

Architectuur voor uniforme bronontsluiting Bijlage Beleidsperspectief

Versie: 21-01-2026

concept

1.	Inleiding	2
2.	Uniforme Bronontsluiting	2
3.	Verstrekingen en attribuutverificatie	3
3.	Overkoepelende projectkeuzes	5
4.	Projectkeuzes specifiek voor attribuutverificatie	10

1. Inleiding

Gemeenten moeten steeds meer gegevens digitaal beschikbaar stellen aan burgers, ondernemers en publieke dienstverleners in de Europese Economische Ruimte (EER). Dat gebeurt via verschillende kanalen, zoals het Once Only Technical System (OOTS) en het European Digital Identity (EUDI) Ecosysteem. De verordeningen waarin deze kanalen hun grondslag hebben, stellen elk eigen eisen aan gemeenten. Soms zijn de eisen gelijk of vergelijkbaar, maar vaak verschillend. De diversiteit aan verplichtingen maakt de implementatie-opgave voor gemeenten omvangrijk en complex¹. De VNG ontzorgt gemeenten bij het digitaal verstrekken van gegevens via deze kanalen, zodat zij gegevens kunnen verstrekken met één set van afspraken en standaarden en ondersteund door (vrijwillig te gebruiken) voorzieningen. Uniforme Bronontsluiting is de technische oplossing die de VNG hiervoor ontwikkelt.

Met beproevingen toetst de VNG samen met verschillende stakeholders of de afspraken, standaarden en voorzieningen voor Uniforme Bronontsluiting geschikt zijn. De beproevingen richten zich nu op de ontsluiting van gemeentelijke gegevens naar het OOTS (fase 1) en de EUDI-wallet (fase 2), maar worden uitgevoerd met een bredere gegevensverstrekking in gedachten. Breder door de gewenste uitbreiding naar andere kanalen (zoals private verstrekkingen met toestemming, DvTP) en breder door de gewenste toepassing van uniforme bronontsluiting bij niet-gemeentelijke bronhouders.

Deze bijlage geeft inzicht in de veronderstellingen die het project *in fase 2 (beproeving met de EUDI-wallet)* heeft gemaakt die te maken hebben met onderwerpen die in het beleidsvormingsproces bij minBZK/DO besproken worden of zouden kunnen worden. Het is bedoeld om transparant te zijn in de projectkeuzes en biedt de opdrachtgever de mogelijkheid om de opgedane inzichten te benutten in de beleidspraktijk.

2. Uniforme Bronontsluiting

Het project Uniforme bronontsluiting wordt uitgevoerd in een context waarin nog allerlei ontwikkelingen gaande zijn. De European Digital Identity Wallet is bijvoorbeeld nog niet volledig gespecificeerd en is nog niet beschikbaar voor burgers en ondernemers, oplossingen voor de EUDI-wallet worden nog ontworpen en beproefd in Large Scale Pilots en ook nationaal zijn standaarden (zoals Digikoppeling REST API profiel en FSC) nog niet uitontwikkeld.

De architectuur voor Uniforme bronontsluiting is opgesteld vanuit de wetenschap dat er in deze nationale en Europese dynamiek geen moment gaat komen waarop alle schuivende panelen tot stilstand zijn gekomen. Afwachten heeft geen zin en leidt er alleen toe dat gemeenten steeds meer met voldongen feiten geconfronteerd worden, de ontwikkelingen niet in eigen hand hebben en achter gaan lopen bij implementatie van eigen ambities. Dit project is daarom uitgevoerd met als

¹ Gemeenten moeten gegevens in verschillende samenstelling, met verschillende gegevensdefinities en in verschillende technische formaten via de kanalen beschikbaar stellen. Elk kanaal stelt eigen (kwaliteitseisen) aan de te verstrekken gegevens en de beheerprocessen die daarvoor ingericht moeten worden, zoals incidentmanagement en changemanagement. Het is waarschijnlijk dat elk kanaal eigen voorzieningen krijgt voor het registreren van gemeentelijke metadata, zoals de gegevensbronnen, hun data services, certificaten en end-points en de bereikbaarheid daarvan. Gemeenten moeten ervoor zorgen dat hun metadata op verschillende plekken beschikbaar komt en actueel blijft.

