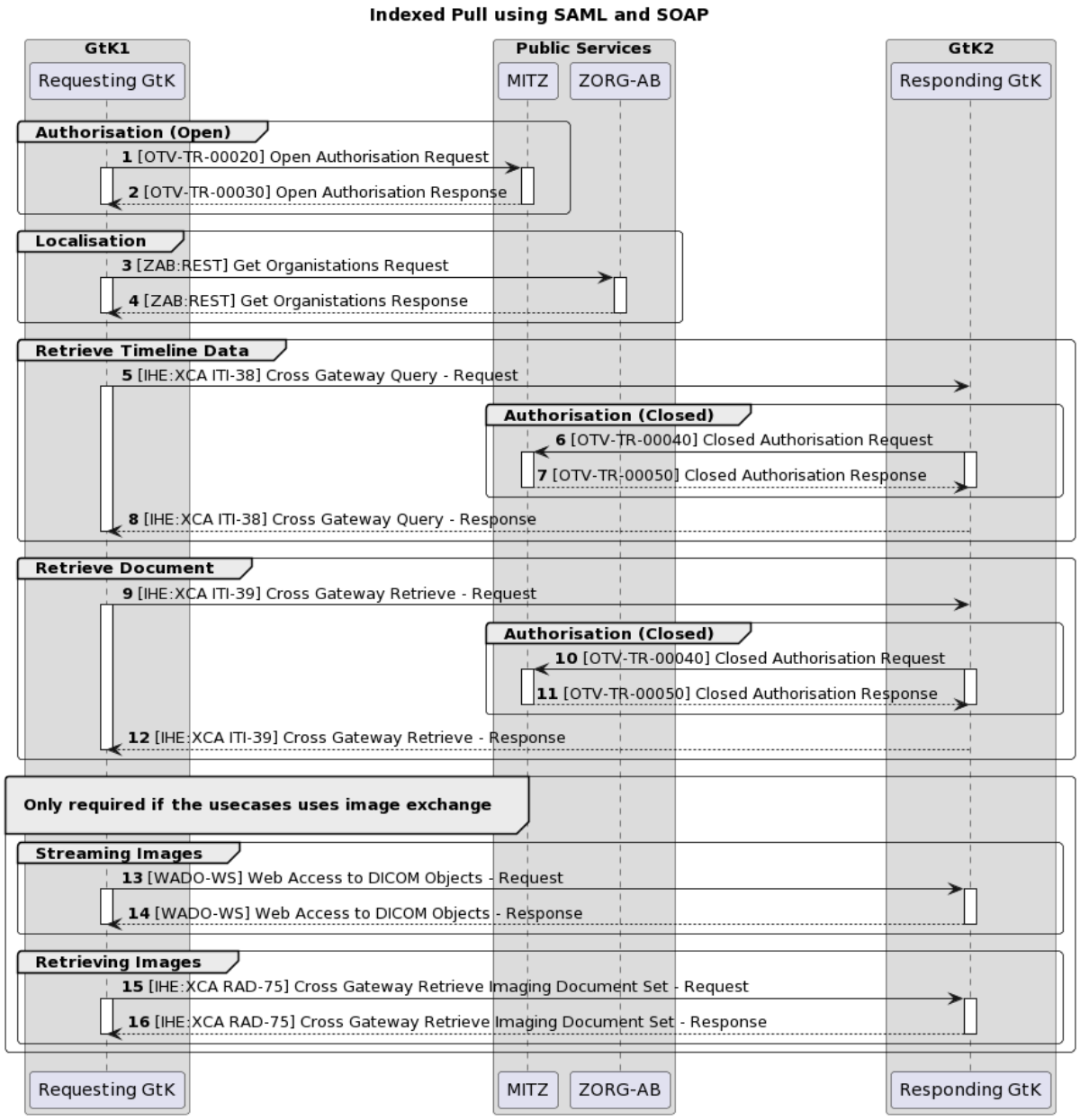
This Twiin Technical Agreement (TTA) describes and specifies technical responsibilities to which parties agree when connecting to exchange transactions to facilitate the Indexed Pull.

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



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.

10.4.5 | IHE ITI-40 | Provide X-User Assertion

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'

		10.3.14.2 | Mitz Transacties - 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 10.3.14.2 | Mitz Transacties - 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 10.3.14.1 | ZORG-AB Transacties
	4	ZORG-AB replies to this request with the endpoints 10.3.14.1 | ZORG-AB Transacties
Retrieve Timeline data	5	Using the endpoints the GtK uses this information to send the query. With this transaction a SAML token is included 10.4.2 | IHE ITI-38 | Cross Gateway Query 10.4.2.1 | ITI-38 examples | ITI 38 request
	6	The responding GtK then checks if the patients permission is in check at MITZ 10.3.14.2 | Mitz Transacties - OTV-TR-00040
	7	A response is sent back 10.3.14.2 | Mitz Transacties - 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. 10.4.2 | IHE ITI-38 | Cross Gateway Query 10.4.2.1 | 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. 10.4.3 | IHE ITI-39 | Cross Gateway Retrieve 10.4.3.1 | ITI-39 examples | ITI 39 request
	10	(see step 6) 10.3.14.2 | Mitz Transacties - OTV-TR-00040
	11	(see step 7) 10.3.14.2 | Mitz Transacties - 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 10.4.3 | IHE ITI-39 | Cross Gateway Retrieve

		10.4.3.1 | 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. 10.3.6 | Twiin-06 | WADO-WS
	14	The images are sent back in the requested format 10.3.6 | Twiin-06 | WADO-WS
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. 10.4.6 | IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set 10.4.6.1 | RAD-75 examples | RAD 75 request
	16	The images are sent back 10.4.6 | IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set 10.4.6.1 | RAD-75 examples | RAD 75 response

10.2 | Kern Volume 2a - Twiin Technical Agreements

10.2.3.1 Notified Pull - Data interactions

10.2.2 | TTA SOAP - Push

Work in progress. Please inform us via info@twiin.nl if you use IHE XDR in a production scenario.

10.2.3 | TTA FHIR - Notified pull

This Twiin Technical Agreement (TTA) describes and specifies 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, with the normative specifications remaining unchanged. The informative specifications however have been described with a specific implementation.

The possibility to exchange a patient's medical record is for example required in case of a patient referral or transfer. When different healthcare organizations are involved in a patient'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.

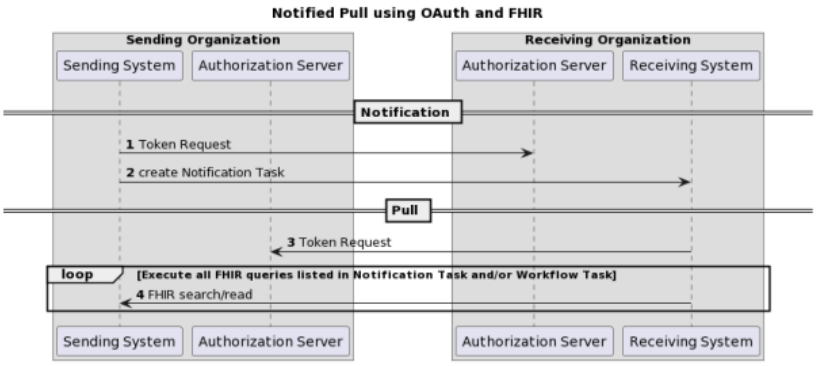
Relation to other documents

This document is written with the following documents as reference:

- Nictiz - Informatiestandaard BgZ MSZ
- TA Notified Pull v0.99

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 10.2.5 | TTA FHIR - Authentication & Authorization. Interaction number 2 is described in 10.2.3.1 | Notified Pull - Data interactions . A part of interaction number 4 is also described in 10.2.3.1 | Notified Pull - Data interactions, for specifics of the context of the Notified Pull see Nictiz information standards.

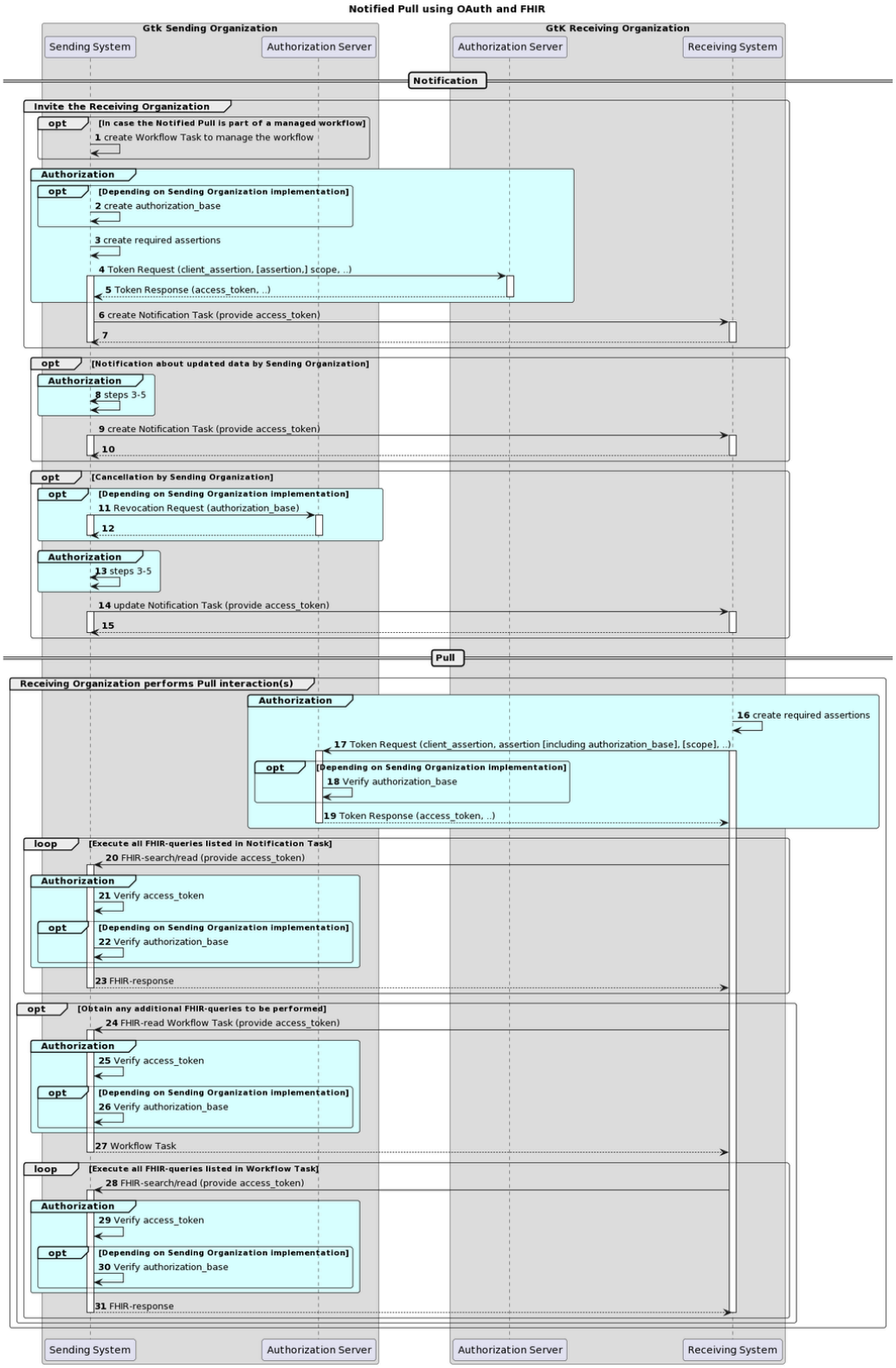
The sequence diagram below provides a complete sequence diagram that covers both the resource interactions and the authorization interactions of the complete Notified Pull interaction sequence.

The Twiin specific solutions for identification and addressing can be found in 10.2.5 | TTA FHIR - Authentication & Authorization and 10.2.8 | TTA - Addressing 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 10.2.3.1 Notified Pull - Data interactions) and in authorization layer using OAuth 2.0 (marked cyan, described in 10.2.10 | Netwerk level security mTLS 1.3).

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 a 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 others) 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).

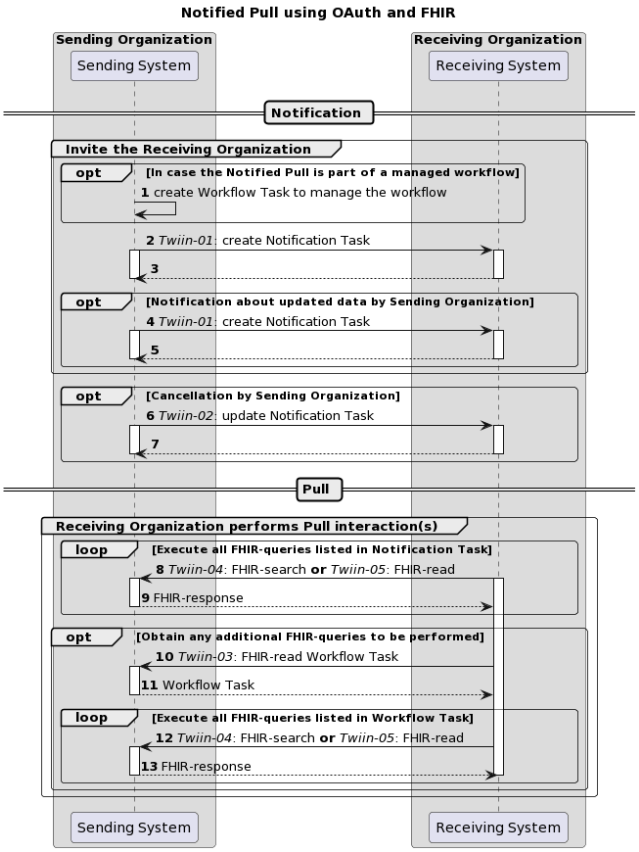
		The Receiving System must treat the access token as an opaque element. The Receiving System should not depend on any information contained in the access token.
	20-23	The Receiving System initiates the intended interactions and processes the responses. The Sending System verifies the access token and 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.

10.2.3.1 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 10.3.1 | Twiin-01 | Send Notification Task 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 10.3.1 | Twiin-01 | Send Notification Task 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 10.3.2 | Twiin-02 | Cancel Notification Task 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 10.3.5 | Twiin-05 | Retrieve Resource for a detailed description for the retrieval of resources referenced in Task.input:read-available-resources. See 10.3.4 | Twiin-04 | Search Resource(s) 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 10.3.3 | Twiin-03 | Get workflow Task
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 10.3.5 | Twiin-05 | Retrieve Resource for a detailed description for the retrieval of resources referenced in Task.input:read-available-resources. See 10.3.4 | Twiin-04 | Search Resource(s) 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 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.

10.2.3 | TTA FHIR - Notified pull

10.2.10 | Netwerk level security mTLS 1.3

10.2.4 | TTA FHIR - Pull

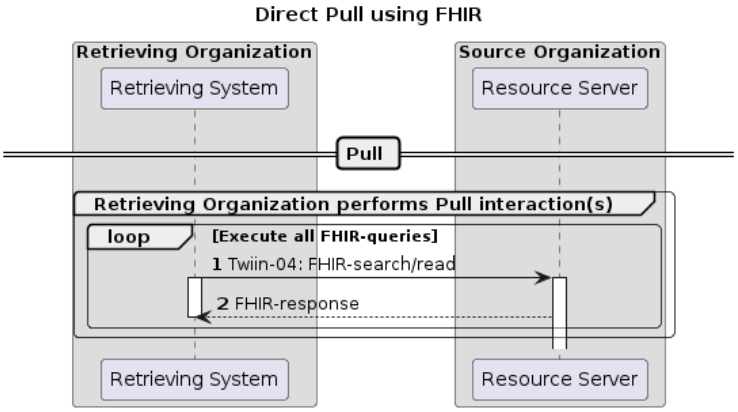
⚠ This exchange pattern (Direct Pull) is Draft, intended for further coordination with suppliers and healthcare providers.

This Twiin Technical Agreement (TTA) describes and specifies technical responsibilities to which parties agree when connecting to exchange transactions to facilitate the Direct Pull.

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 10.3.4 | Twiin-04 | Search Resource(s) for a detailed description for the retrieval of resources.

10.2.5 | TTA FHIR - Authentication & Authorization

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 RFC 6749: The OAuth 2.0 Authorization Framework. 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 RFC 6750: The OAuth 2.0 Authorization Framework: Bearer Token Usage.

Client authentication

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 (RF C 6749: The OAuth 2.0 Authorization Framework) 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 RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.

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 RFC 7518: JSON Web Algorithms (JWA). Must be one of PS256, PS384, PS512, ES256, ES384 or ES512.	Yes
kid	Identifier of the key pair used to sign this JWT. See RFC 7515: JSON Web Signature (JWS).	Yes

The payload contains a set of claims listed below:

Claim	Description	Required
jti	Unique identifier of the client assertion. See RFC 7519: JSON Web Token (JWT).	Yes
iss	Identifier of the system that issued the client assertion. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
iat	The time at which the client assertion was issued. See RFC 7519: JSON Web Token (JWT). 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 RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
nbf	The time before which the token shall not be accepted for processing. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	No

aud	Identifier of the authorization server token endpoint where this client assertion is to be used. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	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 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). 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 RFC 6749: The OAuth 2.0 Authorization Framework "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. RFC 6749: The OAuth 2.0 Authorization Framework. 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 RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants 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 RFC 7518: JSON Web Algorithms (JWA). Must be one of PS256, PS384, PS512, ES256, ES384 or ES512.	Yes
kid	Identifier of the key pair used to sign this JWT. See RFC 7515: JSON Web Signature (JWS).	Yes

The payload contains a set of claims that carry information required by NEN7512 and NEN7513.

Claim	Description	Required
jti	Unique identifier of the authorization assertion. See RFC 7519: JSON Web Token (JWT).	Yes
iss	Identifier of the system that issued the authorization assertion. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
iat	The time at which the authorization assertion was issued. See RFC 7519: JSON Web Token (JWT).	Conditional

	This is only required if there is an agreed age of an authorization assertion.	
exp	The expiration time on or after which the authorization assertion shall not be accepted for processing. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
nbf	The time before which the token shall not be accepted for processing. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	No
aud	Identifier of the authorization server token endpoint where this authorization assertion is to be used. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
sub	Identifier of the **organization** (healthcare supplier) 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	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 a authorization base when requesting patient information.	Conditional
user_id	Identifier of the **responsible user** (healthcare professional) or the **system** who requests access. **Preferred: UZI nummer** The codesystem (`issuing_system`) for the identifier is also mandatory. For UZI this is OID: 2.16.528.1.1007.3.1 5.1 | Vertrouwen: Identificatie **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** 5.1 | Vertrouwen: Identificatie The codesystem (`issuing_system`) for the identifier is also mandatory. For UZI role code this is OID: 2.16.840.1.113883.2.4.15.111 User role is required when the responding party needs to validate the role of the user before responding to the request. For instance when a user does not have a authorization base when requesting patient information.	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	Yes
authorization_base	See Authorization base	No
patient	Identifier of the patient for whom data is exchanged. Must be an OID encoded BSN (I.e., BSN with the “urn:oid:2.16.840.1.113883.2.4.6.3.” prefix and without a leading zero) 5.1 | Vertrouwen: Identificatie 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 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 RFC 6749: The OAuth 2.0 Authorization Framework . 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 App Launch: Scopes and Launch Context - SMART App Launch v2.2.0 . 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.nl/fhir/NamingSystem/TaskCode|pull-notification (create)
  - system/Task.u?code=http://fhir.nl/fhir/NamingSystem/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).

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 RFC 6749: The OAuth 2.0 Authorization Framework 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 Client authentication.	Yes
client_id	ID of the resource client. This ID is issued by the authorization server. If present, the value of the "client_id" parameter must identify the same client as is identified by the client assertion.	No
scope	Space separated list of requested scopes, see paragraph Authorization scope.	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 RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens , 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.

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 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). 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):

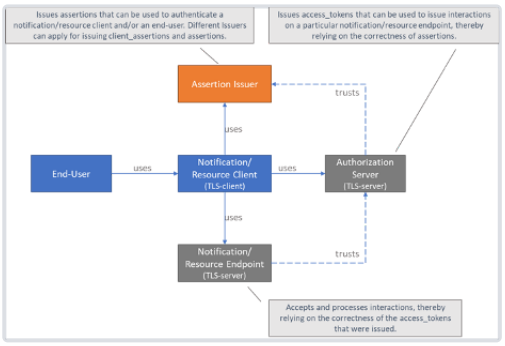
- **sub**: Identifier of the healthcare organization
- **user_id**: Identifier of the responsible user (healthcare professional)

- **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 an 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.

