Lessons learned

UNIFORME BRONONTSLUITING/ BRONCONNECT FASE 2

VNG, Rijswijk, RINIS, Enable-U, Cleverbase

Lessons learned Uniforme Bronontsluiting (fase 2) 3
Inleiding 3
Documentatie 4
Samenvatting Lessons Learned 6
Werkwijze en aanpak 6
Samenwerking en governance 6
Technische lessen 6
Specifieke inzichten voor eIDAS en wallet 7
Juridische en organisatorische lessen (DPIA) 8
Belangrijkste knelpunten en open vragen 8
Belangrijkste aanbevelingen 9
Conclusie 10
Lessons Learned 11
1. Algemene lessen 11
1.1 Geleerde lessen 11
Werken met expliciete aannames in een beleidsomgeving die volop in beweging is 11
Waarde van samenwerking met markt, Europese Commissie en LSP's. 12
Belang van demonstraties en testopnames. 13
Releases standaarden 13
1.2 Aanbevelingen 13
1.3 Openstaande punten 14
2. Lessen Techniek 15
2.1 Geleerde lessen 15
Signing & encryptie 15
Gebruik van 'properties' in de FSC standaard 15
Delegatie 16
DATA-API specificaties 17
(Her)gebruik functionaliteit Basisinrichting OOTS 17
1.3 Aanbevelingen 17
2.3 Openstaande punten 19
3. Specifieke inzichten voor eIDAS 20
3.1 Geleerde lessen 20
Verificatie(module) 20
Toepassing EU Common Services (CS) door QTSP 21
Toepassing eDelivery netwerk voor QTSP's 22
Toepassing NL Wallet in de beproeving 23

3.2 Aanbevelingen 23
3.3 Openstaande punten 24
4. Juridische en organisatorische lessen 26
4.1 Geleerde lessen 26
4.2 Aanbevelingen 26
4.3 Openstaande punten 27
Adviezen voor borging en beheer 28
Buiten scope geplaatst voor fase 2 (of voor vervolg) 30

Lessons learned Uniforme Bronontsluiting (fase 2)

Beproeving Uniforme bronontsluiting, fase 2 (Oktober 2025 – Juli 2026)

Dit document bevat enkele lessen die geleerd zijn in de uitvoering van de beproeving Uniforme bronontsluiting fase 2. In de eerste fase is het ontwerp en de specificaties voor uniforme bronontsluiting gedefinieerd en toegepast op de aansluiting door een gemeente op de basisinrichting voor OOTS (zie hieronder voor toelichting) bij RINIS. In de tweede fase is de oplossing voor Uniforme bronontsluiting hergebruikt voor het uitwisselen van gegevens met gekwalificeerde vertrouwensdienstverleners (QTSP's) in het kader van eIDAS. Het gaat om twee usecases waarbij gegevens uit de bron worden uitgewisseld met het doel om de EUDI wallet te voorzien van gekwalificeerde attesten over informatie uit de bron (zie hieronder voor toelichting).

Inleiding

Vanuit de Europese digitale transformatie, ook bekend als de EU Digital Decade, komen er verschillende digitaliseringswet- en regelgevingen op ons af. Een aantal van deze wetten richten zich op informatieverstrekking en informatiedeling. Hierbij worden de volgende wetten expliciet benoemd: Single Digital Gateway, met het Once-Only Technical System (OOTS) als voorziening en eIDAS 2.0 waarbij de EUDI Wallet zowel als inlogmiddel als gegevensdrager is voorzien. Naast deze twee wetten is de European Interoperability Act een ander wet die ingaat op het realiseren, verbeteren en optimaliseren van interoperabiliteit (samenwerking tussen wetten, organisaties, informatie en techniek). In de twee eerstgenoemde wetten zijn ook zogenaamde bewijsstukken, attestaties en/of getuigschriften genoemd. Afhankelijk van de wetgeving wordt één van de termen gebruikt. Voor de eenvoud wordt in dit document gesproken over een bewijsstuk en daarmee als enkelvoudige term gebruikt.

Als houder van verschillende bewijsstuk registers, denk bijvoorbeeld aan de bevolkingsregisters (GBA en Burgerlijke Stand), maar ook vergunningen en ontheffingen of gemeentelijke vergoedingen in het kader van inclusiviteit, zorgen ervoor dat gemeenten soortgelijke gegevens voor verschillende doeleinden dienen te delen. In het project 'Uniforme Bronontsluiting, afgekort UBO' is gekeken of gewenste informatie objecten uniform en eenduidig geleverd kunnen worden zodat deze in meerdere toepassingen hergebruikt kunnen worden.

Om gemeenten, o.a. wegens kostenbesparing en onderhoud, te ondersteunen bij een éénmalige verstrekking voor meervoudig gebruik is er een praktijkbeproeving uitgevoerd. Deze praktijkbeproeving heeft zich in de tweede fase van de beproeving gericht op ontsluiting van de gegevens en het aanbieden vanuit gemeenten aan zogenoemde gekwalificeerde vertrouwensdienstverleners (QTSP's). In de beproeving is daarbij hergebruik gemaakt van functionaliteit van de basisinrichting OOTS bij RINIS (onder verantwoordelijkheid van het ministerie van BZK). Er wordt in de beproeving dus niet alleen hergebruik gemaakt van de oplossing voor Uniforme bronontsluiting aan de kant van de gemeente, maar ook van functionaliteit dat centraal beschikbaar is vanuit OOTS. Dit sluit aan bij de adviezen die de Europese Commissie zelf geeft aan de lidstaten voortkomend uit het 'Synergies project' waarbij diverse onderlinge synergiën tussen de eIDAS en SDG/OOTS zijn verkend. In de beproeving is samengewerkt met de gemeente Rijswijk, softwareleverancier Enable-U in die gemeente, RINIS (basisinrichting OOTS), bureau Nationaal Coördinator SDG, vertrouwensdienstverlener (QTSP) Cleverbase en DigiLab.

In de beproeving in fase 2 werden twee verschillende usecases voor de uitwisseling met QTSP's uitgewerkt en getest. Op die manier ontstaat ook de daadwerkelijke beproeving van de 'uniformiteit' van de oplossing voor Uniforme bronontsluiting. Lukt het in de beproeving om de oplossing bij de gemeente uit fase 1 zonder aanpassingen te hergebruiken in fase 2 (met uitzondering van het doorvoeren van geleerde lessen uit fase 1)? De volgende twee usecases zijn beproefd in fase 2:

1. EUDI-wallet 1: verstrekken van een QEAA

In deze use case wil een burger zijn geboortegegevens als een hoog-betrouwbare attestatie in zijn EUDI-wallet krijgen. De burger gaat daarvoor naar een loket van de daarvoor door de gemeente aangewezen QTSP (bijvoorbeeld via de gemeentelijke website) en vraagt de attestatie op. De QTSP haalt de gegevens bij de gemeente op en verstrekt ze aan de EUDI-wallet van de gebruiker.

2. EUDI-wallet 2: attribuutverificatie

In deze use case verstrekt de burger een kopie van zijn geboortegegevens (bijvoorbeeld de oorspronkelijke akte) aan een QTSP met het verzoek de informatie als hoog betrouwbare attestatie in zijn wallet te zetten. De QTSP vraagt de gemeente om de authenticiteit van de geboortegegevens te controleren. Als de gemeente constateert dat de informatie klopt, kan de QTSP de geboortegegevens als QEAA aan de wallet verstrekken.

De beproeving heeft plaatsgevonden onder de volgende condities:

- Het gaat om het uitwisselen van gestructureerde data over geboorte (EU-schema)
- Gestructureerde data in JSON formaat (gestructureerde EU XML nog niet gereed)
- Allereerst met 1 testpersoon uit 1 gemeente (Rijswijk), waarbij de gegevens van de testpersoon uit de lokale (onpremises) bronapplicatie worden opgehaald.
- Belangrijkste focus ligt op het testen van de infrastructuur. Indien gebruikersfunctionaliteit niet volledig werkte of aanwezig was is deze gesimuleerd.
- Beproeving usecase 1 via hackathons met bijeenkomst op 16 december 2025.
- Beproeving usecase 2 via hackathons met bijeenkomst op 18 maart 2026.
- Uitwisseling vindt plaats met QTSP en presentatie van het attest over de geboortegegeven in de wallet van de deelnemende QTSP (Vidua).
- In de beproeving wordt ook getracht het attest in te laten lezen in de NL publieke wallet die in ontwikkeling is bij ICTU (in opdracht van ministerie van BZK).
- Documentatie, bevindingen en aanbevelingen uit de beproeving worden breed beschikbaar gesteld.

