Reactie op VWS-memo "Harmonisatie van authenticatie en autorisatie"

Van: Kring Techniek, Stichting Nuts | **Status:** analyse op eigen titel, zie paragraaf 1.1

1. Inleiding

Het VWS-memo kiest een federatief vertrouwensmodel: iedere zorgaanbieder is zelf verantwoordelijk voor de eigen medewerkers en systemen, en over de organisatiegrens heen wordt alleen de identiteit van de organisatie vastgesteld, geborgd op de applicatielaag en niet in de netwerkverbinding. Die richting onderschrijven wij; het is ook de richting van het authenticatiemodel in de Nuts-community. Het verschil zit in de invulling: het memo laat wezenlijke verklaringen oncontroleerbaar. Wie er namens de organisatie handelt, met welk doel, en onder welke afspraken en delegatie kan een ontvanger niet in de transactie zelf vaststellen. In het Nuts-model zijn dit controleerbare, getekende verklaringen, zoveel mogelijk uit de authentieke bron.

Deze reactie doet drie dingen. Ten eerste analyseren wij het voorstel juridisch (hoofdstuk 2): het behandelt een aantal open termen uit de wet en hoe die door NEN-normen worden ingevuld. Met name NEN 7512 is hier relevant: die vereist per uitwisseling een kader, met een risicoafweging door een kaderstellende partij. Het memo noemt deze normen wel, maar dit kader niet. Daardoor doet het memo uitspraken die aan de kaderstellende partijen zijn, leunt het op een vertrouwensmodel waarvan de dragers nog ontbreken, en projecteert het conclusies over gericht verzenden op use cases waar die niet gelden.
Ten tweede analyseren wij het voorstel technisch (hoofdstuk 3): een aantal ontwerpvragen is onbeantwoord en een aantal waarborgen die het memo claimt, worden door de gekozen techniek niet waargemaakt. Ten derde stellen wij een plateau-aanpak voor (hoofdstuk 4): positioneer het memo als een eerste plateau met expliciet benoemde beperkingen en randvoorwaarden, binnen een architectuurpad naar een gezamenlijke SOLL. Dat maakt de beperkingen bespreekbaar als architectuurkeuze in plaats van als kritiek, en maakt bestaande oplossingen zoals Nuts en AORTA plotbaar op datzelfde pad.

Voor de weging van deze reactie: sommige dingen zijn blokkerend, anderen kunnen parallel lopen. Blokkerend zijn drie punten: een keuze wie de ondertekensleutel beheert en hoe die aan de organisatie-identiteit is gebonden (3.1), bescherming van het uitwisselingsdoel tegen wijziging onderweg, of expliciete acceptatie van dat risico in de risicoafweging (3.2), en het kader per uitwisseling dat NEN 7512 vereist (2.1). Al het overige, waaronder de DPIA-handreiking, de impactanalyse en het gemeenschappelijke autorisatiecontract, kan parallel aan invoering worden opgepakt. Waar het memo gaten laat, bieden wij bestaande, werkende invullingen aan.

1.1 Status van deze reactie en het vervolg

Deze analyse is opgesteld door de Nuts Kring Techniek als technisch geweten van de Nuts-community. De reactietermijn bood helaas geen ruimte voor afstemming met de deelnemers en haar toepassingen, noch voor een gedragen impactanalyse.

Daarnaast zien wij vier stappen die nog moeten worden doorlopen voordat dit memo de status kan krijgen die het nodig heeft om in de toepassingen te worden opgenomen. Wij beschouwen deze consultatie als een technische toets; deze ontbrekende stappen vragen een eigen ronde met de betrokken partijen.