10.2.5.1 | 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"
}
```

10.2.6 | TTA - Localisation

Localisation is searching the sources that (might) have relevant information on the patient. Localisation on a broad level is done via an interface Mitz offers. This means the GtK should offer Mitz Connector functionality.

With the so-called open authorization query a healthcare provider can ask Mitz which other healthcare providers maintain records of a certain patient may and can be consulted for one or more data categories. The result gives 0 or more healthcare providers (identified with URA) that have patient consent to share the requested data 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 parameters to find corresponding Twiin GtK interfaces in ZORG-AB (see addressing).

10.2.7 | 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 1.0.1.

10.2.8 | TTA - Addressing

GtK applications can choose how they want to solve the addressing issues themselves. However, 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, so the ZORG-AB interface is now mandatory to use.

To search for GtK endpoints with ZORG-AB, you can use the Get_Organization and Get_Endpoint transactions.

{temporary solution} When additional internal routing is necessary, the Twiin Participant is question is responsible to communicatie the relevant information to the other participants.

10.2.9 | 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.

10.4.1 | IHE ITI-20 | Record Audit Event

10.2.10 | Netwerk level security mTLS 1.3

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 published data.

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 system are mutually verifying each other's identity before establishing a secure connection. In this way only systems that are trusted (are a GtK) 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 alerting 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.

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

On 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 IT Security Guidelines for Transport Layer Security (TLS) require version 1.3 of the TLS standard for the security level “Good”.

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 RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens as an additional security measure on application level. See section Resource server authorization: OAuth 2.0 for requirements on application level security using OAuth 2.0.

CRL / OCSP / CPS

Minimaal elk uur check.

PKIoverheid

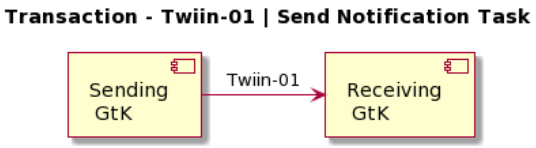
Both the client and server certificates must be PKIo-certificates that are issued under the CA “Staat der Nederlanden Private Services CA – G1” (this includes UZI server certificates issued by UZI-registry (CIBG)). Overview of PKIoverheid certificates

Note: that the requirements as specified in this paragraph apply to **Notification, FHIR, and token** endpoints.

10.3.1 | Twiin-01 | Send Notification Task

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 🔥 Index - FHIR v3.0.2

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
- Identification of the patient who is the subject of information exchange
- References to individual FHIR® resources that have been made available at the Sending GtK
- FHIR® search queries that can be used to retrieve FHIR® resources that have been made available at the Sending GtK
- Authorization base (see Authorization base)

The payload of this message consists of a 🔥 Task - FHIR v3.0.2 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 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 Task - FHIR v3.0.2 .

Attribute	Card.	Description
definitionReference	0..1	This element will be used for routing purposes. The value could determine the department which will handle the notification. The display of this reference should be filled. See also: 10.2.8 | TTA - Addressing
basedOn	0..*	Optional reference to a request-Type resource 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.
status	1..1	The state communicated by this event. Fixed value: • requested See also: Valueset-request-status - FHIR v3.0.2
intent	1..1	Indicates the "level" of actionability associated with the Task[2]. Preferred value: • proposal See also: Valueset-request-intent - FHIR v3.0.2
code.coding	**1**..1	A code briefly describing what the task involves: • system = "http://fhir.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/CodeSystem/ura”
owner.identifier	**1**..1	Identifier of the Receiving Healthcare Organization. The identifier shall be in the system “http://fhir.nl/fhir/CodeSystem/ura”
input:authorization-base	0..**1**	The authorization base to be used when retrieving the data. Constraints: • type.coding ◦ system = "http://fhir.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.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 of:) ◦ *Generic typing:* ▪ system = "http://fhir.nl/fhir/CodeSystem/TaskParameter" ▪ code = "read-resource" ◦ *SNOMED CT typing:* ▪ system = “http://snomed.info/sct” ▪ code = a SNOMED CT code ◦ *LOINC typing:* ▪ system = “http://loinc.org”

		▪ code = a LOINC code • 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 of:) ◦ *Generic typing:* ▪ system = "http://fhir.nl/fhir/CodeSystem/TaskParameter" ▪ code = "search-resource" ◦ *SNOMED CT typing:* ▪ system = “http://snomed.info/sct” ▪ code = a SNOMED CT code ◦ LOINC typing: ▪ system = “http://loinc.org” ▪ code = a LOINC code • 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.nl/fhir/CodeSystem/TaskParameter"
- Task.input.type.coding.value: “get-workflow-task”
- ask.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 Notification response.

The Notification should trigger an event in the Receiving GtK to process the expected Pull.

Persistence of the Notification Task as a FHIR® resource is not necessary.

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.

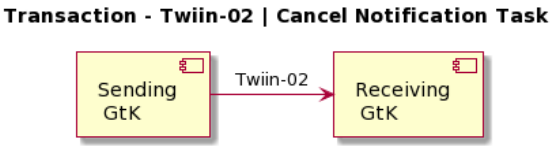
Whether or not the resources in input can be retrieved shall not be a factor in the HTTP status.

The Sending GtK processes the response according to application defined rules.

10.3.2 | 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.

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 🔥 Index - FHIR v3.0.2

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 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 🔥 Task - FHIR v3.0.2 .

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]. Preferred value: • proposal See also: Valueset-request-intent - FHIR v3.0.2

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.

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.

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.

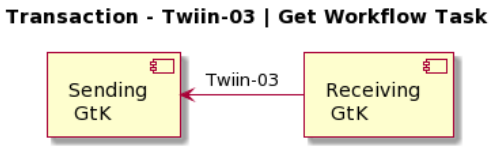
Whether or not the resources in input can be retrieved shall not be a factor in the HTTP status.

The Sending GtK processes the response according to application defined rules.

10.3.3 | Twiin-03 | Get workflow Task

This section describes the transaction of the retrieval of the workflow Task.

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 🔥 Task - FHIR v3.0.2 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.:

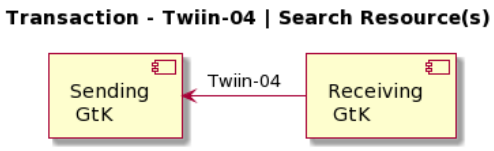
- `200` OK – The request is accepted and responded
- `401` Not Authorized - Authorization is required for the interaction that was attempted
- `404` Not Found – The request could not be processed, i.e. the resource with that id doesn't exist.
- `410` Gone – The request could not be processed, because the resource does not exist anymore.

The requesting system processes the response according to application defined rules.

10.3.4 | Twiin-04 | Search Resource(s)

This section describes the transaction of the retrieval of the FHIR® resources referenced in the input field of the Notification or Workflow Task.
These input fields contain valueString with either the generic type code “search-resource” or a LOINC or SNOMED CT code.

1. Scope



This transaction supports the request of resources by the Requesting System to the Resource Server.

2. Use Case Roles

Actor: Receiving GtK

Role: Sends a request for resources on behalf of a retrieving user.

Actor: Sending GtK **(**Resource Server)

Role: Processes the request and responds with the requested resources.

3. Referenced Standards

- HL7® FHIR® standard STU3 🔥 Index - FHIR v3.0.2

4. Messages

4.1. Request message

The requesting system 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
```

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.

4.2. Response message

The resource server 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 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.

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.:

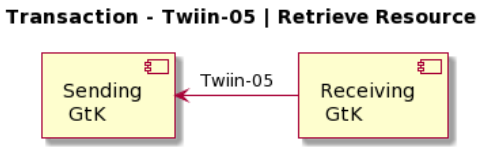
- `200` OK - The search was processed and a valid response was returned
- `400` Bad Request - The search could not be processed or failed basic FHIR® validation rules
- `401` Not Authorized - Authorization is required for the interaction that was attempted
- `404` Not Found - The resource type not supported

The requesting system processes the response according to application defined rules.

10.3.5 | Twiin-05 | Retrieve Resource

This page describes the transaction of the retrieval of the FHIR® resources referenced in the input field of the Notification or Workflow Task. These input fields contain valueReference combined with the input type “read-resource” or a LOINC or SNOMED CT code.

Scope



This transaction supports the request of resources by the Requesting System to the Resource Server.

Use Case Roles

Actor: Receiving GtK

Role: Sends a request for a specific resource on behalf of a retrieving user.

Actor: Sending GtK (Resource Server)

Role: Processes the request and responds with the requested resource.

Referenced Standards

- HL7® FHIR® standard STU3 🔥 Index - FHIR v3.0.2

Messages

Request message

The requesting system 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 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 resource that is requested.

The payload of this message is the requested FHIR® resource. 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.

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 system processes the response according to application defined rules.

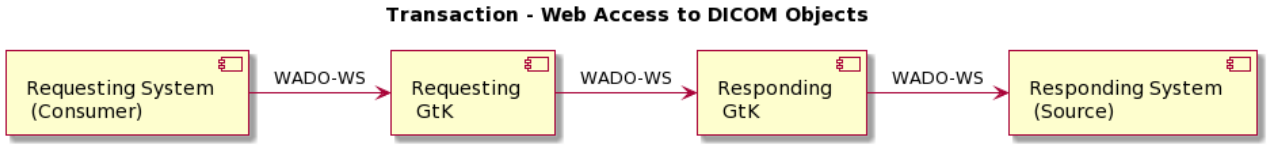
10.3.6 | Twiin-06 | WADO-WS

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



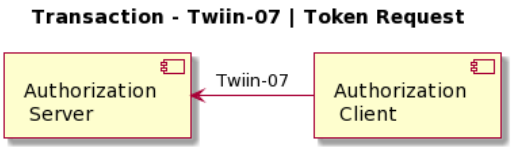

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- This wsdl file is for an XDS-I.b Imaging Document Source Actor
It can be used 'as is' to support Retrieve Imaging Document Set Transaction [RAD-69]
using Synchronous Web Services.-->
<definitions name="ImagingDocumentSource" targetNamespace="urn:ihe:rad:xdsi-b:2009" xmlns="http://schemas.xmlsoa
<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:2
<xsd:import namespace="urn:ihe:rad:xdsi-b:2009" />
</xsd:schema> </types>
<message name="RetrieveImagingDocumentSetRequest_Message"> <documentation>Retrieve Imaging Document Set</documen
<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:RetrieveImagingDocumentS
wsaw:Action="urn:ihe:rad:2009:RetrieveImagingDocumentSet" /> <output message="tns:RetrieveDocumentSetResponse_Me
wsaw:Action="urn:ihe:iti:2007:RetrieveDocumentSetResponse" /> </operation>
<operation name="ImagingDocumentSource_RetrieveRenderedImagingDocumentSet"> <input message="tns:RetrieveRendered
wsaw:Action="urn:dicom:wado:ws:2011:RetrieveRenderedImagingDocumentSet" /> <output message="tns:RetrieveRendered
wsaw:Action="urn:dicom:wado:ws:2011:RetrieveRenderedImagingDocumentSetResponse" /> </operation>
<operation name="ImagingDocumentSource_DeprecatedRetrieveRenderedImagingDocumentSet"> <input message="tns:Deprec
wsaw:Action="urn:dicom:ws:wado:2011:RetrieveRenderedImagingDocumentSet" /> <output message="tns:RetrieveDocument
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:
<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 loca
</port> </service> </definitions>
```

10.3.7 | 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

Referenced 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.
- *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.
- *RFC7515*: JSON Web Signature (JWS), May 2015.
- *RFC7518*: JSON Web Algorithms (JWA), May 2015.

- *RFC4648*: The Base16, Base32, and Base64 Data Encodings, October 2006

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 (RFC RF C 6749: The OAuth 2.0 Authorization Framework) 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 RFC RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.

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 RFC RFC 7518: JSON Web Algorithms (JWA). Must be one of PS256, PS384, PS512, ES256, ES384 or ES512.	Yes
kid	Identifier of the key pair used to sign this JWT. See RFC RFC 7515: JSON Web Signature (JWS).	Yes

The payload contains a set of claims listed below:

Claim	Description	Required
jti	Unique identifier of the client assertion. See RFC RFC 7519: JSON Web Token (JWT).	Yes
iss	Identifier of the system that issued the client assertion. See RFC RFC 7519: JSON Web Token (JWT) and RFC RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
iat	The time at which the client assertion was issued. See RFC RFC 7519: JSON Web Token (JWT). 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 RFC RFC 7519: JSON Web Token (JWT) and RFC RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
nbf	The time before which the token shall not be accepted for processing. See RFC RFC 7519: JSON Web Token (JWT) and RFC RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	No
aud	Identifier of the authorization server token endpoint where this client assertion is to be used. See RFC RFC 7519: JSON Web Token (JWT) and RFC RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants. System vendors have to make mutual agreements about the value of this identifier.	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

	System vendors have to make mutual agreements about the value of this identifier.	

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 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). 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 RFC 6749: The OAuth 2.0 Authorization Framework "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. RFC 6749: The OAuth 2.0 Authorization Framework. 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 RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants 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 RFC 7518: JSON Web Algorithms (JWA). Must be one of PS256, PS384, PS512, ES256, ES384 or ES512.	Yes
kid	Identifier of the key pair used to sign this JWT. See RFC 7515: JSON Web Signature (JWS).	Yes

The payload contains a set of claims that carry information required by NEN7512 and NEN7513.

Claim	Description	Required
jti	Unique identifier of the authorization assertion. See RFC 7519: JSON Web Token (JWT).	Yes
iss	Identifier of the system that issued the authorization assertion. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants. System vendors have to make mutual agreements about the value of this identifier.	Yes
iat	The time at which the authorization assertion was issued. See RFC 7519: JSON Web Token (JWT). 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 RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes

nbf	The time before which the token shall not be accepted for processing. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	No
aud	Identifier of the authorization server token endpoint where this authorization assertion is to be used. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
sub	Identifier of the **healthcare organization** that requests access. **URA nummer** 5.1 | Vertrouwen: Identificatie	Yes
user_id	Identifier of the **responsible user** (healthcare professional) who requests access. **Preferred: UZI nummer** 5.1 | Vertrouwen: Identificatie 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
user_role	Code of the role of the responsible user (healthcare professional) who requests access. **Preferred: UZI rolcode** 5.1 | Vertrouwen: Identificatie 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** 5.1 | Vertrouwen: Identificatie	Yes
authorization_base	See Authorization base	No
patient	Identifier of the patient for whom data is exchanged. Must be an OID encoded BSN (I.e., BSN with the “urn:oid:2.16.840.1.113883.2.4.6.3.” prefix and without a leading zero) 5.1 | Vertrouwen: Identificatie 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 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 RFC 6749: The OAuth 2.0 Authorization Framework . 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 App Launch: Scopes and Launch Context - SMART App Launch v2.2.0 . 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.nl/fhir/NamingSystem/TaskCode|pull-notification (create)
  - system/Task.u?code=http://fhir.nl/fhir/NamingSystem/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).

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 RFC 6749: The OAuth 2.0 Authorization Framework 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 Client authentication.	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

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 RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens , 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.

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 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). 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.

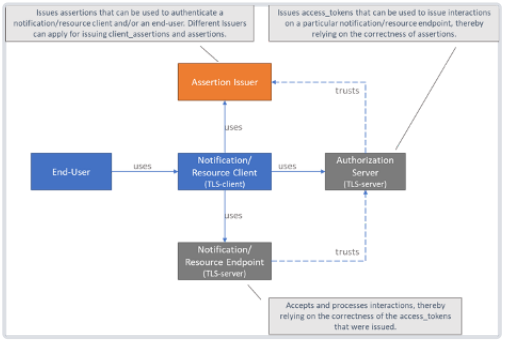
The Sending System can identify the healthcare professional at the receiving organization that is requesting patient data by the following claims in the authorization assertion of the access token request (see Authorization grant):

- **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 an 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.

10.3.14 | Transacties naar gemeenschappelijke voorzieningen

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:

- 10.3.14.1 | ZORG-AB Transacties
- 10.3.14.2 | Mitz Transacties

10.3.14.1 | ZORG-AB Transacties

Beschreven in de "VZVZ ZORG-AB Implementatiehandleiding". Voor meer informatie:

Dit is een externe transactie. Zie voor meer informatie: ZORG-AB voor leveranciers | VZVZ

Binnen Twiin worden de volgende transacties gebruikt:

- Get Organization
- Get Endpoint

ZORG-AB 2.9.1 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 Elektronic Services erin te kunnen registreren. Dit wordt 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).

Het gebruik van de ZORG-AB interfaces en transacties door een GtK is niet verplicht, maar wel de plek waar de adressen van GtKs worden gepubliceerd.

10.3.14.2 | 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

10.4 | Kern Volume 2c - Transactions - IHE

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.

10.4.1 | 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: IHE ITI TF Vol2

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."

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

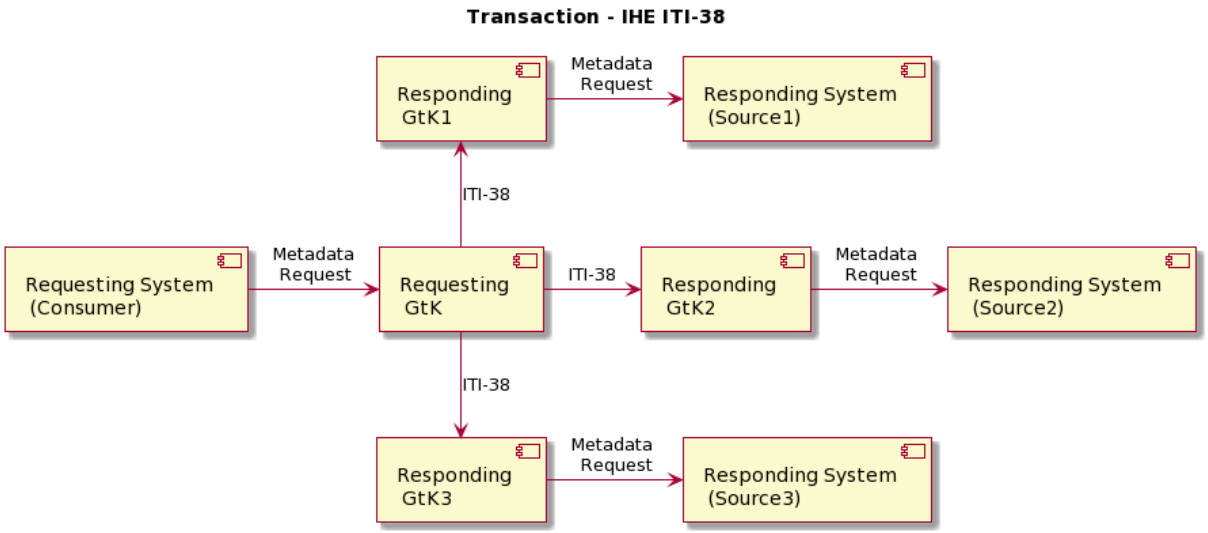
10.4.2 | IHE ITI-38 | Cross Gateway Query

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 at: 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.

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: IHE ITI TF Vol2

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.”

10.4.2.1 | ITI-38 examples

> For reference only

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:7ed
                    <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:Cla
                        <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:Cla
                        <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:Cla
                        <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:Cla
                        <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:Cla
                        <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:Cla
                        <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
```

```
                        <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
                        <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/2004/0
            <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/nd3SoL7aRpj96
                    <ds:KeyInfo>
                        <ds:X509Data>
                            <ds:X509Certificate>MIIDyzCCArMCAQEwDQYJKoZIhvcNAQELBQAwgasxCzAJBgNVBAYTAk5MMRUwEwYDVQQIDAxadWlk
LUhvbGxhbmQxHzAdBgNVBAcMFkNhcGVsbGUgYWFuIGRlbiBJSnNzZWwxGjAYBgNVBAoMEVZBTkFE
IEhlYWx0aCBDYXJlMRQwEgYDVQQLDAtEZXZlbG9wbWVudDELMAkGA1UEAwwCY2ExJTAjBgkqhkiG
9w0BCQEWFnhkc3RlYW1AdmFuYWRncm91cC5jb20wHhcNMTcxMTI4MTQyMzM5WhcNMTgxMTI4MTQy
MzM5WjCBqjELMAkGA1UEBhMCTkwxFTATBgNVBAgMDFp1aWQtSG9sbGFuZDEfMB0GA1UEBwwWQ2Fw
ZWxsZSBhYW4gZGVuIEllKc3NlbDEaMBgGA1UECgwRVkFOQUQgSGVhbHRoIENhcmUxFDASBgNVBAsM
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>
```

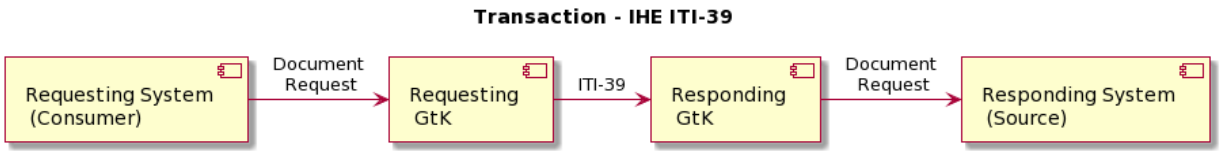
```
            <saml2:AttributeStatement>
                <!-- Beroepsgroep verantwoordelijke zorgverlener -->
                <saml2:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">
                    <saml2:AttributeValue>
                        <Role xmlns="urn:hl7-org:v3"
                            xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance code="01.013" codeSystem="2.16.840.1.113883.2.4.15.111" codeSystemName="RoleCode
                    </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
                    </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
                    </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>
```

10.4.3 | 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



Referenced standards

Implementers of this transaction shall comply with all requirements described in Web Services for IHE Transactions.

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: IHE ITI TF Vol2

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."

10.4.3.1 | 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</Acti
        <MessageID xmlns="http://www.w3.org/2005/08/addressing">urn:uuid:818cf943-1127-47b9-b5d7-16feedac311b</M
        <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</Relat
    </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-
                </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" IssueInstan
            <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#" Pref
                            </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
                <ds:KeyInfo>
                    <ds:X509Data>
                        <ds:X509Certificate>MIIDyzCCArMCAQEwDQYJKoZIhvcNAQELBQAwgasxCzAJBgNVBAYTAk5MMRUwEwYDVQQ
LUhvbGxhbmQxHzAdBgNVBAcMFkNhcGVsbGUgYWFuIGRlbiBJSnNzZWwxGjAYBgNVBAoMEVZBTkFE
IEhlYWx0aCBDYXJlMRQwEgYDVQQLDAtEZXZlbG9wbWVudDELMAkGA1UEAwwCY2ExJTAjBgkqhkiG
9w0BCQEWFnhkc3RlYW1AdmFuYWRncm91cC5jb20wHhcNMTcxMTI4MTQyMzM5WhcNMTgxMTI4MTQy
MzM5WjCBqjELMAkGA1UEBhMCTkwxFTATBgNVBAgMDFp1aWQtSG9sbGFuZDEfMB0GA1UEBwwWQ2Fw
ZWxsZSBhYW4gZGVuIEllKc3NlbDEaMBgGA1UECgwRVkFOQUQgSGVhbHRoIENhcmUxFDASBgNVBAsM
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:AuthnContext
                </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.
                    </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"
                    </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"
                    </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.
                    </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="2.16.840.1.113883.1.11.2
```

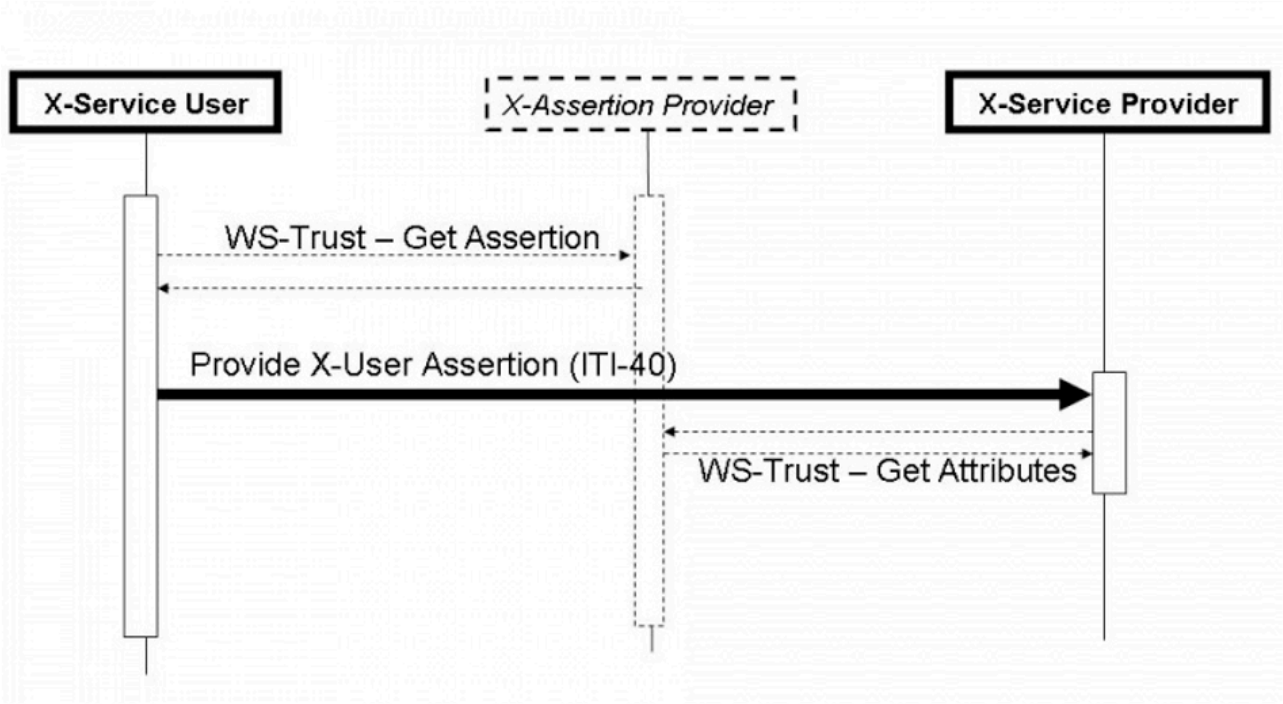
```
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                </saml2:AttributeStatement>
            </saml2:Assertion>
        </wsse:Security>