Meer informatie over de oplossing is te vinden in de opgeleverde documentatie:

https://digilab.overheid.nl/projecten/beproeving-eenvoudig-en-eenduidig-gegevens-uitwisselen/

https://gitlab.com/digilab.overheid.nl/ecosystem/uniforme-bronontsluiting

Documentatie

De volgende documentatie is opgeleverd vanuit het project en beschikbaar gesteld op de Digilab projectpagina of de gitlab omgeving van het project:

- Plan van aanpak voor fase 1

- Plan van aanpak voor fase 2
- Lessons learned document fase 1
- Lessons learned document fase 2 (dit document)
- Architectuur Uniforme bronontsluiting
- Ontwerpkeuzes fase 1
- Ontwerpkeuzes fase 2 (met beleidsadviezen) als bijlage bij de architectuur
- Specificaties verificatiefunctie in de basisinrichting
- Specificaties DATA-API (gemeente)
- Technische documentatie Enable-U
- Technische documentatie RINIS
- Specificaties uitwisseling QTSP usecase 1 (met gap analyse later verschenen ETSI standaard)
- Specificaties uitwisseling QTSP usecase 2
- Rulebook Geboortegegevens (attestatieschema)

Samenvatting Lessons Learned

Hieronder een samenvatting van de *"Lessons learned beproeving uniforme bronontsluiting fase 2"*. De samenvatting bundelt de belangrijkste inzichten, lessen en aanbevelingen.

Werkwijze en aanpak

- **Werken met aannames en iteratief testen werkt goed** in een onduidelijk beleidslandschap.
- **Strakke scope-afbakening is essentieel**: uitbreidingen tijdens het project veroorzaakten direct interoperabiliteitsproblemen.
- **Gebruik van bestaande infrastructuur** (zoals OOTS bij RINIS) versnelt ontwikkeling en bevordert herbruikbaarheid.
- **Afstemming met EU-initiatieven** (zoals ETSI, Synergies project) is cruciaal om aan te sluiten op toekomstige standaarden.

Samenwerking en governance

- Goede samenwerking tussen gemeenten, leveranciers, QTSP's en nationale partijen is noodzakelijk, maar:
    - Rollen en verantwoordelijkheden zijn nog onvoldoende uitgewerkt.
    - Beheer van configuraties en "common services" mist duidelijke afspraken.
- Voor opschaling is een duidelijke **governance- en beheersstructuur** nodig.

Technische lessen

Security (signing & encryptie)

- Noodzaak tot betere uitwerking van security in standaarden (zoals Digikoppeling API).
- Gebruik van moderne encryptie (eIDAS) i.p.v. verouderde standaarden is wenselijk.
- Onvoldoende richtlijnen voor:
    - wat wel/niet te versleutelen
    - sleuteluitwisseling

⇒ Er is behoefte aan **concrete implementatierichtlijnen en standaardisatie**.

FSC (data-uitwisseling en contracten)

- FSC biedt een sterke basis voor data-uitwisseling, maar:
    - Contractstructuren worden snel complex, vooral met delegatie.
    - Properties (contextinformatie) zijn nuttig maar niet gestandaardiseerd.
- Er is behoefte aan:
    - standaardisatie van FSC-properties

    - ondersteuning voor autorisatie (via FTV)
    - tooling zoals een **signing service** om contracten eenvoudiger te beheren.

DATA-API en gegevensmodellen

- Huidige aanpak legt **vertaling naar EU-schema's bij de bronhouder (gemeente)**.
- Dit kan leiden tot complexiteit en inconsistenties.
- Alternatief: data "as-is" aanbieden en vertaling bij afnemer leggen.
- Belangrijke verbeterpunten:
    - duidelijkere specificaties
    - betere documentatie
    - test- en validatiemogelijkheden

⇒ Advies: ontwikkelen van **validatieservices en referentiemodellen**.

Standaarden en versies

- Snelle opvolging van nieuwe versies (bijv. FSC) veroorzaakt integratieproblemen.
- Gebrek aan backward compatibility bemoeilijkt samenwerking.

⇒ Noodzaak voor **versiebeheer en release-afstemming** tussen nationale en EU-standaarden.

Specifieke inzichten voor eIDAS en wallet

Verificatiefunctie

- Centrale verificatie (bijv. via RINIS) biedt flexibiliteit en ontkoppeling van EU-schema's.
- Belangrijke aandachtspunten:
    - omgaan met verschillen in data (zoals spelfouten → fuzzy matching)
    - privacy vs. debugging (wel/geen data teruggeven)
    - nieuwe eis: verificatieresultaten moeten digitaal ondertekend worden
- Foutafhandeling en logging moeten beter worden ingericht voor productie.

Common Services (EU)

- Huidige implementatie is gebaseerd op OOTS en nog niet volledig geschikt voor eIDAS.
- Gebrek aan:
    - duidelijke semantiek (bewijs vs. attribuut)
    - gebruiksvriendelijke zoekfunctionaliteit
- Open vragen:
    - hoe om te gaan met meerdere bronnen en attributen
    - hoe gebruikersinteractie vorm te geven

eDelivery en toegang QTSP's

- eDelivery is logisch vanuit OOTS, maar:
    - QTSP's mogen huidige OOTS-netwerk niet direct gebruiken
- Er is Europese besluitvorming nodig over:
    - onboarding van QTSP's
    - identificatie en certificering

⇒ Anders zijn alternatieve architecturen nodig.

Juridische en organisatorische lessen (DPIA)

- DPIA is complex door:
    - technische aard van UBO
    - variatie in implementatie per gemeente
- Gemeenten blijven **zelfstandig verantwoordelijk** in een keten met meerdere partijen.
- Belangrijke vraagstukken:
    - AVG-grondslagen per usecase
    - rechten van burgers (inzage, logging)
    - dynamiek van gegevens en API's

⇒ Advies: ontwikkeling van een **model-DPIA en ondersteunende documentatie**.

Belangrijkste knelpunten en open vragen

- Noodzaak voor meer **beleidsmatige keuzes en landelijke/Europese kaders**
- Onvoldoende standaardisatie in:
    - gegevensmodellen
    - contractstructuren
    - security-implementaties
- Complexiteit in:
    - delegatie en contractbeheer
    - samenwerking tussen partijen
- Onzekerheid over:
    - rolverdeling (gemeente, RINIS, QTSP, EU)
    - beheer van centrale voorzieningen

Belangrijkste aanbevelingen

Voor techniek en implementatie

- Werk standaarden (Digikoppeling, FSC, API's) verder uit op basis van de leerervaringen
- Ontwikkel:
    - validatieservices
    - testfaciliteiten
    - referentie-implementaties
- Richt **beheer van API's en schema's** centraal of gestandaardiseerd in

Voor governance en organisatie

- Definieer duidelijke **rollen, verantwoordelijkheden en beheerprocessen**
- Zorg voor ondersteuning voor partijen (gemeenten, leveranciers, QTSP's)
- Werk aan Europese afstemming (eIDAS, ETSI, Common Services)

Voor beleid en opschaling

- Maak expliciete beleidskeuzes voor:
    - architectuur
    - gegevensdeling
    - verificatie
- Borg oplossing binnen:
    - GBO (Gemeenschappelijke Bronontsluiting)
    - Federatief Datastelsel
- Ontwikkel ondersteunende producten zoals:
    - model-DPIA
    - standaardcontracten
    - implementatiestappenplannen

Strategisch

- Zet in op **centrale voorzieningen (zoals RINIS/OOTS)** voor schaalvoordelen
- Stimuleer **hergebruik en interoperabiliteit binnen EU**
- Zorg dat oplossingen **uitlegbaar en toepasbaar** zijn voor gemeenten en andere gebruikers

Conclusie

De beproeving toont aan dat **uniforme bronontsluiting technisch haalbaar en herbruikbaar is**, ook voor nieuwe toepassingen zoals de EUDI wallet. Tegelijkertijd zijn er nog belangrijke uitdagingen op het gebied van **standaardisatie, governance, beleid en beheer**.