- **Een risicoafweging per uitwisseling** (NEN 7512 hoofdstuk 5), vastgesteld door de kaderstellende partijen van de BgZ respectievelijk de eOverdracht. Zonder dit document kan geen zorgaanbieder toetsen of deelname past bij zijn eigen risicobereidheid, wat de norm wel van hem vraagt (zie 2.1).
- **Een onderzoek naar de zekerheden van het gebruikte identificatiestelsel** (NEN 7512 6.1.3), met de verplichting dit aan de deelnemende partijen te verstrekken.
- **Een DPIA-handreiking.** De DPIA zelf is aan iedere verwerkingsverantwoordelijke afzonderlijk; een handreiking voorkomt dat honderden zorgaanbieders dezelfde analyse opnieuw doen. Het memo moet dan wel de keuzes openlaten die in die DPIA thuishoren.
- **Een impactanalyse op het veld en de bestaande implementaties.** In het Wegiz-EHDS-traject is impactanalyse voorafgaand aan vaststelling inmiddels de gangbare werkwijze; wij stellen voor die hier ook te volgen. Wij merken daarbij op dat ook aan onze kant zo'n gedragen analyse nog ontbreekt (zie hierboven).

Daarnaast blijven onze procesvragen staan: waar landt dit memo besluitvormend en wat is de status van het concept na verwerking van de reacties; hoe verhoudt het memo zich tot de design authority en de bestaande architectuurgremia, en wie stelt het uiteindelijk vast; en komt er een nieuwe reviewronde op de verwerkte versie, met een termijn die impactanalyse en community-afstemming toelaat?

2. Juridische analyse

Vooraf: wij zijn geen juristen en dit hoofdstuk is geschreven vanuit een architectuurperspectief. De rolverdeling en het federatieve model in het juridisch kader van het memo onderschrijven wij. Onze vragen gaan over iets anders. De wet werkt met open termen, zoals "passende maatregelen". Wat dat in de praktijk betekent wordt met NEN normen ingevuld. Generiek, via de Wabvpz, zijn dat NEN 7510, 7512 en 7513 en specifiek voor de BgZ en de eOverdracht zijn dat NEN 7540 respectievelijk NEN 7545. Het memo noemt de eerste drie als mechanisme dat vertrouwen afdwingt, maar gebruikt geen van de normen als bron van eisen; NEN 7540 en 7545 komen niet voor. Bij het nalezen kwamen wij drie punten tegen waar dat mogelijk tot een probleem leidt.

2.1 Wie stelt het kader vast?

Afspraken over uitwisseling worden op drie lagen gemaakt. Op stelselniveau maakt VWS als stelselhouder zorgbrede afspraken over generieke standaarden, zoals eerder het FHIR-besluit. Op uitwisselingsniveau geldt het kader van NEN 7512, en de norm is daar expliciet over: een vertrouwensbasis geldt voor een specifieke uitwisseling, niet generiek. Er is dus een kader voor de BgZ en een kader voor de eOverdracht nodig, elk met een gedocumenteerde risicoafweging, een onderzoek naar het identificatiestelsel en concrete toetredingseisen. Op infrastructuurniveau leveren afsprakenstelsels bouwstenen waarnaar zo'n kader kan verwijzen.

Het Twiin Afsprakenstelsel is daarmee de misschien een voor de hand liggende kandidaat om deze kaderrol voor de BgZ te vervullen, maar vervult die vandaag niet. Het stelsel verplicht deelnemers tot naleving van NEN 7510/7512/7513 en toetst dat bij validatie, maar dat is iets anders dan wat de norm van kaderstellende partijen vraagt: een vastgelegde risicoafweging per uitwisseling (hoofdstuk 5 van de norm) en een onderzoek naar het identificatiestelsel dat aan de communicatiepartijen wordt verstrekt (6.1.3). Voor de eOverdracht geldt bovendien dat deze niet in het Twiin Afsprakenstelsel is opgenomen en in de praktijk deels over andere infrastructuur loopt, zodat een deel van de communicatiepartijen tot geen enkel kader is toegetreden.

Harmonisatie van authenticatie en autorisatie hoort op de eerste laag, en daar is dit memo op zijn plaats. De conclusie van het memo doet echter een uitspraak op de tweede: dat de risico's vooraf via toetredingseisen, doorlopend via toezicht en achteraf via logging en aansprakelijkheid zijn afgedekt, is de uitkomst van een risicoafweging die per uitwisseling nog gemaakt moet worden. Die afweging is niet vrijblijvend. Zij bepaalt onder meer hoeveel beveiligingslagen vereist zijn: bij de hoogste risicoklassen drie (veilig netwerk, versleuteld bericht, versleuteld kanaal), waar het voorstel er nu een levert. En zij is de voorwaarde voor een plicht van iedere deelnemer afzonderlijk: elke zorgaanbieder moet zelf toetsen of de gemaakte afweging past bij zijn risicobereidheid, en mag zonder geldig kader niet uitwisselen.

