Dekkingsmatrix FO en TO ToN 360° cliëntbeeld

Werkdocument
Datum 26-08-2026

Inleiding

Dit document is de dekkingsmatrix tussen het Functioneel Ontwerp (FO) en het Technisch Ontwerp (TO) van de Toepassing op Nuts 360° cliëntbeeld. De matrix legt per onderwerp naast elkaar wat het FO functioneel beschrijft en hoe dit in het TO wordt of kan worden afgedekt. Daarmee ondersteunt het document de afstemming tussen FO en TO en maakt het zichtbaar waar nog verduidelijking of verdere uitwerking nodig is.

Bij voorkeur groeit zo'n matrix mee tijdens het opstellen van het TO. Bij deze toepassing is dat proces in de praktijk minder volgtijdelijk verlopen. Het FO was al beschikbaar toen het TO verder werd uitgewerkt, waardoor de afstemming tussen FO en TO deels parallel aan en deels na de technische uitwerking heeft plaatsgevonden. Daarbij bleek dat enkele begrippen, keuzes en uitgangspunten nog nadere duiding of afstemming vroegen.

Om die reden is deze dekkingsmatrix opgesteld. De matrix brengt deze punten bij elkaar en helpt om inzichtelijk te maken hoe de functionele wensen uit het FO in het TO zijn of worden afgedekt. Omdat een deel van deze afstemming nog gaande is, heeft dit document het karakter van een werkdocument. Dat past bij de bredere context waarin ToN 360° cliëntbeeld wordt ontwikkeld. De omgeving verandert de komende tijd, onder meer door de ontwikkeling van generieke functies, landelijke voorzieningen voor lokalisatie en adressering, en aanpalende wet- en regelgeving. Ook tijdens de verdere ontwikkeling van de toepassing kunnen nog aanpassingen plaatsvinden in dit document, het FO en het TO.

Dit document is daarmee geen eindpunt, maar een hulpmiddel dat meebeweegt met de toepassing, haar omgeving en de verdere afstemming tussen FO en TO. Het kan daarnaast als voorbeeld dienen voor andere toepassingen op Nuts waarvoor een FO, TO en dekkingsmatrix worden opgesteld.

Zie TO ToN 360° cliëntbeeld hier.

Doel

Dit document legt de functionele eisen uit het Functioneel Ontwerp (FO) ToN 360° cliëntbeeld, zoals opgeleverd op 30 juni 2026, naast de vraag die het Technisch Ontwerp (TO) moet beantwoorden. Het is bedoeld voor de groep die het TO van de toepassing op Nuts 360° cliëntbeeld heeft gemaakt, en is dus niet rechtstreeks bedoeld voor de individuele leveranciers. Na invulling door de TO-makers kan het document mogelijk ook door de leveranciers worden gebruikt.

Het document bevat geen technische oplossingsrichting — dat is aan de TO-makers — maar een opsomming van wat we als belangrijkste nu vanuit het FO onderbouwd inzichtelijk willen hebben, zodat we weten wat hoe is afgedekt.

Wat is een FO-TO-dekkingsmatrix?

Een dekkingsmatrix tussen Functioneel Ontwerp (FO) en Technisch Ontwerp (TO) is een overzicht dat per functionele eis of wens uit het FO laat zien of, en hoe, deze in het TO is afgedekt. Het is daarmee een controle- en afstemmingsinstrument: het maakt aantoonbaar dat het TO daadwerkelijk realiseert wat het FO vraagt, en het maakt zichtbaar waar dat (nog) niet, deels, of op een afwijkende manier gebeurt.

De achterliggende gedachte volgt uit de verhouding tussen beide documenten. Het FO beschrijft in begrijpelijke taal wat de toepassing moet doen: de processen, gegevens, rollen en functionaliteit, en de eisen en wensen van de betrokkenen. Het TO beschrijft vervolgens hoe dat technisch wordt gerealiseerd. Het TO wordt op basis van een goedgekeurd FO gemaakt en zou elke functionele eis moeten kunnen herleiden naar een technische invulling. De dekkingsmatrix maakt die herleiding expliciet.

Om die reden werkt deze matrix per onderwerp met een vaste opbouw: de eis of wens uit het FO en de bijbehorende vraag, de vindplaats in het FO, het antwoord vanuit het TO, en waar nodig een analyse met openstaande punten. Bij elk onderdeel dat het TO oppakt, hoort dus niet alleen de technische oplossing, maar ook de verwijzing naar het onderdeel van het FO waarop het is gebaseerd, met een toelichting waaróm het zo is ingevuld.

Een belangrijk uitgangspunt daarbij is de leesbaarheid. De matrix is zo opgesteld dat zij ook bruikbaar is voor betrokkenen zonder technische achtergrond. Technische begrippen en keuzes worden waar nodig toegelicht in gewone taal, zodat inzichtelijk wordt hoe het TO-invulling geeft aan de wensen en eisen uit het FO en waar nog nadere afstemming nodig is.

Werkwijze

Per Nictiz-laag (dezelfde indeling als het FO zelf hanteert) staat de FO-eis samengevat, inclusief de vraag die deze eis aan het TO stelt, en de vindplaats in het FO. De kolom 'Antwoord TO' bevat de technische duiding of invulling vanuit het TO: welk technisch mechanisme of welke ontwerpkeuze de eis afdekt, en welke partij (Nuts-stelsel, generieke functie, individuele leverancier) daarvoor aan zet is.

Vervolg

Wanneer de afstemming tussen de FO- en TO-werkgroepen heeft plaatsgevonden, kan de FO-werkgroep beoordelen hoe de wensen uit het FO zijn ingevuld en eventuele hiaten bespreken.

Na deze afstemming kan het document worden meegestuurd naar de individuele leveranciers (Nedap/Ons, RIVO/Zorgviewer, Erasmus MC/Digizorg, Versneld verbinden), zodat zij weten hoe de generieke technische keuzes zich verhouden tot de eisen uit het FO wanneer zij hun eigen FO/TO voor hun software uitwerken.

Organisatie en beleid

FO-eis	Vindplaats in FO	Antwoord TO
Autorisatie voor toegang tot cliëntgegevens wordt organisatorisch vastgesteld (rol, behandelrelatie, toestemming), maar de uitvoering vindt plaats in de bronsystemen, op basis van de Nuts-voorzieningen voor authenticatie en autorisatie. ***Vraag:*** *Hoe wordt de vertaling van het organisatorische autorisatiebeleid naar een technisch afdwingbare autorisatiebeslissing op ketenniveau gerealiseerd? Welke rol vervullen de Nuts-voorzieningen daarin concreet?*	Autorisatie	Authenticatie gebeurt op basis van de standaard Nuts v6 techniek en de credentials die afgesproken zijn in Zorginzage 2026. Dat zijn een Organisatie, Rol van de applicatie/gebruiker en medewerker (employee) credential te gebruiken. In de applicatie die bronhouder is, worden de autorisatieregels uit volume 2 van het TO toegepast (paragraaf 3.4.5), eventueel met behulp van de opgestelde rego policy. De bronhouder autoriseert alleen op organisatieniveau; de authenticatie en de autorisatie op zorgverlener-rol vinden lokaal in de raadplegende applicatie plaats. Dit sluit aan op wat het FO aangeeft. Zie toelichting over 2 soorten autorisatie in hoofdstuk 'Autorisatie, beleid en rego'.
Toestemming wordt vastgelegd bij de dossierhouder; de technische uitwerking (MITZ, lokale registratie, toekomstig register) valt buiten de functionele eis, maar moet wel ergens technisch geborgd worden. ***Vraag:*** *Hoe wordt de toestemmingsstatus vóór het ophalen van gegevens technisch geraadpleegd en gecontroleerd? Welke voorziening wordt hiervoor in versie 1 gebruikt?*	Toestemming	In volume 2 staat omschreven dat er drie manieren zijn waarop je toestemming mag vaststellen. Consent in een voorziening zoals Mitz, lokaal geregistreerde toestemming of een andere juridische grondslag. Als die laatste twee gebruikt worden, mag de leverancier zelf kiezen wat de technische uitvoering is.
Zolang de generieke functies (identificatie, authenticatie, autorisatie van organisaties) nog niet beschikbaar zijn, wordt vertrouwen tussen organisaties tijdelijk geborgd met een vooraf afgesproken lijst van deelnemende zorgorganisaties, die leveranciers in hun software verwerken. ***Vraag:*** *Hoe wordt deze tijdelijke lijst technisch beheerd en gedistribueerd naar de aangesloten leveranciers? Hoe verloopt*	Vertrouwen tussen deelnemende organisaties	De te vertrouwen organisaties worden vooralsnog geregistreerd via de tijdelijke Discovery service, waarmee dan adresgegevens worden uitgewisseld. Er wordt nu gekeken naar de discovery server van Ecare en Versneld verbinden, dat is nog niet helemaal uitgewerkt. *Zie werkdocument hier in Proton van Jorrit over discovery service.*