Lessons Learned

Betrokken partijen hebben gezamenlijk de voorbereiding voor de beproeving in fase 2 opgepakt aan het begin van het vierde kwartaal van 2025. Op basis van de voorstellen die hieruit zijn gekomen, heeft de beproeving van de eerste usecase plaatsgevonden in de maanden november en december. De beproeving van de tweede usecase vond plaats in de maanden april en mei van 2026. Meer informatie over de opzet van de beproeving is terug te lezen in het plan van aanpak voor fase 2. Informatie over de architectuur en de gemaakte ontwerpkeuzes is terug te lezen in het architectuurdocument. Daarbij is een bijlage opgeleverd met ontwerpkeuzes die vragen om beleidsmatige toets en afwegingen.

Uit de beproeving zijn de geleerde lessen opgetekend door de betrokken partijen en in dit document opgenomen. Voor de overzichtelijkheid zijn de lessen opgenomen in categorieën. Naast lessons learned zijn er ook vraagstukken, aandachtspunten en vervolgacties opgenomen. Bij alle punten in dit document is geprobeerd aan te geven of het specifieke ervaringen of aandachtspunten zijn voor eIDAS, dan wel breed voor uniforme bronontsluiting, en of het gemeentespecifieke aandachtspunten zijn of overheidsbreed gelden.

Uit de eerste fase van de beproeving zijn lessons learned gedocumenteerd. Hiervoor is een apart document beschikbaar en gepubliceerd op Digilab: Lessons learned uniforme bronontsluiting fase 1(v3) In fase 2 zijn een aantal aanbevelingen uit die geleerde lessen opgepakt en beproefd. Deze zijn meegenomen in dit document.

1. Algemene lessen

1.1 Geleerde lessen

Hieronder worden de geleerde lessen en vraagstukken vanuit de beproeving over de voorbereiding en uitvoering van de beproeving opgesomd:

Werken met expliciete aannames in een beleidsomgeving die volop in beweging is

Ook in deze fase is niet afgewacht welke keuzes er in Nederland worden gemaakt ten aanzien van de inrichting van het stelsel ten behoeve van bronontsluiting naar QTSP's. Op basis van bestaande informatie uit de verordening, het Architectural Reference Framework (ARF), de Large Scale Pilots (LSP) in de EU, het synergie project van de EU, de ontwikkeling van standaarden in de EU (o.a. bij ETSI) en beschikbare documentatie in Nederland (waaronder de Q&A op artikel 45 van het ministerie van Economische Zaken) zijn diverse voorstellen uitgewerkt voor een realistisch scenario per usecase. Geen tijd voor het afwachten van allerhande discussies die nog lopen (bijvoorbeeld over de architectuur voor QTSP's), maar focus op hetgeen bij de gemeente moet worden geïmplementeerd en vrij stabiel kan worden ingezet in lopende ontwikkelingen. Bovendien kan daarmee de verdere beleidsontwikkeling mogelijk nog worden beïnvloed in het voordeel van uniforme bronontsluiting en efficiënte en effectieve implementatie bij gemeenten.
Geleerde les: het heeft voor het doel van dit project goed gewerkt om aannames te formuleren en van daaruit een concrete oplossing te ontwikkelen en beproeven.

En ook in deze fase heeft het goed gewerkt om met partijen een duidelijk doel met strakke tijdslijnen af te spreken (de uitwisseling kunnen laten zien op de geplande bijeenkomsten) en een duidelijke scope afbakening: vooral beproeving van de gegevensuitwisseling (niet de gebruikersflow) en hergebruik van bestaande inrichting bij alle partijen. Sterker nog, op momenten dat er gaandeweg wat scope uitbreidingen plaatsvonden, was dat meestal meteen een moment waarop er problemen ontstonden met de onderlinge interoperabiliteit. In sommige gevallen werd dit veroorzaakt door tussentijdse wijzigingen van de standaarden die werden toegepast. Hierover later in dit document meer.
Geleerde les: het is essentieel voor dit project gebleken om de afgesproken scope vast te houden. Dit was niet makkelijk in een omgeving met veel schuivende panelen. De neiging is groot om het project steeds mee te laten bewegen met nieuwe keuzes en afspraken. Daar waar dit is gebeurd, bleek het meebewegen steeds een nadelig effect te hebben op het projectresultaat.

Aandachtspunt is dat er geen duidelijkheid vooraf is gekomen dat de architectuur compliant is met het Nederlands beleid en de uitwerking van het EDI stelsel met bijbehorende architectuurvoorstellen daar. Het project heeft daarom de diverse ontwerpkeuzes met mogelijk effect voor beleidsuitgangspunten en architectuur op nationaal niveau voor EDI opgenomen als bijlage in het architectuurdocument en besproken met het verantwoordelijk departement (BZK). Op die manier kunnen leerervaringen worden meegenomen in de verdere ontwikkeling en definitie van het beleid en het EDI stelsel. Deze vraagstukken zijn ook van belang voor de toekomstige inzet van de oplossing die is beproefd, evenals het borgen daarvan. Het document bevat daarmee de lessons learned met een beleidscomponent. De beleidsvraagstukken uit fase 1 blijven daarnaast onverminderd van kracht. Fase 2 van de beproeving heeft het belang van die vraagstukken, en met name het komen tot een oplossing hiervoor, herbevestigd. Enkele van die vraagstukken zijn inmiddels ook opgenomen in een zogenoemde Uitvoeringsstrategie EDI van het Netwerk van Publieke Dienstverleners (NPD) en de VNG, aangeboden aan de ministeries van BZK en EZ.
Geleerde lessen: er zijn belangrijke beleidsmatige aannames gedaan die nog niet zijn bekrachtigd. Bredere implementatie is alleen goed mogelijk na beleidsmatige keuzes (opgenomen als bijlage bij de architectuur).

Waarde van samenwerking met markt, Europese Commissie en LSP's.

Er is de nodige afstemming geweest met medewerkers van de Europese Commissie over de voorstellen in het project. Er is onder andere voortgeborduurd op hetgeen is neergezet en uitgewerkt voor het EU Synergies project tussen OOTS en de wallet. Zo kon het project gebruik maken van hieruit voorgestelde specificaties voor berichten met de QTSP die in ETSI verband verder tot standaard worden gedefinieerd. En is gebruik gemaakt van de proefomgeving voor de common services en de toepassing daarvan in usecase 2 van de beproeving. Zonder deze voorbereidingen in EU verband had het project meer zelf moeten uitwerken aan specificaties en proefomgeving. Bovendien kan zo worden voorgesorteerd op EU brede oplossingen en kan het project vanuit de beproeving enigszins sturing geven aan de verdere ontwikkeling van oplossingen op EU niveau.
Geleerde les: de afstemming met de EC heeft het project geholpen om de Common services in te zetten voor de EUDI-wallet en heeft de EC geholpen bij het doorontwikkelen ervan.

In deze fase hielp het dat er vanuit Cleverbase veel kennis en ervaring aanwezig was ten aanzien van de door de EU voorgestelde standaarden en infrastructuur. Cleverbase werkte met

Domnibus referentiecomponenten die voor beide usecases minimaal moesten worden ingericht om uitwisseling moeglijk te maken. Dit is door Cleverbase ervaren als een laagdrempelige manier om aan te sluiten voor QTSP's met behulp van bestaande infrastructuur. Op het moment dat er daadwerkelijk gegevensuitwisseling naar productie gaat en er meer QTSP's aansluiten, is het wel belangrijk na te denken over de ondersteuning bij bijvoorbeeld het testen, het registreren en beheren van de common services, en andere randvoorwaarden die nu door Cleverbase en RINIS zijn ingevuld voor de beproeving.
Geleerde les: het ontbreekt aan afspraken over het beheer van de configuratie van de gegevensuitwisseling in de common services, zodra die ook ingezet worden voor de EUDI-wallet.

Belang van demonstraties en testopnames.

Van de demonstratie van beide usecases is een filmpje opgenomen. De opname hebben we gebruikt in meerdere andere presentaties over Uniforme bronontsluiting. Een enkele keer hebben we de live demonstratie herhaald, bijvoorbeeld op de demonstratiedag van het innovatiebudget Digitale Overheid op 12 februari 2026.
Geleerde les: het is belangrijk opnames te maken van de testflows.