        <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>
```

10.4.5 | 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 Default Community home - OASIS
- SAMLCore SAML V2.0 Core standard
- WSS10 OASIS Standard, "OASIS Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)", March 2004.
- WSS11 OASIS Standard, "OASIS Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)", February 2006.
- WSS:SAMLTokenProfile1.0 OASIS Standard, “Web Services Security: SAML Token Profile”, December 2004
- WSS:SAMLTokenProfile1.1 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 Profile

- Enterprise User Authentication Profile
- Basic Patient Privacy Consents Profile

- OASIS
  - SAML V2.0 Standards Default Community home - OASIS .
  - 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: IHE ITI TF Vol2

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>`

Alternative Identification *verantwoordelijke* provider Opt.:	**Required, URA**
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

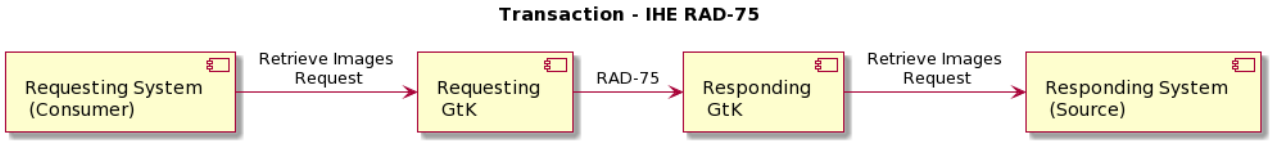
Purpose of use		
Name:	urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	
Type:	urn:hl7-org:v3#CV	
Example:	<AttributeValue DataType=" urn:hl7-org:v3#CV"> <CodedValue xmlns="urn:hl7-org:v3" code="TREAT" codeSystem="2.16.840.1.113883.1.11.20448" displayName="treatment" /> </AttributeValue>	
Opt.:	**Required**	

10.4.6 | 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 '10.4.2 | IHE ITI-38 | Cross Gateway Query 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



Referenced standards

Implementers of this transaction shall comply with all requirements described in Web Services for IHE Transactions.

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.
NB: All transactions are logged with an ITI-20 audit transaction, see IHE:ITI volume 2 for the correct implementation."

10.4.6.1 | 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</M
        <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/a
        </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:CrossGatewayRetrieveImagingDocumen
        <MessageID xmlns="http://www.w3.org/2005/08/addressing">urn:uuid:8f62a0f3-1906-4b32-9b22-e37585fb4cc5</M
        <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</Relat
    </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-
                </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</Actio
        <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</
        <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/
        </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" IssueIn
                <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#"
                                </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/GVZ6pkmbkwNPZ
                    <ds:KeyInfo>
                        <ds:X509Data>
                            <ds:X509Certificate>MIIDyzCCArMCAQEwDQYJKoZIhvcNAQELBQAwgasxCzAJBgNVBAYTAk5MMRUwEwY
LUhvbGxhbmQxHzAdBgNVBAcMFkNhcGVsbGUgYWFuIGRlbiBJSnNzZWwxGjAYBgNVBAoMEVZBTkFE
IEhlYWx0aCBDYXJlMRQwEgYDVQQLDAtEZXZlbG9wbWVudDELMAkGA1UEAwwCY2ExJTAjBgkqhkiG
9w0BCQEWFnhkc3RlYW1AdmFuYWRncm91cC5jb20wHhcNMTcxMTI4MTQyMzM5WhcNMTgxMTI4MTQy
MzM5WjCBqjELMAkGA1UEBhMCTkwxFTATBgNVBAgMDFp1aWQtSG9sbGFuZDEfMB0GA1UEBwwWQ2Fw
ZWxsZSBhYW4gZGVuIEllKc3NlbDEaMBgGA1UECgwRVkFOQUQgSGVhbHRoIENhcmUxFDASBgNVBAsM
```

```
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:AuthnCon
                    </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
                        </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="C
                        </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="C
                        </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=" 2.16.528.1.1
                        </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
                            </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>
```

10.4.7 | IHE ITI-81 | Retrieve Audit Record

This transaction is informative. Not for implementation in Twiin 1.2

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

10.4.8 | IHE ITI-82 | Retrieve Syslog Event

This transaction is informative. Not for implementation in Twiin 1.2

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

10.5 | Kern Volume 3 - Content

Dit volume bevat de content, zoals bijvoorbeeld metadata, die overkoepelend voor de zorgtoepassingen geldt en relevante verwijzing naar de content van andere afsprakenstelsel en voorzieningen voor generieke functies

10.5.1 | Document/beeld gebaseerde Metadata

Metadata geïndexeerde bevraging

Disclaimer

Voor de vulling van metadata is gebruik gemaakt van de Nictiz Metadataset: XDS metadata - Nictiz

De Nictiz metadata set is document gebaseerd en niet 1 op 1 van toepassing op b.v. resource gebaseerde uitwisseling.

APPLICATIE-LAAG

Het uitwisselpatroon geïndexeerde bevraging 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
patientId	R	'123456789^^^&2.16.840.1.113883.2.4.6.3&ISO'	BSN van patiënt
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

healthcareFacility TypeCode	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
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 1.3 Zorgtoepassingen

De implementatiewijzers zijn 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: 10 | Technische kern 5 | Vertrouwensmodel 9 | Voorwaarden

In de onderliggende pagina's zijn de implementatiewijzers beschreven voor de databeschikbaarheid van de zorgtoepassingen

- Z1 | BgZ: Implementatiewijzer Basisgegevensset Zorg - 1.2.0 Trial
- Z2 | BB: Implementatiewijzer Beeldbeschikbaarheid 1.3.0 Trial
- Z3 | COR: implementatiewijzer Correspondentie 1.2.0 Trial

Volgens het releasebeheer onderkennen we de volgende statussen aan de zorgtoepassingen:

- **informative** Een informatieve toelichting over wat Twiin voor deze zorgtoepassing te bieden heeft
- **draft**: Een conceptuele beschrijving, vaak nog onvolledig. Ter informatie
- **review**: Een versie ter review
- **trial**: Een versie voor beproeving
- **zonder toevoeging** is de status normatief

Z1 | BgZ: Implementatiewijzer Basisgegevensset Zorg - 1.2.0 Trial

⚠ Zorgtoepassing BgZ **versie 1.2.0 trial** onderdeel van Twiin Release 1.2

Deze zorgtoepassing is klaar voor beproeving. Meewerken aan deze beproeving?

Laat het ons weten door te e-mailen naar info@twiin.nl

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, Twiin Implementatiewijzer Zorgtoepassingen, Vertrouwensmodel, Voorwaarden,

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 VIPP5) en aanstaande wet- en regelgeving bestaat een toenemende behoefte om de BgZ op een veilige en gestandaardiseerde wijze beschikbaar te stellen tussen zorgaanbieders. VIPP5 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 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.
- Volume 2a bevat de technische afspraken voor de uitwisseling van de BgZ. Dit noemen we ook wel de Twiin Technische Afspraak (TTA).
- Volume 2b bevat alle losse transacties die gebruikt worden voor de uitwisseling van de BgZ.
- Volume 3 is een verwijzing naar de informatiestandaard en de meta-informatie.

Vanuit bovenstaande 4 secties zijn ook de Eisen overzichtelijk beschreven, deze zijn terug te vinden via de BgZ: Samenvatting PvE.

Vanuit Twiin wensen we je veel lees- en ontwikkel plezier.

Z1.1 | BgZ Volume 1 - Functioneel overzicht

Inleiding

In dit volume:

- een beschrijving van de functionele use-casus 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;
- een beschrijving of verwijzing naar de eisen die gesteld zijn door organisaties, programma's en/of informatiestandaarden.

In volume 2 volgen de uitwerking van de transacties van de uitwisselpatronen voor de zorgtoepassing BgZ (in het Engels)

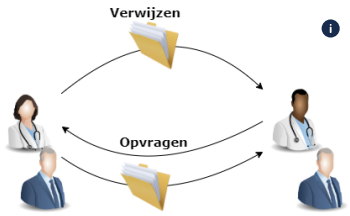
Versie informatie

Versie Zorgtoepassing	Compatibel met Twiin Afsprakenstelsel release	Wijzingen
1.2.0	1.2.0 en alle opvolgende binnen de major release 1.x.x	

Functionele use cases

In de NEN7540 (BgZ) en de informatiestandaard BgZ voor uitwisseling tussen medisch specialistische instellingen zijn 2 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 2 manieren om de BgZ beschikbaar te stellen:

1. Uitwisseling 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. Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden

Deze zijn overgenomen in de onderliggende pagina’s.

- Z1.1.1 | Uitwisseling BgZ bij verwijzing of overdracht
- Z1.1.2 | Opvraging BgZ bij eerdere behandelaar

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 beschrijft de technische invulling van deze uitwisseling binnen Twiin.

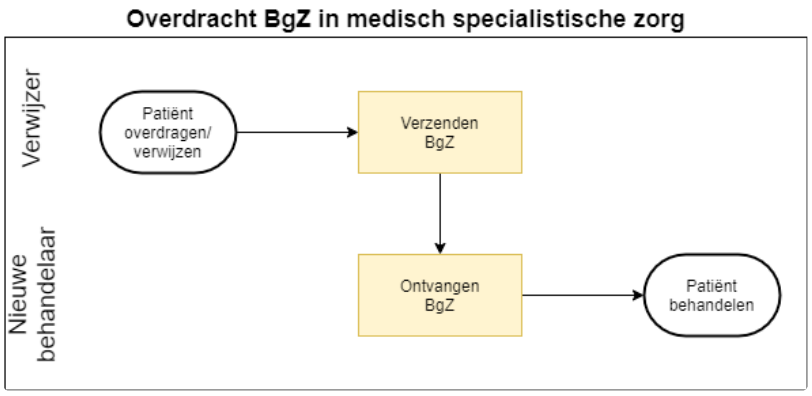
Proudly copied from Nictiz: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden

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 afgestemd met de volgende koepels FMS, NVZ, NFU en ZKN en wordt tot nader order gehanteerd als veldnorm.

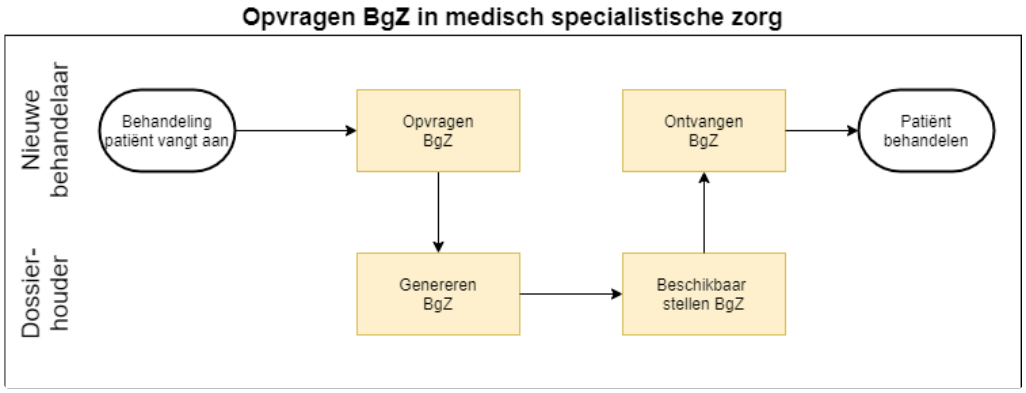
Z1.1.2 | Opvraging BgZ bij eerdere behandelaar

Deze pagina beschrijft de uitwisseling in het geval van een opvraging van de BgZ bij een eerdere behandelaar. De Z1.2.2 | TTA Retrievi ng BgZ - FHIR Direct Pull beschrijft de technische invulling van deze uitwisseling binnen Twiin.

Proudly copied from Nictiz: https://informatiestandaarden.nictiz.nl/wiki/BgZ:V1.0_BgZ_MSZ_Informatiestandaard#Use_case_2:_Opvraging_BgZ_bij_eerdere_behandelaar

Doel en relevantie

Bij deze use case is sprake van 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 2a - 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.

onderliggende pagina's

- Z1.2.1 | TTA Exchanging BgZ - FHIR Notified Pull
- Z1.2.2 | TTA Retrieving BgZ - FHIR Direct Pull
- Z1.2.3 | TTA Retrieving BgZ - SOAP Indexed Pull
- Z1.2.4 | TTA Exchanging BgZ - SOAP PUSH

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 10.2.3 | TTA FHIR - Notified pull

This Twiin Technical Agreement (TTA) describes and specifies 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, with the normative specifications remaining unchanged. The informative specifications however have been described with a specific implementation.

The possibility to exchange a patient's medical record is for example required in case of a patient referral or transfer. When different healthcare organizations are involved in a patient'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.

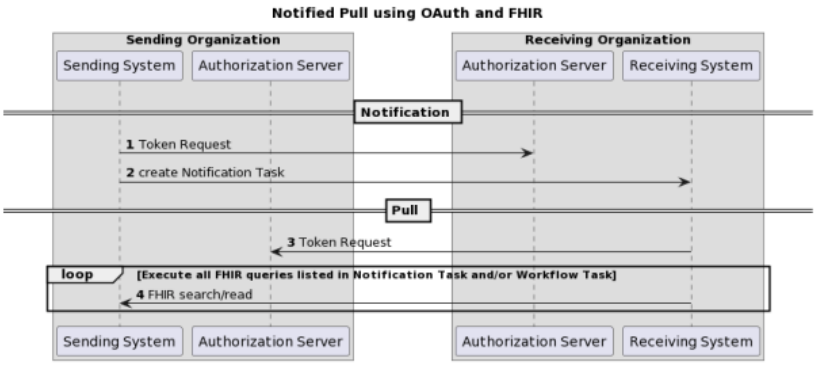
Relation to other documents

This document is written with the following documents as reference:

- Nictiz - Informatiestandaard BgZ MSZ
- TA Notified Pull v0.99

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 10.2.5 | TTA FHIR - Authentication & Authorization. Interaction number 2 is described in 10.2.3.1 | Notified Pull - Data interactions . A part of interaction number 4 is also described in 10.2.3.1 | Notified Pull - Data interactions, for specifics of the context of the Notified Pull see Nictiz information standards.

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

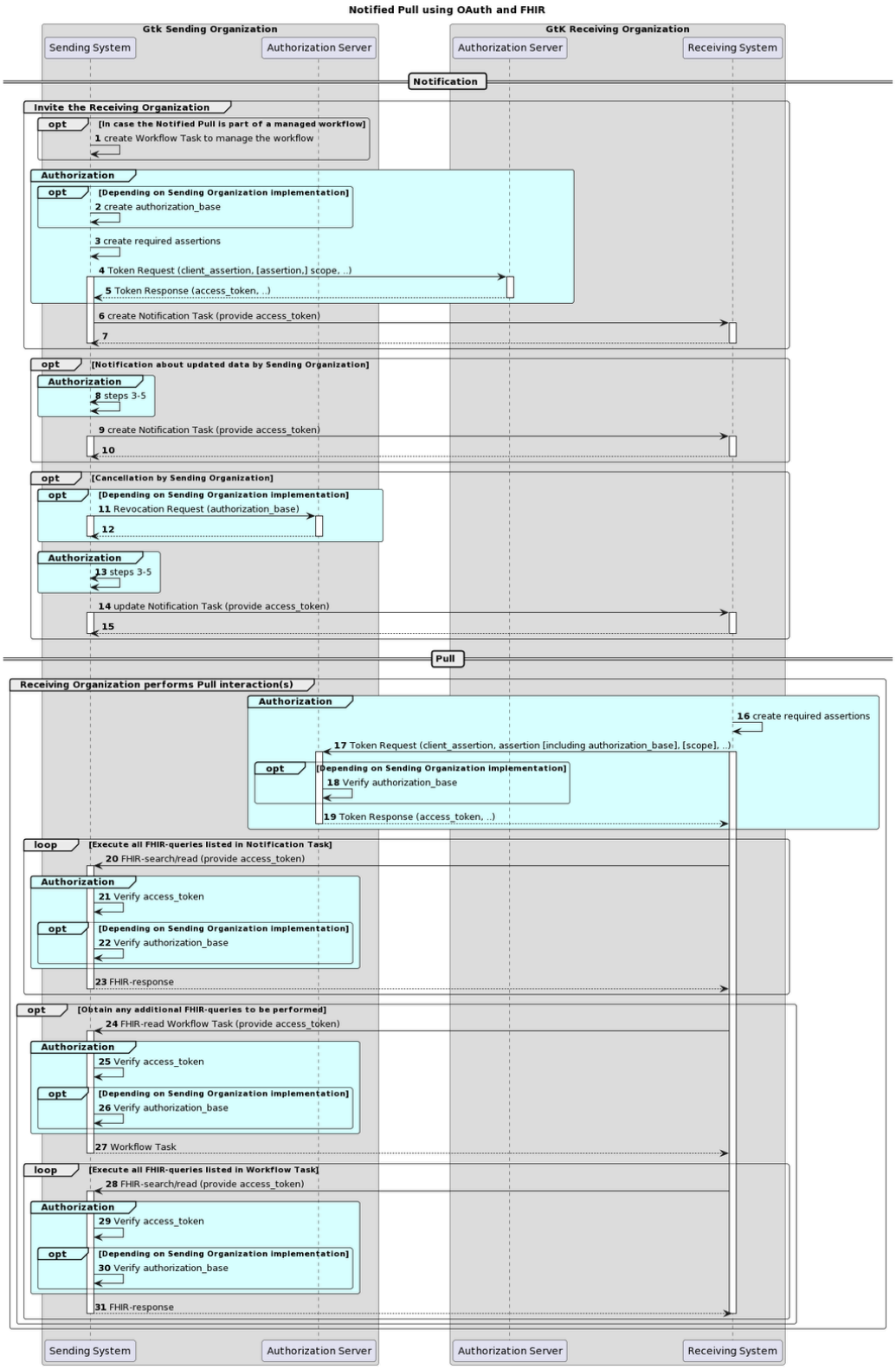
The Twiin specific solutions for identification and addressing can be found in 10.2.5 | TTA FHIR - Authentication & Authorization and 10.2.8 | TTA - Addressing respectively.

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 10.2.3.1 Notified Pull - Data interactions) and in authorization layer using OAuth 2.0 (marked cyan,

described in 10.2.10 | Netwerk level security mTLS 1.3).

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 a 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 others) 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.

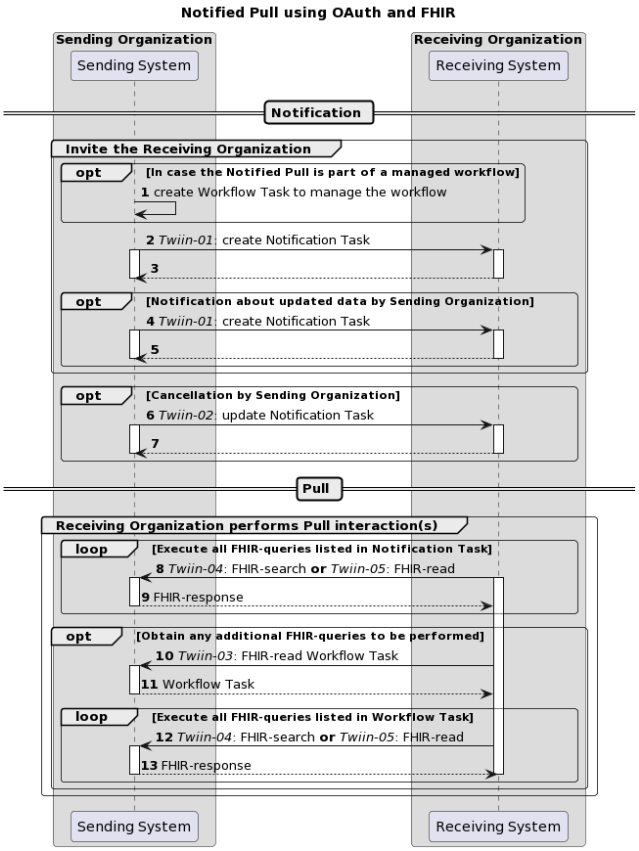
Z1.2.1.1 | BgZ - data interactions

Original page can be found at: 10.2.3.1 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 10.3.1 | Twiin-01 | Send Notification Task 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 10.3.1 | Twiin-01 | Send Notification Task 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 10.3.2 | Twiin-02 | Cancel Notification Task 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 10.3.5 | Twiin-05 | Retrieve Resource for a detailed description for the retrieval of resources referenced in Task.input:read-available-resources. See 10.3.4 | Twiin-04 | Search Resource(s) 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 10.3.3 | Twiin-03 | Get workflow Task
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 10.3.5 | Twiin-05 | Retrieve Resource for a detailed description for the retrieval of resources referenced in Task.input:read-available-resources. See 10.3.4 | Twiin-04 | Search Resource(s) 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 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.

10.2.3 | TTA FHIR - Notified pull

10.2.10 | Netwerk level security mTLS 1.3

Z1.2.1.2 | BgZ: Authentication & Authorization

Original page can be found at: 10.2.5 | TTA FHIR - Authentication & Authorization

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 RFC 6749: The OAuth 2.0 Authorization Framework. 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 RFC 6750: The OAuth 2.0 Authorization Framework: Bearer Token Usage.

Client authentication

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 (RFC 6749: The OAuth 2.0 Authorization Framework) 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 RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.

