Review PvE GBC Opvragend Systeem naast het Solution Design

PvE v0.1 van 30 juli 2026, gelegd naast de PSA en de AORTA on FHIR specificaties. Een deel van de punten komt uit het overleg van 3 september tussen Bart, Ron en Steven. Bedoeld als input voor de reviewronde, niet als lijst met verplichte wijzigingen. Waar iets diep in AORTA zit en in de pilot niet echt in de weg zit, staat het hier als punt voor latere harmonisatie en niet als iets dat nu moet.

Scope

Het PvE beschrijft eigenlijk pilot 1 uit hoofdstuk 9 van de PSA: Nuts vraagt gegevens op bij een LSP-partij. Dat staat nu nergens, terwijl het voor veel eisen hieronder bepaalt hoe hard ze zijn. Een korte scopeparagraaf in hoofdstuk 1 zou al helpen, met daarin wat voor pilot 1 buiten beeld blijft: revocation, DPoP, delegatie-informatie in de AS-metadata, de brede bevraging met audience binding en de NVI. Dan leest een leverancier eisen niet als definitief, en is meteen duidelijk dat de tokenrespons voorlopig Bearer is.

Tokens en credentials

In 2.2.1, 2.2.3 en 2.2.5 zit de SAML-tokenwereld, en 2.2.7 voegt daar een VC-wereld aan toe. In het overleg is afgesproken dat alleen de relevante tokeneisen zijn opgenomen en dat die op VC’s toepasbaar moeten zijn. Bij een paar eisen wringt dat:

- GBX.OPV.e4110.1 en GBX.AUT.e4521.3 schrijven het verwijderen van verlopen tokens en mandaattokens voor. Voor VC’s is dat niet nodig: een verlopen VC wordt door geen verifier meer geaccepteerd, en zonder toegang tot de private key van het subject heeft een VC sowieso geen waarde. Verwijderen voegt dus niets toe. Gaat het eigenlijk om het ongeldig maken van nog geldige credentials, dan is dat een intrekkingsmechanisme (buiten scope voor pilot 1) of een kortere geldigheidsduur voor pilot 1.
- GBX.OPV.e4160.1 en GBX.AUT.e4519 beschermen “tokens die meerdere malen gebruikt kunnen worden”. Dat zijn alle VC’s, en het gevoelige deel is vooral de private key. Splitsen in een sleutelbeschermingseis en een eis voor credentials met persoonsgegevens ligt dan meer voor de hand.
- GBX.FBH.e4070.2 behandelt alle tokens als medische gegevens. Alleen het PatientEnrollmentCredential bevat patiëntgegevens; HPDC, SPC en SPDC niet.
- GBX.OPV.e4170.1 (misbruik van tokens) geldt nu alleen voor tokens. Zou dat niet ook voor Verifiable Presentations moeten gelden?

Het consenttoken in e4110.1 en e4160.1 bestaat niet in het credentialmodel. Het staat er als voorbeeld, dus een bestaand credential in de plaats zetten is genoeg. Wat het document echt zou helpen is een tabelletje vooraan dat per tokenbegrip zegt welk credential uit het Solution Design ermee bedoeld wordt.

Geldigheidsduur van het inschrijftoken (GBX.OPV.e4100.1)

Dat de geldigheid van het UZI-certificaat geen invloed heeft op het inschrijftoken is een bewuste keuze, zo is in het overleg toegelicht: anders moet een inschrijving vlak voor de pasvervaldatum meteen weer opnieuw, en dat werkt niet. Anderhalf jaar wel.

Het aandachtspunt is dat CRL en OCSP na het verlopen van een certificaat niet meer worden bijgewerkt. Een verlopen of verloren pas komt dus nooit meer op een intrekkingslijst, terwijl je er nog wel mee kunt ondertekenen met een uitgiftedatum in het oude venster. De PSA is hier zelf ook niet consistent: §10.3.5 begrenst de geldigheid van did:x509-credentials tot die van het certificaat, terwijl §10.6.5 voor het PatientEnrollmentCredential zegt dat latere intrekking

niet uitmaakt. Een maatregel aan de uitgiftekant helpt maar beperkt, want de signing service is gewoon software en wie een gestolen pas heeft bouwt zijn eigen variant.

Voorstel: de anderhalf jaar voor pilot 1 laten staan en dit, samen met de tegenstrijdigheid in de PSA, meenemen naar de verdere harmonisatie.

Intrekken van credentials

Het PvE kent alleen verwijderen, geen intrekken. Voor pilot 1 klopt dat met de PSA, waar revocation buiten scope valt. Het zou wel goed zijn de consequentie te benoemen: een HPDC of SPDC kan niet worden teruggetrokken als een zorgverlener uit dienst gaat of een overeenkomst eindigt, en de enige rem is dan de geldigheidsduur. Voor productie ligt StatusList2021 uit PSA §10.9 voor de hand, inclusief hosting, cacheduur en wat je doet als de statuslijst onbereikbaar is.