Releases standaarden

In de beproeving zijn meerdere bestaande standaarden toegepast. Er is veel afhankelijkheid en impact van de verschillende releasecycli van deze standaarden. Enkele leerervaringen volgend hieruit:

- Gedurende de uitvoering van de beproeving kwamen nieuwe versies van de FSC standaard uit (en verschillende releasecandidates) met bijbehorende vertaling naar de open source bouwstenen. Niet alle versies waren backwards compatible. Daarnaast was het voor de beproeving noodzakelijk specifiek gebruik te maken van functionaliteit uit de nieuwe versie van de standaard. Dat betekent dat iedere betrokken partij over moest naar dezelfde nieuwe versie. De snelle opvolging van versies (of gebruik van release candidates) zorgde in het project voor problemen in de onderlinge uitwisseling.
- De specificaties voor de uitwisseling tussen QTSP en RINIS platform zijn voor usecase 1 specifiek voor die beproeving opgesteld, omdat de huidige ETSI standaarden voor de uitwisseling tussen QTSP's en bronnen nog niet beschikbaar waren. Nu deze er wel zijn, is een gapanalyse opgesteld ten opzichte van de specificaties uit usecase 1 en opgenomen in de documentatie. Het is belangrijk om deze ontwikkeling in de gaten te houden en de oplossing hierop verder aan te passen.

1.2 Aanbevelingen

Bij het verder opschalen van een oplossing is het goed om een overkoepelend overzicht te houden over welke versie van standaarden zijn geïmplementeerd, hoe die onderling effect hebben en of daarmee bepaalde functionele wensen/ afspraken over de gegevensuitwisseling wel/niet kunnen worden uitgevoerd. Daarmee kan mede de roadmap voor toepassing en implementatie worden bepaald.

Er zal duidelijkheid moeten komen over rolverdeling tussen alle betrokken partijen (wat doet de gemeente, wat doet de leverancier van de gemeente, wat doet RINIS, wat doet bNC, wat doet de QTSP, wat doet de EU Commissie?) en noodzakelijke stappen in voorbereiding op productiegang.

Dit betekent dus ook het opzetten en inrichten van een governance rond configuratiebeheer en ketenafspraken.

1.3 Openstaande punten

Voor uiteindelijke opschaling is het van belang om de beleidsmatige vraagstukken uit deze fase van beproeving die gaan over EDI, evenals de verschillende ontwerpkeuzes te borgen binnen EDI wetgeving, EDI beleid en het EDI-stelsel.

Daarnaast is voor opschaling van belang dat voorzieningen productiewaardig worden ontworpen en ontwikkeld. Mogelijk kunnen generieke functies die nodig zijn om bronontsluiting voor de eIDAS usecases werkend te krijgen, worden ontwikkeld binnen het programma Gemeenschappelijke Bronontsluiting.

2. Lessen Techniek

2.1 Geleerde lessen

Signing & encryptie

Toepassen van signing en encryptie van de berichtinhoud als extra beveiliging van de gevoelige gegevens die worden uitgewisseld. Het voorstel hiervoor is opgesteld met behulp van een aanvulling op de signing en encryptie in de DigiKoppeling standaard en verder uitgewerkt voor uitwisseling via het REST API profiel door het project. Specificaties zijn gepubliceerd als onderdeel van de specificaties voor Uniforme Bronontsluiting. Toelichting is gegeven in het document met Interface specification versie 2.1. Hieronder zijn de geleerde lessen uit de beproeving weergegeven:

- In de beproeving is targeted encryptie toegepast (alleen op privacygevoelige gegevens, ipv alles encrypten). Deze keuze is gemaakt om troubleshooting mogelijkheden over te houden met behulp van niet encrypted gegevens.
- In de beproeving is gebruik gemaakt van het algoritme vanuit eIDAS 2 voor encryptie in plaats van de verouderde versie voor Digikoppeling. Dit is als wijziging op de standaard ingediend bij Logius.
- Signing & encryptie is onderdeel van de specificatie van het Digikoppeling Rest API-profiel, maar daarin nog onvoldoende uitgewerkt voor implementatie in de praktijk. Het project heeft voorstellen voor uitwerking gedaan.
- Er ontbreekt een richtlijn voor het bepalen welk deel van de gegevens versleuteld moeten worden en welk deel onversleuteld getransporteerd mogen worden (over een beveiligde verbinding). In de beproeving zijn hiervoor eigen keuzes gemaakt binnen implementatie van de get Data Digikoppeling API.
- Ervaringen met het gebruiken van de door Digikoppeling standaard aanbevolen library t.b.v. signing functie (DSS – Digital Signing Service open source software library) is opgenomen in de nieuwe versie van de Uniforme Bronontsluiting specificatie (2.1)
- Ervaringen met het gebruiken van de Nimbus library t.b.v. encryptie functie is opgenomen in de nieuwe versie van de Uniforme Bronontsluiting specificatie (2.1)

Gebruik van ‘properties’ in de FSC standaard

Properties zijn in FSC bedoeld om contracten van elkaar te kunnen onderscheiden en de vragende peer in staat te stellen naar het contract te verwijzen dat de grondslag voor de bevraging biedt. In de opzet van de beproeving is ervoor gekozen om AVG grondslag, verwerkingsrelatie en het kanaal van waaruit de bevraging volgt, mee te kunnen laten geven via deze properties. Op die manier kan duidelijk worden gemaakt vanuit welke achtergrond de basisinrichting OOTS een bevraging start op de gemeentelijke bron, aangezien RINIS voor verschillende usecases de bevraging van de bron organiseert als ‘brugfunctie’ naar organisaties buiten de Nederlandse overheid. De gemeente kan deze informatie vervolgens loggen. Het toepassen van deze contractparameters (FSC-properties) is mogelijk door een uitbreiding van de FSC standaard. De voorgestelde 3 propertiesoorten die zijn gebruikt in de beproeving worden meegegeven aan FSC beheer voor mogelijk hergebruik door andere deelnemers in het FSC netwerk. Meer toelichting is gegeven in het architectuurdocument Uniforme Bronontsluiting

onder paragraaf 2.6 FSC configuratie. Hieronder volgen een aantal geleerde lessen uit de beproeving hiervan:

- FSC biedt een solide basis voor het beheren van de datauitwisselingen tussen publieke bronhouders enerzijds en OOTS/EUDI-wallet anderzijds. Voor bredere implementatie van UBO zijn FSC properties nodig om de FSC datacontracten van elkaar te onderscheiden. Het project heeft drie properties gedefinieerd en beproefd.
- Voor bredere implementatie is een oplossing nodig voor autorisatie op de gegevenssets van een dataservice (FTV). Contractparameters worden niet gebruikt voor toegangsverlening tot (sets van) attributen, maar alleen om aan de bron door te geven vanuit welke grondslag/rol/context de vraag aan de bron is gesteld (om dat te kunnen loggen). FSC gaat namelijk over de verbinding, niet wat er over die verbinding wordt uitgewisseld. Als de usecases voor uniforme bronontsluiting uiteindelijk vereisen dat er onderscheid gemaakt moet worden in welke gegevens door welke partijen benaderd mogen worden dan is het goed om te werken met een policy voor toegang op gegevenssets/ bepaalde attributen. Het project Federatieve Toegangsverlening (FTV) werkt hiervoor nationale afspraken en standaarden uit. Daar kan de oplossing voor uniforme bronontsluiting in de toekomst bij aansluiten.