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 RFC 7518: JSON Web Algorithms (JWA). Must be one of PS256, PS384, PS512, ES256, ES384 or ES512.	Yes
kid	Identifier of the key pair used to sign this JWT. See RFC 7515: JSON Web Signature (JWS).	Yes

The payload contains a set of claims listed below:

Claim	Description	Required
jti	Unique identifier of the client assertion. See RFC 7519: JSON Web Token (JWT).	Yes
iss	Identifier of the system that issued the client assertion. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
iat	The time at which the client assertion was issued. See RFC 7519: JSON Web Token (JWT). 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 RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes

nbf	The time before which the token shall not be accepted for processing. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	No
aud	Identifier of the authorization server token endpoint where this client assertion is to be used. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	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 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). 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 RFC 6749: The OAuth 2.0 Authorization Framework "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. RFC 6749: The OAuth 2.0 Authorization Framework. 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 RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants 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 RFC 7518: JSON Web Algorithms (JWA). Must be one of PS256, PS384, PS512, ES256, ES384 or ES512.	Yes
kid	Identifier of the key pair used to sign this JWT. See RFC 7515: JSON Web Signature (JWS).	Yes

The payload contains a set of claims that carry information required by NEN7512 and NEN7513.

Claim	Description	Required
jti	Unique identifier of the authorization assertion. See RFC 7519: JSON Web Token (JWT).	Yes

iss	Identifier of the system that issued the authorization assertion. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
iat	The time at which the authorization assertion was issued. See RFC 7519: JSON Web Token (JWT). 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 RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
nbf	The time before which the token shall not be accepted for processing. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	No
aud	Identifier of the authorization server token endpoint where this authorization assertion is to be used. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
sub	Identifier of the **organization** (healthcare supplier) 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	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 a authorization base when requesting patient information.	Conditional
user_id	Identifier of the **responsible user** (healthcare professional) or the **system** who requests access. **Preferred: UZI nummer** The codesystem (`issuing_system`) for the identifier is also mandatory. For UZI this is OID: 2.16.528.1.1007.3.1 5.1 | Vertrouwen: Identificatie **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** 5.1 | Vertrouwen: Identificatie The codesystem (`issuing_system`) for the identifier is also mandatory. For UZI role code this is OID: 2.16.840.1.113883.2.4.15.111	Conditional

	User role is required when the responding party needs to validate the role of the user before responding to the request. For instance when a user does not have a authorization base when requesting patient information.	
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	Yes
authorization_base	See Authorization base	No
patient	Identifier of the patient for whom data is exchanged. Must be an OID encoded BSN (I.e., BSN with the "urn:oid:2.16.840.1.113883.2.4.6.3." prefix and without a leading zero) 5.1 | Vertrouwen: Identificatie 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 a ll not require the authorization serv

The exchange of the public 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 RFC 6749: The OAuth 2.0 Authorization Framework . 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 App Launch: Scopes and Launch Context - SMART App Launch v2.2.0 . 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.nl/fhir/NamingSystem/TaskCode|pull-notification (create)
  - system/Task.u?code=http://fhir.nl/fhir/NamingSystem/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).

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 RFC 6749: The OAuth 2.0 Authorization Framework 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 Client authentication.	Yes
client_id	ID of the resource client. This ID is issued by the authorization server. If present, the value of the "client_id" parameter must identify the same client as is identified by the client assertion.	No
scope	Space separated list of requested scopes, see paragraph Authorization scope.	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 RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens , 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.

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 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). 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):

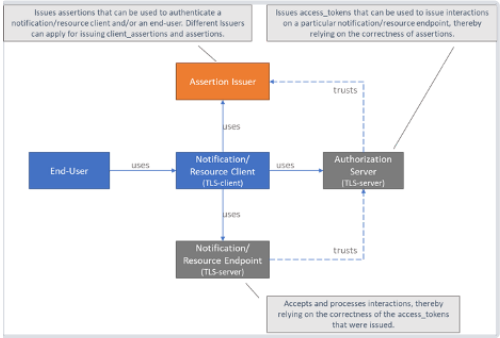
- **sub**: Identifier of the healthcare organization

- **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 an 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.

Z1.2.2 | TTA Retrieving BgZ - FHIR Direct Pull

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: 10.2.4 | TTA FHIR - Pull

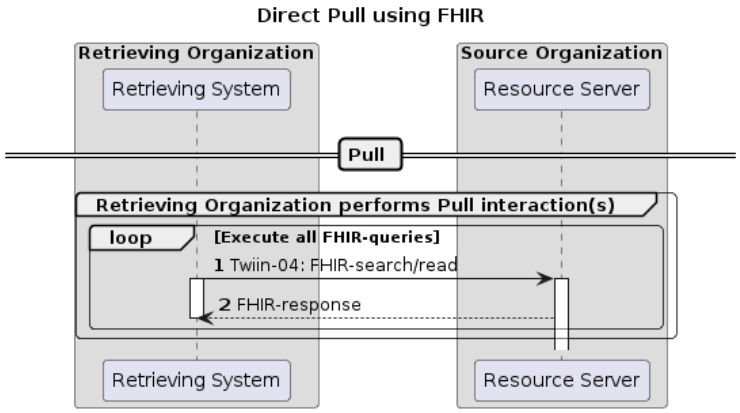
This exchange pattern (Direct Pull) is Draft, intended for further coordination with suppliers and healthcare providers.

This Twiin Technical Agreement (TTA) describes and specifies technical responsibilities to which parties agree when connecting to exchange transactions to facilitate the Direct Pull.

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 10.3.4 | Twiin-04 | Search Resource(s) 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 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

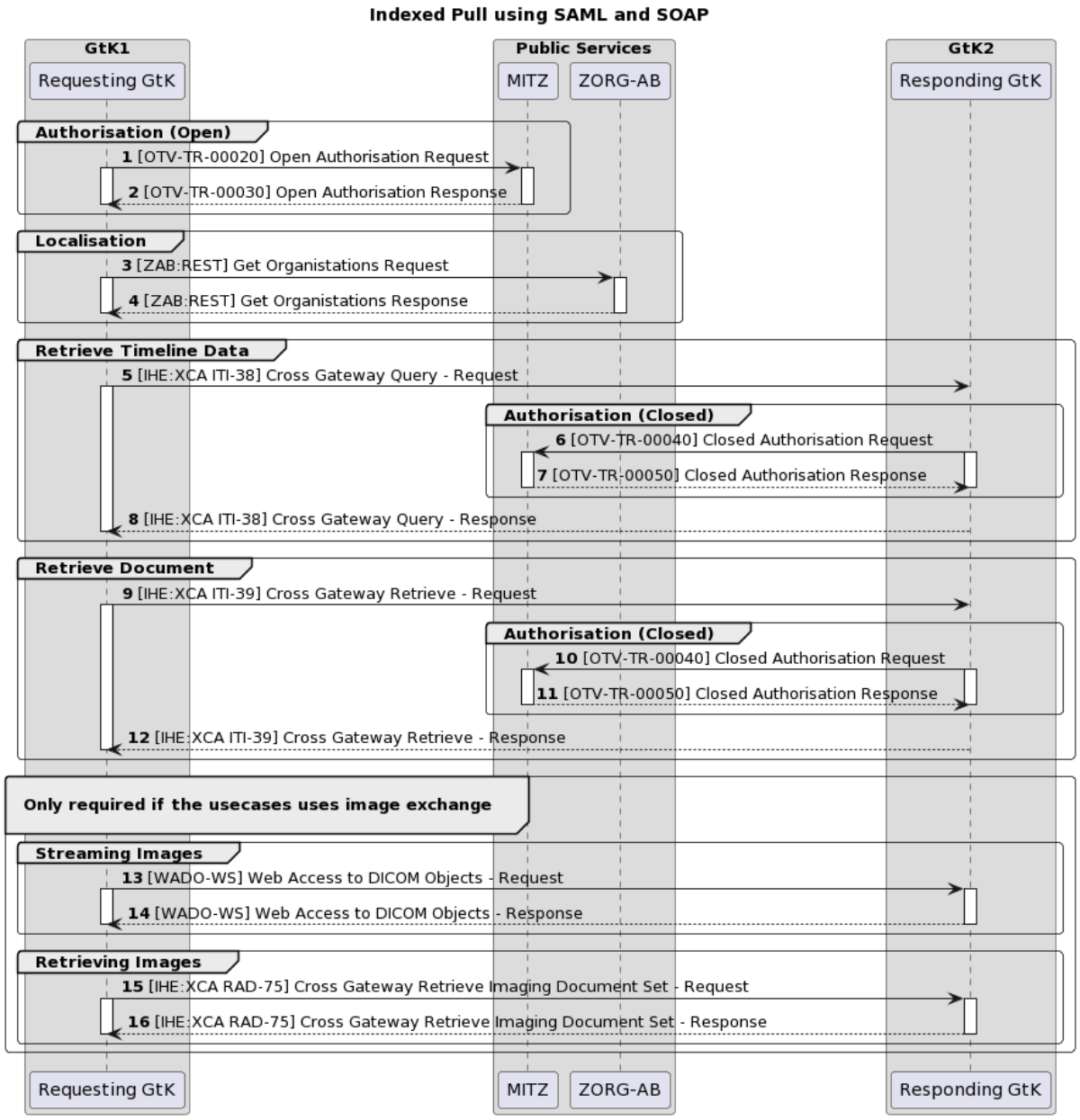
This Twiin Technical Agreement (TTA) describes and specifies technical responsibilities to which parties agree when connecting to exchange transactions to facilitate the Indexed Pull.

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



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.

10.4.5 | IHE ITI-40 | Provide X-User Assertion

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'

		10.3.14.2 | Mitz Transacties - 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 10.3.14.2 | Mitz Transacties - 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 10.3.14.1 | ZORG-AB Transacties
	4	ZORG-AB replies to this request with the endpoints 10.3.14.1 | ZORG-AB Transacties
Retrieve Timeline data	5	Using the endpoints the GtK uses this information to send the query. With this transaction a SAML token is included 10.4.2 | IHE ITI-38 | Cross Gateway Query 10.4.2.1 | ITI-38 examples | ITI 38 request
	6	The responding GtK then checks if the patients permission is in check at MITZ 10.3.14.2 | Mitz Transacties - OTV-TR-00040
	7	A response is sent back 10.3.14.2 | Mitz Transacties - 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. 10.4.2 | IHE ITI-38 | Cross Gateway Query 10.4.2.1 | 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. 10.4.3 | IHE ITI-39 | Cross Gateway Retrieve 10.4.3.1 | ITI-39 examples | ITI 39 request
	10	(see step 6) 10.3.14.2 | Mitz Transacties - OTV-TR-00040
	11	(see step 7) 10.3.14.2 | Mitz Transacties - 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 10.4.3 | IHE ITI-39 | Cross Gateway Retrieve

		10.4.3.1 | 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. 10.3.6 | Twiin-06 | WADO-WS
	14	The images are sent back in the requested format 10.3.6 | Twiin-06 | WADO-WS
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. 10.4.6 | IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set 10.4.6.1 | RAD-75 examples | RAD 75 request
	16	The images are sent back 10.4.6 | IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set 10.4.6.1 | RAD-75 examples | RAD 75 response

10.2 | Kern Volume 2a - Twiin Technical Agreements

10.2.3.1 Notified Pull - Data interactions

Z1.2.4 | TTA Exchanging BgZ - SOAP PUSH

Informative only. Please contact info@twiin.nl 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 if you use IHE XDR in a production scenario.

Z1.3 | BgZ Volume 2b - Transactions

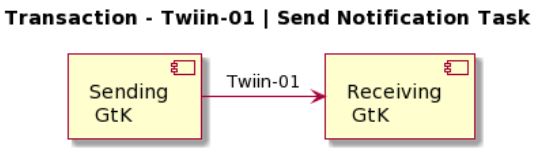
Within this volume the transactions that are used within the exchange of the BgZ are described.

Z1.3.1 | Twiin-01 | Send BgZ Notification Task

This section is the same as the generic 10.3.1 | Twiin-01 | Send Notification Task

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 Index - FHIR v3.0.2

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
- Identification of the patient who is the subject of information exchange
- References to individual FHIR® resources that have been made available at the Sending GtK
- FHIR® search queries that can be used to retrieve FHIR® resources that have been made available at the Sending GtK
- Authorization base (see Authorization base)

The payload of this message consists of a Task - FHIR v3.0.2 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 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 Task - FHIR v3.0.2 .

Attribute	Card.	Description
definitionReference	0..1	This element will be used for routing purposes. The value could determine the department which will handle the notification. The display of this reference should be filled. See also: 10.2.8 | TTA - Addressing
basedOn	0..*	Optional reference to a request-Type resource 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.
status	1..1	The state communicated by this event. Fixed value: • requested See also: Valueset-request-status - FHIR v3.0.2
intent	1..1	Indicates the "level" of actionability associated with the Task[2]. Preferred value: • proposal See also: Valueset-request-intent - FHIR v3.0.2
code.coding	**1**..1	A code briefly describing what the task involves: • system = "http://fhir.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/CodeSystem/ura”
owner.identifier	**1**..1	Identifier of the Receiving Healthcare Organization. The identifier shall be in the system “http://fhir.nl/fhir/CodeSystem/ura”

input:authorization-base	0..**1**	The authorization base to be used when retrieving the data.
		
		Constraints:
		
		• type.coding
		  ◦ system = "http://fhir.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.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 of:)
		  ◦ *Generic typing:*
		  ▪ system = "http://fhir.nl/fhir/CodeSystem/TaskParameter"
		  ▪ code = "read-resource"
		  ◦ *SNOMED CT typing:*
		  ▪ system = “http://snomed.info/sct”
		  ▪ code = a SNOMED CT code
		  ◦ *LOINC typing:*
		  ▪ system = “http://loinc.org”
		  ▪ code = a LOINC code
		• 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 of:) ◦ *Generic typing:* ▪ system = "http://fhir.nl/fhir/CodeSystem/TaskParameter" ▪ code = "search-resource" ◦ *SNOMED CT typing:* ▪ system = “http://snomed.info/sct” ▪ code = a SNOMED CT code ◦ LOINC typing: ▪ system = “http://loinc.org” ▪ code = a LOINC code • 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.nl/fhir/CodeSystem/TaskParameter"
- Task.input.type.coding.value: “get-workflow-task”
- ask.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 Notification response.

The Notification should trigger an event in the Receiving GtK to process the expected Pull.

Persistence of the Notification Task as a FHIR® resource is not necessary.

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 in input can be retrieved shall not be a factor in the HTTP status.

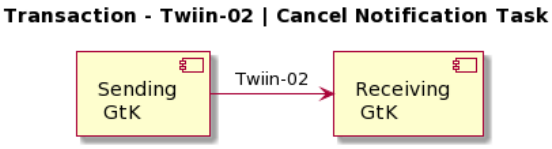
The Sending GtK processes the response according to application defined rules.

Z1.3.2 | Twiin-02 | Cancel BgZ Notification Task

This page is the same as the generic 10.3.2 | 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.

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 Index - FHIR v3.0.2

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 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 Task - FHIR v3.0.2 .

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]. Preferred value: • proposal See also: Valueset-request-intent - FHIR v3.0.2

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.

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.

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.

Whether or not the resources in input can be retrieved shall not be a factor in the HTTP status.

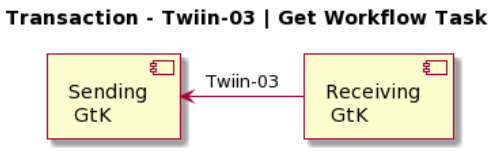
The Sending GtK processes the response according to application defined rules.

Z1.3.3 | Twiin-03 | Get BgZ workflow Task

This page is the same as the generic 10.3.3 | Twiin-03 | Get workflow Task

This section describes the transaction of the retrieval of the workflow Task.

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 🔥 Task - FHIR v3.0.2 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.

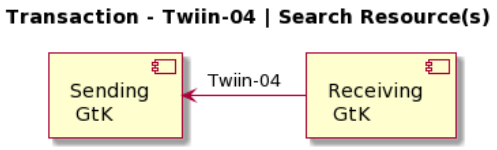
The requesting system processes the response according to application defined rules.

Z1.3.4 | Twiin-04 | Search BgZ Resource(s)

This page is the same as the generic 10.3.4 | Twiin-04 | Search Resource(s)

This section describes the transaction of the retrieval of the FHIR® resources referenced in the input field of the Notification or Workflow Task.
These input fields contain valueString with either the generic type code “search-resource” or a LOINC or SNOMED CT code.

1. Scope



This transaction supports the request of resources by the Requesting System to the Resource Server.

2. Use Case Roles

Actor: Receiving GtK

Role: Sends a request for resources on behalf of a retrieving user.

Actor: Sending GtK **(**Resource Server)

Role: Processes the request and responds with the requested resources.

3. Referenced Standards

- HL7® FHIR® standard STU3 Index - FHIR v3.0.2

4. Messages

4.1. Request message

The requesting system 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
```

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.

4.2. Response message

The resource server 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 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.

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

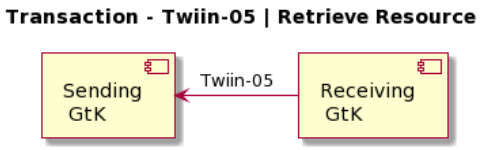
The requesting system processes the response according to application defined rules.

Z1.3.5 | Twiin-05 | Retrieve BgZ Resource

This page is the same as the generic 10.3.5 | Twiin-05 | Retrieve Resource

This page describes the transaction of the retrieval of the FHIR® resources referenced in the input field of the Notification or Workflow Task. These input fields contain valueReference combined with the input type “read-resource” or a LOINC or SNOMED CT code.

Scope



This transaction supports the request of resources by the Requesting System to the Resource Server.

Use Case Roles

Actor: Receiving GtK

Role: Sends a request for a specific resource on behalf of a retrieving user.

Actor: Sending GtK (Resource Server)

Role: Processes the request and responds with the requested resource.

Referenced Standards

- HL7® FHIR® standard STU3 Index - FHIR v3.0.2

Messages

Request message

The requesting system 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 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 resource that is requested.

The payload of this message is the requested FHIR® resource. 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.

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

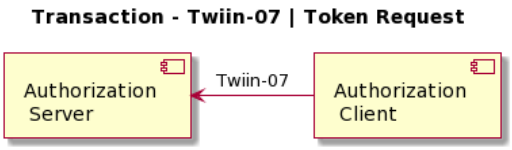
The requesting system processes the response according to application defined rules.

Z1.3.7 | Twiin-07 | Token Request

This page is the same as the generic 10.3.7 | Twiin - 07 | Token Request

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

Referenced 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.
- *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.

- *RFC7515*: JSON Web Signature (JWS), May 2015.
- *RFC7518*: JSON Web Algorithms (JWA), May 2015.
- *RFC4648*: The Base16, Base32, and Base64 Data Encodings, October 2006

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 (RFC RF C 6749: The OAuth 2.0 Authorization Framework) 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 RFC RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.

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 RFC RFC 7518: JSON Web Algorithms (JWA). Must be one of PS256, PS384, PS512, ES256, ES384 or ES512.	Yes
kid	Identifier of the key pair used to sign this JWT. See RFC RFC 7515: JSON Web Signature (JWS).	Yes

The payload contains a set of claims listed below:

Claim	Description	Required
jti	Unique identifier of the client assertion. See RFC RFC 7519: JSON Web Token (JWT).	Yes
iss	Identifier of the system that issued the client assertion. See RFC RFC 7519: JSON Web Token (JWT) and RFC RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
iat	The time at which the client assertion was issued. See RFC RFC 7519: JSON Web Token (JWT). 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 RFC RFC 7519: JSON Web Token (JWT) and RFC RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
nbf	The time before which the token shall not be accepted for processing. See RFC RFC 7519: JSON Web Token (JWT) and RFC RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	No
aud	Identifier of the authorization server token endpoint where this client assertion is to be used. See RFC RFC 7519: JSON Web Token (JWT) and RFC RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants. System vendors have to make mutual agreements about the value of this identifier.	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.	Yes

	Note that the client is specified as the system that submits the access token request. System vendors have to make mutual agreements about the value of this identifier.	

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 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). 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 RFC 6749: The OAuth 2.0 Authorization Framework "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. RFC 6749: The OAuth 2.0 Authorization Framework. 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 RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants 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 RFC 7518: JSON Web Algorithms (JWA). Must be one of PS256, PS384, PS512, ES256, ES384 or ES512.	Yes
kid	Identifier of the key pair used to sign this JWT. See RFC 7515: JSON Web Signature (JWS).	Yes

The payload contains a set of claims that carry information required by NEN7512 and NEN7513.

Claim	Description	Required
jti	Unique identifier of the authorization assertion. See RFC 7519: JSON Web Token (JWT).	Yes
iss	Identifier of the system that issued the authorization assertion. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants. System vendors have to make mutual agreements about the value of this identifier.	Yes
iat	The time at which the authorization assertion was issued. See RFC 7519: JSON Web Token (JWT). 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 RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
nbf	The time before which the token shall not be accepted for processing. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	No
aud	Identifier of the authorization server token endpoint where this authorization assertion is to be used. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
sub	Identifier of the **healthcare organization** that requests access. **URA nummer** 5.1 | Vertrouwen: Identificatie	Yes
user_id	Identifier of the **responsible user** (healthcare professional) who requests access. **Preferred: UZI nummer** 5.1 | Vertrouwen: Identificatie 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
user_role	Code of the role of the responsible user (healthcare professional) who requests access. **Preferred: UZI rolcode** 5.1 | Vertrouwen: Identificatie 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** 5.1 | Vertrouwen: Identificatie	Yes
authorization_base	See Authorization base	No
patient	Identifier of the patient for whom data is exchanged. Must be an OID encoded BSN (I.e., BSN with the "urn:oid:2.16.840.1.113883.2.4.6.3." prefix and without a leading zero) 5.1 | Vertrouwen: Identificatie 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 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 RFC 6749: The OAuth 2.0 Authorization Framework . 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 App Launch: Scopes and Launch Context - SMART App Launch v2.2.0 . 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.nl/fhir/NamingSystem/TaskCode|pull-notification (create)
  - system/Task.u?code=http://fhir.nl/fhir/NamingSystem/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).

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 RFC 6749: The OAuth 2.0 Authorization Framework 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 Client authentication.	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

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 RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens , 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.

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 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). 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.

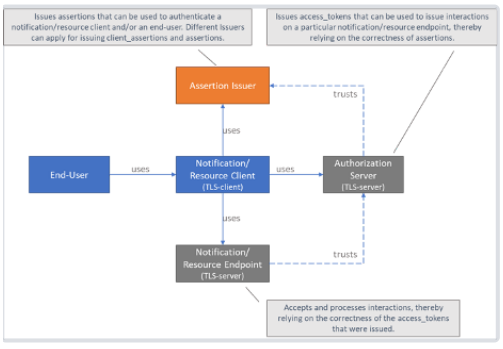
The Sending System can identify the healthcare professional at the receiving organization that is requesting patient data by the following claims in the authorization assertion of the access token request (see Authorization grant):

- **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 an 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.

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

BgZ medisch-specialistische zorg Technical Implementation Guide 1.0 - informatiestandaarden

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.

Z1.4.1 | BgZ: FHIR Task reference codes

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
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).

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
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	
-- patientInformation	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“79191-3”
-- -- -- -- display	0..1	string	“Patient demographics panel”
-- -- text	1..1	string	“Patient information”
-- -- valueString	1..1	string	“/Patient?_include=Patient:general-practitioner”
-- paymentDetails	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“48768-6”
-- -- -- -- display	0..1	string	“Payment sources”
-- -- 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	
-- -- -- LOINC	1..1	Slice	

-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“11291000146105”
-- -- -- -- display	0..1	string	“Treatment instructions”
-- -- text	1..1	string	“Known treatment directives”
-- -- valueString	1..1	string	“/Consent?category=http://snomed.info/sct|11291000146105”
-- advanceDirective	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“11341000146107”
-- -- -- -- display	0..1	string	“Living will and advance directive record”
-- -- 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	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“47420-5”
-- -- -- -- display	0..1	string	“Functional status assessment note”
-- -- 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”
-- problems	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”

-- -- -- -- code	1..1	code	“11450-4”
-- -- -- -- display	0..1	string	“Problem list”
-- -- text	1..1	string	“All known problems”
-- -- valueString	1..1	string	“/Condition”
-- livingSituation	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	“365508006”
-- -- -- -- display	0..1	string	“Finding of residence and accommodation circumstances”
-- -- text	1..1	string	“Current living situation”
-- -- valueString	1..1	string	“/Observation/$lastn?code=http://snomed.info/sct|365508006”
-- drugUse	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	“228366006”
-- -- -- -- display	0..1	string	“Finding relating to drug misuse behavior”
-- -- 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	
-- -- -- SNOMED	1..1	Slice	
-- -- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- -- code	1..1	code	“228273003”
-- -- -- -- display	0..1	string	“Finding relating to alcohol drinking behavior”
-- -- 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	
-- -- -- SNOMED	1..1	Slice	
-- -- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- -- code	1..1	code	“365980008”
-- -- -- -- display	0..1	string	“Finding of tobacco use and exposure”
-- -- 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	
-- -- -- SNOMED	1..1	Slice	
-- -- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- -- code	1..1	code	“11816003”
-- -- -- -- display	0..1	string	“Diet education”
-- -- text	1..1	string	“All known dietary recommendations”
-- -- valueString	1..1	string	“/NutritionOrder”
-- alert	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“75310-3”
-- -- -- -- display	0..1	string	“Health concerns”
-- -- text	1..1	string	“All known alerts”
-- -- valueString	1..1	string	“/Flag”
-- allergyIntolerance	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	

-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“48765-2”
-- -- -- -- display	0..1	string	“Allergies and adverse reactions”
-- -- 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	
-- -- -- SNOMED	1..1	Slice	
-- -- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- -- code	1..1	code	“16076005”
-- -- -- -- display	0..1	string	“Prescription”
-- -- 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	
-- -- -- SNOMED	1..1	Slice	
-- -- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- -- code	1..1	code	“422037009”
-- -- -- -- display	0..1	string	“Provider medication administration instructions”
-- -- 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	
-- -- -- SNOMED	1..1	Slice	
-- -- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- -- code	1..1	code	“422979000”
-- -- -- -- display	0..1	string	“Medication regimen behavior finding”
-- -- 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	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“46264-8”
-- -- -- -- display	0..1	string	“History of medical device use”
-- -- 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	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“11369-6”
-- -- -- -- display	0..1	string	“Immunization”
-- -- text	1..1	string	“Known vaccinations”
-- -- valueString	1..1	string	“/Immunization?status=completed”
-- bloodPressure	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	

-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“85354-9”
-- -- -- -- display	0..1	string	“Blood pressure panel”
-- -- text	1..1	string	“Last known blood pressure”
-- -- valueString	1..1	string	“/Observation/$lastn? code=http://loinc.org|85354-9”
-- bodyWeight	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“29463-7”
-- -- -- -- display	0..1	string	“Body weight”
-- -- text	1..1	string	“Last known body weight”
-- -- valueString	1..1	string	“/Observation/$lastn? code=http://loinc.org|29463-7”
-- bodyHeight	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“8302-2”
-- -- -- -- display	0..1	string	“Body height”
-- -- text	1..1	string	“Last known body height”
-- -- valueString	1..1	string	“/Observation/$lastn? code=http://loinc.org|8302- 2,http://loinc.org|8306- 3,http://loinc.org|8308-9”
-- results	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	“15220000”

-- -- -- -- display	0..1	string	“Laboratory test”
-- -- text	1..1	string	“Last known laboratory results per type”
-- -- 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	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“47519-4”
-- -- -- -- display	0..1	string	“History of procedures”
-- -- 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	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“46240-8”
-- -- -- -- display	0..1	string	“Hospitalizations+Outpatient visits”
-- -- 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”
-- plannedCare	0..4	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“18776-5”

-- -- -- -- display	0..1	string	“Plan of care note”
-- -- text	1..1	string	“Known planned care activities”
-- -- valueString	1..1	string	“/ProcedureRequest?status=active” or “/ImmunizationRecommendation” or “/DeviceRequest?status=active&_include=DeviceRequest:device” or “status=booked,pending,proposed”

As described in the section Notified Pull interaction every reference can be coded specific to the part. The codes of all HCIMs are in the table below.

HCIM	Code	System
Patient	79191-3	http://loinc.org
MaritalStatus ContactPerson HealthProfessional		
Payer	48768-6	http://loinc.org
TreatmentDirective	1129100014610 5	http://snomed.info/sct
AdvanceDirective	1134100014610 7	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
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

Z1.4.3 | 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.nl/fhir/NamingSystem/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://example.com/fhir/NamingSystem/dummy",
       "value": "sending-organization-id"
```

```
      }
    }
  },
  "owner": {
    "identifier": {
      "system": "http://example.com/fhir/NamingSystem/dummy",
      "value": "receiving-organization-id"
    }
  },
  "input": [
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.nl/fhir/NamingSystem/TaskParameter",
            "code": "authorization-base"
          }
        ]
      },
      "valueString": "ZGFhNDFjY2MtZGFmMi00YjZkLThiNDYtN2JlZDk1MWEyYzk2"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.nl/fhir/NamingSystem/TaskParameter",
            "code": "read-resource",
            "display": "Laboratory test"
          }
        ]
      },
      "valueReference": {
        "reference": "Observation/123456"
      }
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "77599-9",
            "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"
}
```