FO-eis	Vindplaats in FO	Antwoord TO
de overgang naar de landelijke generieke functies zodra die beschikbaar zijn, zonder dat de keten daarbij stilvalt?		
Bij het filteren van informatie in de viewer wordt niet alleen rekening gehouden met autorisatie, maar ook met de persona van de gebruiker (in versie 1: arts of verpleegkundige, inclusief specialisaties). ToN 360° schrijft zelf geen vaste gegevensset per persona voor. ***Vraag**: Hoe herkent de opvragende applicatie welke persona de aanvraag doet — arts of verpleegkundige? Wordt deze persona-informatie als onderdeel van de bevraging technisch meegegeven door ToN 360°, of is dit volledig een lokale verantwoordelijkheid van de raadplegende applicatie, los van de uitwisseling zelf?*	Weergave en presentatie/ Uitgangspunten (punt 4)	De bronapplicatie ontvangt de rol van de zorgverlener wel, maar het is een lokale rolcode van de raadplegende organisatie zonder landelijke standaardisatie; de bronhouder kan die niet eenduidig interpreteren en gebruikt die niet voor de toegangsbeslissing. De rolbepaling (arts of verpleegkundige) en de filtering op basis daarvan gebeuren daarom in de raadplegende applicatie, op grond van de eigen autorisatie. Het TO verplicht wél om bij de bevraging de identiteit van de zorgverlener mee te sturen (via het medewerkercredential); de rol reist daarbij mee als niet-identificerend gegeven, niet als grondslag voor toegang. De bronhouder kan de meegestuurde gegevens vastleggen voor audit logging. Zie toelichting in het hoofdstuk 'Autorisatie, beleid en rego'.
ToN 360° schrijft geen vaste set aan gegevens *per persona of rol* voor; de raadplegende organisatie is zelf verantwoordelijk voor het inrichten van autorisaties van haar gebruikers per persona binnen het eigen systeem. ***Vraag**: Op welke manier ondersteunt het TO organisaties om deze inrichting per persona daadwerkelijk te kunnen doen? En hoe wordt voorkomen dat elke leverancier/organisatie hier een eigen invulling aan geeft, waardoor hetzelfde 360° beeld bij de ene organisatie voor een verpleegkundige er wezenlijk anders uitziet dan bij een andere?*	Autorisatie binnen eigen organisatie	Het FO schrijft geen vaste set gegevens voor per persona, dus het TO geeft daar ook geen technische invulling aan. Het FO spreekt over regionale verschillen, en bevraagt de makers van het TO. *Er zal vanuit de TO-groep met leveranciers besproken worden in hoeverre hier al iets mee gedaan wordt in de eigen applicatie. We stellen voor als FO- en TO-groep dan vanaf medio september 2026 te bespreken wat we hiermee kunnen doen. Mogelijk dan in een volgende versie te implementeren.*

Processen en werkwijze

FO-eis	Vindplaats in FO	Antwoord TO
De reactietijd voor het tonen van gevraagde informatie bedraagt maximaal 10 seconden (zorgverlener-eis), met een bandbreedte van 4 tot 30 seconden. ***Vraag:** Welke technische maatregelen borgen dat deze reactietijd wordt gehaald? Is dit onderbouwd met een doorrekening of proof of concept? Als het aan leveranciers wordt overgelaten, (hoe) zorgt het TO dan voor kaders?*	Werkbaarheid in het zorgproces	Zie wat in het TO staat hiervoor. Het TO legt prestatieverwachtingen vast, geen afdwingbare service levels. De drie vragen kort beantwoord: *Welke technische maatregelen borgen de reactietijd?* Elke zib is een losse bevraging en kan parallel worden opgevraagd, zodat gegevens getoond kunnen worden zodra ze binnenkomen (progressieve weergave, conform de FO-wens). Omdat het alleen om leesbevragingen gaat, kan de bronhouder horizontaal schalen om de performance te verbeteren. De raadpleger hanteert een timeout van 60 seconden per verzoek en bewaart opgehaalde gegevens tijdelijk (niet vaker dan eens per 5 minuten dezelfde resource per sessie; niet duurzaam bewaren). *Is dit onderbouwd met een doorrekening of PoC?* Nee. Er is geen doorrekening of proof of concept; het zijn verwachtingen, geen afdwingbare service levels. De TO-groep maakt zich geen zorgen over de capaciteit van de systemen (met uitzondering van Versneld verbinden).

FO-eis	Vindplaats in FO	Antwoord TO
		Als het aan leveranciers wordt overgelaten, geeft het TO dan kaders? Ja. Er wordt een maximale reactietijd per individueel verzoek afgesproken (4 seconden per losse resource, 30 seconden voor de complete set), samen met de kaders voor parallelle bevraging, horizontale schaalbaarheid, timeout en caching. Zie toelichting in hoofdstuk 'Reactietijd en werkbaarheid'.
Bij een langere ophaal- en presentatietijd kan onderscheid gemaakt worden tussen een eerste weergave binnen de reactietijd en latere detailinformatie (progressieve opbouw); de gebruiker moet kunnen zien dat er geladen wordt. ***Vraag:*** *Hoe wordt progressief laden technisch gerealiseerd, en hoe wordt de laadstatus aan de gebruiker getoond?*	Werkbaarheid in het zorgproces	• Elke zib wordt los opgevraagd en kan daarom direct worden weergegeven als die binnenkomt. • Weergave vraagstukken zijn buiten de scope van het technisch ontwerp. Die raadplegende applicatie kan hier zelf keuzes in maken.
De zorgprofessional heeft bij voorkeur een knop of tabblad in het eigen bronsysteem waarmee het 360° cliëntbeeld wordt opgeroepen; een aparte viewer applicatie is alleen een alternatief als het niet anders kan. ***Vraag:*** *Doet het TO hier uitspraken over als kaders voor de leveranciers? Hoe wordt de aanroep vanuit het bronsysteem technisch gefaciliteerd vanuit het TO? Wat is de technische impact op leveranciers die dit moeten inbouwen?*	Processen en werkwijzen (algemeen)	In het TO is hier geen uitwerking voor gemaakt. De leveranciers pakken dit op en baseren zich op het FO. Alle aanroepen (queries, bevragingen) die je mag doen vanuit het TO zijn gedocumenteerd in zowel tekst als code (toegangsbeleid). Zie TO in tab Volume 3.  Zib / HTTP Method / FHIR version / Query / Supported profiles (_profile) Ademhaling / GET / STU3 / /Observation?patient={patientId}&_profile=http://nictiz.nl/fhir/StructureDefinition/zib-Respiration / http://nictiz.nl/fhir/StructureDefinition/zib-Respiration Ademhaling / GET / R4 / /Observation?patient={patientId}&_code=http://snomed.info/sct|422834003 / retired in zib2020 (R4); STU3 zib2017 only
Bevragingsfrequentie moet begrensd worden om bronsystemen te beschermen tegen overbelasting en oneigenlijk gebruik; concrete grenswaarden vallen buiten de scope van dit FO. ***Vraag:*** *Welke technische mechanismen kunnen worden toegepast, aan zowel de brengende als de halende kant, en zijn hierover met softwareleveranciers al gesprekken gevoerd, cq. afspraken over gemaakt hoe zij dit (in SLA's) borgen?*	Werkbaarheid in het zorgproces	Het TO legt geen algemene begrenzing van de bevragingsfrequentie of limiet per tijdseenheid vast. Wel is er een cache-afspraak die herhaald opvragen tegengaat: de raadpleger bewaart een opgehaalde respons tijdelijk en haalt dezelfde resource binnen één gebruikerssessie niet vaker dan eens per 5 minuten opnieuw op, ter bescherming van de bronhouder tegen herhaalde identieke verzoeken. Dit beschermt tegen onnodig herhaald opvragen, maar is geen frequentiebegrenzing tegen overbelasting of oneigenlijk gebruik in bredere zin. Zie hier in TO. Het TO biedt hiermee voldoende grenzen op basis waarvan leveranciers aanvullende maatregelen kunnen nemen om hun software hier tegen te verweren.