Delegatie

In de architectuur (paragraaf 2.6) is aangegeven welke rollen en daarmee welke delegatie van verantwoordelijkheid voor de gegevensuitwisseling wordt vastgelegd en uitgevoerd via de FSC standaard. Het toepassen van delegatie heeft in fase 1 nog niet plaatsgevonden. In de 2e fase is dit toegepast door Enable-U namens Rijswijk deel te laten nemen en RINIS namens Cleverbase (QTSP). Om deze delegatiemogelijkheden te ondersteunen is behoefte aan een ‘signing service’ waarmee de delegatie eenvoudig door gemeente en QTSP kan worden vastgelegd via een portaal zonder als organisatie die alles heeft uitbesteed zelf een FSC manager te moeten implementeren. De partijen ondertekenen via de signing service de onderlinge datacontracten die worden toegepast in de gegevensuitwisseling. Door FSC beheer wordt gewerkt aan deze service. Vanuit de beproeving is input geleverd voor het ontwerp daarvan, geredeneerd vanuit praktijkervaring en behoeften. De oplossing zelf is nog niet beproefd. In de laatste beproeving is gewerkt met een situatie waarbij RINIS voor alle betrokken partijen een FSC manager hostte en daarmee de delegatiemogelijkheden toch konden beproeven. Uit het meedenken over de signing service en het beproeven van delegatie via FSC komen de volgende leerervaringen:

- FSC-contractrelaties kunnen verschillen per use-case en in FSC snel complex worden. Er is een goed contractontwerp nodig voor implementatie van een use-case. Er moet overeenstemming over dit ontwerp zijn vanuit praktisch en juridisch perspectief.
- Delegerende partijen ervaren het installeren en gebruiken van een eigen FSC-manager als een grote inspanning ten opzichte van hun rol in de inrichting van de gegevensuitwisseling. Er is behoefte aan de FSC signing service (in ontwikkeling) om delegerende partijen te ontlasten.
- Er is nog een ingewikkeld vraagstuk bij de inrichting van de FSC signing service voor partijen die geen eHerkenning kunnen of mogen gebruiken. Er zijn momenteel nog geen goede (Europese) alternatieven voorhanden voor het inloggen namens een bedrijf dat niet in Nederland geregistreerd is.

DATA-API specificaties

Er is één service gedefinieerd (DATA-API) waaraan vragende partijen verschillende gegevens ten behoeve van OOTS bewijsstukken of wallet attestaties kunnen vragen aan die API. Daarachter moet je de gegevens verzamelen bij de bron om het via de API beschikbaar te stellen. Uit de implementatie en toepassing van de specificaties komen de volgende leerervaringen:

- Met deze oplossing wordt van de verstrekker (de gemeentelijke bron in deze beproeving) verwacht een vertaalslag te maken van de eigen data uit de applicaties naar de gevraagde Europese, kanaal specifieke objecten in de DATA-API. Nieuwe bewijsstukken worden gematcht met de bestaande API en de verstrekker moet hiervoor een nieuwe vertaalslag maken. Daarmee zijn de taken voor vertaling naar het gevraagde schema bij de bewijsverstrekker neergelegd. De vraag is of dit de beste manier voor verdere implementatie en opschaling is. Een andere optie is om de data als bron aan te bieden (as is) en de vertaalslag bij aanvrager leggen. Zo voorkom je wellicht ook leverancierspecifieke interpretatie en implementatie van de DATA-API gebaseerd op de vraagschema's.
- De ervaring vanuit Enable-U is dat de huidige specificaties zonder toelichting niet direct duidelijk maken wat je als leverancier moet doen. Daar is nu uitleg bij nodig geweest vanuit het project, maar zou meer uit zichzelf begrepen moeten kunnen worden. Zo zijn er bijvoorbeeld onduidelijkheden over wat je met de metadata moet doen en welke type gegevens worden gevraagd. Aangezien later de encryptie is toegevoegd is daarmee ook niet duidelijk voor de gegevens of je die encrypted en unencrypted kan verstrekken. Laatste aandachtspunt is dat het lastig is te testen of de API goed is geïmplementeerd. Dat heeft ook te maken met het voorgaande punt. Of de API goed is geïmplementeerd weet je pas in ketentesten met andere partijen. Terwijl je als leverancier ook graag zelf zou willen testen. Geleerde les: voor bredere uitrol van UBO is een uitgebreidere specificatie nodig van de manier waarop bronhouders de DATA API moeten aanbieden. Verder is er behoefte aan een validatieservice, waarmee bronhouders of hun ICT leveranciers hun implementatie van de DATA API kunnen toetsen.

(Her)gebruik functionaliteit Basisinrichting OOTS

In de tweede fase van de beproeving is hergebruik gemaakt van stukken van de functionaliteit van de Basisinrichting OOTS bij RINIS. Deze basisinrichting levert niet alleen de gegevens via de in de EU afgesproken standaarden en infrastructuur aan bij de QTSP, maar ondersteunt ook de verificatiefunctie die de bedoelde verificatie van de authentieke bron volgens artikel 45 uit eIDAS mogelijk maakt. Daarvoor is onder andere een kopie van de zogenoemde OOTS-V backend ingezet in de combinatie met de open FSC componenten en het eDelivery toegangspunt. Aangezien in de beproeving gekozen is voor een aansluiting van QTSP's via het eDelivery netwerk en standaarden, kon ook deze component uit de OOTS basisinrichting worden hergebruikt. Er zijn in de beproeving geen relevante geleerde lessen en vraagstukken over het gebruik van deze functies opgetekend. Er zijn wel aanbevelingen en openstaande punten benoemd in de volgende paragrafen.

1.3 Aanbevelingen

Uit bovenstaande leerervaringen volgen onderstaande aanbevelingen voor verdere ontwikkeling en implementatie van de oplossing.

De FSC-properties zijn nog niet gestandaardiseerd. Er is een afspraak nodig over de te gebruiken properties zodat ze eenduidig geïnterpreteerd kunnen worden door alle deelnemers. Het project heeft hier een voorstel voor gedaan.

Er is behoefte aan een Signing Service en het is aan te bevelen deze verder te ontwikkelen.

Bij verdere ontwikkeling en implementatie is het belangrijk om release- en versiebeheer te organiseren voor alle toegepaste standaarden binnen de oplossing. Het is goed om op de hoogte te blijven van de releasekalender van die standaarden. En in de gaten houden of er nieuwe standaarden worden uitgebracht met effect op de architectuur. Voor UBO is het bovendien van belang om die releases in relatie te zien tot releases van de infrastructuur, zoals het platform bij RINIS, alsmede de releases van de EU standaarden. Op die manier kunnen eventuele onderlinge effecten van en relaties tussen die wijzigingen worden gedetecteerd en kan worden bepaald hoe daarmee om te gaan.

In de beproeving is gewerkt met attributen uitgegeven door de QTSP met een geldigheid van 24u. Op die manier waren afspraken over revocatie en de implementatie daarvan binnen de beproeving niet nodig. Voor de uiteindelijke toepassing in de praktijk is het goed om afspraken te maken over revocatiebeleid. Het wekt verwarring bij gebruikers als iedere gemeente daarin voor dezelfde (type) gegevens ander beleid kiest. En voor het stelsel is het een last als bronnen allemaal een andere keuze voor de techniek en standaarden voor revocatie kiezen (binnen de voorstellen die de ARF benoemt). Dit aandachtspunt is ook opgenomen in de eerdergenoemde uitvoeringsstrategie EDI van de NPD en VNG.

In de beproeving is het format voor de geboortegegevens beschreven aan de hand van een eerste opzet van een schema voor het geboortebewijs uit een samenwerking tussen een aantal EU lidstaten binnen OOTS verband. Dat schema was nog in ontwikkeling. Inmiddels is een laatste versie van de XML schema voor geboortegegevens uit OOTS beschikbaar (versie 6.4). Het is noodzakelijk om nog een vertaling naar dit nieuwe schema te maken voordat uitwisseling in productie vorm kan krijgen. Het is belangrijk om een beheerproces voor de API specificaties in te richten die aansluit bij de ontwikkeling van de schema's voor bewijzen (OOTS) en attributen (eIDAS) in EU verband. Voor de Nederlandse standaarden voor gegevensuitwisseling is het van belang de EU standaardisatie te volgen voor maximale interoperabiliteit over de grenzen heen.

Het is ook goed om aandacht te geven aan ondersteuningsmiddelen richting de partijen die moeten implementeren, bijvoorbeeld voor:

- Hoe te bouwen
- Hoe te testen (bijvoorbeeld een validatieservice)
- Hoe zichtbaar krijgen voor het netwerk welke gegevens je beschikbaar hebt
- Referentiemodellen
- Welke usecases

De conclusies en bevindingen met betrekking tot het hergebruik van functionaliteit is input voor het project Gemeenschappelijke Bronontsluiting (GBO) van het ministerie van BZK bij ICTU. Dit project ontwerpt en ontwikkelt generieke functionaliteit voor de gegevensuitwisseling. Zie o.a.: https://ictu.github.io/GBO/voorblad/

2.3 Openstaande punten

Uit de beproeving van de techniek zijn nog de volgende openstaande punten van belang.