Onze vraag: klopt het dat dit memo een basis op stelselniveau beschrijft en dat de kaders per uitwisseling nog volgen? Zo ja, wie stelt die op, en worden zorgaanbieders en standaardhouders daarbij betrokken?

2.2 Het vertrouwensmodel mist zijn eigen dragers

Het memo dekt de risico's bewust buiten de transactie af: vooraf via toetredingseisen, doorlopend via audits en toezicht, achteraf via logging en aansprakelijkheid. Dat is een legitiem model, het is ook het model van NEN 7512. Maar elk van de drie pijlers heeft een mechanisme nodig, en dat ontbreekt driemaal.

Vooraf. Deelname is voor de bronhouder niet vaststelbaar. Het enige dat de transactie bewijst is een geldig UZI-certificaat: de tegenpartij is een geregistreerde zorgaanbieder. Niet dat zij tot het

kader is toegetreden, niet dat zij NEN 7510 naleeft. NEN 7512 verplicht partijen juist om voorafgaand aan elke uitwisseling te controleren of het kader geldig is. Er is geen register, lijst of verklaring waarmee dat kan.

Achteraf. De aansprakelijkheid is niet toerekenbaar. Het memo stelt dat het doel meereist als verklaring van de ontvangende organisatie, "die daarvoor verantwoordelijk en aansprakelijk is". Maar die verklaring is niet door de ontvangende organisatie ondertekend: zij is alleen door transportbeveiliging beschermd en wijzigbaar door iedere partij die de verbinding termineert (zie 3.2). Aansprakelijkheid achteraf vereist dat achteraf bewijsbaar is wie wat verklaarde. Hetzelfde geldt binnen de organisatiegrens: bij een sleutel die bij een of meer dienstverleners in beheer is, is niet vast te stellen welke partij feitelijk handelde (zie 3.1).

Doorlopend. Toezicht veronderstelt een maatstaf, en dat is het kader uit 2.1, dat er nog niet is.

Wij vragen VWS per pijler het mechanisme te benoemen: een vaststelbaar toetredingsfeit, een door de ontvangende organisatie getekende verklaring, en het kader per uitwisseling. Geen van de drie vraagt een centrale voorziening; hoofdstukken 3 en 4 doen hiervoor federatieve voorstellen.

2.3 Gericht is de grens, en de transactie legt gerichtheid niet vast

De grondslag van het memo rust op het gerichte karakter van de uitwisseling, in de normen "gericht beschikbaar stellen" genoemd: er is een verwijzing of overdracht, dus een bekende ontvanger en een bekende patiënt, en daaruit volgt de veronderstelde toestemming (WGBO art. 7:457). Die redenering onderschrijven wij. Maar van de drie elementen waar dit op rust, legt de transactie er maar één vast. De ontvangende organisatie is cryptografisch gebonden; de patiënt en de verwijzing reizen niet mee. Voor de bron is een verzoek dat bij een verwijzing hoort niet te onderscheiden van ieder ander verzoek van dezelfde organisatie met het doel "behandeling". NEN 7540 vraagt van de bronhouder nu juist dat die zekerstelt dat de ontvanger een behandelrelatie met de patiënt heeft of krijgt, en daarvoor een geïmplementeerd autorisatieprotocol gebruikt. Die toets is in de voorgestelde flow niet uitvoerbaar, en daarmee valt in de logging ook niets te vermelden bij het veld dat NEN 7513 daarvoor kent.