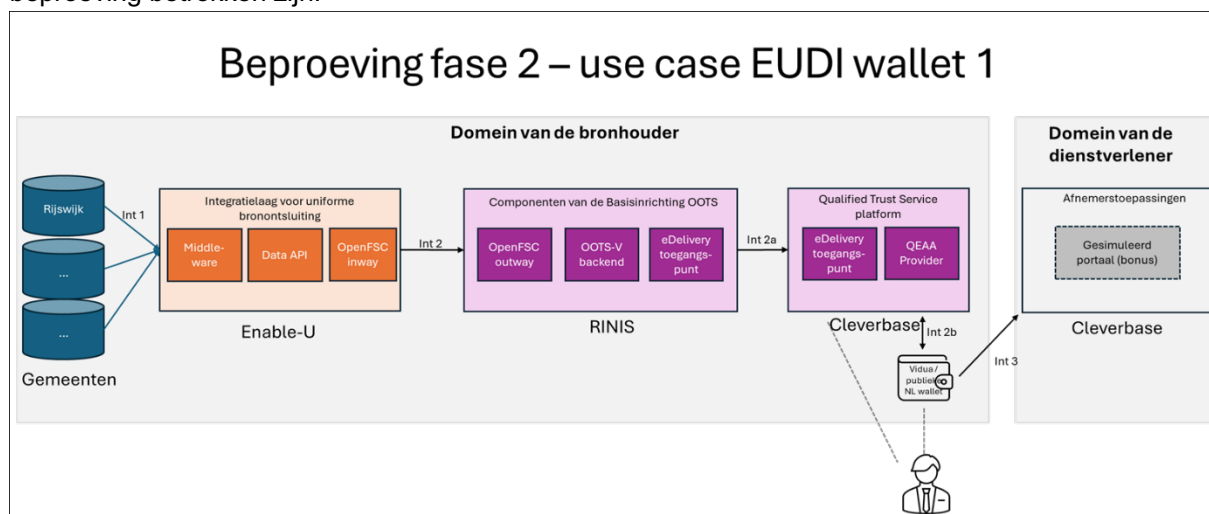
startpunt de zaken die al wél bekend zijn, zoals de inrichting van het OOTS, en doet “veronderstellingen” over de werking van nog onbekende onderdelen, zoals de EUDI-wallet, de interactie met QTSP’s, etc. Deze veronderstellingen zijn gedurende het project afgestemd met stakeholders, zoals het EDI-programma, TIP, gemeentelijke softwareleveranciers, QTSP’s, FDS, GBO en bNC SDG om ervoor te zorgen dat ze zo plausibel mogelijk zijn. VNG accepteert de situatie dat sommige veronderstellingen in de praktijk uiteindelijk onverhoopt niet correct blijken en aanpassingen nodig zijn.