Er is nog discussie over het uitwisselen van cryptografische sleutels tussen partijen. Dit is binnen Digikoppeling API versie 3.1 nog niet uitgewerkt. Het voorstel om via metadata endpoint van FSC manager sleutels dynamisch op te halen is besproken beheerder van de Digikoppeling standaard (Logius). In de beproeving hebben we deze sleutels statisch vooraf tussen partijen uitgewisseld.De genoemde optie voor het beschikbaar stellen van de data as is en het toepassen van het gewenste schema voor verdere uitwisseling bij de vraagsteller ook beproeven en te bepalen wat de beste keuze is voor verdere uitrol.

De volgende functies van de Basisinrichting OOTS zijn in de beproeving nu niet hergebruikt. In de verdere doorontwikkeling naar een schaalbare oplossing binnen GBO is het van belang te onderzoeken of deze functies ook een rol kunnen spelen voor meerdere kanalen en dus mogelijk hergebruikt kunnen worden:

- (re)authentication
- Preview
- Confirmation to send the data
- Logging & audit trail
- Payment

Een QTSP en een bron moeten kunnen aantonen dat gegevens bij de bron zijn opgehaald, dat de juiste bron is benaderd en dat de manier waarop de routering is uitgevoerd aantoonbaar en volgbaar is. RINIS heeft een rol in die processen en moet mogelijk richting aangesloten bronnen en QTSP's informatie aan kunnen leveren die voor de auditprocessen van die partijen weer van belang zijn, dan wel via wetgeving bepaalde verantwoordelijkheden hiervoor kennen. Incidenten die plaatsvinden bij RINIS en de aangesloten partijen benadeeld, moeten door de partijen weer gerapporteerd kunnen worden. Zeker de QTSP's die daarvoor diverse verplichtingen kennen richting auditors. Onafhankelijk toezicht en toetsing op RINIS, als die een dergelijke rol krijgt zoals in de beproeving, is dan aan de orde. Voordeel van centrale functionaliteit bij RINIS is wel dat het toezicht minder complex en omvangrijk kan zijn, dan de situatie waarbij vele partijen de rol invullen van routeren, generieke functies e.a. Toezicht is makkelijker als dat meer uniform en meer centraal wordt gerealiseerd.

3. Specifieke inzichten voor eIDAS

3.1 Geleerde lessen

Verificatie(module)

In het document met specificaties verificatiefunctie is het ontwerp van deze generieke functie voor attribuutverificatie opgenomen als bijlage bij de architectuur UBO. In het document staan de verschillende ontwerpbeslissingen en aandachtspunten bij het ontwerp opgenomen. In het document is voor verschillende onderdelen van het ontwerp steeds opgenomen welke keuzes er zijn gemaakt voor de beproeving onder het kopje 'Vereenvoudigingen voor beproeving'. Uit deze punten zijn leerervaringen te destilleren en aanwijzingen voor acties die nodig zijn om de functionaliteit uiteindelijk in een productiesituatie te kunnen toepassen. Hieronder volgen een aantal leerervaringen uit het ontwerpen en beproeven van de verificatiefunctie.

- Het voordeel van een landelijke verificatiefunctie in het intermediaire platform is dat geen harde koppeling meer is aangebracht tussen keuzes in Europa over prioritering en uitwerking van attributenschema's en de bundeling van gegevens tot een attribuut en de schema's die in Nederland en bijvoorbeeld in het Federatief Datastelsel beschikbaar zijn. Kortom, de implementatie in Nederland hoeft niet te wachten tot er op Europees niveau afspraken zijn gemaakt over de exacte gegevensset/ wat een (set van) attribuut is. In de verificatiefunctie kan een match worden gerealiseerd tussen hetgeen aan standaarden in Nederland beschikbaar is, met hetgeen QTSP's aan vragen en schema's beschikbaar hebben.
- Een te verwachten issue in de toepassing van de verificatiefunctie die momenteel niet in scope van de beproeving lag: Wat doe je met misspelling en andere type lettergebruik e.d.? Er zijn nu eenmaal andere taalmodellen in Europa en gebruikers kunnen makkelijk typefouten maken, dan wel registers bevatten een net andere spelling van bijvoorbeeld een adres of woonplaats. Zeker in de situatie dat bestaande documenten worden gescand en omgezet naar een set te verifiëren gegevens vanuit de QTSP kunnen makkelijk fouten ontstaan. Het concept van 'fuzzy matching' speelt dan een rol.
- In de beproeving is ervoor gekozen om de gegevensset die gebruikt is voor verificatie ook mee te geven met het antwoord, omdat dit kan helpen bij eventuele foutopsporing. En dat kan ook helpen bij eventuele 'fuzzy matching'. De vraag is of dit voor de uiteindelijke situatie ook voldoende reden is, of dat het vanuit privacy- en/of beveiligingsredenen beter is om in het antwoord alleen een ja of nee te vermelden. In de ETSI standaard is de keuze gelaten om de gegevensset na de verificatie wel of niet mee te geven in het antwoord terug aan de QTSP. In de laatste conceptversie van de nieuwe uitvoeringshandeling lijkt echter bepaald te zijn dat waarden alleen nog bij een fuzzy match worden teruggegeven.
- Voor toezicht op de QTSP en de oplossing voor verificatie is het straks van belang dat duidelijk is voor een bronhouder dat een gecertificeerd QTSP een vraag stelt en dit doet uit naam van een gebruiker, in plaats van een partij die geen gecertificeerde QTSP is? De oplossing stoelt op 3 ontwerpkeuzes hiervoor en bijbehorende aandachtspunten:
  1) Er is in het voorstel sprake van een afgeschermd eDelivery netwerk waar alleen geaccrediteerde QTSP toegang toe moeten krijgen, evenals namens de lidstaten de

nationale verificatiepunten. We willen graag dat de EU Commissie dat gaat inrichten, al dan niet vanuit nationale input hierover via de coördinatoren.

2) Met behulp van FSC datacontracten wordt vastgelegd wie de bron mag benaderen en cryptografisch ondertekend door de eigenaar van de bron. In FSC moet dan worden vastgelegd en ondertekend dat RINIS specifieke API bevragingen bij bronnen mag doen ten behoeve van de uitvoering van verificatie namens QTSP's (die alleen via het vertrouwde netwerk communiceren met RINIS, zie punt 1).
3) De QTSP wordt geaudit op de uitvoering van haar processen conform de richtlijnen. Eén van de richtlijnen zou moeten zijn dat de QTSP alleen een verificatie uitvoert als zij daarvoor een toestemming hebben gekregen van de gebruiker en deze hebben vastgelegd in logging. In de ETSI standaard voor de berichten tussen QTSP en bron (toegepast op de uitwisseling tussen QTSP en RINIS) is wel de mogelijkheid opgenomen om aan te geven dat de gebruiker de toestemming heeft gegeven (ja/nee), maar dat is altijd ja, anders werkt de gegevensuitwisseling niet. Liever hebben wij een digitale handtekening/ bewijs van de gebruiker die dan doorgegeven wordt. Daarvoor zijn de ETSI specs onvoldoende volwassen op dit moment.