Het antwoord kan zijn dat de binding in het voorafgaande proces zit, bij de verwijzing of overdracht zelf. Voor gericht verzenden is dat verdedigbaar. Maar dan is het een randvoorwaarde waar de architectuur op rust, en die moet expliciet zijn (zie hoofdstuk 4). Het memo doet het omgekeerde: paragraaf 7 stelt dat voor een bevraging (ongericht beschikbaar stellen) "hetzelfde model past" en dat een extra attribuut volstaat. Bij bevraging is er echter geen voorafgaand proces dat de binding levert; de veronderstelde toestemming, de niet-vastgelegde behandelrelatie en het achterwege laten van de toestemmingscontrole, de drie juridische conclusies van het memo, vervallen daar alle drie. Het memo erkent dat zelf half, waar het schrijft dat de behandelrelatie dan waarschijnlijk een aanvullende maatregel en een eigen analyse vraagt.

Wij vragen VWS de grens van gericht beschikbaar stellen expliciet te maken en de suggestie te schrappen dat ongericht beschikbaar stellen met een extra attribuut binnen bereik ligt: daarvoor zijn een eigen kader, een eigen risicoafweging en een toetsbare behandelrelatie en/of toestemming nodig.

3. Technische analyse

De juridische analyse ging over wat er geregeld moet zijn; dit hoofdstuk gaat over wat de gekozen techniek waarmaakt. Het memo claimt dat de organisatie-identiteit cryptografisch verifieerbaar is op elk punt in de keten, dat systemen en handelingen herleidbaar zijn en dat de techniek voorbereid is op andere use cases. Wij lopen die claims na aan de hand van de aangehaalde standaarden.

3.1 De relatie tussen sleutelmateriaal en URA

In het memo wordt de client-assertion getekend met "de private sleutel behorend bij het UZI-certificaat" maar maar wordt gevalideerd via het "het JWKS-endpoint van die organisatie". Er is niet gespecificeerd hoe de binding tussen het endpoint en URA tot stand komt. Dit is een gat in de specificatie en raakt aan een diepere discussie over het beoogde gebruik van sleutelmateriaal en hoe een sleutel een bewijs is voor bezit van een URA (proof of possession). Zonder die binding is de claim "de organisatie-identiteit (URA) is cryptografisch verifieerbaar" niet waargemaakt.

Er liggen hier twee samenhangende, onbeantwoorde ontwerpvragen:
Sleutelhouderschap: (a) de leveranciers delen de private sleutel van het UZI-certificaat van de zorgaanbieder, of (b) er wordt per leverancier per zorgaanbieder een eigen UZI-certificaat uitgegeven of (c) elke leverancier heeft een eigen private key, los van het UZI-certificaat.
Validatie van de binding sleutel-URA: (x) x5c-inbedding van de UZI-keten in de JWT-header, gevalideerd tegen de UZI-root, of (y) een register dat URA aan het leveranciers JWKS-endpoint koppelt, of (z) een (bijv. met het UZI certificaat) ondertekend bewijs van delegatie aan de leverancier.

De assen combineren op de volgende manier:

	A: Gedeeld UZI cert	B: Eigen UZI cert	C: Eigen sleutel
X: Embedded chain (x5c)	mogelijk; rotatie/intrekken = certuitgifte, raakt alle leveranciers tegelijk	mogelijk; rotatie = certuitgifte per leverancier	n.v.t. (keten bewijst geen URA)
Y: register + JWKS	overbodig (cert bewijst URA al)	overbodig	mogelijk; vertrouwen rust volledig op

			register
Z: Delegatieverklaring + leveranciers certificaat	overbodig	overbodig	Rotatie via leveranciers certificaat, UZI sleutel offline

Sleutelrotatie

FAPI 2.0 par. 5.4.2 adviseert JWKS vanwege sleutelrotatie (par. 6.8) en ontraadt alleen x5u en jku; over x5c zegt het niets. Let wel: als de sleutel certificaatgebonden blijft, is sleutelrotatie feitelijk certificaatuitgifte via het UZI-register, en vervalt het rotatievoordeel waarvoor FAPI JWKS aanbeveelt. Het memo moet op beide vragen kiezen en beantwoordt er geen van beide.