3. Verstrekkingen en attribootverificatie

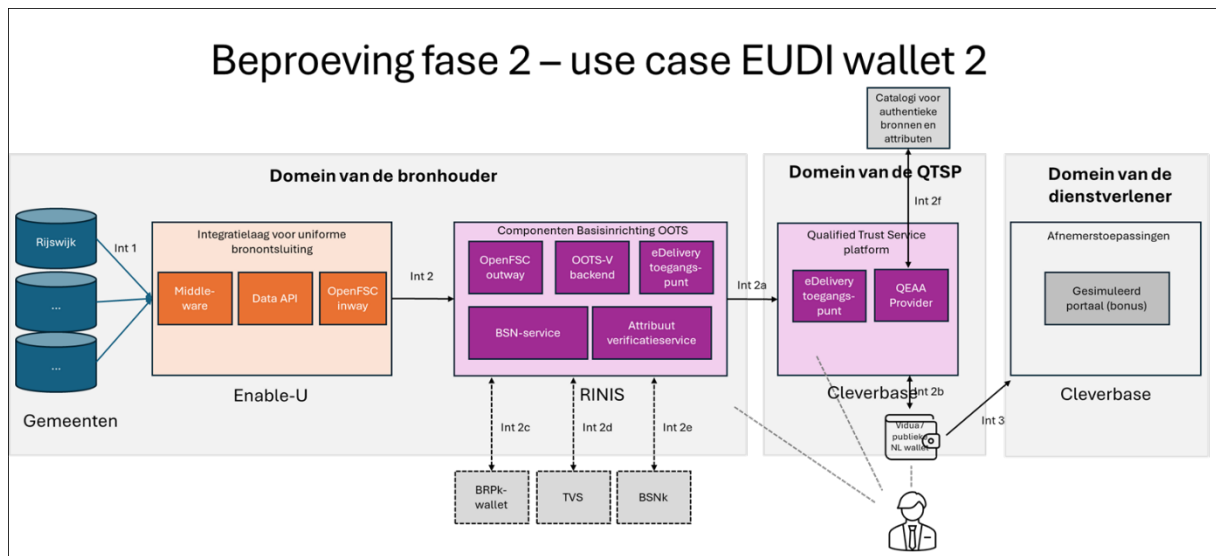
Fase 2 van het project Uniforme Bronontsluiting maakt onderscheid in twee use cases:

1. Verstrekkingen aan de EUDI-wallet. In deze use case verstrekt een gemeente geboortegegevens uit de bronadministratie aan een EUDI-wallet. De gemeente contracteert een QTSP om de attestatie uit te geven. Deze verstrekking is in de eIDAS-verordening niet verplicht.
2. Attribootverificatie van een QTSP bij de gemeentelijke bron. In deze use case laat een geaccrediteerde QTSP op verzoek van een gebruiker de authenticiteit van geboortegegevens door de gemeente controleren. Dit recht op verificatie bij de authentieke bron is opgenomen in de eIDAS-verordening en verplicht de bronhouders van de in annex VI van de verordening gespecificeerde gegevens om de verificatiemogelijkheid aan te bieden.

Onderstaande afbeeldingen tonen de ICT-componenten die voor beide use cases in de beproeving betrokken zijn.



Afbeelding: componenten voor beproeving van de verstrekking aan de EUDI-wallet



Afbeelding: componenten voor attribuutverificatie

Opgemerkt dient te worden dat de rol van de QTSP in beide use cases anders is. In de eerste use case handelt de QTSP in opdracht van de gemeente die de gegevens aan de EUDI-wallet beschikbaar stelt. De gemeente kan (a) de gegevens zelf beschikbaar stellen in de vorm van een Pub-EAA al dan niet door inschakeling van subcontractors of (b) dit uitbesteden aan een QTSP die een QEAA uitgeeft². In beide gevallen is de gemeente verantwoordelijk voor het proces. Dat is anders in de tweede use case. Elke QTSP (geaccrediteerde organisaties) heeft het wettelijk recht om in opdracht van de gebruiker een attribuutverificatie uit te laten voeren. De QTSP handelt in deze use case niet in opdracht van de gemeente, maar heeft met de gemeente wel contact voor het uitvoeren van de verificatie.

Ondanks dat de verantwoordelijkheden verschillend zijn, zijn de in te zetten ICT-componenten en de interacties daartussen zo ontworpen dat ze in beide use cases erg vergelijkbaar zijn. De verwachting is dat dit de implementatie vereenvoudigt en lock-ins bij leveranciers voorkomt. Dit ontwerpprincipe sluit aan bij de ETSI-standaard die in ontwikkeling is voor de interactie met QTSP's. Deze standaard baseert de berichten voor beide use cases eveneens op het datamodel van OOTS.

De architectuur voor uniforme bronontsluiting bevat meer informatie en is beschikbaar op: [Beproeving: eenvoudig en eenduidig gegevens uitwisselen — Digilab](#)

² In de beproeving is gekozen voor variant b.