Inrichting of implementatie

De grens tussen inrichting en implementatie is nog niet scherp, en dat bepaalt of iets in het PvE hoort of in de technische specificaties. Het DID-management staat nu in de AORTA on FHIR specificaties onder Interfaces GBC Client (getDIDdocumentGBC en GBC-I.DID.100.v1), inclusief did:web-resolutie, de vereiste DID-documenteigenschappen en sleutelrotatie. Maar lees je de specificaties als implementatie, dan blijft er een inrichtingskant over die nergens staat. Een leverancier of zorgaanbieder moet bijvoorbeeld een .nl-domein hebben waar het DID-document staat, met geldig TLS-certificaat en voldoende beschikbaarheid. Dat voelt meer als PvE dan als specificatie.

Dus de vraag: welk deel van het DID-management is implementatie en welk deel inrichting, en waar landt wat?

Los daarvan: de eis uit PSA §10.7.2 dat de sleutel voor het ondertekenen van VP’s een andere is dan die in assertionMethod komt in geen van beide documenten terug. Die moet ergens een plek krijgen.

Vertrouwensniveau midden en de VVT (GBX.VC.e4050, GBX.IDA.e4080.5)

Het PvE voegt twee handelingen samen die je beter uit elkaar houdt: het beheren en uitgeven van credentials, en het inloggen om gegevens te raadplegen. Voor dat laatste gebruikt de VVT geen UZI-passen, dus GBX.IDA.e4080.5 zou kunnen aansluiten bij hoe de VVT nu inlogt. PSA §9.1.1 zegt ook dat pilot 1 zich beperkt tot de UZI-pas met ZorgID en dat taakcodes voor niet-BIG-geregistreerde medewerkers later komen.

Voor het uitgeven past GBX.VC.e4050 niet op alle credentials. Het ServiceProviderDelegationCredential wordt niet met een UZI-pas ondertekend en is geen handeling van een zorgverlener, maar van iemand die namens (het bestuur van) de organisatie handelt. Dat is een eis aan de software, namelijk wie bij de assertion key mag, niet aan het vertrouwensniveau van een zorgverlener.

De dienstverlener

De PSA maakt een duidelijke knip tussen zorginstelling en dienstverlener (AUTH-019) en kent een multi-tenant knooppunt (OAUTH-012). Het PvE niet: hoofdstuk 2.1 gaat uit van een zorgaanbieder die het systeem zelf draait, met systeembeheerder en vervangers, toegangslogbeheerder, beheerlog, een GBX-workshop per organisatie en een servicedesk die ook buiten kantooruren bereikbaar is.

Mogelijk redeneert AORTA hier bewust vanuit juridische verantwoordelijkheid, waarbij de dienstverlener geen eigen rol heeft en de zorgaanbieder taken uitbesteedt. Ik ken AORTA daar niet goed genoeg voor: zit dat impliciet in de verschillende GBx'en?

Is het handig om de dienstverlener expliciet toe te voegen, zodat het PvE aansluit op de rolverdeling in de PSA? Als dat binnen het huidige AORTA lastig is, dan is het prima om het als punt voor latere harmonisatie te parkeren. Hetzelfde geldt voor de rol van samenwerkingsverband of afsprakenstelsel, die in geen van beide documenten voorkomt.

Credentials: verplicht, conditioneel en scope

- SPDC.CRED.e4020 staat op conditioneel. In het overleg is afgesproken de conditie eraf te halen, en pas weer een conditie toevoegen als de use-case bekend is.
- HPDC.CRED.e4020 heeft de conditie in de eistekst met MoSCoW Verplicht, terwijl SPDC een apart Condities-blok met MoSCoW Conditioneel gebruikt. Eén conventie zou fijn zijn.
- SPC.CRED.e4010 is nog uit te werken. De uitgever is inmiddels bekend (VZVZ als stelselbeheerder tijdens de pilots). Wat nog open staat is hoe een service provider wordt geïdentificeerd, een vraag die PSA hoofdstuk 9 ook stelt: VC, certificaat, OID of FQDN.
- GBX.OPV.e4090.2 laat een zorgverlener een systeem mandateren via een applicatie-id, terwijl het subject van het HPDC in de PSA de did:web van de zorginstelling is. In het overleg is afgesproken het applicatieregister niet te gebruiken.

Over die granulariteit kwam in de uitwerking iets aardigs boven. PSA §8.3.2 laat toe dat het subject een zorginstelling of een afdeling is, dus je kunt per afdeling een DID maken. Zo'n afdelings-DID kun je vervolgens alleen laden met een URA, want het HealthcareProviderCredential komt van een UZI-servercertificaat op organisatieniveau. De delegatie is daarmee feitelijk gescoped op de applicatie die de private key van dat DID heeft. In de praktijk geef je dus een applicatie-instantie toegang, en dat komt behoorlijk in de buurt van een applicatie-id.

Het enige verschil dat ik zie: bij een DID is die binding impliciet. De verifier ziet alleen een DID en kan niet vaststellen welke applicatie de sleutel houdt. Voor audit en verantwoording is dat wel een ander verhaal. Mis ik hier iets?