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.nl/fhir/NamingSystem/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://example.com/fhir/NamingSystem/dummy",
       "value": "sending-organization-id"
     }
   }
 },
 "owner": {
   "identifier": {
     "system": "http://example.com/fhir/NamingSystem/dummy",
     "value": "receiving-organization-id"
   }
 },
```

```
"input": [
  {
    "type": {
      "coding": [
        {
          "system": "http://fhir.nl/fhir/NamingSystem/TaskCode",
          "code": "authorization-base"
        }
      ]
    },
    "value": "ZGFhNDFjY2MtZGFmMi00YjZkLThiNDYtN2JlZDk1MWEyYzk2"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://loinc.org",
          "code": "79191-3",
          "display": "Patient demographics panel"
        }
      ]
    },
    "valueString": "Patient?_include=Patient:general-practitioner"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://loinc.org",
          "code": "48768-6",
          "display": "Payment sources Document"
        }
      ]
    },
    "valueString": "Coverage?_include=Coverage:payor:Organization&_include=Coverage:payor:Patient"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://snomed.info/sct",
          "code": "11291000146105",
          "display": "Treatment instructions"
        }
      ]
    },
    "valueString": "Consent?category=http://snomed.info/sct|11291000146105"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://snomed.info/sct",
          "code": "11341000146107",
          "display": "Living will and advance directive record"
        }
      ]
    },
```

```
    "valueString": "Consent?category=http://snomed.info/sct|11341000146107"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://loinc.org",
          "code": "47420-5",
          "display": "Functional status assessment note"
        }
      ]
    },
    "valueString": "Observation/$lastn?category=http://snomed.info/sct|118228005, "
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://loinc.org",
          "code": "11450-4",
          "display": "Problem list - Reported"
        }
      ]
    },
    "valueString": "Condition"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://snomed.info/sct",
          "code": "365508006",
          "display": "Residence and accommodation circumstances - finding"
        }
      ]
    },
    "valueString": "Observation/$lastn?code=http://snomed.info/sct|365508006"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://snomed.info/sct",
          "code": "228366006",
          "display": "Finding relating to drug misuse behavior"
        }
      ]
    },
    "valueString": "Observation?code=http://snomed.info/sct|228366006"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://snomed.info/sct",
          "code": "228273003",
          "display": "Finding relating to alcohol drinking behavior"
        }
```

```
        ]
      },
      "valueString": "Observation?code=http://snomed.info/sct|228273003"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://snomed.info/sct",
            "code": "365980008",
            "display": "Tobacco use and exposure - finding"
          }
        ]
      },
      "valueString": "Observation?code=http://snomed.info/sct|365980008"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://snomed.info/sct",
            "code": "11816003",
            "display": "Diet education"
          }
        ]
      },
      "valueString": "NutritionOrder"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "75310-3",
            "display": "Health concerns Document"
          }
        ]
      },
      "valueString": "Flag"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "48765-2",
            "display": "Allergies and adverse reactions Document"
          }
        ]
      },
      "valueString": "AllergyIntolerance"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://snomed.info/sct",
            "code": "422979000",
```

```
          "display": "Known medication use"
        }
      ]
    },
    "valueString": "MedicationStatement?category=urn:oid:2.16.840.1.113883.2.4.3.11.60.20.77.5.3|6&_include=Me
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://snomed.info/sct",
          "code": "16076005",
          "display": "Known medication agreements"
        }
      ]
    },
    "valueString": "MedicationRequest?category=http://snomed.info/sct|16076005&_include=MedicationRequest:medi
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://snomed.info/sct",
          "code": "422037009",
          "display": "Known administration agreements"
        }
      ]
    },
    "valueString": "MedicationDispense?category=http://snomed.info/sct|422037009&_include=MedicationDispense:m
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://loinc.org",
          "code": "46264-8",
          "display": "Known medical aids"
        }
      ]
    },
    "valueString": "DeviceUseStatement?_include=DeviceUseStatement:device"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://loinc.org",
          "code": "11369-6",
          "display": "History of Immunization Narrative"
        }
      ]
    },
    "valueString": "Immunization?status=completed"
  },
  {
    "type": {
      "coding": [
        {
```

```
          "system": "http://loinc.org",
          "code": "85354-9",
          "display": "Blood pressure"
        }
      ]
    },
    "valueString": "Observation/$lastn?code=http://loinc.org|85354-9"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://loinc.org",
          "code": "29463-7",
          "display": "Body weight"
        }
      ]
    },
    "valueString": "Observation/$lastn?code=http://loinc.org|29463-7"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://loinc.org",
          "code": "8302-2",
          "display": "Body height"
        }
      ]
    },
    "valueString": "Observation/$lastn?code=http://loinc.org|8302-2,http://loinc.org|8306-3,http://loinc.org|8
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://snomed.info/sct",
          "code": "15220000",
          "display": "Laboratory test"
        }
      ]
    },
    "valueString": "Observation/$lastn?category=http://snomed.info/sct|275711006&_include=Observation:related-
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://loinc.org",
          "code": "47519-4",
          "display": "History of Procedures"
        }
      ]
    },
    "valueString": "Procedure?category=http://snomed.info/sct|387713003"
  },
  {
    "type": {
```

```
      "coding": [
        {
          "system": "http://loinc.org",
          "code": "46240-8",
          "display": "History of Hospitalizations+Outpatient visits Narrative"
        }
      ]
    },
    "valueString": "Encounter?class=http://hl7.org/fhir/v3/ActCode|IMP,http://hl7.org/fhir/v3/ActCode|ACUTE,ht
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://loinc.org",
          "code": "18776-5",
          "display": "Plan of care note"
        }
      ]
    },
    "valueString": "ProcedureRequest?status=active"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://loinc.org",
          "code": "18776-5",
          "display": "Plan of care note"
        }
      ]
    },
    "valueString": "ImmunizationRecommendation"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://loinc.org",
          "code": "18776-5",
          "display": "Plan of care note"
        }
      ]
    },
    "valueString": "DeviceRequest?status=active&_include=DeviceRequest:device"
  },
  {
    "type": {
      "coding": [
        {
          "system": "http://loinc.org",
          "code": "18776-5",
          "display": "Plan of care note"
        }
      ]
    },
    "valueString": "Appointment?status=booked,pending,proposed"
  },
```

```
   {
     "type": {
       "coding": [
         {
           "system": "http://loinc.org",
           "code": "77599-9",
           "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 opgesteld. Aan de hand van deze autorisatierichtlijn wordt bepaald welke type zorgverleners de BgZ kunnen verzenden en opvragen en welke niet. 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 patiënten wordt verwezen of overgedragen. Hiervoor geldt dezelfde autorisatie.

Deze autorisatie-afspraken gaan over de samenwerking tussen zorgprofessionals werkzaam voor:

- Ziekenhuizen
- Universitair medische centra
- Zelfstandige klinieken

Voor een BgZ-uitwisseling via Twiin zien we geen reden om af te wijken van de autorisatierichtlijn die de betrokken zorgkoepels hebben afgesproken. Twiin ondersteunt daarom hetgeen wat in deze autorisatierichtlijn is afgesproken. Dit betekent concreet dat de alleen de volgende rollen de BgZ mogen versturen en/of raadplegen:

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
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
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: 10.2.5 | TTA FHIR - Authentication & Authorization
- Bij Notified pull: Wanneer het verzenden wordt gedaan via het notified pull communicatiepatroon dient de gebruiker die de notificatie verstuurd 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 rol geautoriseerd te worden.

Z1.5 | BgZ: PvE

1. Validatie eisen

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie
BgZ-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. Autorisatiematrix: Z1.4.4 | BgZ: Autorisatie | autorisatiematrix BgZ Transacties: 10.3.4 | Twiin-04 | Search Resource(s) , 10.3.5 | Twiin-05 | Retrieve Resource Autorisatierichtlijn: Autorisatierichtlijn Basisgegevensset Zorg (BgZ) | AORTA-LSP
BgZ-2a-TANP-01	TA NP	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. Z1.2.1 | TTA Exchanging BgZ - FHIR Notified Pull
BgZ-2a-TANP-02	TA NP	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. Z1.2.1 | TTA Exchanging BgZ - FHIR Notified Pull
BgZ-2a-TANP-03	TA NP	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. Z1.2.1 | TTA Exchanging BgZ - FHIR Notified Pull
BgZ-2a-TANP-04	TA NP	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 (10.3.14.1 | ZORG-AB Transacties) 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. Z1.2.1 | TTA Exchanging BgZ - FHIR Notified Pull
BgZ-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 (10.3.14.1 | ZORG-AB Transacties) 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. Z1.2.1 | TTA Exchanging BgZ - FHIR Notified Pull
BgZ-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 Z1.2.1.2 | BgZ: Authentication & Authorization
BgZ-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 Z1.2.1.2 | BgZ: Authentication & Authorization
BgZ-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: 10.2.5 | TTA FHIR - Authentication & Authorization | Client authentication
BgZ-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 Z1.2.1.2 | BgZ: Authentication & Authorization
BgZ-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 Z1.2.1.2 | BgZ: Authentication & Authorization
BgZ-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 Z1.2.1.2 | BgZ: Authentication & Authorization | Authorization base
BgZ-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: 10.2.5 | TTA FHIR - Authentication & Authorization | Authorization grant
BgZ-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: Z1.2.1.2 | BgZ: Authentication & Authorization | Access token request
BgZ-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: Z1.2.1.2 | BgZ: Authentication & Authorization | Client authentication , Z1.2.1.2 | BgZ: Authentication & Authorization | Access token request
BgZ-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: Z1.2.1.2 | BgZ: Authentication & Authorization | Access token request
BgZ-2a-AA-11	BgZ Authn en Authz	GtK verzender	GtK verzender borgt dat de autorisatierichtlijn BgZ is toepast. 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	Access Policy: GtK verzender moet borgen dat alleen gebruikers met de in de autorisatiematrix opgesomde rollen BgZ notificaties mogen versturen: Z1.4.4 | BgZ: Autorisatie | autorisatiematrix BgZ

			vertrouwen op de interne autorisatieregels bij de GtK ontvanger (indien deze een valide authorization base heeft, zie ook BgZ-1-authz-03)	
BgZ-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: 10.2.5 | TTA FHIR - Authentication & Authorization | Client authentication
BgZ-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: Z1.2.1.2 | BgZ: Authentication & Authorization | Access token request
BgZ-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: Z1.2.1.2 | BgZ: Authentication & Authorization | Access token request
BgZ-2a-AA-15	BgZ Authn en Authz	GtK verzender	GtK verzender heeft het afgesproken access policy geïmplementeerd op het resource server endpoint.	Access Policy: GtK verzender mag alleen data opleveren aan gebruikers met de in de autorisatiematrix opgesomde rollen: Z1.4.4 | BgZ: Autorisatie | autorisatiematrix BgZ
BgZ-2a-NS-01	network security	GtK verzender, GtK ontvanger	GtK verzender en GtK ontvanger maken gebruik van mutual TLS (mTLS) versie 1.3.	Zie 10.2.10 | Netwerk level security mTLS 1.3
BgZ-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 10.2.10 | Netwerk level security mTLS 1.3
BgZ-2a-NS-03	network security	GtK verzender, GtK	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 ICT-beveiligingsrichtlijnen voor Transport Layer Security v2.1 (TLS)

		ontvanger		
BgZ-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 10.2.10 | Netwerk level security mTLS 1.3
BgZ-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, artikel 4.5.2 CRL's: Certificate Revocation Lists (CRL's) | Zorg CSP
BgZ-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
BgZ-2b-trans-01	Transactions - BgZ interactions	GtK verzender	GtK verzender is in staat een Workflow-Task aan te maken	Transactie 1 van Z1.2.1.1 | BgZ - data interactions
BgZ-2b-trans-02	Transactions - BgZ interactions	GtK verzender	GtK verzender is in staat een notificatie-create-request te versturen	Transactie 2 van Z1.2.1.1 | BgZ - data interactions Specificatie: 10.3.1 | Twiin-01 | Send Notification Task | Request message
BgZ-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 Z1.2.1.1 | BgZ - data interactions Specificatie: 10.3.1 | Twiin-01 | Send Notification Task | Response message
BgZ-2b-trans-04	Transactions - BgZ inter	GtK verzender	GtK verzender is in staat een notificatie-create-request te versturen wanneer de dataset van de verwijzing is geüpdatet	Transactie 4 van Z1.2.1.1 | BgZ - data interactions Specificatie: 10.3.1 | Twiin-01 | Send Notification Task | Request message

	actions			
BgZ-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 Z1.2.1.1 | BgZ - data interactions Specificatie: 10.3.1 | Twiin-01 | Send Notification Task | Response message
BgZ-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 Z1.2.1.1 | BgZ - data interactions Specificatie: 10.3.2 | Twiin-02 | Cancel Notification Task | Request message
BgZ-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 Z1.2.1.1 | BgZ - data interactions Specificatie: 10.3.2 | Twiin-02 | Cancel Notification Task | Notification response
BgZ-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 Z1.2.1.1 | BgZ - data interactions Specificatie: 10.3.5 | Twiin-05 | Retrieve Resource De read-operaties zijn opgenomen in de notificatie-task onder Task.input:read-available-resources.
BgZ-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 Z1.2.1.1 | BgZ - data interactions Specificatie: 10.3.5 | Twiin-05 | Retrieve Resource
BgZ-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 Z1.2.1.1 | BgZ - data interactions Specificatie: 10.3.4 | Twiin-04 | Search Resource(s) De search-operaties zijn opgenomen in de notificatie-task onder Task.input:query-available-resources.
BgZ-2b-trans-	Transactions - BgZ	GtK verzender	GtK verzender is in staat binnenkomende search-requests af te handelen en een passende response te versturen.	Transactie 9 van Z1.2.1.1 | BgZ - data interactions Specificatie: 10.3.4 | Twiin-04 | Search Resource(s)

09.search	interactions			
BgZ-2b-trans-10	Transactions - BgZ 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 Z1.2.1.1 | BgZ - data interactions Specificatie: 10.3.3 | Twiin-03 | Get workflow Task 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	Transactions - BgZ 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 Z1.2.1.1 | BgZ - data interactions
BgZ-2b-trans-12.read	Transactions - BgZ 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 Z1.2.1.1 | BgZ - data interactions Specificatie: 10.3.5 | Twiin-05 | Retrieve Resource De read-operaties zijn opgenomen in de workflow-task onder `Task.input:read-available-resources`.
BgZ-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 Z1.2.1.1 | BgZ - data interactions Specificatie: 10.3.5 | Twiin-05 | Retrieve Resource
BgZ-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 Z1.2.1.1 | BgZ - data interactions Specificatie: 10.3.4 | Twiin-04 | Search Resource(s) De search-operaties zijn opgenomen in de workflow-task onder `Task.input:query-available-resources`.
BgZ-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 Z1.2.1.1 | BgZ - data interactions Specificatie: 10.3.4 | Twiin-04 | Search Resource(s)

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
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
BgZ-3-3	content	GtK verzender	GtK verzender dient een Notificatie-task aan te maken die voldoet aan het afgesproken profiel.	Profiel: 10.3.1 | Twiin-01 | Send Notification Task | Request message Referentiecodes: Z1.4.1 | BgZ: FHIR Task reference codes
BgZ-3-4	content	GtK ontvanger	GtK ontvanger dient een Notificatie-task die voldoet aan het afgesproken profiel te kunnen interpreteren.	Profiel: 10.3.1 | Twiin-01 | Send Notification Task | Request message Referentiecodes: Z1.4.1 | BgZ: FHIR Task reference codes
BgZ-3-5	content	GtK verzender	GtK verzender dient FHIR-resources conform de implementation guide van de informatiestandaard BgZ beschikbaar te kunnen stellen.	Profielen: BgZ medisch-specialistische zorg Technical Implementation Guide 1.0 - informatiestandaarden
BgZ-3-6	content	GtK ontvanger	GtK ontvanger dient FHIR-resources conform de implementation guide van de informatiestandaard BgZ te kunnen interpreteren.	Profielen: BgZ medisch-specialistische zorg Technical Implementation Guide 1.0 - informatiestandaarden
BgZ-3-7	content	GtK verzender	GtK verzender dient correspondentie/ niet-discrete data conform Z3 | COR: implementatiewijzer Correspondentie 1.2.0 Trial beschikbaar te kunnen stellen.	
BgZ-3-8	content	GtK ontvanger	GtK ontvanger dient correspondentie/ niet-discrete data conform Z3 | COR: implementatiewijzer Correspondentie 1.2.0 Trial te kunnen interpreteren.	
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 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	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.