Sleutelbeheer

Met welke sleutel wordt ondertekend (zowel het tokenverzoek als het token zelf) heeft ook gevolgen voor wie de sleutel op welke manier beschikbaar moet hebben. Bij gebruik van de private sleutel van het UZI-certificaat moeten zowel de clients als de AS'en over deze sleutel beschikken. Een multi-tenant AS van een leverancier of infrastructuurpartij houdt dan de UZI-private keys van al zijn klanten, terwijl het token-endpoint per definitie internet-facing is: de meest blootgestelde component heeft toegang tot alle organisatie-identiteiten, en compromittering betekent mogelijk stelselbrede impersonatie van al die organisaties. Verwacht ook organisatorische weerstand: een infrastructuurpartij als VZVZ (LSP) zal deze sleutels niet in beheer willen nemen, omdat dit een neutrale infrastructuurrol verandert in sleutelbeheerder met bijbehorende NEN 7512-aansprakelijkheid.

Naast het technische argument delen we graag onze eigen organisatorische ervaring: het beheer van een enkel certificaat is voor veel zorginstellingen al een hoge drempel, laat staan een certificaat per leverancier.

Delegatie van taken naar de leverancier

In het memo is de delegatie impliciet: wie de sleutel beheert, handelt als de organisatie, zonder dat dit zichtbaar of begrensd is. De normen vragen juist dat delegatie kenbaar is: NEN 7512, 7540 en 7545 eisen dat contracten met derde partijen voor de uitwisselingspartijen opvraagbaar zijn en dat bekend is wie het beheer voert. Ook vanuit sleutelbeheer is het delen van certificaten tussen leveranciers onwenselijk.

Vanuit technisch en security-perspectief zou Nuts de combinatie van eigen leverancierssleutels met een delegatieverklaring (C+Z) aanbevelen. De leveranciers hebben eigen certificaten met daarin bijvoorbeeld een KVK-nummer. De zorginstelling heeft een UZI-certificaat onder eigen beheer en ondertekent daarmee een delegatieverklaring (bijvoorbeeld een JWS) met daarin de KVK van de leverancier, met de certificaatketen embedded via de x5c-header. De leveranciers ondertekenen de tokens en tokenverzoeken zelf met hun eigen leverancierscertificaat en

voegen de delegatieverklaring toe. De verklaring kan daarnaast een referentie aan het onderliggende contract bevatten, waarmee ook de opvraagbaarheidseis uit de normen is ingevuld. De vertrouwensketen blijft daarbij intact (UZI-root, UZI-certificaat, delegatieverklaring, leverancierscertificaat, handtekening): het bewijs van URA-bezit verschuift van de tokenhandtekening naar de verklaring, zonder aan kracht te verliezen.

Bij verklaringen moet rekening worden gehouden met houdbaarheid en intrekbaarheid. Intrekken vereist een distributiemechanisme voor de intrekking. Een korte houdbaarheid vraagt administratieve handelingen voor heruitgifte. Het beëindigen van de relatie is dan simpelweg stoppen met hertekenen. Compromittering van de leverancier zelf is afgedekt via intrekking van het leverancierscertificaat. Hier staat tegenover dat de certificaatgebonden opties (A en B) intrekking al geregeld hebben via het UZI-register (OCSP/CRL), zoals de flow in het memo ook toont; C+Z levert daar iets in en verdient dat terug met offline UZI-sleutels en vrije sleutelrotatie.

3.2 authorization_details is niet getekend

Het RAR-object is een losse POST-parameter in het tokenverzoek. De private_key_jwt client-assertion tekent alleen de eigen claims (iss, sub, aud, jti, exp), niet de overige requestparameters (RFC 7523 par. 2.2, RFC 9396 par. 6.1). Het doel van de uitwisseling is dus alleen hop-by-hop door TLS beschermd: per verbindingssegment, waarbij elke intermediair die TLS termineert de plaintext ziet en kan wijzigen. Ook DPoP mitigeert dit niet; de DPoP-proof tekent alleen HTTP-methode en URI (RFC 9449), niet de request body. Het memo motiveert de scheiding van transport- en applicatievertrouwen (GISA A44) juist met het argument dat intermediairs de transportverbinding termineren. Precies die intermediairs kunnen purpose_of_use ongemerkt wijzigen, waarna de AS de gewijzigde waarde in een getekend access token echoot en daarmee legitimeert. De organisatie-identiteit is berichtniveau-beveiligd, de autorisatiecontext niet: inconsistent binnen de eigen logica van het memo, en direct de pijler "achteraf" uit 2.2, want de verklaring waarvoor de ontvangende organisatie aansprakelijk zou zijn, is niet door haar getekend. FAPI 2.0 basis tekent tokenverzoeken niet; daarvoor bestaat FAPI 2.0 Message Signing, of, in het Nuts-model, opname van de claims in de getekende VP van de authorization grant.