3. Overkoepelende projectkeuzes

Betrokkenheid van QTSP's in beide use cases

Situatie:

Het is voor de verstrekking van gegevens aan EUDI-wallets (use case 1 verstrekkingen) aan elk van de publieke bronhouders om te bepalen op welke manier zij hoog-betrouwbare attestaties aan de wallet gaan verstrekken. Het project onderkent verschillende varianten:

1. De authentieke bron geeft een Pub-EAA uit, waarbij de bronhouder kan besluiten om een subcontractor in te schakelen voor het leveren van de benodigde functionaliteit. Dat mag een QTSP zijn, maar die handelt in dit geval als leverancier voor de gemeenten en uit hoofde van de gemeente.
2. De authentieke bron geeft een Pub-EAA uit via een aangewezen publieke Pub-TSP, waarbij de bronhouder op een nationale voorziening leunt voor de uitgifte van de Pub-EAA. De nationale voorziening is aangewezen als issuer voor gespecificeerde attestaties. Er is geen initiatief om tot een nationale Pub-TSP te komen.
3. De authentieke bron contracteert een QTSP, die vanuit zijn status als geaccrediteerde organisatie QEAA's uitgeeft. De QTSP is in dit model issuer van publieke gegevens en heeft een zelfstandige verantwoordelijkheid om aan de vereisten voor een QTSP te voldoen. Hiervoor staat het onder nationaal toezicht.

Elke QTSP heeft onder de eIDAS-verordening het recht om de attributen uit annex VI van de verordening bij de authentieke bron te verifiëren (use case 2 attribuutverificatie).

Keuze voor beproeving:

- Voor use case 1: verstrekkingen:
Het zelf ontwikkelen van de eigen functionaliteit voor de uitgifte van Pub-EAA (variant 1) was niet passend binnen de scope van het project en werd beoordeeld als een model dat niet wenselijk is voor gemeenten (342x aantal bronsystemen implementeren). Gebruik van een nationaal bruikbare oplossing (variant 2) was ook niet mogelijk binnen de scope van de kleinschalige beproeving, maar wordt beschouwd als een werkbaardere oplossing voor gemeenten. Het project heeft gekozen voor variant 3 en maakt gebruik van een koplopende private QTSP voor het verstrekken van attestaties aan de EUDI-wallet.
- Voor use case 2: verificatie
Dezelfde QTSP participeert in de attribuutverificatie use case. Dat geeft het project de snelheid en wendbaarheid die het nodig heeft.

Beleidsbelang:

- Er is in het project geen eenduidigheid gekregen over de drie varianten die het project ziet voor use case 1 "verstrekkingen". Zijn ze alle drie juridisch mogelijk? En wat zijn de consequenties voor de bronhouder bij keuze voor een van de drie? De verwachting is dat meer bronhouders hierin onduidelijkheid ervaren. Geadviseerd wordt de gevraagde duidelijkheid aan bronhouders te verstrekken.
- Voor inzet van QTSP's voor vertrekkingen op grotere schaal dan dit project is het wenselijk dat de optie voor het verstrekken van (gemeentelijke) gegevens via gecontracteerde QTSP's beleidsmatig gesteund wordt.

Voorschot op uniforme afspraken en specificaties

Situatie:

Beide use cases maken gebruik van een QTSP voor het interacteren met de EUDI-wallet. Voor verstrekkingen werkt de QTSP in het domein van de bronhouder, voor verificatie handelt de QTSP onder eigen verantwoordelijkheid. Ondanks dat de rollen van de QTSP in beide situaties anders zijn, komt de interactie met de QTSP's inhoudelijk en technisch sterk overeen. Om te voorkomen dat deze interactie door elke bronhouder individueel ontworpen moet worden en het risico van lock-in te vermijden, vindt het UBO-project het belangrijk dat er één set van afspraken en standaarden komen over de te implementeren protocollen en interfaces. Het project sorteert hierop voor.