Informatie

FO-eis	Vindplaats in FO	Antwoord TO
Het FO kijkt niet of er bestaande FHIR-profielen zijn voor de geselecteerde zibs; dit is expliciet benoemd als een wisselwerking met het TO. ***Vraag:*** *Welke lijst zibs stelt het TO voor/ is in het TO gekozen? Is voor de geselecteerde zibs een nieuw FHIR-profiel nodig? Zo ja: welk, en wie ontwikkelt dit?*	Uitgangspunten informatie Excel-lijst	Zie volume 3 voor de gemaakte keuzes. Voor de geselecteerde zibs zijn geen nieuwe FHIR-profielen opgesteld; er is teruggevallen op bestaande profielen. Alleen waar geen bruikbaar FHIR-profiel beschikbaar was, wordt gericht bevraagd op basis van een SNOMED-code (via de _code=-parameter): niet een compleet zib-profiel, maar een gerichte zoekopdracht op observaties met die betekeniscode.

FO-eis	Vindplaats in FO	Antwoord TO
		Dit betreft vier zibs, alle in de R4-variant: • Ademhaling/R4 • Gezinssituatie/R4 • VermogenTotVerpleegtechnischeHandelingen/R4 • VermogenTotZelfstandigMedicatiege-bruik/R4 Alle gegevens zijn opvraagbaar in zowel de STU3- als de R4-variant. Zie volume 3 van het TO. Deze keuzes van zibs zijn ook verwerkt in het Excel dat vanuit FO was opgesteld. De leverancier moet zelf zorgdragen dat interne verwerkingen in de eigen applicatie blijven aansluiten om de SNOMED-standaard, zodat uitwisseling mogelijk blijft.
"Conclusies uit medische correspondentie" is functioneel wenselijk in versie 1, maar hiervoor bestaat geen zib. (zie regel 95 Correspondentie in sheet zibs) ***Vraag:*** *Hoe wordt dit gegeven technisch ontsloten zonder bestaande zib-structuur?*	Selectie van uit te wisselen zibs voor versie 1	Hiervoor is geen zib nodig. Correspondentie wordt ontsloten via de generieke FHIR-resource DocumentReference, opgevraagd op basis van een patient-id en een status. Zo kan het gegeven worden opgehaald zonder dat er een specifieke zib-structuur voor bestaat. Zie hiervoor TO Volume 3 onder Correspondentie. Correspondentie GET STU3 /DocumentReference?patient={patientId}&status=current and then follow the reference n/a Correspondentie GET R4 /DocumentReference?patient={patientId}&status=current and then follow the reference n/a
"De laatste verslaglegging vanuit de VVT" is functioneel wenselijk, in lijn met de ToN ANW-werkwijze; de invulling moet met het TO worden afgestemd. ***Vraag:*** *Welke technische invulling wordt hiervoor gekozen, en sluit deze aan bij de bestaande ANW-werkwijze?*	Selectie van uit te wisselen zibs voor versie 1	Zie volume 3 van het TO. Hiervoor bestaat reeds een werkend profiel: in de ANW is dit het element **Rapportage met FHIR-profiel nl-core-nursingreport**. Het ontbrak/ontbreekt in het excel de 360°-informatie-analyse sheet omdat Jorrit die zib niet had opgenomen, en we het dus niet daarin verwerkt hebben. De wens is breed gedragen, daarom staat het zo duidelijk in het FO. Omdat het profiel al bestaat en de wens breed gedragen wordt door de zorgorganisaties, is het zoals er staat vanuit het FO wenselijk. Dus dit kan worden opgenomen in het TO. De volgende stap is om te bespreken of de leveranciers dit element kunnen en willen ontsluiten. Zodra dat bevestigd is, wordt het toegevoegd aan de dataset-specificatie en daarmee ook aan het TO.
De informatie wordt getoond als één generiek totaaloverzicht, met dynamische filters vanuit het ECD van de lezer en een filter op tijdsduur (24 uur / 7 dagen / 3 maanden / 1 jaar / alles). ***Vraag:*** *Welk component voert de filtering uit (viewer, opvragende applicatie)? Hoe wordt het generieke totaaloverzicht technisch samengesteld uit meerdere brondata tegelijk?*	Weergave en presentatie	Consolidatie, weergave en filtering vinden plaats bij de raadpleger. Met consolidatie wordt bedoeld: het samenbrengen van de losse gegevens die uit meerdere bronnen binnenkomen tot één samenhangend totaaloverzicht van de cliënt — inclusief het naast elkaar tonen of samenvoegen van gegevens die over hetzelfde onderwerp gaan maar van verschillende bronnen komen. Dit is een expliciete keuze van de TO-groep. De onderbouwing is dat de gegevens bij de bron blijven en per bron kunnen verschillen in vorm en kwaliteit — denk aan verschillende zib-versies, ontbrekende codes, of bronnen die over hetzelfde onderwerp iets anders vastleggen. Die gegevens worden getoond zoals ze uit de bron komen, zonder ze aan de bronzijde te corrigeren. Het samenbrengen van gegevens uit meerdere bronnen tot één overzicht, inclusief het omgaan met zulke verschillen in de weergave, kan daarom alleen bij de partij die het geheel samenstelt en toont: de raadpleger.

FO-eis	Vindplaats in FO	Antwoord TO
		Over wat wel en niet wordt afgedwongen: de raadpleger vraagt het volledige dossier op en is vanuit het FO verplicht de filters (waaronder het filter op tijdsduur: 24 uur, 7 dagen, 3 maanden, 1 jaar, alles) in te bouwen. Het TO dwingt dus af dat er gefilterd kan worden. Hoe dat technisch gebeurt, is opengelaten: de mapping tussen de binnenkomende gegevens en de interface en datastructuur van het raadplegende systeem bepaalt elke leverancier zelf, omdat systemen daar hun eigen methoden voor hebben. Aandachtspunt: omdat de filtering aan de raadplegende kant plaatsvindt, wordt in beginsel steeds het volledige dossier opgehaald en pas daarna gefilterd. Het filter op tijdsduur beperkt dan wat wordt getoond, niet wat wordt opgehaald. Voor de eenvoud van filteren is dat logisch, maar het betekent dat het filter de belasting van de bron en de hoeveelheid opgehaalde gegevens niet vermindert (dataminimalisatie). Vanuit de TO-groep is dit punt niet nader besproken of onderzocht. Uitgangspunt TO is dat er in principe niet veel data per cliënt opgehaald zal worden. Wanneer dit soort tijdfilters ingebouwd worden, dan zal de ToN weer moeilijker realiseerbaar worden per applicatie. De FHIR-standaard heeft die mogelijkheid wel maar dan moet de datakwaliteit bij de bron wel op orde zijn. Dit punt wordt meegenomen en beoordeeld in een volgende versie van de ToN.
Voor elk getoond gegeven moet de herkomst herleidbaar zijn: dossierhouder, datum van vastlegging, en waar relevant de rol of persona van de registrerende zorgverlener. ***Vraag:*** *Hoe wordt deze metadata per individueel gegeven meegegeven, opgeslagen en getoond, zonder de leesbaarheid van het totaaloverzicht te verstoren?*	Herkomst en herleidbaarheid van gegevens	Dit is opgelost en in het TO opgenomen conform de eerder besproken voorkeur: de herkomst wordt via de metadata en verwijzingen op elk gegeven meegegeven, niet via losse inhoudelijke velden. Concreet: **Dossierhouder**: elk gegeven wordt toegeschreven aan de URA van het endpoint waar het is opgehaald. De raadpleger moet die toeschrijving behouden wanneer hij gegevens uit meerdere bronnen tot één overzicht samenvoegt. **Datum**: de registratiedatum in de bron, meegegeven via meta.lastUpdated; kent een zib een eigen vastleggingsdatum, dan mag dat element worden gebruikt. **Rol of persona**: waar de zib de registrerende zorgverlener referentieert (bijvoorbeeld via performer, recorder, author of asserter), wordt de rol meegegeven via PractitionerRole.code of een gelijkwaardig rol-element. Dit geldt alleen voor de zibs die hierin voorzien. Hoe deze herkomstgegevens vervolgens leesbaar in het totaaloverzicht worden getoond, is onderdeel van de weergave aan de raadplegende kant. Zie hier in het TO.
Datakwaliteitsissues die voortkomen uit het registratieproces (bijvoorbeeld ontbrekende SNOMED-codes) moeten zichtbaar worden gemaakt in de viewer, zonder ze op te lossen of te transformeren. ***Vraag:*** *Hoe wordt een datakwaliteitsissue technisch zichtbaar gemaakt in de viewer, op een manier die niet wordt geïnterpreteerd als een fout van de ToN of de viewer zelf?*	Omgaan met datakwaliteitsissues	De FO-eis bevat twee aspecten die uit elkaar gehaald moeten worden. Het eerste is hoe een datakwaliteitsissue in de raadplegende applicatie wordt getoond; dat is weergave en ligt aan de raadplegende kant. Het tweede is dat gegevens worden getoond zoals ontvangen, zonder ze op te lossen of weg te werken; dat is geen weergavekeuze maar een afspraak over de omgang met de data.