3.3 De OAuth-client heeft geen eigen identiteit

In de flow geldt iss = sub = URA: de client valt samen met de organisatie. Er is geen onderscheiden systeem-, deployment- of leveranciersidentiteit. Gevolgen: alle systemen van een organisatie delen feitelijk een sleutel(identiteit), compromittering van een systeem raakt de organisatie-identiteit overal (strijdig met de single-purpose-key aanbeveling in FAPI 2.0 par. 6.8); least privilege per systeem is voor de AS onmogelijk (FAPI 2.0 par. 5.3.2.1 punt 14); en de herleidbaarheid op systeemniveau die het memo zelf claimt, is voor de verifier onzichtbaar (zie 3.8 voor de loggingkant). RFC 7523 scheidt client-authenticatie expliciet van de authorization grant; de Nuts GF gebruikt die scheiding zodat de client (leverancier of systeem) een eigen, verifieerbare identiteit heeft naast de organisatie namens wie hij optreedt.

3.4 Self-asserted claims waar authentieke bronnen bestaan

purpose_of_use als eigen verklaring is verdedigbaar (het is inherent een intentieverklaring). Het organisatietype is dat niet: het is een feit met een authentieke bron en het stuurt in de bevraging-usecase de Mitz-toestemmingsbeslissing. Een onjuist self-asserted type verandert een toestemmingsuitkomst. Het memo stelt expliciet dat tekenen door een authentieke bron onnodig is; dat bestrijden wij voor toestemmingsrelevante claims. Verifieerbaarheid van dit soort claims is wat plateau 2 toevoegt (hoofdstuk 4). Daarnaast is de plaatsing een categoriefout: RAR beschrijft de gevraagde autorisatie (doel, resources, acties), terwijl subject_organisation_type een identiteitsclaim over de aanvrager is. Die hoort in de authenticatielaag (client assertion of grant), maar de gekozen client-credentials flow biedt daar geen plek voor, waardoor de identiteitsclaim in de enige ongetekende component van het verzoek belandt en de problemen uit 3.2 en deze paragraaf op precies dit veld samenkomen. In het VC-model is dit triviaal: de bron geeft het type uit als credential, de verifier valideert zonder de bron online te bevragen, en de claim reist in het getekende deel van het verzoek (de RFC 7523 grant).

3.5 URA afhankelijkheid en niet-zorgaanbieders buiten bereik

Het memo verankert de URA als enige organisatie-identificatie. Voor BgZ en eOverdracht is dat werkbaar; deelname van niet-URA-partijen (PGO, onderzoek, sociaal domein) is een plateau-vraagstuk (zie de SOLL in hoofdstuk 4). De toets voor plateau 1 is alleen dat deze keuze de latere verbreding niet blokkeert; identifier-agnostische claims houden dat pad open.

3.6 Het autorisatiedeel is leeg

Het memo harmoniseert authenticatie en autorisatie, maar het autorisatiedeel bestaat uit een claim (purpose_of_use) en een besluit ("o.b.v. purpose_of_use=TREAT"). Alles wat een autorisatiebesluit inhoud geeft ontbreekt: waartoe (scope), voor wie (patiënt), waarop gebaseerd (verwijzing of aanmelding). Dat de werkgroepen per uitwisseling dit invullen is een verdedigbare taakverdeling, maar dan moet dit memo het gemeenschappelijke contract definiëren, anders divergeren de uitwisselingen precies op het punt dat het memo moest harmoniseren. De juridische analyse levert de inhoudsopgave al (2.3): een verplichte patiëntreferentie en een referentie aan de verwijzing of aanmelding, naast doel en scope, in hetzelfde RAR-type voor beide uitwisselingen. RAR is uitbreidbaar, dus dit past in de eigen techniekkeuze van het memo. Het maakt bovendien het autorisatieprotocol-veld en het verplichte cliëntobject in de logging (NEN 7513) vulbaar. Op plateau 2 worden deze casusclaims getekend, in hetzelfde mechanisme als de delegatie in 3.1.