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

BgZ-1-FO-03	FO Nictiz	GtK verzender	GtK verzender maakt informatie beschikbaar conform de BgZ specificatie op basis 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 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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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 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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
BgZ-1-FO-07	FO Nictiz	GtK verzender	GtK verzender moet een BgZ kunnen sturen bij verwijzing naar een andere zorginstelling of zorgverlener.	Specificatie: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
BgZ-1-FO-10	FO Nictiz	GtK antwoorder	GtK antwoorder moet de mogelijkheid bieden om op een opvraging een BgZ beschikbaar te stellen.	Specificatie: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden

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. Voor historische zibs worden de metagegevens zo goed mogelijk gevuld. Specificatie: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
BgZ-1-FO-13	FO Nictiz, metagegevens	GtK verzender	GtK verzender dient, wanneer een gegevenselement van elders betrokken is en er zijn metagegevens op zib-niveau 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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
BgZ-1-FO-14	FO Nictiz, metagegevens	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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
BgZ-1-FO-15	FO Nictiz, metagegevens	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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
BgZ-1-FO-16	FO Nictiz, metagegevens	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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
BgZ-1-FO-17	FO Nictiz, metagegevens	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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden

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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden

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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
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 VIPP5 assessments, bijlage II, paragraaf 1.5, alinea module 3 Zie https://www.vipp-programma.nl/over-vipp/doelstellingen
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 VIPP5 assessments, bijlage II, paragraaf 1.5, alinea module 3 Zie https://www.vipp-programma.nl/over-vipp/doelstellingen
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 VIPP5 assessments, bijlage II, paragraaf 1.5, alinea module 3 Zie https://www.vipp-programma.nl/over-vipp/doelstellingen

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 VIPP5 assessments, bijlage II, paragraaf 1.5, alinea module 3 Zie https://www.vipp-programma.nl/over-vipp/doelstellingen
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.

Z2 | BB: Implementatiewijzer Beeldbeschikbaarheid 1.3.0 Trial

⚠ Zorgtoepassing Beeldbeschikbaarheid **versie 1.3.0 trial** onderdeel van Twiin Release 1.3

Deze zorgtoepassing is klaar voor beproeving. Meewerken aan deze beproeving?

Laat het ons weten door te e-mailen naar info@twiin.nl

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, Twiin Implementatiewijzer Zorgtoepassingen, Vertrouwensmodel, Voorwaarden,

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 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 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 1 - 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 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

10.1.2 | Communicatiepatroon : Indexed Pull

10.1.3 | Communicatiepatroon : Push

Pakket van Eisen - BB Vol. 1 ARCHIVED

✅ 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, in- 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

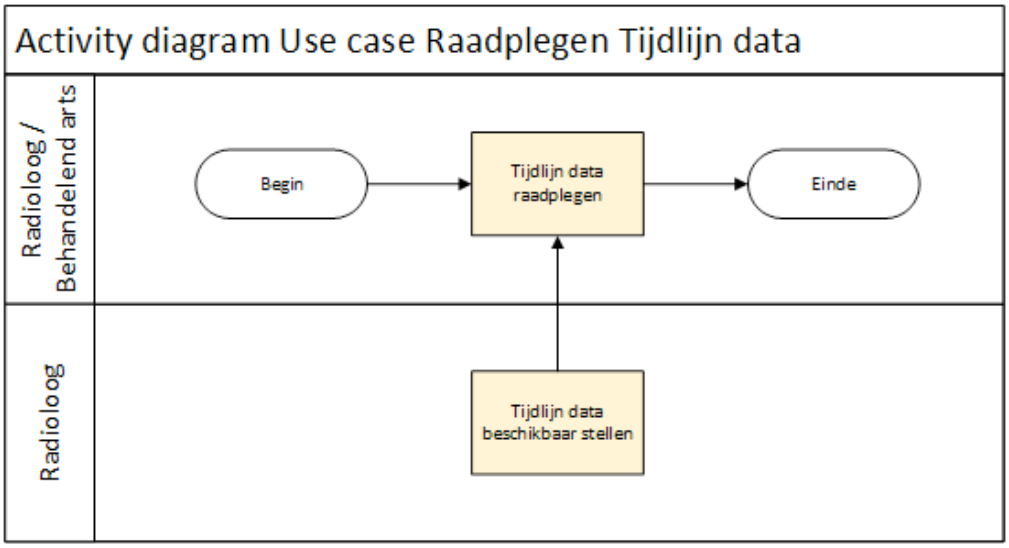
- De radioloog / behandelend arts raadpleegt de "tijdlijn radiologische onderzoeken"

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

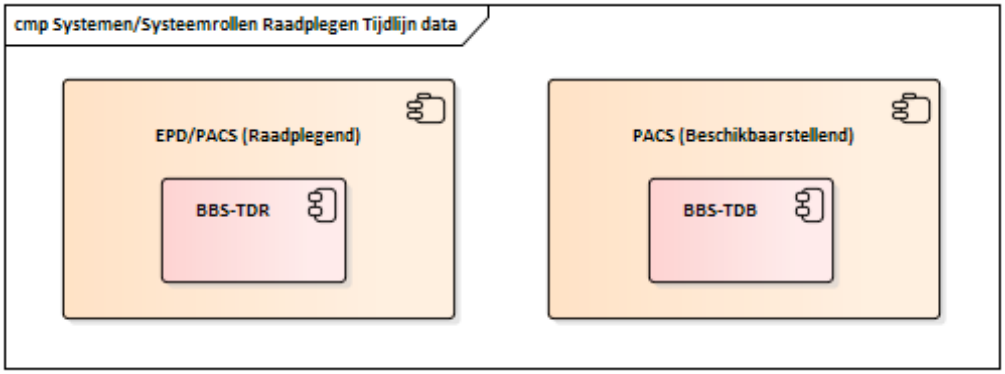
Systemen & Systeemrollen

Systemen:

- PACS/EPD van de raadplegende organisatie
- PACS van de beschikbaarstellende, producerende organisatie

Systeemrollen:

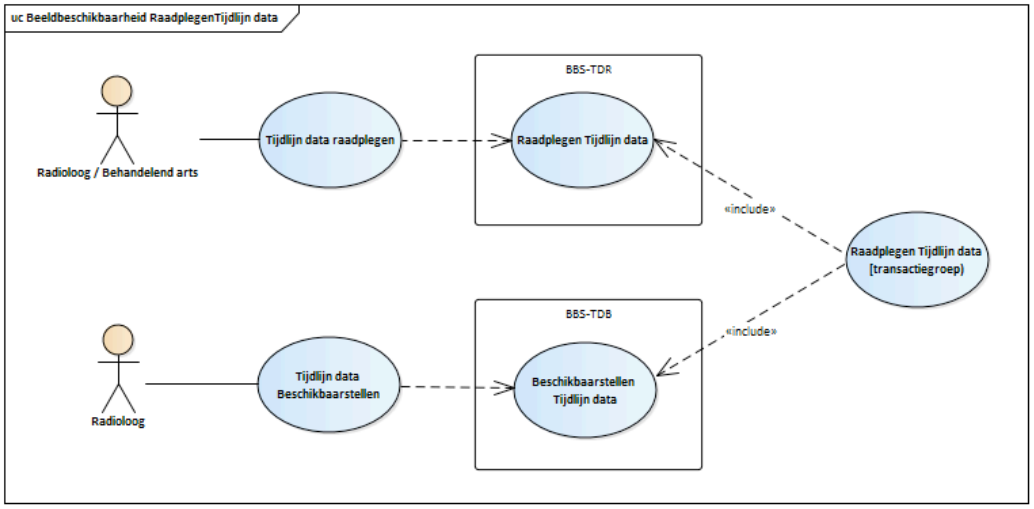
- Raadplegend Systeem EPD / PACS
  - TijdlijnDataRaadplegendSysteem (BBS-TDR)
- Beschikbaarstellend systeem PACS (producerende organisatie)
  - TijdlijnDataBeschikbaarstellendSysteem (BBS-TDB)



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
	Beschikbaarstellen tijdlijn data	BBS-TDB	PACS	Radioloog	V1.0.0-alpha.2

✅ 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 volledieger 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 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

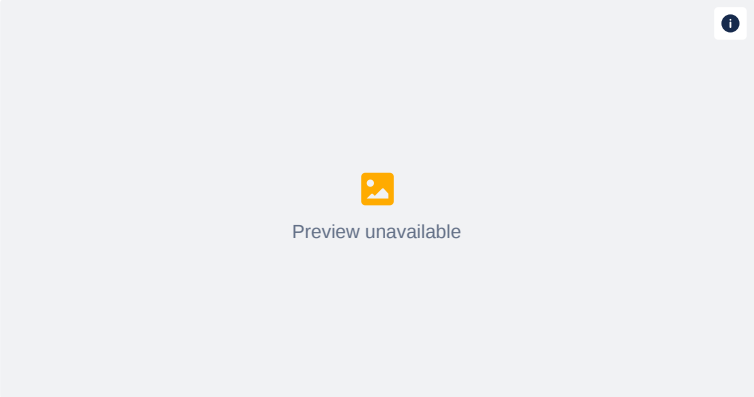
- De radioloog / behandelend arts raadpleegt het verslag via de tijdlijn radiologische onderzoeken.

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

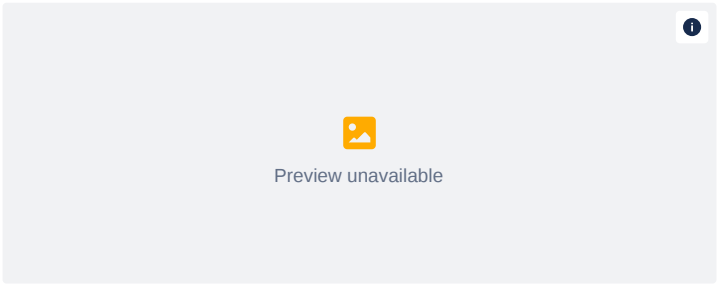
Systemen & Systeemrollen

Systemen:

- PACS/EPD van de raadplegende organisatie
- PACS van de beschikbaarstellende, producerende organisatie

Systeemrollen:

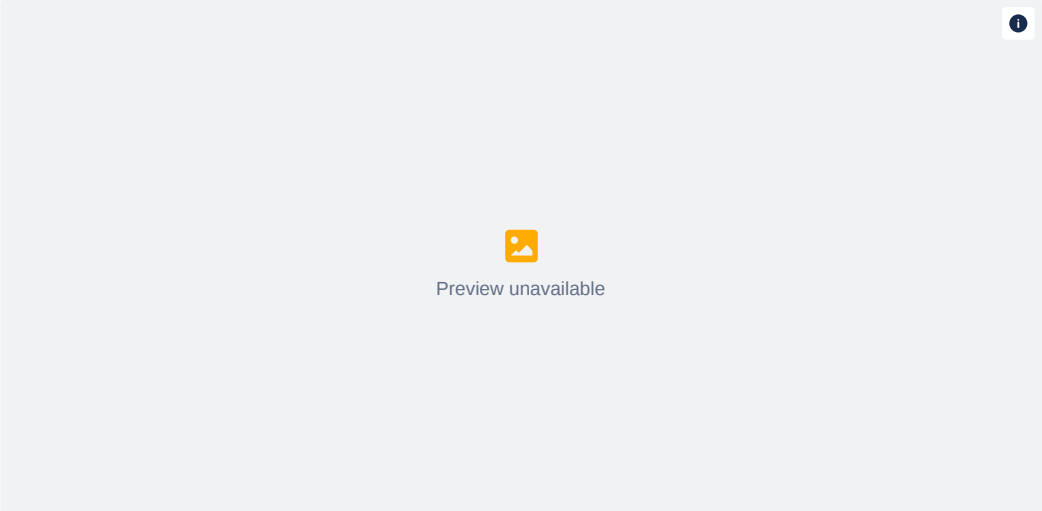
- Raadplegend Systeem EPD / PACS
  - VerslagRaadplegendSysteem (BBS-VR)
- Beschikbaarstellend systeem PACS (producerende organisatie)
  - VerslagBeschikbaarstellendSysteem (BBS-VB)



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
	Beschikbaarstellen verslagen	BBS-VB	PACS	Radioloog	V1.0.0-alpha.2

✅ 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 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.

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

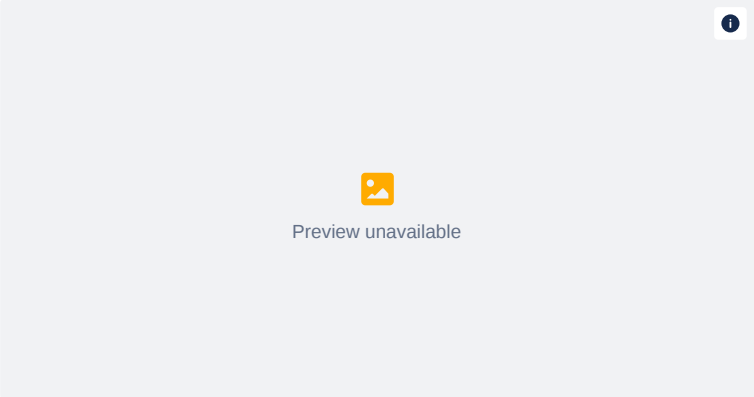
- De radioloog / behandelend arts raadpleegt de beelden via de tijdlijn radiologische onderzoeken.

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

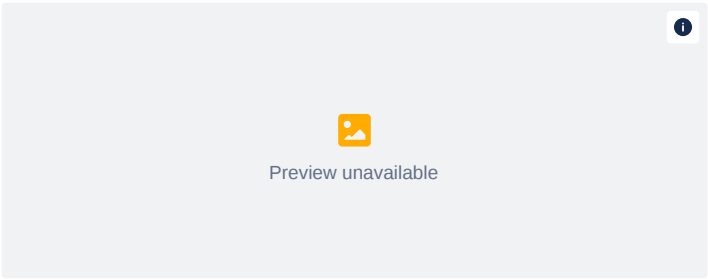
Systemen & Systeemrollen

Systemen:

- PACS/EPD van de raadplegende organisatie
- PACS van de beschikbaarstellende, producerende organisatie

Systeemrollen:

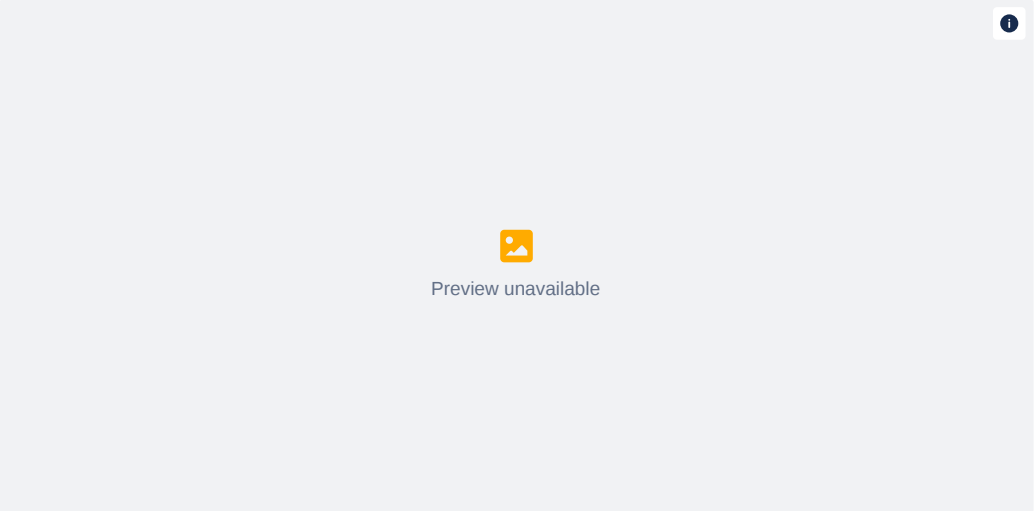
- Raadplegend Systeem EPD / PACS
  - BeeldRaadplegendSysteem (BBS-BR)
- Beschikbaarstellend systeem PACS (producerende organisatie)
  - BeeldBeschikbaarstellendSysteem (BBS-BB)



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
	Beschikbaarstellen beelden	BBS-BB	PACS	Radioloog	V1.0.0-alpha.2

Z2.2 | BB Volume 2a - 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 1 - Functioneel overzicht, 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

- Z2.1.5 | BB: Sturen verslag ARCHIVED
- Z2.1.4 | BB: Sturen beeld ARCHIVED

Pull

The following Functional Usecases are covered by Z2.2.1 | BB: Indexed Pull

- ✅ Z2.1.1 | BB: Raadplegen Tijdlijn Data
- ✅ Z2.1.2 | BB: Raadplegen Verslag
- https://vzvz.atlassian.net/wiki/pages/createpage.action?spaceKey=Twiin&title=Z2.1.1%20%7C%20BB%3A%20Raadplegen%20beelden

Z2.2.1 | BB: Indexed Pull

Original page can be found at 10.2.1 | TTA SOAP - Indexed Pull

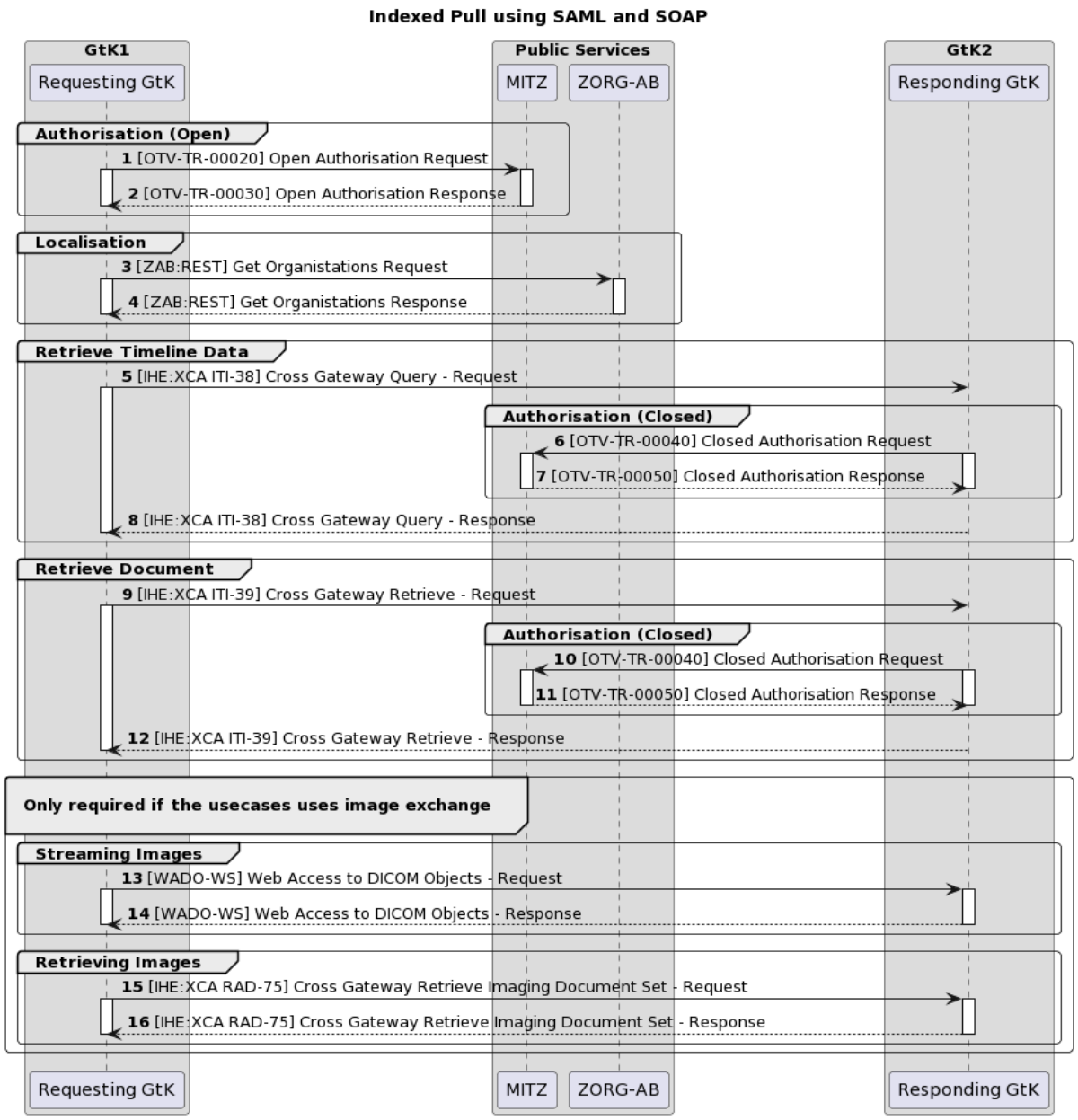
This Twiin Technical Agreement (TTA) describes and specifies technical responsibilities to which parties agree when connecting to exchange transactions to facilitate the Indexed Pull.

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



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.

10.4.5 | IHE ITI-40 | Provide X-User Assertion

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'

		10.3.14.2 | Mitz Transacties - 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 10.3.14.2 | Mitz Transacties - 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 10.3.14.1 | ZORG-AB Transacties
	4	ZORG-AB replies to this request with the endpoints 10.3.14.1 | ZORG-AB Transacties
Retrieve Timeline data	5	Using the endpoints the GtK uses this information to send the query. With this transaction a SAML token is included 10.4.2 | IHE ITI-38 | Cross Gateway Query 10.4.2.1 | ITI-38 examples | ITI 38 request
	6	The responding GtK then checks if the patients permission is in check at MITZ 10.3.14.2 | Mitz Transacties - OTV-TR-00040
	7	A response is sent back 10.3.14.2 | Mitz Transacties - 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. 10.4.2 | IHE ITI-38 | Cross Gateway Query 10.4.2.1 | 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. 10.4.3 | IHE ITI-39 | Cross Gateway Retrieve 10.4.3.1 | ITI-39 examples | ITI 39 request
	10	(see step 6) 10.3.14.2 | Mitz Transacties - OTV-TR-00040
	11	(see step 7) 10.3.14.2 | Mitz Transacties - 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 10.4.3 | IHE ITI-39 | Cross Gateway Retrieve

		10.4.3.1 | 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. 10.3.6 | Twiin-06 | WADO-WS
	14	The images are sent back in the requested format 10.3.6 | Twiin-06 | WADO-WS
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. 10.4.6 | IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set 10.4.6.1 | RAD-75 examples | RAD 75 request
	16	The images are sent back 10.4.6 | IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set 10.4.6.1 | RAD-75 examples | RAD 75 response

10.2 | Kern Volume 2a - Twiin Technical Agreements

10.2.3.1 Notified Pull - Data interactions

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.twiin.nl/project-dvdexit

In a future release (not version 1.2) it is intended to create an open architecture.