FO-eis	Vindplaats in FO	Antwoord TO
		In het TO zal dit duidelijker als eis beschreven worden, als het er nog niet staat, in lijn met wat het TO elders al vastlegt over het ongewijzigd doorgeven van gegevens.
Verschillen tussen zib-versies (2017, 2020, 2024) worden zoveel mogelijk aan de weergavezijde opgelost, niet aan de bronzijde. ***Vraag:*** *Welk technisch mechanisme lost verschillen tussen zib-versies op aan de weergavezijde?*	Omgaan met verschillende zib-versies	Het TO schrijft hiervoor geen technisch mechanisme voor. Het TO beperkt zich bewust tot de gegevensuitwisseling en niet tot de consolidatie en weergave; het oplossen van verschillen tussen zib-versies hoort daarmee bij de raadplegende kant, waar elke leverancier zijn eigen mechanisme voor mag gebruiken. De onderbouwing van de TO-groep is dat leveranciers dit nu al ieder op hun eigen manier doen, en dat het lastig zou zijn hier één algemene, aan iedereen opgelegde afspraak voor te maken. Dit sluit aan op het FO, dat het oplossen van versie verschillen zelf al aan de weergavezijde (de tonende applicatie) belegt en aangeeft dat dit bij inzage minder complex is dan bij overdracht, omdat het om weergave gaat en niet om verwerking. Het antwoord op de vraag welk mechanisme dit oplost, is daarmee: het TO wijst geen specifiek mechanisme aan; dit is per raadplegende applicatie verschillend.
Het actuele zorgnetwerk (hoofdbehandelaar, bereikbaarheid, functies) is een vereiste voor versie 1; in de praktijk worden hiervoor losse zibs gebruikt in plaats van de zib Zorgteam zelf. ***Vraag:*** *Hoe worden de losse zibs samengevoegd tot één samenhangend zorgnetwerkbeeld?*	Zorgnetwerk en cliëntnetwerk rondom de cliënt	De losse onderdelen kunnen worden opgevraagd; hoe dat technisch gebeurt, staat in volume 3 van het TO. Het samenvoegen van die losse zibs tot één samenhangend zorgnetwerkbeeld ligt bij de opvragende partij (de raadpleger). Het TO legt hiervoor geen regels vast: er is niet afgesproken hoe je de losse gegevens verplicht tot één beeld samenbrengt. Daar de zib Zorgteam wel degelijk ook in het toepasbare zibs staat, en valt onder de regel 'betrek er bij' is het logischer dat deze zib hiervoor gebruikt gaat worden. De TO-groep geeft aan dit gebruik van het Zorgteam nu niet technisch afdwingbaar (verplicht) gesteld kan worden, dan valt er te veel uit. Daarom is het vanuit FO-perspectief en vanuit de zorgorganisaties wenselijk om hier de komende tijd expliciet op te sturen, zodat dit wel gebruikt gaat worden.

Applicaties

FO-eis	Vindplaats in FO	Antwoord TO
Een applicatie is een bronsysteem als zij de actuele bronstatus van cliëntgegevens levert; datawarehouses en rapportagesystemen vallen buiten scope. ***Vraag:*** *Hoe wordt per aan te sluiten applicatie technisch vastgesteld of zij aan het criterium "actuele bronstatus" voldoet?*	Scope van te ontsluiten applicaties	Het TO stelt eisen aan identiteit en bevoegdheid, niet aan het criterium "actuele bronstatus". Een bronsysteem moet de cryptografisch ondertekende credentials aanbieden die in de Zorginzage-specificatie zijn omschreven; het zorgaanbieder-credential is ondertekend met een X509-servercertificaat (nu uitgegeven door het CIBG). Daarmee toont het systeem aan dat het namens de zorgaanbieder mag handelen en kan het zich als bron bekendmaken in de Discovery Service. De credentials tonen dus aan wie de bron is en dát die namens de zorgaanbieder mag optreden, maar zeggen niets over de vraag of de aangeboden gegevens de actuele bronstatus vertegenwoordigen. Het onderscheid dat het FO maakt — een bronsysteem levert de actuele bronstatus, datawarehouses en

FO-eis	Vindplaats in FO	Antwoord TO
		rapportagesystemen vallen buiten scope — wordt technisch niet vastgesteld of afgedwongen; het berust op de logische organisatorische afspraak en dat alleen systemen die aan dit criterium voldoen worden aangesloten.
Er komt een disclaimer bij de viewer over de afwegingen bij het tonen van data. ***Vraag:*** *Waar en hoe wordt deze disclaimer technisch getoond, en is dit eenmalig of bij elke sessie?*	Disclaimer viewer	Dit is geen onderdeel van het TO. De disclaimer is een element in de weergave aan de raadplegende kant en raakt de gegevensuitwisseling tussen bron en raadpleger niet. Het is een functionele eis aan de viewer, waarvan de technische uitwerking per raadplegende applicatie verschilt; het is daarmee geen technische afspraak die gezamenlijk kan worden afgedwongen. Dit is consistent met de lijn dat het TO zich beperkt tot de uitwisseling en weergavekeuzes bij de raadpleger laat. De concrete invulling van de FO-vraag — waar en hoe de disclaimer wordt getoond, en of dit eenmalig of per sessie gebeurt — ligt daarmee aan de FO-/weergavekant. Het FO benoemt dat er een disclaimer bij de viewer komt en dat deze ook in de werkinstructie of training wordt opgenomen, maar vult het waar, hoe en de frequentie nog niet in. Aandachtspunt: dit deel van de vraag is dus nog niet beantwoord, maar hoort thuis aan de FO-/raadplegende kant, niet in het TO.

ICT-infrastructuur

FO-eis	Vindplaats in FO	Antwoord TO
De concrete technische uitwerking van de aansluiting — hoe bronapplicaties en zorgplatforms hun Nuts-node inrichten, welke endpoints worden ontsloten, hoe de uitwisseling technisch verloopt — wordt expliciet bij het TO belegd. ***Vraag:*** *Biedt het TO een volledige technische uitwerking? Zo ja waar is die uitgewerkt vindbaar?*	ICT-infrastructuur	Ja, het TO biedt hiervoor een uitwerking, verspreid over twee samenhangende specificaties. Hoe Nuts werkt staat in de Nuts-documentatie; in het Zorginzage-bouwblok is vastgelegd welke credentials worden gebruikt en hoe de Nuts-node wordt geconfigureerd. Samen vormt dat de invulling van de aansluiting, en de specificatie omvat naast de Nuts-node ook de andere generieke functies. Concreet is dit vindbaar in de Zorginzage-IG en in de 360-IG, die daarop aanvult. Voor de Zorginzage-IG: authenticatie, adressering en autorisatie in volume 2a (https://nuts-foundation.github.io/nl-zorginzage-ig/vol2a.html). Registratie en pull in volume 2b (https://nuts-foundation.github.io/nl-zorginzage-ig/vol2b.html). De datasets in volume 3 (https://nuts-foundation.github.io/nl-zorginzage-ig/vol3.html). Voor de 360-IG: performance, audit trail en lineage in volume 2a (https://nuts-foundation.github.io/nl-360-ig/vol2a.html). De datasets en het Capability Statement in volume 3 (https://nuts-foundation.github.io/nl-360-ig/vol3.html). De algemene Nuts-documentatie staat op https://nuts-foundation.github.io/ en https://wiki.nuts.nl. Nuts schrijft in principe de specificaties zo dat de Nuts-tooling niet per se nodig is als je de specificaties gaat volgen. Dat geldt ook voor de Nuts-node. Nuts zal

FO-eis	Vindplaats in FO	Antwoord TO
		overzicht en het toepassen van de Nuts-tooling wel beter gaan positioneren en publiceren op desbetreffende sites. Denk ook aan een soort voorbeeld architectuurplaat naast het sequence diagram dat wel in het TO voorkomt.