3.7 Logging: correlatie en inzage

De keten van organisatieloggingen waar het memo op leunt vraagt twee kleine toevoegingen. Een correlatiekenmerk dat met de uitwisseling meereist, waarvoor NEN 7513 traceparent en

traceresponse al kent, zodat de gebeurtenissen bij bron en ontvanger aan elkaar te leggen zijn. En de afspraak over wederzijdse inzage in logging met een termijn, die NEN 7512 vereist; dat is een kaderpunt (2.1), geen techniek.

4. Voorstel: een plateau-aanpak

Het memo presenteert een eindoplossing en claimt terloops dat die "voorbereid is op uitbreiding naar andere use cases". Wij stellen voor dit om te draaien: definieer een SOLL met plateaus ernaartoe. Een plateau is een set requirements, geen oplossing. Oplossingen voldoen aan een plateau en hebben een status (landelijk of niet). Welk plateau vereist is, volgt uit het communicatiepatroon van de zorgtoepassing (gericht of ongericht beschikbaar stellen), niet uit de voorkeur van individuele partijen. Dit hoofdstuk schetst de richting en de uitwerking is een gezamenlijk vervolgtraject.

SOLL

Elke vertrouwensbeslissing rust op verifieerbare verklaringen: identiteit van organisatie en systeem, organisatietype, leveranciersdelegatie en deelname aan het kader van de uitwisseling reizen als getekende claims van authentieke bronnen mee in de transactie, in de attestatieformaten die onder eIDAS 2.0 (QEAA, EUDI-wallets) Europees gestandaardiseerd worden. Elke claim heeft een natuurlijke uitgever: het CIBG attesteert de URA, de kaderstellende partij het deelnamebewijs. Of een partij deel uitmaakt van een (sub)stelsel is daarmee geen papieren feit meer, maar in de transactie controleerbaar. Deelname is niet beperkt tot URA-houders.

Plateau 1: organisatie-authenticatie met self-asserted context

Voldoende voor gericht administratief verzenden (PUSH), na bijvoorbeeld een verwijzing of bij overdracht van zorg. Het VWS-memo is de landelijk voorgestelde oplossing op dit plateau, mits de openstaande vragen uit hoofdstuk 3 worden beantwoord en de beperkingen expliciet worden benoemd: geen integriteitsbescherming van de autorisatiecontext, geen zichtbare systemen of leveranciers, self-asserted claims, URA verplicht (3.1 t/m 3.7). Voordeel: uitsluitend commodity-techniek.

Randvoorwaarde bij plateau 1. Dit plateau geldt uitsluitend voor uitwisselingen waarbij de bronhouder per geval, voorafgaand aan de transactie en aantoonbaar, de ontvanger en de patiënt heeft bepaald. Bevraging zonder voorafgaande verwijzing of aanmelding valt daar per definitie buiten (zie 2.3). Binnen de randvoorwaarde moet de oplossing aan een compacte set eisen voldoen.

Aan de transactie: de identiteit van beide organisaties is eenduidig en gedurende de bewaartermijn herleidbaar vastgesteld; doel en adressering zijn op berichtniveau beschermd

tegen wijziging door intermediairs; de transactie is herleidbaar naar de casus (patiënt en verwijzing of aanmelding); de velden voor logging conform NEN 7513 zijn leverbaar; en de techniek blokkeert noch een extra beveiligingslaag (zie 2.1) noch het migratiepad naar plateau 2.

Aan het kader, te leveren voor ingebruikname: de risicoafweging en het identificatiestelsel-onderzoek uit hoofdstuk 1; een kaderdocument met scope, geldigheidsduur en ondertekening per partij; toetredingseisen die op het moment van uitwisseling vaststelbaar zijn; een afspraak over wederzijdse inzage in logging met termijn; en kenbaarheid van delegatie aan dienstverleners (contract opvraagbaar, beheerder bekend).