Keuze voor beproeving:

Er is nog geen standaardinterface voor de interactie met QTSP's (of meer algemeen: met issuers van attestaties), maar er zijn wel initiatieven die hieraan werken. ETSI werkt aan een Europese standaard en TIP aan de Nederlandse toepassing daarvan. Beide ontwikkelingen lopen nog. Het project past dezelfde uitgangspunten toe als beide initiatieven en neemt beschikbare (concept) specificaties uit deze initiatieven over indien die tijdig beschikbaar komen.

Hieruit volgt:

- Uniforme bronontsluiting kiest voor inzet van eDelivery voor de interactie met de QTSPs. TIP hanteert eDelivery ook als standaard voor de interactie met QTSP's en ETSI werkt aan de onderliggende standaard. eDelivery levert de ketenpartners een aantal waarborgen voor vertrouwelijkheid en onweerlegbaarheid die zodoende niet op een andere wijze gerealiseerd hoeven te worden.
- Uniforme bronontsluiting kiest voor het inzetten van het OOTS berichtenmodel als basis voor deze specificaties. DG DIGIT heeft dit datamodel al beproefd in het kader van het 'Synergies OOTS en EUDI wallet' project. De uitwerking van DIGIT wordt zoveel mogelijk overgenomen, zodat de kans op een bredere inzetbaarheid in de EER gemaximeerd wordt. Inzet van dit datamodel sluit aan bij de richting die de ETSI werkgroep op beweegt met TS 119 478.

Beleidsbelang:

De overtuiging is dat er behoefte ontstaat aan het formaliseren van deze afspraken. Dit vereenvoudigt de aansluiting van bronhouders op de EUDI-wallet en leidt tot meer efficiënte besteding van overheidsmiddelen. Bij voorkeur kiezen de beleidsdepartementen één standaard interface voor interactie met issuers van attestaties.

Inzet van Nederlandse OOTS-componenten

Situatie:

Voor de (gemeentelijke) bronontsluiting hanteert Uniforme Bronontsluiting de nationale standaarden Digikoppeling REST API-profiel en FSC. De interactie met QTSP's vindt plaats in lijn met de voorgenomen ETSI- en TIP-standaarden: eDelivery een (uitgebreid) OOTS berichtenmodel. Het project wil zo veel mogelijk voorkomen dat publieke bronhouders zowel nationale als Europese standaarden naast elkaar moeten implementeren en bijhouden.

Keuze voor beproeving:

Het project overbrugt beide standaarden met een voorziening die de functionaliteit voor bronontsluiting ontkoppelt van die voor verstrekking via het OOTS of de EUDI-wallet (een "intermediaire component"). Voor de beproeving wordt ingezet op hergebruik van componenten die al beschikbaar zijn. Voor interactie met de QTSP zet het project (een kopie van de) de Basisinrichting OOTS in: FSC outway, FSC manager, OOTS-V (backend integratie) en het eDelivery access point. Er is voor de inzet van deze componenten gekozen, omdat de componenten de bronhouders in de OOTS-route ook al ontzorgen door het ontkoppelen van dezelfde nationale en Europese standaarden. Inzet voorkwam dat nieuwe componenten met vergelijkbare functionaliteit ontwikkeld moesten worden.

De componenten van de Basisinrichting OOTS zijn ook ingezet in cases 1 van de EUDI-wallet: het verstrekken van brongegevens via een QTSP aan de EUDI-wallet, terwijl hiervoor ook een 1-op-1 aansluiting van bronhouder op QTSP mogelijk zou zijn. Er is voor use case 1 gekozen voor inzet van de OOTS componenten, omdat dit leidt tot:

- Een identieke bronontsluiting voor de use case OOTS, use case EUDI-1 (verstrekking) én use case EUDI-2 (attribuutverificatie);
- uniformiteit in de implementatie bij alle gemeenten die deze standaard volgen (efficiëntie bij uitrol);
- beperking van het risico op een lock-in van een gemeente bij een specifieke QTSP, omdat de verwachting is dat meerdere QTSP's de standaard interfaces gaan aanbieden omdat er meerdere klanten voor zijn;
- vergroting van de marktkansen voor gemeenten, omdat QTSP's uit andere lidstaten geen Nederlandse standaarden hoeven te implementeren en gemeenten hen naar verwachting tegen lagere kosten kunnen contracteren (vergeleken met het opleggen van nationale of gemeentelijke standaarden).