Het BSN in het PatientEnrollmentCredential

PSA §10.6.5 definieert het BSN als verplicht veld in klare tekst, terwijl §8.2.2 en §8.3.2 spreken van "waar nodig gepseudonimiseerd" en "optioneel gepseudonimiseerd". In de praktijk is die keuze er niet. De huidige PRS maakt alleen pseudoniemen per organisatie, en je eigen pseudoniem kun je niet delen met een andere partij; dat moet worden omgezet naar een versleuteld pseudoniem voor die specifieke ontvanger. Dat zou een apart credential per ontvanger betekenen, en dat kan niet. Dit ontwerp zit dus vast aan een plain BSN.

Suggestie: §8.2.2 en §8.3.2 gelijktrekken met §10.6.5, zodat er geen verwachting ontstaat die de PRS niet kan waarmaken. Dat een pseudoniem formeel ook een bijzonder persoonsgegeven is verandert daar niets aan, maar de vorm bepaalt wel hoe gevoelig de opslag is, en dus hoe SYS.BVL.e4010.2 hier uitpakt.

TLS-parameters (GBX.CON.e4080.6)

De eis vraagt om vernieuwing van tijdelijke sleutels via TLS Secure Renegotiation, maar dat mechanisme bestaat in TLS 1.3 niet meer, terwijl punt 5 van dezelfde eis wel de hoogste ondersteunde TLS-versie voorschrijft. AOF-I.GEN.210.v2 eist TLS 1.3 als minimum, en PSA §10.3.4 noemt 1.3 aanbevolen en 1.2 toegestaan. Drie documenten, drie antwoorden. Zullen we die gelijktrekken? GBX.CON.e4090.3 heeft dezelfde constructie.

Kleinere punten

- GBX.SBH.e4035 (ZORG-AB actueel houden) blijft een Twiin-onderwerp. Als hij blijft staan, dan misschien conditioneel op deelname aan het Twiin-afsprakenstelsel in plaats van onvoorwaardelijk verplicht.
- GBX.VC.e4030 (delen van VP's) stelt dat verifiers vertrouwd moeten zijn en in ZORG-AB staan. Dat is een vertrouwenseis, geen opdracht om ZORG-AB tijdens de transactie te bevragen, dus handmatig configureren van vertrouwde partijen past in de pilot. Het is wel goed om erbij te zetten dat dit interim is, omdat in pilot 1 nog geen delegatie-informatie in de AS-metadata zit.
- GBX.VC.e4020 (niet exporteren sleutels) is haalbaar, maar nu niet overal het geval. Voor pilot 1 misschien conditioneel met een migratiedatum. Let wel op de spanning met GBX.CON.e4050.2 (Nederlandse wet- en regelgeving): van de key vaults die de Nuts-node ondersteunt kan op dit moment alleen Azure de hardwaregarantie geven.
- GBX.PST.e4015 (0,3 seconde verwerkingstijd) zou gedefinieerd kunnen worden als responstijd exclusief externe afhankelijkheden zoals DID-resolutie, of met een apart budget voor het tokenpad.
- GBX.CON.e4010.1 (communicatie via een GZN): verificatie vereist het ophalen van DID-documenten van een .nl-domein en straks statuslijsten, allebei publieke internetendpoints. Zijn die vanuit het GZN bereikbaar, of komt daar een resolver binnen het GZN voor?
- GBX.IDA.e4050.1 (bijhouden behandelrelatie): in de VVT ligt de behandelrelatie op team- of organisatieniveau, niet bij een individuele behandelaar. In de PSA is het subject van het PatientEnrollmentCredential de zorginstelling en is enrolledBy alleen degene die de BSN-validatie deed. Levert de UZI-gebonden registratie in het PvE hier een probleem op, of valt dat in de praktijk mee?
- GBX.OPV.e4020.1 (toets op behandelrelatie) is verplicht maar leunt op GBX.IDA.e4050.1, dat optioneel is. De behandelrelatie kan ook uit de werkcontext blijken; als dat expliciet wordt is de combinatie sluitend. En GBX.IDA.e4060.1 verwijst naar e4010, e4020, e4040 en e4050, maar niet naar GBX.IDA.e4030.2, terwijl die juist de definitieve koppeling vastlegt.

Verwijzingen en redactie

De link naar de AORTA on FHIR specificaties in §1.4 werkt niet meer: aorta-on-fhir.scrollhelp.site is verhuisd naar aorta-on-fhir.public.vzvz.nl. Twee van de vijf verwijzingen hebben alleen een naam, geen URL.

Vraag over de methodiek: bijna heel 2.2.7.2 staat op Vzvz_Req_Verificatie: Monitoring, terwijl het om eisen gaat als "het systeem dient een credential aan te kunnen maken". Wat houdt Monitoring als verificatiemethode in, en is dat hier bedoeld of past Acceptatietest beter?

Verder wat kleine dingen: tokenRequest staat een paar keer als tokenRquest; AGE.LOG.e4050 heeft een kop "Toestemming" waar "Toelichting" bedoeld lijkt; 2.1.5 heeft Vzvz_Req_Soort: Product waar Req_Type hoort; de figuurnummering springt van 1 naar 3 en van 7 naar 9; en de eistekst van SPDC.CRED.e4020 eindigt in een onafgemaakte zin.