Toepassing EU Common Services (CS) door QTSP

Het voorstel voor attribuutverificatie gaat uit van gebruik van de Common Services (CS) door de QTSP bij het zoeken naar de betreffende bron voor een set van attributen ter verificatie. Voor de beproeving zijn specificaties opgesteld voor het bevragen van de CS door de QTSP en de proefomgeving van de CS hiervoor ter beschikking gesteld. Toepassing ervan is geschetst in de eindpresentatie van Cleverbase. In de Common Services is voor de QTSP het schema van het geboortebewijs voor verificatie terug te vinden (om een mapping te maken met de gegevens die de gebruiker heeft aangeleverd bij de QTSP) en adresseringsinformatie in de vorm van het eindpunt van de verificatie service (in de beproeving bij RINIS) evenals informatie over de authentieke bron (in dit geval de gemeente Rijswijk). In de bevraging door de QTSP naar de verificatiefunctie wordt die informatie gebruikt: een atributt Identifier, die een link heeft naar bijhorende attestatie schema van normatieven attributen om te weten welk attestatietype er geverifieerd moet worden en wat de authentieke bron moet leveren. Ten aanzien van het gebruik van de Common Services zijn de volgende geleerde lessen opgetekend:

- In de beproeving is gewerkt met de functionaliteit die bedoeld is voor OOTS en niet is aangepast op eventuele toepassing van de Common Services in eIDAS verband (zoals voorgeschreven in de ETSI specificatie). Dat betekent ook dat er een workaround is gebruikt door de bestaande asset type "evidence_type" uit OOTS in te vullen met het attribuut type binnen eIDAS. Ook de manier van zoeken is hierop aangepast. Mogelijk wordt in de toekomst wel een speciaal "attribuut"-type toegevoegd voor eIDAS doeleinden, samen met aanpassingen aan de Common Services als gevolg van de lopende synergiediscussie OOTS-eIDAS. We hebben het werkend gekregen met de huidige userinterface, maar alleen al het verschil in woordgebruik laat zien dat er behoefte is aan meer wallet terminologie (zoals bewijstype vs attestatietype). Dit vraagt aandacht om dat meer passend te maken. Goed om onze leerervaringen mee te geven aan EU commissie.
- Als er meerdere bronnen zijn, hoe werkt dan opzoeken in de semantic repository door de QTSP in afstemming met de gebruiker? Hoe gaat de flow eruitzien als er steeds meer attestaties en bronnen beschikbaar komen? Hoe ga je dat laten zien aan de gebruiker? Voor elke nieuwe attestatieschema moet de QTSP functionaliteit ontwikkelen om de gebruiker door de bronnen heen te leiden. Hoe zou je de common services dynamisch kunnen gebruiken en interactie met de gebruiker organiseren hiervoor? Huidige zoekfunctie en

interface zijn niet echt geschikt voor dynamisch opzoeken. Wellicht is het beter om die interactie binnen de Common Services zelf mogelijk te maken en functionaliteit hiervoor aan te bieden richting de gebruiker. Hiervoor kan worden afgekeken bij de OOTS-A functie van de basisinrichting OOTS die het zoeken in de Common Services begeleid.

- Belangrijke keuze die voor het gebruik van de Common Services door de QTSP nog gemaakt moet worden, is of je de beide gebruiksacties altijd bij elke interactie met een gebruiker moet uitvoeren. Het gebruik van de Common Services bestaat uit twee stappen: 1. attribuut schema behorend bij de gegevens opvragen, 2. Adres opvragen van het verificatie endpoint/ bron. Er zijn een drietal mogelijkheden om die stappen uit te voeren:
  1. Beide stappen bij elke verificatie opnieuw doorlopen voorafgaand aan het verificatieverzoek (met als risico: extra activiteit en dus doorlooptijd met kans op fouten, terwijl deze informatie vrij statisch is);
  2. Voor een bepaald document/ set gegevens beide stappen één keer uitvoeren en vervolgens alleen het verificatieverzoek per gebruikersinteractie (met als risico: dat bij wijzigingen in schema of endpoint er fouten optreden in het uitvoeren van het verificatieverzoek);
  3. De eerste stap één keer uitvoeren, en vervolgens bij elke gebruikersinteractie het endpoint opvragen en verificatieverzoek uitvoeren.
- Cleverbase destilleert de gegevens van de geboorteakte die de burger aanlevert bij Cleverbase (in de beproeving via upload van het document in een portaal) en bekijkt welke daarvan nodig zijn voor de standaard attributenset die hoort bij het equivalent van de geboorteakte. Het is de vraag hoe dit precies gaat werken uiteindelijk. Geeft de burger aan wat die nodig heeft, doet Cleverbase een voorstel op basis van bekende attributenschema's? In de beproeving is gewerkt vanuit het voorstel dat de QTSP weet welke QEAA afgegeven kan worden (configuratie van de QTSP). De QTSP informeert de gebruiker over de QEAA die het kan krijgen. Als er meerdere QEAA's uitgegeven kunnen worden op basis van een geboorteakte, kiest de gebruiker welke hij wil. De gebruiker uploadt zijn geboorteakte. De QTSP interpreteert de akte op een standaard en geautomatiseerde manier en destilleert daaruit de (kandidaat) QEAA-attributen. De QTSP biedt die ter verificatie aan.

NB: dit is wat anders dan de attribuutmapping van de Verificatieservice. Die mapt de attributen uit de bron naar de QEAA attributen die de QTSP heeft aangeleverd. De QTSP heeft een andere mapping nodig: elementen uit de geboorteakte naar QEAA attributen. Samen maken ze de keten compleet: document -> QEAA attributen -> bronattributen.
NB2: het proces kan ook omgedraaid worden: de gebruiker geeft aan dat die de QEAA Geboortebewijs nodig heeft, waarna de QTSP aangeeft welk document/ welke documenten de gebruiker daarvoor moet uploaden ten behoeve van het omzetten daarvan en de bijbehorende verificatie hiervoor.

Toepassing eDelivery netwerk voor QTSP's

In de beproeving is uitgegaan van een situatie waarin QTSP's via het eDelivery netwerk uitwisselen met bronnen voor minimaal de verificatiedoeleinden. Op die manier sluit die uitwisseling namelijk het meest aan op hetgeen al is ingericht aan bronontsluiting voor OOTS. De ervaring is dan ook dat zowel RINIS als Cleverbase deze verbinding makkelijk werkend kregen.

In de uitvoeringshandeling eIDAS, die onder andere gaat over de verificatie van de authentieke bron door QTSP's en uitwisseling van QTSP's met authentieke bronnen, worden twee standaarden genoemd die beide kunnen worden toegepast. De ISO15000 optie volgt de specificaties die ook in het eDelivery netwerk worden toegepast. Echter, QTSP's mogen geen

gebruik maken van het eDelivery netwerk van het OOTS. In de beproeving is dan ook een eigen apart netwerk voor gebruik door Cleverbase opgezet. De huidige opzet van de beproeving binnen UBO werkt alleen onder de aanname dat er een proces van onboarding van QTSP's komt die uitwisseling via (een apart virtueel netwerk binnen) eDelivery voor QTSP's met authentieke bronnen (via intermediaire (OOTS) platforms mogelijk maakt. Hier zal de EU commissie actie op moeten ondernemen. Gebeurt dit niet, dan is het zinvol om andere mogelijkheden uit te werken en te beproeven voor de uitwisseling met QTSP's.

Toepassing NL Wallet in de beproeving

In de hackathon van 16 december 2025 is getracht de interoperabiliteit met de NL Wallet te testen door het gekwalificeerde attest voor de geboortegegevens niet alleen in te laden in de Vidua wallet van Cleverbase, maar ook in de NL-wallet van het ministerie van BZK. Dit is voor deze hackathon niet gelukt. Er is een document vanuit Cleverbase opgesteld met bevindingen en aanbevelingen uit deze test. Belangrijkste bevinding is dat er nu NL-wallet specifieke toevoegingen zijn opgenomen in de profielen voor uitwisseling met de NL-wallet. Die specifieke toevoegingen in de profielen zijn nu blokkerend voor het uitgeven van attributen door partijen die geen gebruik maken van de publieke NL Wallet issuer/verifier op de server, zoals toekomstige QTSP's en andere private partijen met eigen uitgifte. Om te voorkomen dat er te veel verschillen tussen implementaties in de EU gaan ontstaan, is er in EU verband gewerkt aan een standaard profiel, het zogenoemde HAIP profiel. Het advies vanuit het project is om dit profiel ook bij de NL-wallet te implementeren. Vanuit de ontwikkelaars van de NL-wallet is bevestigd dat gewerkt wordt aan het toepassen van het HAIP profiel.

3.2 Aanbevelingen

Hieronder volgen de aanbevelingen uit de voorgaande leerervaringen.

Bij een mismatch in de verificatie kan de oorzaak op verschillen plekken liggen (bij de bron, bij de vertaling van de bron naar de API, in de verificatie of in het verzoek van de QTSP). Het is belangrijk om bij productiegang na te denken over de ondersteuning van foutopsporing, zowel in de techniek, als in de onderlinge afstemming tussen betrokken ketenpartijen en de ondersteuning van gebruikers waarbij een fout optreedt.