Z2.3 | BB: Volume 2b - 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	IHE ITI-38 | Cross Gateway Query IHE ITI-39 | Cross Gateway Retrieve IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set

Tussen de GtK's is het van belang dat er gebruik gemaakt wordt van een SAML token. Binnen het kern document is deze transactie verder uitgewerkt:

IHE ITI-40 | Provide X-User Assertion

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

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 uitwisselconcepten:

Geïndexeerde bevraging	[IHE:XDS ITI-18] Opvraag metadata bij een GtK-applicatie [IHE:XDS ITI-43] Opvraag gegevens bij een andere GtK-applicatie [IHE:XDS RAD-69] Opvraag beelden bij via een GtK-applicatie
Push - Versturen	[IHE:XDS ITI-41] Aanmelden documenten [IHE:XDS ITI-42] Registreren metadata [IHE:XDS RAD-68] Aanmelden Beelden

NB. ten opzichte van de transacties die in de kern zijn beschreven, zijn er voor beeldbeschikbaarheid geen aanvullingen

{}

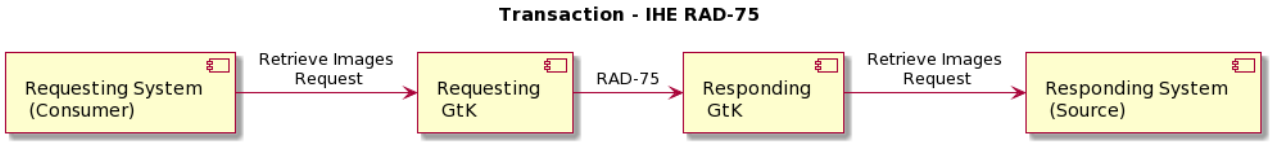
✅ Z2.3.1 | BB: IHE RAD-75 | Cross Gateway Retrieve Imaging Document Set

This section is the same as the generic 10.4.6 | 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 ' 10.4.2 | IHE ITI-38 | Cross Gateway Query 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



Referenced standards

Implementers of this transaction shall comply with all requirements described in Web Services for IHE Transactions.

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.
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

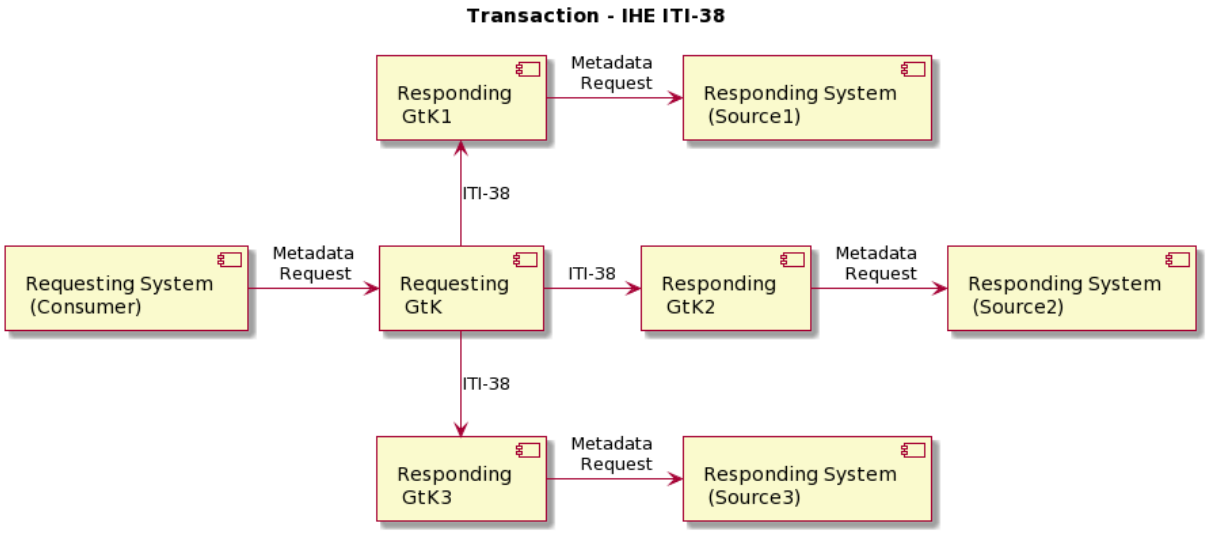
This section is the same as the generic 10.4.2 | IHE ITI-38 | Cross Gateway Query

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 at: 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.

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: IHE ITI TF Vol2

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.”

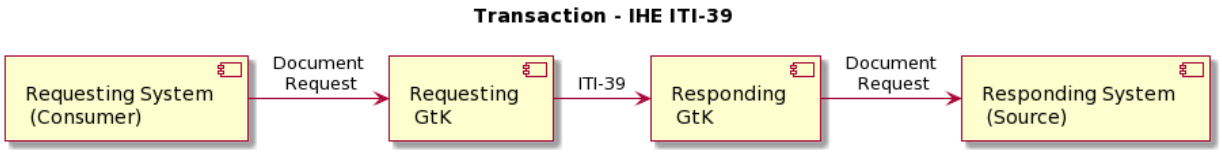
✅ Z2.3.3 | BB: IHE ITI-39 | Cross Gateway Retrieve

This section is the same as the generic 10.4.3 | 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



Referenced standards

Implementers of this transaction shall comply with all requirements described in Web Services for IHE Transactions.

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: IHE ITI TF Vol2

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."

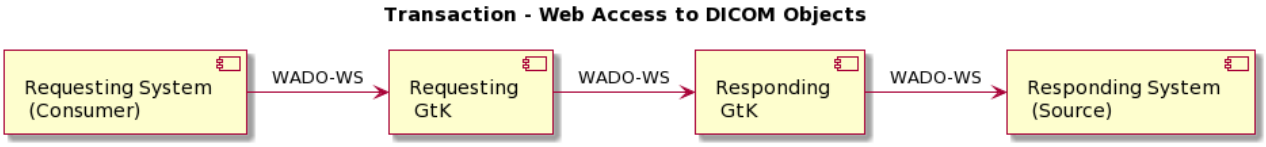
BB: WADO-WS

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.xmlsoa
<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:2
<xsd:import namespace="urn:ihe:rad:xdsi-b:2009" />
</xsd:schema> </types>
<message name="RetrieveImagingDocumentSetRequest_Message"> <documentation>Retrieve Imaging Document Set</documen
<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:RetrieveImagingDocumentS
wsaw:Action="urn:ihe:rad:2009:RetrieveImagingDocumentSet" /> <output message="tns:RetrieveDocumentSetResponse_Me
wsaw:Action="urn:ihe:iti:2007:RetrieveDocumentSetResponse" /> </operation>
<operation name="ImagingDocumentSource_RetrieveRenderedImagingDocumentSet"> <input message="tns:RetrieveRendered
wsaw:Action="urn:dicom:wado:ws:2011:RetrieveRenderedImagingDocumentSet" /> <output message="tns:RetrieveRendered
wsaw:Action="urn:dicom:wado:ws:2011:RetrieveRenderedImagingDocumentSetResponse" /> </operation>
<operation name="ImagingDocumentSource_DeprecatedRetrieveRenderedImagingDocumentSet"> <input message="tns:Deprec
wsaw:Action="urn:dicom:ws:wado:2011:RetrieveRenderedImagingDocumentSet" /> <output message="tns:RetrieveDocument
wsaw:Action="urn:ihe:iti:2007:RetrieveDocumentSetResponse" /> </operation>
</portType>
```

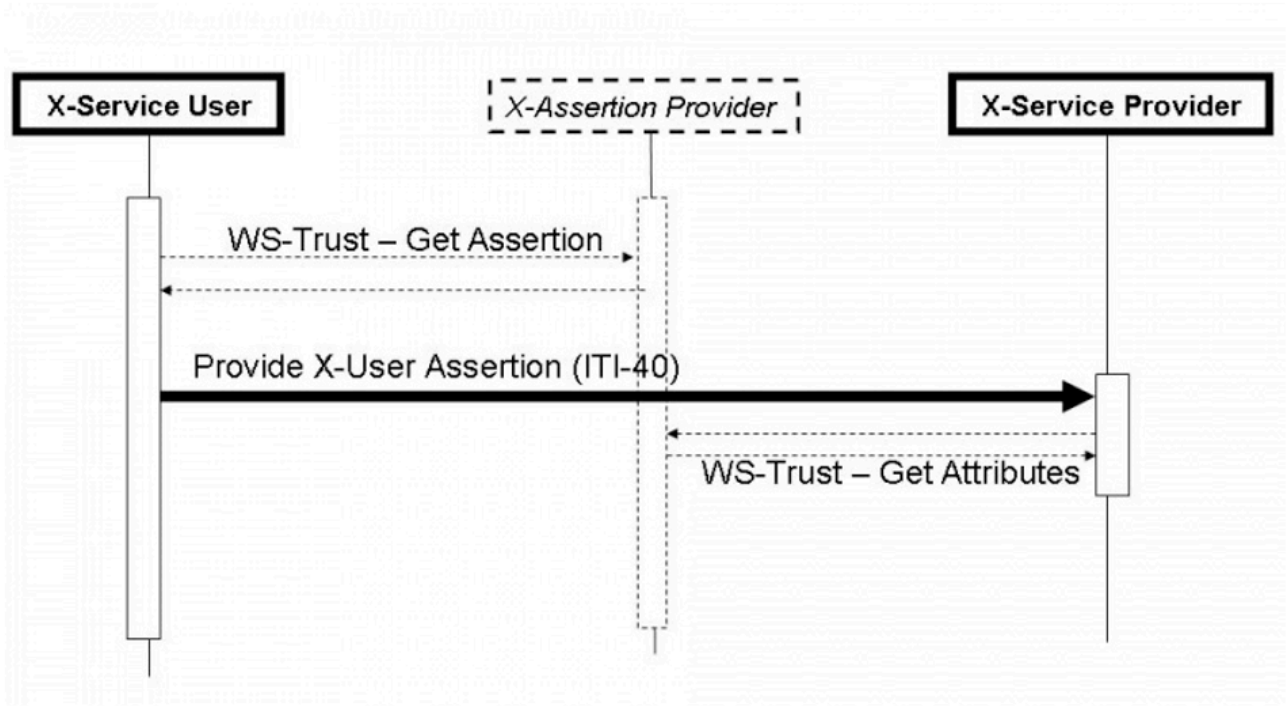
```
<binding name="ImagingDocumentSource_Binding" type="tns:ImagingDocumentSource_PortType">
<soap12:binding style="document" transport="http://schemas.xmlsoap.org/soap/http" /> <wsaw:UsingAddressing wsdl:
<operation name="ImagingDocumentSource_RetrieveImagingDocumentSet">
<soap12:operation soapActionRequired="false" /> <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 loca
</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 Default Community home - OASIS
- SAMLCore SAML V2.0 Core standard
- WSS10 OASIS Standard, "OASIS Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)", March 2004.
- WSS11 OASIS Standard, "OASIS Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)", February 2006.
- WSS:SAMLTokenProfile1.0 OASIS Standard, “Web Services Security: SAML Token Profile”, December 2004
- WSS:SAMLTokenProfile1.1 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 Profile
  - Enterprise User Authentication Profile
  - Basic Patient Privacy Consents Profile

- OASIS
  - SAML V2.0 Standards Default Community home - OASIS .
  - 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: IHE ITI TF Vol2

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**	

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

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 10.5.1 | Document/beeld gebaseerde Metadata 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 versla g
- 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 o nderzoek Radiologie (DICOM)

Metadata geïndexeerde bevraging

Disclaimer

Voor de vulling van metadata is gebruik gemaakt van de Nictiz Metadataset: XDS metadata - Nictiz

De Nictiz metadata set is document gebaseerd en niet 1 op 1 van toepassing op b.v. resource gebaseerde uitwisseling.

APPLICATIE-LAAG

Het uitwisselpatroon geïndexeerde bevraging 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
patientId	R	'123456789^^^&2.16.840.1.113883.2.4.6.3&ISO'	BSN van patiënt
referenceIdList	O	642356235^^^&1.2.3.4.5.6&ISO^urn:ihe:iti:	Koppeling met ander document of beeld

		xds:2013:accession	
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
healthcareFacility TypeCode	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
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

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.

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

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
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	Structuur van onderste gedeelte van romp
38266002	Gehele lichaam in totaliteit
53120007	Structuur van bovenste extremiteit
61685007	Structuur van onderste extremiteit
67734004	Structuur van bovenste deel van romp
774007	Structuur van hoofd-halsregio
113257007	Structuur van tractus circulatorius
80891009	Structuur van hart
76752008	Structuur van mamma
737561001	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
  Bron; http://dicom.nema.org/medical/dicom/current/output/html/part16.html#sect_CID_4
  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

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

Zoals wordt beschreven op pagina Eerste stap autorisatie binnen Twiin biedt Twiin voor de zorgtoepassing beeldbeschikbaarheid een aantal extra handvatten voor ziekenhuizen om aan hun verantwoordelijkheid als bron te kunnen voldoen, onder andere:

- Een door de koepels van zorgaanbieders en beroepsgroepen, betrokken bij radiologisch onderzoek, opgestelde concept autorisatierichtlijn beeldbeschikbaarheid radiologie.
- Een mappingtabel van de autorisaties op de bij XDS gebruikte rolcodes en de UZI-rolcodes.

Autorisatierichtlijn

Onderstaand is de autorisatierichtlijn, zoals opgesteld door de koepels van zorgaanbieders en de beroepsgroepen, betrokken bij radiologisch onderzoek weergegeven. Deze richtlijn is na uitgebreid overleg met betrokkenen tot stand gekomen. Deze richtlijn geeft richting naar de stip op de horizon. Op termijn zullen de koepels gevraagd worden de autorisatierichtlijn te autoriseren. Wanneer een instelling beelden gaat uitwisselen past zij deze richtlijn toe of legt uit op welke alternatieve wijze zij dit heeft ingevuld.

Mappingtabel

Onderstaand vindt u de mappingtabel. Hierin staat aangegeven welke UZI-rol welke informatie via een uitwisselingssysteem kan opvragen. Daarnaast staat gemapt welke UZI beroepsgroep welke rol in XDS rolcode krijgt. De XDS rol "Medical doctor" kan zowel de tijdlijn (metadata), als het beeld en het verslag via een uitwisselingssysteem kan opvragen.

Voorbeeld: De anesthesioloog, met UZI-rolcode 1.003 kan zowel de metadata als het beeld en het verslag opvragen via een uitwisselingssysteem. Wanneer gewerkt wordt met XDS-rolcodes, krijgt de anesthesioloog de XDS-rolcode "medical doctor".

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 Z2.3.5 | BB: IHE ITI-40 | Provide X-User Assertion
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 Z2.3.5 | BB: IHE ITI-40 | Provide X-User Assertion Z2.4.1.1 | BB: Metadata
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 Z2.3.5 | BB: IHE ITI-40 | Provide X-User Assertion
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 Z2.3.5 | BB: IHE ITI-40 | Provide X-User Assertion BB: Metadata Radiologisch verslag BB: Metadata Beeldvormend onderzoek Radiologie (DICOM)
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 Z2.3.5 | BB: IHE ITI-40 | Provide X-User Assertion
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 Z2.3.5 | BB: IHE ITI-40 | Provide X-User Assertion

TTA-BB-07	TTA BB	GtK Vrager	De GtK Vrager zal bij ontvangst van een opgevraagd document de vastgestelde formats kunnen verwerken.	Z2.4.1 | BB: Metadata | Content
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.	Z2.4.1 | BB: Metadata | Content

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.
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.
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.
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.
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.
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 1.2.0 Trial

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 zijn 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
- Volume 2a bevat de technische afspraken voor de uitwisseling van de correspondentie. Dit noemen we ook wel de Twiin Technische Afspraak (TTA)
- Volume 2b bevat de technische uitwerkingen van de transacties die gebruikt worden in de TTA
- Volume 3 een verwijzing naar de meta-informatie

Z3.1 | COR: Volume 1 - 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)

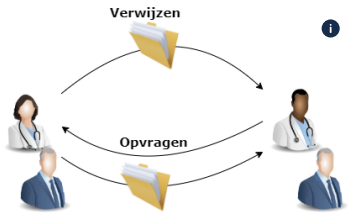
Versie informatie

Versie	Compatibel met Twiin Afsprakenstelsel release	Wijzingen
0.1	1.2.0 en alle opvolgende binnen de major release 1.x.x	

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

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 beschrijft de technische invulling van deze uitwisseling binnen Twiin.

Gebaseerd op het functionele ontwerp Nictiz: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden

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.

Z3.2 | COR: Volume 2a - 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 10.2.3 | TTA FHIR - Notified pull

This Twiin Technical Agreement (TTA) describes and specifies 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, with the normative specifications remaining unchanged. The informative specifications however have been described with a specific implementation.

The possibility to exchange a patient's medical record is for example required in case of a patient referral or transfer. When different healthcare organizations are involved in a patient'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.

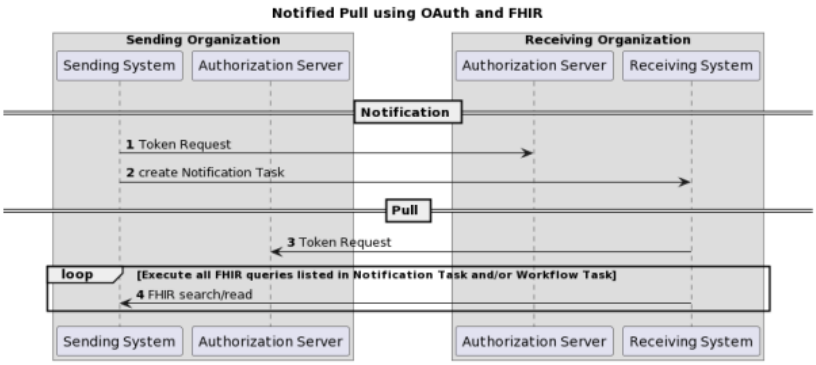
Relation to other documents

This document is written with the following documents as reference:

- Nictiz - Informatiestandaard BgZ MSZ
- TA Notified Pull v0.99

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 10.2.5 | TTA FHIR - Authentication & Authorization. Interaction number 2 is described in 10.2.3.1 | Notified Pull - Data interactions . A part of interaction number 4 is also described in 10.2.3.1 | Notified Pull - Data interactions, for specifics of the context of the Notified Pull see Nictiz information standards.

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

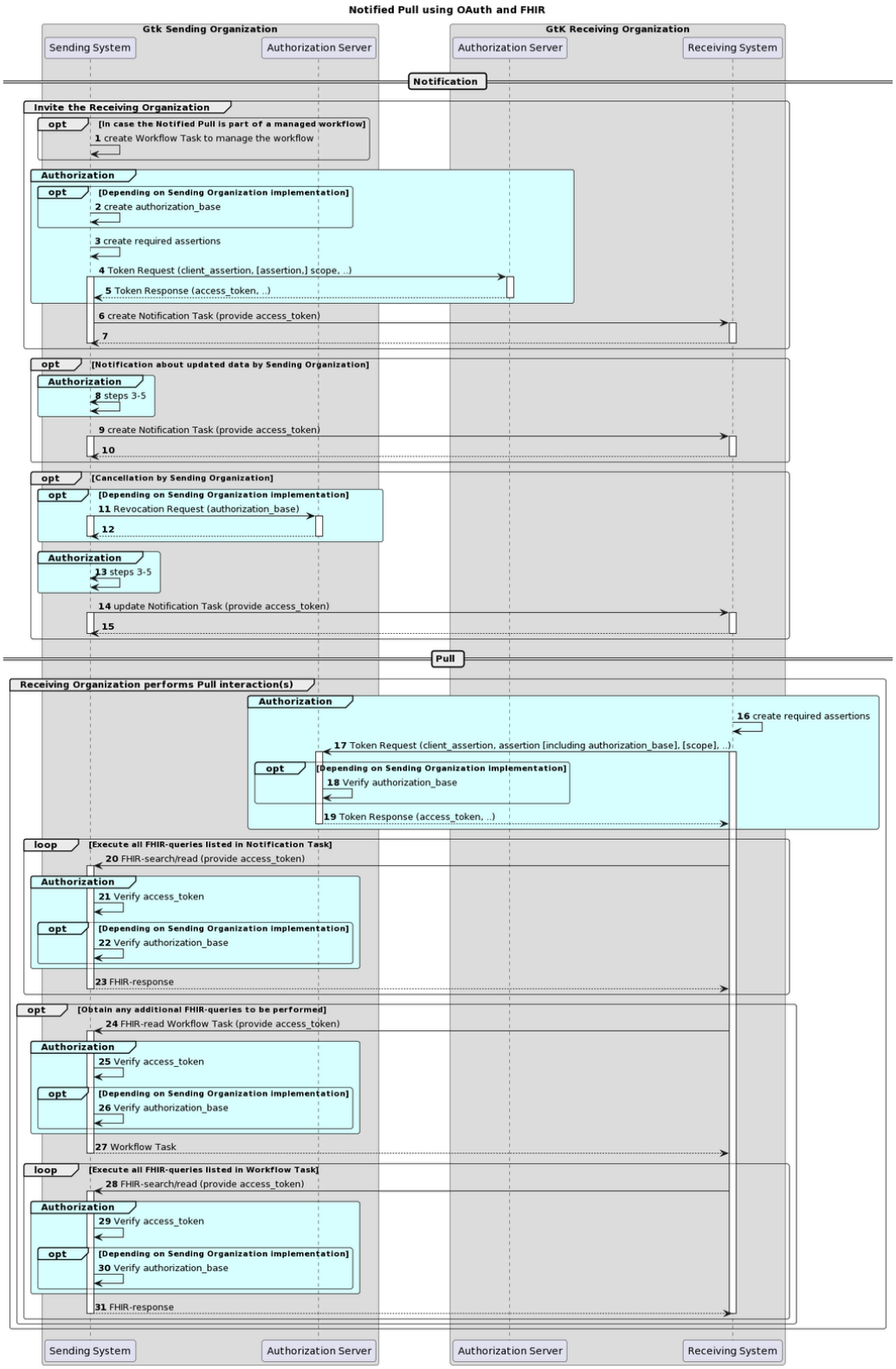
The Twiin specific solutions for identification and addressing can be found in 10.2.5 | TTA FHIR - Authentication & Authorization and 10.2.8 | TTA - Addressing respectively.

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 10.2.3.1 Notified Pull - Data interactions) and in authorization layer using OAuth 2.0 (marked cyan,

described in 10.2.10 | Netwerk level security mTLS 1.3).

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 a 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 others) 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.