Wet- en regelgeving

FO-eis	Vindplaats in FO	Antwoord TO
ToN 360° maakt gebruik van generieke functies voor lokalisatie, identificatie, authenticatie en autorisatie; zolang deze nog niet operationeel zijn, gelden tijdelijke onderlinge afspraken. ***Vraag:*** *Zie ook de vraag hierboven bij "Vertrouwen tussen deelnemende organisaties": hoe is de tijdelijke oplossing voor generieke functielokalisatie en adressering ingericht, en hoe wordt de overgangsperiode naar de landelijke voorziening technisch begeleid?*	Generieke functies	Het antwoord valt uiteen in twee sporen: adressering en lokalisatie. **Adressering**: nu wordt tijdelijk de Nuts Discovery Service gebruikt als gedeeld adresboek van de aangesloten organisaties; straks wordt dit de GF Adressering. **Lokalisatie**: nu geldt gericht bevragen; straks komt daar geïndexeerd bevragen via de NVI bij. De overgang wordt begeleid doordat de oude en de nieuwe voorziening een periode naast elkaar actief kunnen zijn; die overgangsperiode loopt naar verwachting tot en met begin 2027. Voor de volledige uitwerking, zie het hoofdstuk 'Adressering, gericht bevragen en toestemming'.

Informatiebeveiliging

FO-eis	Vindplaats in FO	Antwoord TO
ToN 360° regelt welke gegevens tussen organisaties worden uitgewisseld; de eigen organisatie blijft zelf verantwoordelijk voor de autorisatie van haar gebruikers binnen het eigen systeem. ***Vraag:*** *Hoe wordt deze knip tussen ketenautorisatie en organisatie-interne autorisatie technisch geborgd, zodat een organisatie haar eigen autorisatiebeleid onafhankelijk kan blijven inrichten?*	Autorisatie binnen de eigen organisatie	De knip is geborgd doordat in de keten alleen op organisatieniveau wordt geautoriseerd en niet op zorgverlener; de autorisatie van de eigen gebruikers richt elke organisatie zelf in binnen haar eigen systeem. Zie toelichting over de twee soorten autorisatie in het hoofdstuk 'Autorisatie, beleid en rego'.
Elk gebruik van ToN 360° wordt vastgelegd in een toegangslog met minimaal: raadpleger, cliënt, geraadpleegde gegevens, tijdstip, doel van de raadpleging en resultaat (geslaagd/geweigerd), conform NEN 7513. ***Vraag:*** *Hoe wordt dit toegangslog technisch vastgelegd, en welke partij is verantwoordelijk voor de realisatie ervan?*	Logging en inzage in gebruik	Het TO belegt de logging aan beide kanten conform NEN 7513: zowel de bronhouder als de raadplegende organisatie houdt een audit trail bij. De bronhouder logt minimaal elke access token-aanvraag (inclusief doel van de raadpleging en of toegang is verleend), elke introspectie en elke gegevensaanvraag, met per gebeurtenis het tijdstip, de opvragende organisatie (URA en facility type), de opvragende zorgverlener (identifier en rol), de betrokken cliënt en de opgevraagde resource(s). De raadplegende organisatie logt de lokale toegang: welke zorgverlener welke cliëntgegevens wanneer heeft ingezien. Volgens de TO-makers voert de Nuts-node een deel van deze logging al standaard uit; het is goed dit expliciet vast te leggen. Daarbij geldt dat alleen de

FO-eis	Vindplaats in FO	Antwoord TO
		toegang wordt gelogd en niet de klinische inhoud, en dat de cliënt bij voorkeur via het FHIR Patient-id wordt vastgelegd in plaats van via het BSN. Zie hiervoor TO hier.

Toelichtingen bij analyse FO en TO

Onderstaand een uitwerking van termen en verwijzingen die in de dekkingsmatrix staan van het FO en TO toepassing op Nuts 360° cliëntbeeld.

Termen in TO

Rollen van applicaties: bronhouder en raadpleger

In de usecase van ToN 360° cliëntbeeld worden gegevens niet centraal opgeslagen, maar bij de bron gehouden en op verzoek opgehaald en getoond. Een applicatie vervult in deze toepassing daarom één van twee rollen: die van bronhouder of die van raadpleger. Dezelfde applicatie kan in de praktijk beide rollen vervullen, afhankelijk van of zij gegevens levert of gegevens opvraagt, maar de rollen zijn functioneel verschillend.

Bronhouder

De bronhouder is de partij, en de bijbehorende applicatie, die de actuele gegevens over een cliënt houdt en op verzoek levert. Het gaat dan om de actuele status van die gegevens zoals die in die applicatie zijn vastgelegd. De bronhouder blijft eigenaar en beheerder van de eigen gegevens; deze worden niet gekopieerd naar een centrale plek.

Raadpleger

De raadpleger is de partij, en de bijbehorende applicatie, van waaruit een zorgverlener werkt en een vraag stelt over een bepaalde cliënt. Het is de kant die de gegevens opvraagt, samenbrengt en toont. De raadpleger is verantwoordelijk voor het consolideren van de opgehaalde gegevens tot één overzicht, voor de weergave daarvan en voor het toepassen van filters.

Samenhang tussen beide rollen

De twee applicatie-rollen vormen samen de kern van de uitwisseling ten behoeve van het 360° cliëntbeeld: de bronhouder houdt en levert de gegevens, de raadpleger vraagt ze op en toont ze. Bij een bevraging maakt de raadpleger zich kenbaar en toont aan dat hij bevoegd is; de bronhouder controleert dit en levert vervolgens de gevraagde gegevens. Omdat de gegevens bij de bron blijven en pas bij een concrete vraag worden opgehaald, ontstaat het 360°-beeld steeds opnieuw op het moment van raadplegen, samengesteld uit de gegevens van een of meer bronhouders tegelijk. Het onderscheid tussen beide rollen is bewust: het bepaalt welke partij waarvoor verantwoordelijk is, en voorkomt dat de bronhouder wordt verward met het systeem waarin het beeld uiteindelijk wordt bekeken.

Landelijke registers voor adressering en identiteit (LRZa)

Wat het FO vraagt - ToN 360° leunt voor het vinden van en vertrouwen in deelnemende organisaties op landelijke voorzieningen; zolang die er niet zijn, gelden tijdelijke afspraken. De vraag aan het TO is hoe de tijdelijke oplossing zich verhoudt tot de landelijke registers die eraan komen, en hoe het migratiepad eruitziet.

Antwoord TO – het LRZa is bijna gereed om als pilot mee te werken, CIBG is hier mee bezig. Komende tijd zal gebruikgemaakt worden van een tijdelijke discovery service (Ecare en Versneld verbinden), later gaat dat over naar GF Adressering.

Waarom en wat van verifiable credentials

Bij het uitwisselen van gegevens tussen organisaties en systemen is het essentieel dat partijen elkaar op een betrouwbare manier kunnen aantonen wie zij zijn en waartoe zij bevoegd zijn, zonder dat daarvoor telkens een centrale partij hoeft te worden geraadpleegd. Verifiable credentials (verifieerbare verklaring, of verifieerbare attestatie, zoals gebruikt in EU verband) maken dit mogelijk en vormen daarmee een van de bouwstenen van het stelsel. Hieronder wordt beschreven wat credentials en verifiable credentials zijn en hoe zij binnen het stelsel worden toegepast.

Credential

Een credential is een verklaring waarmee een persoon, organisatie of systeem bepaalde eigenschappen of bevoegdheden kan aantonen. In het dagelijks leven zijn een paspoort, een diploma of een lidmaatschapspas voorbeelden van credentials.