Getoetst aan deze set voldoet het voorstel op de transactie-eisen deels (organisatie-identiteit wel, casusbinding en integriteit van de context niet, zie hoofdstuk 3) en zijn de kader-eisen alle nog niet geleverd. Dat laatste is met afspraken te dichten en is dus geen bezwaar tegen de techniek, mits het gebeurt.

De kader-eisen worden in de praktijk ingevuld met registers: een vastgelegde toetreding, een vindbare delegatie en een opvraagbaar contract zijn feiten die de tegenpartij moet kunnen opzoeken. Registers beantwoorden stelselvragen (wie doet mee, wie beheert), maar geen casusvragen (heeft deze ontvanger een behandelrelatie met deze patiënt, welke gebruiker handelde). Casusfeiten verschillen per transactie en moeten als verifieerbare verklaring meereizen; dat is wat plateau 2 toevoegt en wat bevraging vereist. Wie de registers bouwt, heeft het kostbare deel al gedaan: dezelfde bron die een register vult, kan getekende claims uitgeven. Wij vragen daarom de plateau 1-registers vanaf het begin als uitgevende bronnen te ontwerpen.

Plateau 2: verifieerbare claims en expliciete delegatie

Vereist voor ongericht beschikbaar stellen (PULL): daar moeten organisatietype, delegatie en deelname aan het kader verifieerbaar zijn. PULL past dus niet op plateau 1; de Twiin-escalatie waarop dit memo antwoordt betrof landelijke databeschikbaarheid en is daarmee een plateau-2-vraag. Er bestaan werkende plateau-2-oplossingen (AORTA: mandaattoken, inschrijftoken; Nuts: Delegaties, kaderlidmaatschap), maar geen daarvan heeft landelijke status. Nadeel: de techniek is nog geen commodity, wat een risico legt bij de partijen die op dit plateau inzetten.

Plateau 3 (SOLL): Europese attestatie-infrastructuur

De plateau-2-claims migreren naar QEAA's en wallets onder eIDAS 2.0; niet-URA-deelnemers en geautomatiseerde uitwisseling sluiten aan. Wordt commodity door Europese regulering.

Gevraagd vervolg

Plateau 2 mist als landelijke afspraak terwijl de PULL-use-case er nu om vraagt. Wij vragen VWS drie dingen: regisseer de convergentie tussen de bestaande plateau-2-oplossingen in plaats van er parallel iets nieuws naast te ontwikkelen (zoals in het LDN werkpakket LSP x Nuts); start met de uitgifte van UZI-gegevens als verifieerbare attestatie (URA-VC, later QEAA) door het CIBG; en toets plateau 1 op een ding, namelijk dat de gekozen techniek het migratiepad naar plateau 2 niet blokkeert. Onze grootste zorg zit in de acceptatie van self-asserted claims in een (ongetekend) RAR-object, die hebben geen pad naar verifieerbare attestaties. Hoofdstuk 3 is vanuit dit perspectief te lezen.

5. Tot slot

Onze punten zijn geen bezwaar tegen de gekozen techniek, maar af te ronden werk (de scheiding tussen blokkerend en parallel staat in hoofdstuk 1). Wij gaan graag met VWS in gesprek over deze reactie en dragen actief bij aan het vervolg: het beantwoorden van de ontwerpvragen, de convergentie naar een landelijke plateau-2-oplossing en, als eerste concrete stap, de uitgifte van UZI-gegevens als verifieerbare attestatie door het CIBG.

Bronnen

VWS-memo Harmonisatie authenticatie en autorisatie (concept 13-07-2026); FAPI 2.0 Security Profile Final (OIDF, 22-02-2025); RFC 7523; RFC 9396; RFC 9449; Nuts nl-generic-functions-ig v0.3.0 (Authentication; Authorization Information Model); AVG art. 24, 25, 28, 29, 32, 35; Wabvpz en Begz; WGBO; NEN 7510-1/-2, NEN 7512:2022, NEN 7513:2024, NEN 7540:2024, NEN 7545:2026; GISA; eIDAS 2.0 (Vo. 2024/1183); EHDS (Vo. 2025/327).