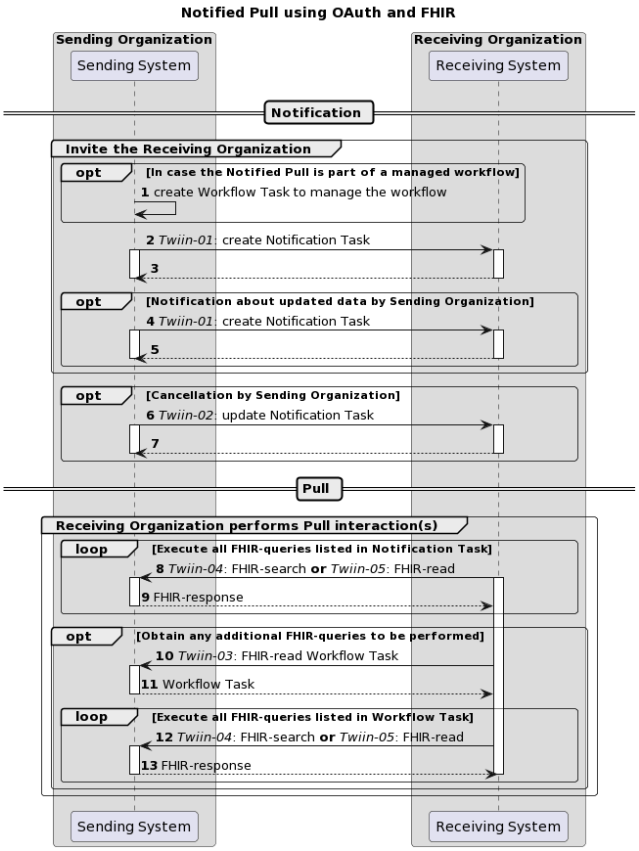
Z3.2.1.1 | COR - Data interactions

Original page can be found at: 10.2.3.1 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 10.3.1 | Twiin-01 | Send Notification Task 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 10.3.1 | Twiin-01 | Send Notification Task 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 10.3.2 | Twiin-02 | Cancel Notification Task 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 10.3.5 | Twiin-05 | Retrieve Resource for a detailed description for the retrieval of resources referenced in Task.input:read-available-resources. See 10.3.4 | Twiin-04 | Search Resource(s) 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 10.3.3 | Twiin-03 | Get workflow Task
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 10.3.5 | Twiin-05 | Retrieve Resource for a detailed description for the retrieval of resources referenced in Task.input:read-available-resources. See 10.3.4 | Twiin-04 | Search Resource(s) 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 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.

10.2.3 | TTA FHIR - Notified pull

10.2.10 | Netwerk level security mTLS 1.3

Z3.2.1.2 | COR: Authentication & Authorization

Original page can be found at: 10.2.5 | TTA FHIR - Authentication & Authorization

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 RFC 6749: The OAuth 2.0 Authorization Framework. 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 RFC 6750: The OAuth 2.0 Authorization Framework: Bearer Token Usage.

Client authentication

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 (RFC 6749: The OAuth 2.0 Authorization Framework) 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 RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.

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 RFC 7518: JSON Web Algorithms (JWA). Must be one of PS256, PS384, PS512, ES256, ES384 or ES512.	Yes
kid	Identifier of the key pair used to sign this JWT. See RFC 7515: JSON Web Signature (JWS).	Yes

The payload contains a set of claims listed below:

Claim	Description	Required
jti	Unique identifier of the client assertion. See RFC 7519: JSON Web Token (JWT).	Yes
iss	Identifier of the system that issued the client assertion. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
iat	The time at which the client assertion was issued. See RFC 7519: JSON Web Token (JWT). 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 RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes

nbf	The time before which the token shall not be accepted for processing. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	No
aud	Identifier of the authorization server token endpoint where this client assertion is to be used. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	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 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). 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 RFC 6749: The OAuth 2.0 Authorization Framework "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. RFC 6749: The OAuth 2.0 Authorization Framework. 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 RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants 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 RFC 7518: JSON Web Algorithms (JWA). Must be one of PS256, PS384, PS512, ES256, ES384 or ES512.	Yes
kid	Identifier of the key pair used to sign this JWT. See RFC 7515: JSON Web Signature (JWS).	Yes

The payload contains a set of claims that carry information required by NEN7512 and NEN7513.

Claim	Description	Required
jti	Unique identifier of the authorization assertion. See RFC 7519: JSON Web Token (JWT).	Yes

iss	Identifier of the system that issued the authorization assertion. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
iat	The time at which the authorization assertion was issued. See RFC 7519: JSON Web Token (JWT). 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 RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
nbf	The time before which the token shall not be accepted for processing. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	No
aud	Identifier of the authorization server token endpoint where this authorization assertion is to be used. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
sub	Identifier of the **organization** (healthcare supplier) 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	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 a authorization base when requesting patient information.	Conditional
user_id	Identifier of the **responsible user** (healthcare professional) or the **system** who requests access. **Preferred: UZI nummer** The codesystem (`issuing_system`) for the identifier is also mandatory. For UZI this is OID: 2.16.528.1.1007.3.1 5.1 | Vertrouwen: Identificatie **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** 5.1 | Vertrouwen: Identificatie The codesystem (`issuing_system`) for the identifier is also mandatory. For UZI role code this is OID: 2.16.840.1.113883.2.4.15.111	Conditional

	User role is required when the responding party needs to validate the role of the user before responding to the request. For instance when a user does not have a authorization base when requesting patient information.	
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	Yes
authorization_base	See Authorization base	No
patient	Identifier of the patient for whom data is exchanged. Must be an OID encoded BSN (I.e., BSN with the "urn:oid:2.16.840.1.113883.2.4.6.3." prefix and without a leading zero) 5.1 | Vertrouwen: Identificatie 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 a ll not require the authorization serv

The exchange of the public 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 RFC 6749: The OAuth 2.0 Authorization Framework . 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 App Launch: Scopes and Launch Context - SMART App Launch v2.2.0 . 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.nl/fhir/NamingSystem/TaskCode|pull-notification (create)
  - system/Task.u?code=http://fhir.nl/fhir/NamingSystem/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).

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 RFC 6749: The OAuth 2.0 Authorization Framework 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 Client authentication.	Yes
client_id	ID of the resource client. This ID is issued by the authorization server. If present, the value of the "client_id" parameter must identify the same client as is identified by the client assertion.	No
scope	Space separated list of requested scopes, see paragraph Authorization scope.	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 RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens , 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.

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 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). 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):

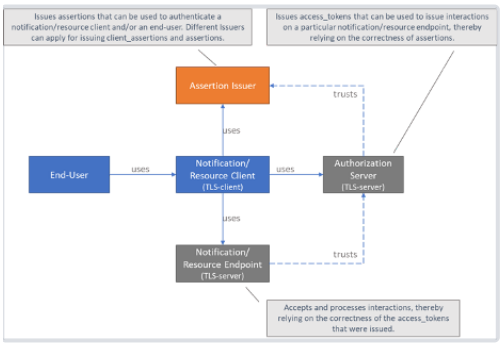
- **sub**: Identifier of the healthcare organization

- **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 an 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.

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).

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 every reference can be coded specific to the part.

Z3.3 | COR Volume 2b - Transacties

The correspondence is communicated using the transactions described under this page.

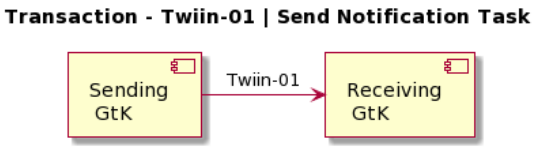
- Z3.3.1 | Twiin-01 | Send COR Notification Task
- Z3.3.2 | Twiin-02 | Cancel COR Notification Task
- Z3.3.3 | Twiin-03 | Get COR workflow Task
- Z3.3.4 | Twiin-04 | Search COR Resource(s)
- Z3.3.5 | Twiin-05 | Retrieve COR Resource
- Z3.3.7 | Twiin-07 | Token Request

Z3.3.1 | Twiin-01 | Send COR Notification Task

This section is the same as the generic 10.3.1 | Twiin-01 | Send Notification Task

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 Index - FHIR v3.0.2

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
- Identification of the patient who is the subject of information exchange
- References to individual FHIR® resources that have been made available at the Sending GtK
- FHIR® search queries that can be used to retrieve FHIR® resources that have been made available at the Sending GtK
- Authorization base (see Authorization base)

The payload of this message consists of a Task - FHIR v3.0.2 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 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 Task - FHIR v3.0.2 .

Attribute	Card.	Description
definitionReference	0..1	This element will be used for routing purposes. The value could determine the department which will handle the notification. The display of this reference should be filled. See also: 10.2.8 | TTA - Addressing
basedOn	0..*	Optional reference to a request-Type resource 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.
status	1..1	The state communicated by this event. Fixed value: • requested See also: Valueset-request-status - FHIR v3.0.2
intent	1..1	Indicates the "level" of actionability associated with the Task[2]. Preferred value: • proposal See also: Valueset-request-intent - FHIR v3.0.2
code.coding	**1**..1	A code briefly describing what the task involves: • system = "http://fhir.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/CodeSystem/ura”
owner.identifier	**1**..1	Identifier of the Receiving Healthcare Organization. The identifier shall be in the system “http://fhir.nl/fhir/CodeSystem/ura”

input:authorization-base	0..**1**	The authorization base to be used when retrieving the data.
		
		Constraints:
		
		• type.coding
		  ◦ system = "http://fhir.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.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 of:)
		  ◦ *Generic typing:*
		  ▪ system = "http://fhir.nl/fhir/CodeSystem/TaskParameter"
		  ▪ code = "read-resource"
		  ◦ *SNOMED CT typing:*
		  ▪ system = “http://snomed.info/sct”
		  ▪ code = a SNOMED CT code
		  ◦ *LOINC typing:*
		  ▪ system = “http://loinc.org”
		  ▪ code = a LOINC code
		• 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 of:) ◦ *Generic typing:* ▪ system = "http://fhir.nl/fhir/CodeSystem/TaskParameter" ▪ code = "search-resource" ◦ *SNOMED CT typing:* ▪ system = “http://snomed.info/sct” ▪ code = a SNOMED CT code ◦ LOINC typing: ▪ system = “http://loinc.org” ▪ code = a LOINC code • 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.nl/fhir/CodeSystem/TaskParameter"
- Task.input.type.coding.value: “get-workflow-task”
- ask.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 Notification response.

The Notification should trigger an event in the Receiving GtK to process the expected Pull.

Persistence of the Notification Task as a FHIR® resource is not necessary.

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 in input can be retrieved shall not be a factor in the HTTP status.

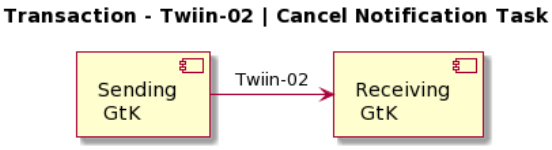
The Sending GtK processes the response according to application defined rules.

Z3.3.2 | Twiin-02 | Cancel COR Notification Task

This page is the same as the generic 10.3.2 | 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.

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 Index - FHIR v3.0.2

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 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 Task - FHIR v3.0.2 .

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]. Preferred value: • proposal See also: Valueset-request-intent - FHIR v3.0.2

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.

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.

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.

Whether or not the resources in input can be retrieved shall not be a factor in the HTTP status.

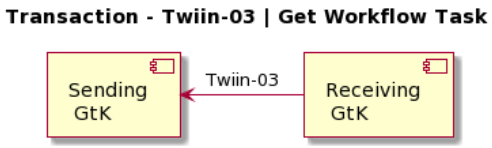
The Sending GtK processes the response according to application defined rules.

Z3.3.3 | Twiin-03 | Get COR workflow Task

This page is the same as the generic 10.3.3 | Twiin-03 | Get workflow Task

This section describes the transaction of the retrieval of the workflow Task.

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 🔥 Task - FHIR v3.0.2 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.

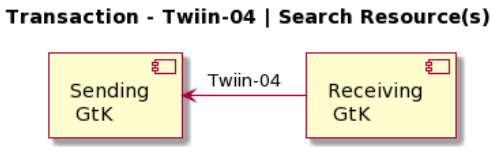
The requesting system processes the response according to application defined rules.

Z3.3.4 | Twiin-04 | Search COR Resource(s)

This page is the same as the generic 10.3.4 | Twiin-04 | Search Resource(s)

This section describes the transaction of the retrieval of the FHIR® resources referenced in the input field of the Notification or Workflow Task.
These input fields contain valueString with either the generic type code “search-resource” or a LOINC or SNOMED CT code.

1. Scope



This transaction supports the request of resources by the Requesting System to the Resource Server.

2. Use Case Roles

Actor: Receiving GtK

Role: Sends a request for resources on behalf of a retrieving user.

Actor: Sending GtK **(**Resource Server)

Role: Processes the request and responds with the requested resources.

3. Referenced Standards

- HL7® FHIR® standard STU3 Index - FHIR v3.0.2

4. Messages

4.1. Request message

The requesting system 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
```

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.

4.2. Response message

The resource server 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 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.

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

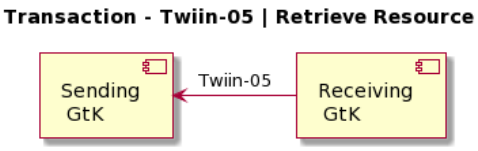
The requesting system processes the response according to application defined rules.

Z3.3.5 | Twiin-05 | Retrieve COR Resource

This page is the same as the generic 10.3.5 | Twiin-05 | Retrieve Resource

This page describes the transaction of the retrieval of the FHIR® resources referenced in the input field of the Notification or Workflow Task. These input fields contain valueReference combined with the input type “read-resource” or a LOINC or SNOMED CT code.

Scope



This transaction supports the request of resources by the Requesting System to the Resource Server.

Use Case Roles

Actor: Receiving GtK

Role: Sends a request for a specific resource on behalf of a retrieving user.

Actor: Sending GtK (Resource Server)

Role: Processes the request and responds with the requested resource.

Referenced Standards

- HL7® FHIR® standard STU3 Index - FHIR v3.0.2

Messages

Request message

The requesting system 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 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 resource that is requested.

The payload of this message is the requested FHIR® resource. 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.

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

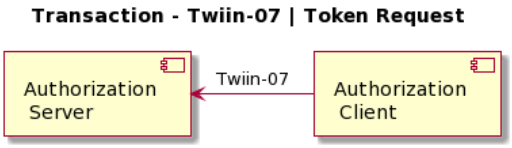
The requesting system processes the response according to application defined rules.

Z3.3.7 | Twiin-07 | Token Request

This page is the same as the generic 10.3.7 | Twiin - 07 | Token Request

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

Referenced 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.
- *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.

- *RFC7515*: JSON Web Signature (JWS), May 2015.
- *RFC7518*: JSON Web Algorithms (JWA), May 2015.
- *RFC4648*: The Base16, Base32, and Base64 Data Encodings, October 2006

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 (RFC RF C 6749: The OAuth 2.0 Authorization Framework) 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 RFC RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.

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 RFC RFC 7518: JSON Web Algorithms (JWA). Must be one of PS256, PS384, PS512, ES256, ES384 or ES512.	Yes
kid	Identifier of the key pair used to sign this JWT. See RFC RFC 7515: JSON Web Signature (JWS).	Yes

The payload contains a set of claims listed below:

Claim	Description	Required
jti	Unique identifier of the client assertion. See RFC RFC 7519: JSON Web Token (JWT).	Yes
iss	Identifier of the system that issued the client assertion. See RFC RFC 7519: JSON Web Token (JWT) and RFC RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
iat	The time at which the client assertion was issued. See RFC RFC 7519: JSON Web Token (JWT). 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 RFC RFC 7519: JSON Web Token (JWT) and RFC RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
nbf	The time before which the token shall not be accepted for processing. See RFC RFC 7519: JSON Web Token (JWT) and RFC RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	No
aud	Identifier of the authorization server token endpoint where this client assertion is to be used. See RFC RFC 7519: JSON Web Token (JWT) and RFC RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants. System vendors have to make mutual agreements about the value of this identifier.	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.	Yes

	Note that the client is specified as the system that submits the access token request. System vendors have to make mutual agreements about the value of this identifier.	

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 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). 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 RFC 6749: The OAuth 2.0 Authorization Framework "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. RFC 6749: The OAuth 2.0 Authorization Framework. 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 RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants 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 RFC 7518: JSON Web Algorithms (JWA). Must be one of PS256, PS384, PS512, ES256, ES384 or ES512.	Yes
kid	Identifier of the key pair used to sign this JWT. See RFC 7515: JSON Web Signature (JWS).	Yes

The payload contains a set of claims that carry information required by NEN7512 and NEN7513.

Claim	Description	Required
jti	Unique identifier of the authorization assertion. See RFC 7519: JSON Web Token (JWT).	Yes
iss	Identifier of the system that issued the authorization assertion. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants. System vendors have to make mutual agreements about the value of this identifier.	Yes
iat	The time at which the authorization assertion was issued. See RFC 7519: JSON Web Token (JWT). 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 RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
nbf	The time before which the token shall not be accepted for processing. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	No
aud	Identifier of the authorization server token endpoint where this authorization assertion is to be used. See RFC 7519: JSON Web Token (JWT) and RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants.	Yes
sub	Identifier of the **healthcare organization** that requests access. **URA nummer** 5.1 | Vertrouwen: Identificatie	Yes
user_id	Identifier of the **responsible user** (healthcare professional) who requests access. **Preferred: UZI nummer** 5.1 | Vertrouwen: Identificatie 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
user_role	Code of the role of the responsible user (healthcare professional) who requests access. **Preferred: UZI rolcode** 5.1 | Vertrouwen: Identificatie 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** 5.1 | Vertrouwen: Identificatie	Yes
authorization_base	See Authorization base	No
patient	Identifier of the patient for whom data is exchanged. Must be an OID encoded BSN (I.e., BSN with the "urn:oid:2.16.840.1.113883.2.4.6.3." prefix and without a leading zero) 5.1 | Vertrouwen: Identificatie 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 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 RFC 6749: The OAuth 2.0 Authorization Framework . 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 App Launch: Scopes and Launch Context - SMART App Launch v2.2.0 . 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.nl/fhir/NamingSystem/TaskCode|pull-notification (create)
  - system/Task.u?code=http://fhir.nl/fhir/NamingSystem/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).

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 RFC 6749: The OAuth 2.0 Authorization Framework 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 Client authentication.	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

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 RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens , 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.

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 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). 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.

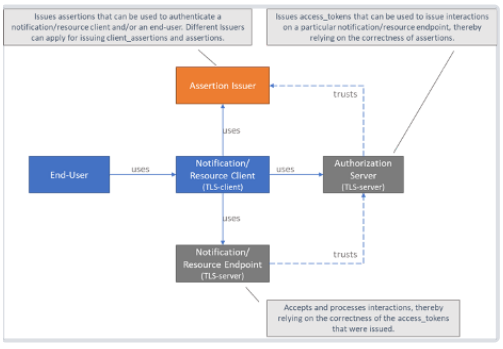
The Sending System can identify the healthcare professional at the receiving organization that is requesting patient data by the following claims in the authorization assertion of the access token request (see Authorization grant):

- **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 an 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.

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: 10.3.5 | Twiin-05 | Retrieve Resource De autorisatierichtlijn van de primaire zorgtoepassing is van toepassing.
COR-2a-TANP-01	TA NP	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 corresponde nce - FHIR Notified Pull
COR-2a-TANP-02	TA NP	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 corresponde nce - FHIR Notified Pull
COR-2a-TANP-03	TA NP	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 corresponde nce - FHIR Notified Pull
COR-2a-TANP-04	TA NP	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 (10.3.

				14.1 | ZORG-AB Transacties) 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 corresponde nce - FHIR Notified Pull
COR-2a-TANP-05	TA NP	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 (10.3. 14.1 | ZORG-AB Transacties) 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 corresponde nce - FHIR Notified Pull
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
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
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: 10.2.5 | TTA FHIR - Authentication & A uthorization | 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
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
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 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: 10.2.5 | TTA FHIR - Authentication & 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: Z3.2.1.2 | COR: Authentication & Authorization | Access token request
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: Z3.2.1.2 | COR: Authentication & Authorization | Client authentication , Z3.2.1.2 | COR: Authentication & Authorization | Access token request
COR-2a-AA-10	BgZ Authn en	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: Z3.2.1.2 | COR: Authentication & Authorization | Access token request

	Auth z			
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: 10.2.5 | TTA FHIR - Authentication & 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: 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: Z3.2.1.2 | COR: Authentication & Authorization | Access token request
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 10.2.10 | Netwerk level security mTLS 1.3
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 10.2.10 | Netwerk level security mTLS 1.3
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 ICT-beveiligingsrichtlijnen voor Transport Layer Security v2.1 (TLS)

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 10.2.10 | Netwerk level security mTLS 1.3
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, artikel 4.5.2 CRL's: Certificate Revocation Lists (CRL's) | Zorg CSP
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
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 Specificatie: 10.3.1 | Twiin-01 | Send Notification Task | Request message
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 Specificatie: 10.3.1 | 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 Specificatie: 10.3.1 | 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 Specificatie: 10.3.1 | 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 Specificatie: 10.3.2 | Twiin-02 | Cancel Notification Task | Request message
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 Specificatie: 10.3.2 | 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 Specificatie: 10.3.5 | Twiin-05 | Retrieve Resource 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 Specificatie: 10.3.5 | Twiin-05 | Retrieve Resource
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 Specificatie: 10.3.4 | Twiin-04 | Search Resource(s) De search-operaties zijn opgenomen in de notificatie-task onder Task.input:query-available-resources.
COR-2b-trans-09.search	Transactions - BgZ inter	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 Specificatie: 10.3.4 | Twiin-04 | Search Resource(s)

	actions			
COR-2b-trans-10	Transactions - BgZ 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 Specificatie: 10.3.3 | Twiin-03 | Get workflow Task 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 - BgZ 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
COR-2b-trans-12.read	Transactions - BgZ 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 Specificatie: 10.3.5 | Twiin-05 | Retrieve Resource De read-operaties zijn opgenomen in de workflow-task onder `Task.input:read-available-resources`.
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 Specificatie: 10.3.5 | Twiin-05 | Retrieve Resource
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 Specificatie: 10.3.4 | Twiin-04 | Search Resource(s) De search-operaties zijn opgenomen in de workflow-
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.	Specificatie: 10.3.4 | Twiin-04 | Search Resource(s)
COR-FO-08	FO - Nictiz	GtK verzender	GtK verzender moet een verwijsbrief in gestructureerd formaat kunnen versturen bij verwijzing naar een andere zorginstelling of zorgverlener.	Specificatie: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden
COR-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: Functioneel Ontwerp BgZ medisch-specialistische zorg 1.0 - informatiestandaarden

2. Aanvullende ketentest eisen

De eisen in dit hoofdstuk zijn niet nodig zijn voor de AMIH validatie van de zorgtoepassing. Deze eisen zijn wel nodig om te voldaan aan de ketentest de informatiestandaard, de VIPP-eisen en eventuele andere functionele eisen.

Eis	Categorie	Actor	Omschrijving	Toelichting inclusief aanvullende documentatie

COR-1-VIPP5-1	VIPP 5	GtK verzender	GtK verzender kan de correspondentie verzenden naar andere instellingen van Medisch Specialistische Zorg.	Zie Handreiking VIPP5 assessments, bijlage II, paragraaf 1.5, alinea module 3 Zie https://www.vipp-programma.nl/over-vipp/doelstellingen
COR-1-VIPP5-2	VIPP 5	GtK ontvanger	GtK ontvanger kan de correspondentie ontvangen vanuit een andere instelling van Medisch Specialistische Zorg.	Zie Handreiking VIPP5 assessments, bijlage II, paragraaf 1.5, alinea module 3 Zie https://www.vipp-programma.nl/over-vipp/doelstellingen
COR-1-VIPP5-4	VIPP 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, 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.