Een uitgevende partij verklaart iets over de houder, en een ontvangende partij vertrouwt op die verklaring. In digitale gegevensuitwisseling vervult een credential dezelfde rol, maar dan in een vorm die door systemen kan worden gelezen en gecontroleerd. Een digitaal credential kan bijvoorbeeld vastleggen dat een systeem namens een bepaalde zorgaanbieder mag handelen, of dat een gebruiker een bepaalde rol vervult.

Verifiable credentials

Een verifiable credential is een digitaal credential dat cryptografisch is ondertekend, zodat de ontvanger kan vaststellen wie de verklaring heeft uitgegeven en dat deze onderweg niet is gewijzigd. Het begrip is vastgelegd in een open standaard van het World Wide Web Consortium (W3C), zie https://www.w3.org/TR/vc-overview/.

In het model achter deze standaard zijn **drie rollen** te onderscheiden:

- de uitgever stelt de verklaring op en ondertekent deze
- de houder bewaart de verklaring en presenteert deze wanneer dat nodig is
- de verifiër controleert de handtekening en gaat na of de uitgever wordt vertrouwd.

De betrouwbaarheid berust dus niet op een centrale bevraging bij de uitgever tijdens het gebruik, maar op de **cryptografische handtekening** die aan de verklaring is meegegeven.

Kenmerkend voor een verifiable credential is verder dat de houder zelf bepaalt welke verklaring op welk moment wordt getoond, en dat elke verklaring afzonderlijk verifieerbaar is. Zo kan per situatie precies dat worden aangetoond wat nodig is, zonder dat de onderliggende bronnen telkens rechtstreeks hoeven te worden geraadpleegd.

Toepassing in ToN 360° cliëntbeeld

Binnen een gegevensuitwisselingsstelsel worden verifiable credentials gebruikt om organisaties en systemen op een controleerbare manier aan elkaar bekend te maken. Elke deelnemende organisatie beschikt daarvoor over een **digitale bewaarplaats** (portemonnee), ook wel een **wallet** genoemd, waarin de credentials van die organisatie worden bewaard. Per toepassing wordt afgesproken welke credentials nodig zijn en welke partij deze cryptografisch ondertekent. Op die manier is voor elke uitwisseling helder welke verklaringen worden verwacht en op welk vertrouwen die berusten.

In de praktijk gaat het doorgaans om een beperkte set credentials met elk een eigen functie. De ToN baseert zich op het bouwblok Zorginzage 2026 en daarin wordt gebruikt:

- een organisatie-credential dat aantoont om welke zorgaanbieder het gaat
- een roltype-credential dat aangeeft in welke hoedanigheid een systeem of gebruiker optreedt
- een medewerker (employee)-credential dat een individuele gebruiker koppelt aan de organisatie namens welke deze handelt

In de infrastructuur die ToN 360° cliëntbeeld gebruikt, is de Nuts-node te zien als de digitale bewaarplaats voor een organisatie (organisatie-wallet) waarin deze verifiable credentials worden bewaard. Per use case wordt afgesproken welke verifiable credentials worden gebruikt en wie deze cryptografisch ondertekent.

In de Zorginzage-specificatie is afgesproken een organisatie-, roltype- en medewerkercredential (Organisatie, Rol Type en Employee credential) te gebruiken; zie hiervoor deze pagina.

Autorisatie, beleid en rego

Twee soorten autorisaties

Autorisatie bepaalt of een geauthenticeerde raadpleger de gegevens die hij opvraagt daadwerkelijk mag inzien. Bij ToN 360° cliëntbeeld spelen daarbij **twee verschillende soorten** autorisatie, die los van elkaar staan en niet met elkaar verward moeten worden.

De eerste is de **autorisatie binnen de eigen organisatie,** die autorisatie bepaalt: welke gebruikers (in jouw organisatie), per rol of persona, mogen welke gegevens zien binnen je eigen applicatie en welke handelingen mogen zij in de eigen applicatie verrichten. Deze autorisatie richt de organisatie zelf in, doorgaans in de autorisatie-inrichting van het ECD, vaak in de vorm van een autorisatiematrix van rollen tegen rechten. Het FO en TO beleggen deze verantwoordelijkheid uitdrukkelijk bij de organisatie zelf.

De tweede is de **autorisatie in de keten**: mag een andere organisatie, de raadpleger, bepaalde gegevens bij jou als bronhouder ophalen. Deze beslissing wordt genomen en afgedwongen aan de bronkant. Het TO hanteert hiervoor een fijnmazig, policygebaseerd model in plaats van een rolgebaseerd model: of een verzoek toegang krijgt, hangt af van of het door de toegangsregels van de bron komt.

Die toegangsregels worden niet door elke organisatie afzonderlijk opgesteld, maar zijn per toepassing centraal en versiebeheerd vastgelegd in een gedeelde policy. Die policy is geschreven in de **taal rego**: een taal om beleidsregels als code vast te leggen, zodat een systeem ze automatisch en eenduidig kan uitvoeren en alle bronhouders van exact dezelfde regels uitgaan. De bronhoudende applicatie past deze regels bij elke bevraging toe via een zogenoemd policy enforcement point, en betrekt daarbij ook de controle op toestemming en eventueel de behandelrelatie. Een organisatie hoeft niet zelf een rego-interpreter in te bouwen, zolang haar oplossing precies dezelfde regels volgt als de vastgelegde rego-policy.

Het onderscheid tussen beide soorten autorisatie is belangrijk. Je beleid over wat je eigen medewerkers intern mogen zien, landt in de autorisatiematrix van je ECD. De regels over wat een andere organisatie bij jou mag ophalen, liggen niet in die matrix, maar in de gedeelde policy die aan de bron wordt afgedwongen. Wat wel bij de organisatie zelf blijft, is de keuze van het toestemmingsmechanisme (lokaal of via een voorziening, zoals bijvoorbeeld Mitz), het eventueel controleren van de behandelrelatie, en de interne autorisatie van de eigen gebruikers.

Waar deze toegangsregels bepalen wat is toegestaan, leggen de eisen hierna vast hoe een raadpleger zijn identiteit en bevoegdheid aantoont — de gegevens waarop de toegangsregels vervolgens worden toegepast. Het TO legt vast welke verifiable credentials een raadpleger daarbij moet aanleveren. Voor een deel bepaalt de organisatie de inhoud daarvan zelf: zij geeft het roltype- en het medewerkercredential zelf uit en verklaart daarmee haar eigen organisatietype en de betrokken medewerker. De organisatie-identiteit ligt daarentegen niet bij de organisatie zelf, maar is verankerd in een extern, gezaghebbend register. In de huidige afspraak wordt het roltype nog zelf uitgegeven; in het doelmodel van de generieke functies is voorzien dat een gezaghebbende partij deze verklaring uitgeeft.

Zie de autorisatie uitwerking in het TO hier.

Autorisatie bij bevraging: identiteit en bevoegdheid

Zie hiervoor paragraaf 3.4.5. Conformance (conformiteitseisen) in TO (zie hier).

Omdat ToN 360° cliëntbeeld gegevens bij de bron ophaalt en niet centraal opslaat, moet bij elke bevraging vaststaan **wie de gegevens opvraagt** en of die **daartoe bevoegd** is. De raadpleger toont dat aan op **drie niveaus**, waarbij elk niveau wordt vastgelegd in een verifieerbare verklaring (verifiable credential) die is gekoppeld aan de digitale identiteit van de Nuts-node (DID). De bronhouder controleert deze verklaringen voordat gegevens worden geleverd.

De drie niveaus zijn:

- de organisatie (welke zorgaanbieder vraagt op)
- het organisatietype (in welke hoedanigheid wordt opgevraagd)
- de individuele zorgverlener (wie handelt namens de organisatie)

Samen maken zij controleerbaar dat een bevraging afkomstig is van een bekende zorgaanbieder, van het juiste type, en door een herleidbare gebruiker.

Het TO legt deze eisen vast als conformiteitseisen: de regels waaraan een implementatie (een applicatie die deze regels toepast) moet voldoen om aan de standaard te voldoen en te mogen aansluiten. Het gewicht van elke regel blijkt uit het woord ‘moet’ (een harde eis; zonder naleving is aansluiting niet mogelijk), tegenover ‘zou moeten’ (een sterke aanbeveling) en ‘mag (optioneel).