Beleidsbelang:

Voor inzet van de Basisinrichting OOTS voor de EUDI-wallet op grotere schaal dan dit project zijn mogelijk aanvullende beleidsmaatregelen nodig. Misschien moet de keuze voor inzet van de Basisinrichting OOTS opgenomen worden in eIDAS-uitvoeringswetgeving en mogelijk is uitbreiding van het Besluit Digitale Overheid nodig³. Het is verder belangrijk dat de bredere inzet van bestaande componenten in GDI-architectuurverband gesteund wordt en kent samenhang met de plannen voor Gemeenschappelijke Bronontsluiting.

³ De Basisinrichting OOTS wordt op dit moment in het Besluit Digitale Overheid opgenomen als voorziening voor het OOTS en niet voor de EUDI-wallet.

Inzet van het OOTS eDelivery netwerk

Situatie:

Er zijn beveiligde verbindingen tussen de intermediaire component en de QTSP's nodig, zodat geborgd wordt dat berichten veilig en betrouwbaar afgeleverd worden en dat op elk moment inzichtelijk gemaakt kan worden.

Keuze voor beproeving:

Het OOTS-netwerk biedt de technische voorzieningen, verbindingen en beheersafspraken om veilige uitwisseling tussen partijen mogelijk te maken. Uitvoeringsverordening 45def staat het lidstaten toe om componenten van het OOTS in te zetten voor de EUDI-wallet (artikel 10). Het project kiest voor inzet van een afgeschermd sectie binnen het huidige OOTS-eDelivery netwerk voor de interactie tussen de intermediaire component en de QTSP. De betrokken QTSP sluit hierop ook aan. Dit voorkomt de inspanningen die nodig zijn voor het inrichten van het eDelivery-netwerk specifiek voor dit project.

Voor consistentie voor de bronhouder tussen use-case 1 en 2 en voor consistentie met de ETSI standaard die in wording is, zet UBO het eDelivery-netwerk voor use case 1 en 2 in.

Beleidsbelang:

Het project veronderstelt dat er uiteindelijk een Europees eDelivery netwerk ingericht wordt waarop alle publieke bronhouders en QTSP's aangesloten zijn, waarbij de toelating van QTSP's op Europees niveau geregeld wordt. Dit netwerk bestaat echter nog niet, maar het project ziet de toegevoegde waarde van zo'n netwerk en Europese governance op toelating van QTSP's. We adviseren BZK dit bij de EC voor te dragen.

BSN verwerking

Situatie:

Bij het bevragen van een gemeentelijke bron voor het ophalen van gegevens over een natuurlijk persoon schrijft de bronhouder meestal het gebruik van het BSN voor. Het gebruik van het BSN is gemeengoed en voorgeschreven in de communicatie tussen publieke instanties en beperkt tot het gebruik in het publieke domein. De QTSP's zijn in beginsel echter niet gerechtigd om het BSN te verwerken.

Keuze voor beproeving:

Voor het verstrekken van gemeentelijke gegevens (use case 1) werkt de QTSP in opdracht van de betreffende gemeente. Het project veronderstelt dat het toegestaan is dat de QTSP het BSN mag verwerken zodra het een passende verwerkersovereenkomst met de gemeente heeft.

Voor attribuutverificatie (use case 2) is er geen contract en verwerkersovereenkomst, maar een wettelijk recht van een QTSP om een attribuutverificatie uit te voeren. Er is geen beleidsinitiatief bekend dat de verwerkingsgrondslag voor de QTSP voor attribuutverificatie gaat bieden. Het project veronderstelt dat de QTSP voor attribuutverificatiedoeleinden het BSN mag verwerken, maar daar lijkt nu geen wettelijke grondslag voor.