De hieronder genoemde eisen zijn alle ‘moet-eisen, hier volgt slechts een vertaling[1]:

- Raadplegers moeten de identiteit van de zorgaanbieder (de **URA**) authenticeren met een X509-verklaring (X509Credential) die is afgeleid van een UZI-servercertificaat, conform Nuts RFC023.
- Raadplegers moeten een zelf-uitgegeven roltypecredential (**HealthcareProviderRoleTypeCredential**) tonen waarin het organisatietype of de organisatietypen zijn vastgelegd.
- Raadplegers moeten de identiteit van de zorgverlener organisatie-overstijgend koppelen (federeren) met een medewerkercredential (NutsEmployeeCredential).

De vertrouwensbasis loopt in de huidige situatie via het UZI-register: de X509-verklaring is afgeleid van een UZI-servercertificaat, en de URA is de unieke identificatie van de zorgaanbieder in dat register. Het UZI-register wordt beheerd door het CIBG. Dit legt vast hoe het vertrouwen tussen organisaties nu is geborgd; welke voorziening deze rol op termijn overneemt, is onderdeel van de openstaande punten bij lokalisatie en adressering.

[1] Dit is slechts een vertaling bedoeld voor verheldering, het TO is leidend en moet altijd gevolgd worden

Autorisatie op organisatieniveau versus zorgverlener-rol

Terminologie: ‘bron’ in het FO en in het TO

Het FO en het TO gebruiken de term ‘bron’ niet constant op dezelfde manier, al delen ze wel hetzelfde beeld. Het TO houdt de twee rollen strikt uit elkaar: de bronhouder houdt en levert de gegevens, de raadpleger vraagt ze op en toont ze.

Het FO hanteert de term bronhouder in principe exact hetzelfde, maar past het soms wat losser toe. In de laag Applicaties komt de definitie overeen met het TO (het bronsysteem is de vastlegger; de inziende applicatie is de raadpleger, en één applicatie kan beide rollen vervullen). In de proceslaag spreekt het FO over het ‘eigen bronsysteem’ van de zorgprofessional: de applicatie waarin de eigen gegevens vast worden gelegd en van waaruit de gebruiker werkt en het 360°-beeld oproept. Dat is hetzelfde ECD, maar dan in zijn rol als raadpleger.

Kort gezegd: hetzelfde ECD is bronhouder voor zijn eigen, origineel vastgelegde gegevens, en raadpleger op het moment dat het een 360°-beeld opvraagt en toont. Wat het FO in de proceslaag ‘eigen bronsysteem’ noemt, is op dat moment de raadpleger.

Autorisatie op organisatieniveau versus zorgverlener-rol

Met deze toelichting passen de keuzes van FO en TO bij elkaar. De bronhouder autoriseert op organisatieniveau: welke organisatie vraagt (de URA), van welk type (het roltype), of er toestemming is en eventueel of er een behandelrelatie bestaat. De rol van de individuele zorgverlener gebruikt de bronhouder niet in de toegangsbeslissing; die rol wordt wel meegestuurd (als niet-identificerend gegeven) en dient aan de bronkant vooral voor logging.

De filtering op rol of persona, of een verpleegkundige een ander beeld ziet dan een arts bijvoorbeeld, gebeurt in de raadplegende applicatie, oftewel het ECD van waaruit de zorgverlener werkt. Dit is ook wat het FO wil: het schrijft geen vaste set per persona of rol voor, maar belegt het inrichten van de autorisaties van de eigen gebruikers bij de raadplegende organisatie zelf (‘Autorisatie binnen de eigen organisatie’), en laat de persona-filtering plaatsvinden in de opvragende applicatie (‘Weergave en presentatie).

FO en TO leggen die rolfiltering dus op dezelfde plek; het FO noemt dat systeem in de proceslaag ‘eigen bronsysteem’ (in de rol van raadpleger), het TO noemt het consequent raadpleger.

Toepassen rol/ persona controle

Bij de bevraging worden twee verschillende dingen meegestuurd:

- Het eerste is de identiteit van de zorgverlener — wie het is — vastgelegd in het medewerkercredential; dit stelt het TO verplicht.
- Het tweede is de rol — arts of verpleegkundige — die als aanvullend, niet-identificerend kenmerk meekomt. Het TO dwingt dus de identiteit af, niet de rol.

De bronhouder ontvangt die rol wel, maar het gaat om een lokale rolcode van de raadplegende organisatie. Omdat er geen landelijke standaard voor zorgverlener-rollen bestaat, kan de bronhouder die rol niet eenduidig interpreteren en neemt hij op grond daarvan ook geen toegangsbeslissing; de bronhouder autoriseert op organisatieniveau. Het herkennen van de rol en het filteren van gegevens op grond daarvan gebeuren daarom in de raadplegende applicatie, op basis van de autorisatie die de gebruiker daar heeft. De meegestuurde identiteit en rol kunnen aan de bronkant wel worden vastgelegd voor audit logging.

Adressering, gericht bevragen en toestemming

De vraag vanuit het FO - *Het FO vraagt hoe de tijdelijke lijst van deelnemende zorgorganisaties technisch wordt beheerd en gedistribueerd naar de aangesloten leveranciers, zolang de generieke functies nog niet beschikbaar zijn.*

Het antwoord vanuit het TO - *Een tijdelijke Discovery Service*

Tijdelijke discovery service

Hiervoor wordt tijdelijk een Nuts Discovery Service ingezet. De Discovery Service werkt als een gedeeld adresboek van de aangesloten organisaties: organisaties registreren zich met hun identiteit en hun technische eindpunten, en een raadpleger kan daarin opzoeken bij welke bekende, vertrouwde organisaties cliëntgegevens kunnen worden opgehaald en waar die organisaties bereikbaar zijn. De organisaties die in dit adresboek staan, zouden dan vooralsnog de zorgorganisaties moeten zijn waarmee in de regionale samenwerking is afgesproken dat er wordt uitgewisseld. Dat moet goed worden afgestemd. Hiermee vervangt de Discovery Service de "vooraf afgesproken lijst" zoals dat in het FO staat door één beheerde, gedeelde voorziening, in plaats van een lijst die elke leverancier los in zijn software bijhoudt. Zodra de generieke functies beschikbaar zijn, wordt deze tijdelijke inrichting uitgefaseerd en vervangen door de landelijke voorzieningen.

Adressering en lokalisatie: twee verschillende vragen

Bij een bevraging spelen twee verschillende vragen. Adressering beantwoordt de vraag waar een bekende organisatie technisch bereikbaar is en of het een vertrouwde deelnemer is; dat is wat de Discovery Service oplost. Lokalisatie beantwoordt de andere vraag: welke organisaties hebben gegevens over een specifieke cliënt. Deze versie van de Zorginzage-specificatie kent nog geen lokalisatiemechanisme. De Discovery Service is dus een adresboek van bekende partijen, geen middel om te achterhalen wie gegevens over een cliënt heeft.

Gericht bevragen nu, geïndexeerd bevragen later

Omdat lokalisatie nog niet is ingevuld, geldt in deze versie gericht bevragen. In de Zorginzage-specificatie 2026 is afgesproken dat de adresgegevens uit de Discovery Service alleen voor een gerichte bevraging mogen worden gebruikt: je bevraagt uitsluitend de organisaties waarmee je in de regionale samenwerking afspraken hebt en die daarom in het adresboek staan. De raadpleger bepaalt dus vóór de bevraging welke organisaties hij wil benaderen.

Let op: in de discovery service staan **alle deelnemers aan ToN 360° cliëntbeeld**. Niet alleen degene waarmee jij als organisatie een regionale samenwerking hebt. Daarom mag je die gegevens niet gebruiken om te lokaliseren. Je moet in versie 1 van deze toepassing (als we nog geen gebruik maken van de generieke functies Adressering en Lokalisatie) gericht bevragen. Dus je moet elders zicht hebben op welke zorgorganisaties je mag bevragen. Het bepalen van wie je gaat bevragen doe je aan de hand van een vastgelegd zorgteam of dat je ergens hebt vastgelegd met wie je een samenwerking hebt. Vervolgens kan je in het adresboek (de discovery service) op zoek naar hoe je die organisaties kan bereiken.

In een volgende versie komt daar dan geïndexeerd bevragen bij, via de landelijke verwijsindex (NVI). Dat is de generieke functie voor lokalisatie, die dan wél per cliënt kan aangeven welke organisaties gegevens hebben. Die functie is nu nog niet beschikbaar; tot die tijd voorziet de tijdelijke Discovery Service in de behoefte, op basis van de regionale samenwerkingsafspraken.

Het zorgteam van de cliënt: nu geen rol in deze toepassing

Een zorgverlener kan van een cliënt horen waar deze nog meer zorg ontvangt. Die kennis kan een rol spelen in het contact tussen zorgverlener en cliënt. Het TO legt onder 3.3 vast dat een zorgteam gebruikt mag worden voor lokalisatie. Op die manier kan er een behandelrelatie worden vastgelegd. Het gestructureerd vastleggen van het zorgteam is een apart vraagstuk dat hier op dit moment buiten beschouwing blijft.

Toestemming

Toestemming staat hier los van en wordt niet in het TO opgelost. Toestemming is een grondslag die de bronhouder controleert voordat gegevens worden geleverd, en het mechanisme wordt aan de zorgorganisatie zelf overgelaten: expliciete toestemming die lokaal is geregistreerd, expliciete toestemming via Mitz, of een andere grondslag.

Elke organisatie regelt de toestemming dus zelf, zoals ook in FO staat.

Reactietijd en werkbaarheid

Het TO legt voor de reactietijd verwachtingen vast, geen afdwingbare servicelevels. Een los gegeven wordt bij voorkeur binnen 4 seconden geleverd en een complete dataset binnen 30 seconden. Deze tijden zijn nadrukkelijk verwachtingen: ze worden tijdens de uitwisseling technisch niet afgedwongen, en er is geen doorrekening of proof of concept aan ten grondslag gelegd. De TO-groep maakt zich geen zorgen over de capaciteit van de betrokken systemen, met uitzondering van Versneld verbinden.

In plaats van een harde garantie leunt het TO op een redenering en op een aantal kaders die de gewenste snelheid haalbaar maken. Elke zib is een losse bevraging, die de raadpleger parallel kan uitvoeren in plaats van na elkaar. Daardoor kunnen gegevens worden getoond op het moment dat ze binnenkomen, wat aansluit op de wens in het FO om met een progressieve opbouw te werken: eerst tonen wat er al is, de rest volgt. Omdat het uitsluitend om leesbevragingen gaat, kan de bronhouder zijn systeem horizontaal schaalbaar maken en zo meer gelijktijdige verzoeken aan.

Aan de kant van de raadpleger gelden aanvullende afspraken. Per afzonderlijk verzoek wordt een maximale reactietijd afgesproken, en de raadpleger wacht per verzoek maximaal 60 seconden op een antwoord (een timeout: daarna wordt niet langer gewacht). Kan een bronhouder een verzoek niet op tijd beantwoorden, dan moet hij toch een geldig, herkenbaar antwoord teruggeven — bijvoorbeeld een melding dat het niet gelukt is — en het verzoek niet zonder bericht laten doodlopen. Zo weet de raadpleger altijd waar hij aan toe is.

Daarnaast worden bronsystemen ontlast door opgehaalde gegevens tijdelijk in de raadplegende applicatie te bewaren, zodat niet telkens hetzelfde opnieuw bij de bron wordt opgevraagd. Binnen één werksessie van een gebruiker wordt hetzelfde gegeven daarom niet vaker dan eens per 5 minuten opnieuw opgehaald. Deze

tijdelijk bewaarde gegevens blijven niet langer bestaan dan de sessie waarin de zorgverlener werkt, en worden hoe dan ook binnen 15 minuten na het ophalen gewist. Ze mogen niet blijvend worden opgeslagen: de bronhouder blijft de gezaghebbende bron, en de raadpleger houdt dus geen eigen, blijvende kopie.

Volgorde waarin gegevens binnenkomen

Het TO schrijft voor dat zibs parallel worden opgevraagd en getoond zodra ze binnenkomen, maar legt geen volgorde of prioritering vast. Er is dus niet geborgd dat de voor het zorgproces meest relevante gegevens als eerste verschijnen. Bij progressieve weergave betekent dit dat de zorgverlener snel íéts ziet, maar niet noodzakelijk eerst het belangrijkste. De vraag die hierbij openstaat, is of het TO hierin een prioritering voorziet — bijvoorbeeld dat bepaalde kerngegevens als eerste geladen worden — of dat dit volledig aan de raadplegende applicatie wordt overgelaten. Dit hangt samen met de FO-eis over de reactietijd: niet alleen dát er snel iets verschijnt telt, maar ook of dat de gegevens zijn die de zorgverlener op dat moment nodig heeft.

Leveringsmogelijkheden (Capability Statement)

Voordat de raadpleger gegevens ophaalt, kan hij bij een bron opvragen welke gegevens die bron überhaupt kan leveren. Dat gebeurt met een zogenoemd **Capability Statement**: een standaardonderdeel van FHIR waarin een systeem opgeeft welke gegevenssoorten — welke zibs of resources — het ondersteunt. Zo weet de raadpleger vooraf welke onderdelen hij bij deze bron kan bevragen, en hoeft hij niet blind alles te proberen. De afspraak hierover is vastgelegd in volume 3 van het TO, zie hier.

Belangrijk is wat het Capability Statement niet zegt. Het geeft aan wat een bron kan leveren, niet wat er voor een specifieke cliënt daadwerkelijk is vastgelegd. Een zib kan dus in principe wel worden aangeboden, terwijl de betreffende zorgorganisatie die in de praktijk mogelijk niet vult. In dat geval wordt de bevraging wel uitgevoerd, maar komt er geen inhoud terug. Het Capability Statement zegt daarmee iets over de mogelijkheid, niet over de aanwezigheid van gegevens.

Dat laatste is over hoe het ontbreken van data wordt weergegeven is niet besproken in het TO. Dit weer in de dataconsolidatie hoek.

Horizontaal schaalbaar

Dit betekent dat de capaciteit van het bronsysteem kan worden vergroot door er meer servers naast elkaar bij te zetten, in plaats van één server zwaarder te maken. Als er meer vraag naar gegevens is, kan het bronsysteem zo worden ingericht dat er automatisch capaciteit wordt bijgeschakeld, en bij minder vraag weer afgeschaald. Dit is goed mogelijk bij het lezen van gegevens, zoals bij deze toepassing het geval is. Bij het schrijven van gegevens is het lastiger, omdat meerdere servers dan onderling consistent moeten blijven; bij alleen lezen speelt dat niet.

Parallel bevragen en het Capability Statement

De gegevens worden per zib opgevraagd. Omdat elke zib een afzonderlijke bevraging is, kan de raadpleger deze bevragingen gelijktijdig (parallel) uitvoeren in plaats van na elkaar. Daardoor komen de gegevens sneller binnen en kunnen ze worden getoond zodra ze beschikbaar zijn.

De raadpleger begint niet blind met het opvragen van alle mogelijke zibs. Elke bronhouder publiceert voor zijn FHIR-server een Capability Statement: een overzicht van wat die server ondersteunt, oftewel welke zibs die aanbieder kan leveren. De raadpleger mag alleen bevragingen sturen die passen binnen dat Capability Statement. Zo is vooraf bekend welke onderdelen bij welke aanbieder opgevraagd kunnen worden, en wordt gericht bevraagd op wat een aanbieder daadwerkelijk biedt. De afspraak hierover is vastgelegd in volume 3 van het TO hier.

Belangrijk is het onderscheid tussen wat een aanbieder biedt en wat er feitelijk aan gegevens is. Het Capability Statement zegt welke zibs een bron ondersteunt, niet of daar voor een specifieke cliënt ook gegevens in zitten. De bevraging gaat bovendien primair op FHIR-profiel: het bronsysteem moet zijn gegevens hebben voorzien van het juiste profielkenmerk.

Het is een eis vanuit het TO dat het bron systeem de gegevens conform het FHIR-profiel behorende bij de zib oplevert. Andere gegevens die wel van het FHIR-resource-type zijn, maar niet aan het profiel voldoen, komen niet mee. Het is niet mogelijk om van die gegevens te identificeren of ze wel aan de informatiestandaard van Nictiz voldoen.