De beproeving zet voor use case 2 (attribuutverificatie) alleen door EUDI-wallets in met een Nederlands PID, zodat de QTSP het BSN uit de PID kan lezen.

Beleidsbelang:

Beleidsbeslissing over BSN-verwerking door een QTSP voor doeleinden van attribuutverificatie. De UBO-architectuur beschrijft drie oplossingen waarlangs een bronhouder – op zijn intermediaire platform – het BSN kan achterhalen indien de QTSP daar niet toe gerechtigd wordt:

1. uitvoeren van een herauthenticatie in het domein van de bronhouder, waarbij het BSN opgevraagd wordt;
2. uitvoeren van identiteitsmatching om aan de hand van de PID-attributen het BSN in De basisregistratie Personen te achterhalen;
3. het opnemen van een tot het BSN te herleiden (polymorf) versleutelde identiteit in de PID of in een aparte attestatie op de EUDI-wallet.

BZK kan deze opties overwegen indien een oplossing nodig is voor de situatie dat de QTSP voor use case 2 niet BSN-gerechtigd wordt.

4. Projectkeuzes specifiek voor attribuutverificatie

Gemeenschappelijk attribuutverificatiepunt

Situatie:

Gemeenten hebben de plicht om attribuutverificatie aan te bieden conform artikel 45 van de eIDAS-verordening en voor de attributen die in annex VI genoemd zijn. EZ en BZK hebben voor zover bekend geen voornemen tot het ontwikkelen van een nationale attribuutverificatievoorziening. Het is niet haalbaar en niet efficiënt om deze functie per authentieke bron door elke gemeente zelf decentraal te laten ontwerpen en ontwikkelen.

Keuze voor beproeving:

Het project ontwerpt daarom een prototype van een gemeenschappelijke attribuutverificatieservice voor – in ieder geval – de deelnemende gemeenten. Het project maakt daarin ook keuzes ten aanzien van de werking van het verificatieproces en de specificatie van het verificatieresultaat dat de QTSP ontvangt. Het project belegt de verificatieservice in het intermediaire platform dat het project ook voor de overige centraal geïmplementeerde services inzet.

Beleidsbelang:

Voor inzet van deze verificatievoorziening op grotere schaal is steunend beleid gewenst. Verder is het belangrijk dat de werking van het verificatieproces en de specificatie van het bijbehorende resultaat in beleidsregels geüniformeerd wordt om de nationale ruimte die de verordening hiervoor biedt zo in te vullen dat een werkbare oplossing voor bronhouders, intermediairs en QTSP's ontstaat.

Inzet van OOTS Gemeenschappelijke diensten

Situatie:

Voor attribuutverificatie heeft de EUDI-wallet catalogi nodig voor attributen en authentieke bronnen. Lidstaten mogen volgens artikel 10 van de Uitvoeringsverordening 45def de OOTS common services inzetten. Er is het project geen besluit bekend of Nederland dat gaat doen.

Keuze voor beproeving:

De beproeving maakt maximaal gebruik van de voorzieningen die er al zijn. Het project zet daarom voor attribuutverificatie de OOTS common services (“gemeenschappelijke diensten”) in als catalogi voor attributen en authentieke bronnen⁴. DG DIGIT heeft al een proef uitgevoerd met inzet van de OOTS Common Services voor attribuutverificatie. Die ervaringen worden in het project benut. Tevens sorteert het project hiermee voor op de ETSI-standaard die in ontwikkeling is en de interactie met de OOTS common services voor attribuutverificatie standaardiseert.

Beleidsbelang:

Het lijkt verstandig om een nationaal standpunt in te nemen over inzet van de OOTS Common Services voor attribuutverificatie, zodat navolgende projecten daarop aan kunnen sluiten. Op dit moment ontbreekt dat standpunt nog.

⁴ Voor het lokaliseren van het Access Point / end-point van de verificatieservice.

Auteurs

Indra Henneman
Aleksandar Simsic
Ivar Vennekens

VNG Realisatie

Nassaulaan 12
2514 JS Den Haag
070 373 80 08