Vanuit Cleverbase zijn bezwaren geuit tegen een oplossing via herauthenticatie van de gebruiker bij RINIS voor het ophalen of laten verifiëren van gegevens bij de bron vanwege de beveiligingsrisico's van een redirect met interface naar de gebruiker in een s2s uitwisseling tussen QTSP en RINIS. De optie die voor nu meest aannemelijk is, is daarom authenticatie bij de QTSP en het geven van toestemming bij de QTSP inbedden in de procedures bij de QTSP die hierop geaudit wordt. Voor de QTSP is dan belangrijk aan te tonen dat Discovery en Toestemming zijn geregeld door de QTSP. Dat kan door goede documentatie van de procedures, testen en logging.

Sluit aan op ETSI-ontwikkelingen vanuit Nederland en de opvolgingen op het UBO project. Op die manier kan input worden geleverd op de gewenste richting voor de standaarden die nodig zijn in de uitwisseling met authentieke bronnen. Bovendien wordt van daaruit duidelijk wat de richting zal zijn en/of blijven hiervoor.

Pas het HAIP-profiel toe voor de uitwisseling met de publieke NL wallet, zodat alle uitgevers van QEAA's op dezelfde manier attestaties kunnen aanleveren.

Ga in gesprek met de EU commissie over de benodigde randvoorwaarden voor de oplossing waarbij QTSP's gebruik maken van het eDelivery netwerk voor uitwisseling met authentieke bronnen. Er zijn Europese afspraken nodig over onboarding QTSP's. Komen die er niet, overweeg dan om onderzoek te doen naar het gebruik van de andere versie van de standaard voor uitwisseling met authentieke bronnen.

3.3 Openstaande punten

Het is belangrijk om verder onderzoek te doen naar het concept van 'fuzzy matching' bij verificatie in Europees verband en aan te sluiten bij oplossingen die op andere ontwikkelingen in Europa al worden bedacht en geïmplementeerd hiervoor. Het is zinvol te kijken naar een uiteindelijke oplossing dat rekening kan houden met dit soort ongelijkheden, dan wel controles uitvoert op format en inhoud van velden, e.d. Ook is het belangrijk om naar productiegang te bepalen wanneer nog wel sprake is van een match of een match met wat onzekerheid. De ETSI specificatie definieert ook de mogelijkheid van een "*fuzzy*" match, maar dit was nu niet in scope van de beproeving.

De uitvoeringshandeling bij artikel 45 uit de verordening, die onder andere nadere regels stelt aan de verificatiefunctie, is in de eerste helft van 2026 aangepast. Uit de wijzigingen komt een extra eis[1] naar voren ten aanzien van de uitwisseling tussen QTSP en de authentieke bron ten behoeve van die verificatie, namelijk het digitaal ondertekenen of verzegelen van het resultaat van de matching door de bronhouder of de nationaal aangewezen intermediair. In het geval van de oplossing die binnen de UBO beproeving is gekozen betekent het dat RINIS als nationaal intermediair voor de uitvoering van de verificatie het digitaal moet ondertekenen of verzegelen. Dat is nu nog niet het geval binnen de huidige opzet van de beproeving en de daarvoor toegepaste standaarden en opgeleverde documentatie.
Bronhouders moeten zelf bepalen hoe granulair het "attribuut" is waarvoor ze een verificatie bieden. Er zijn nu geen richtlijnen voor, dus de bevoegde instantie mag dat zelf bepalen. In de beproeving is ervoor gekozen om het attribuut gelijk te stellen aan de evidence type (geboortebewijs en alle individuele gegevenselementen die hierbij horen). Dat maakt het eenvoudig en overzichtelijk voor beproeving, maar is niet automatisch voor bredere implementatie ook handiger. Bijvoorbeeld als het handiger is op individuele elementen het resultaat van verificatie terug te koppelen. We hebben nu voor een pragmatische oplossing gekozen, maar niet onderzocht hoe je dit grootschalig kunt doen. Dat is een onderzoeksvraag voor vervolg.

Belangrijkste vraag voor uiteindelijke opschaling van de beproefde oplossing waarbij de QTSP via het eDeliverynetwerk communiceren is of de Europese commissie als beheerder van het netwerk dit gaat toestaan en hiervoor procedures gaat inrichten. Bij het toelaten van QTSP's op het eDeliverynetwerk komen vervolgens een aantal vraagstukken op die ook een relatie kennen met audit en toezicht op QTSP's. Hoe doe je straks een conformiteitsbeoordeling van de

[1] Onderdeel van de wijziging op artikel 9 in de uitvoeringshandeling voor artikel 45 beschrijft: 'The verification result shall be signed or sealed by the public sector body responsible for an authentic source, or by the designated intermediary recognised at national level, using at least an advanced electronic signature based on a qualified certificate for electronic signatures or an advanced electronic seal based on a qualified certificate for electronic seals, respectively.'

implementatie van bovenstaande punt door QTSP's, onder andere ook op het vlak van beveiliging en het vertrouwensmodel? Hoe identificeer je de QTSP in het eDeliverynetwerk? Is dat hetzelfde als voor PEPPOL gebeurd (ISO standaard voor identificeren via KvK nr)? Dat is nog niet vastgesteld. En wat is dan de plek om dit vast te stellen en te vereisen?

Er zijn nog geen uitspraken over de uiteindelijk te gebruiken catalogi/ registers en het beheer van de informatie daarin voor eIDAS. De Europese Commissie zal (moeten) voorschrijven hoe bronhouders hun attributen moeten aanmelden. Daar kunnen nu dus nog geen uitspraken over worden gedaan.

4. Juridische en organisatorische lessen

4.1 Geleerde lessen

Er zijn met name lessen op te tekenen uit het nadenken over de onderwerpen die met betrekking tot privacy spelen bij deze uitwisseling en welk effect dat zou kunnen hebben op bestaande of nieuwe afspraken hierover binnen de gemeentelijke organisatie. Door de gemeente Rijswijk is een DPIA uitgevoerd naar de verwerking van persoonsgegevens door de gemeente in de toepassing van uniforme bronontsluiting voor de verschillende usecases. In de beproeving worden geen echte persoonsgegevens verwerkt en uitgewisseld, maar gebruik gemaakt van een testpersoon. Wanneer deze oplossing daadwerkelijk voor productie wordt geïmplementeerd dan worden bij de gemeente persoonsgegevens verwerkt via de UBO oplossing en uitgewisseld voor de doeleinden in de verschillende usecases. Uit het opstellen van de DPIA zijn al een aantal leerervaringen te destilleren en punten voor nader onderzoek:

- Uniforme bronontsluiting/ BronConnect is primair een technisch architectuur- en gegevensverwerkingssysteem. In de DPIA is het daarom van belang om niet alleen naar de juridisch beleidsmatige aspecten te kijken, maar ook naar de systeemarchitectuur, datastromen, e.a. Omdat UBO een set van standaarden en open source bouwstenen betreft kan de uiteindelijke implementatie per gemeente verschillen. En daarmee de conclusies ten aanzien van de specifieke risico's en maatregelen voor de inrichting binnen de gemeente.
- Een DPIA voor UBO vereist input van verschillende technische en operationele specialisten, omdat veel risico's pas goed kunnen worden geïdentificeerd en gemitigeerd wanneer concrete kennis van architectuur, koppelingen en processen beschikbaar is.
- De gemeente heeft een eigenstandige (verwerkings-)verantwoordelijkheid in een keten van organisaties en hun voorzieningen. Het is wat dat betreft alleen al goed om de verschillende onderdelen van de uitwisseling met de daarop van toepassing zijnde frameworks en regels te definiëren en uit te schrijven. Bovendien zijn onderdelen van de keten(s) al onderworpen aan een DPIA met uitspraken over dat deel van de keten en eventueel ook met inzichten in hetgeen de gemeente als bronhouder aan verantwoordelijkheden kent. Voor de gemeente is het van belang die bestaande inzichten te kennen en te kunnen gebruiken bij de eigen analyse.

4.2 Aanbevelingen

Met de eerste uitwerking van de gemeente Rijswijk kan een voorstel worden gedaan voor alle gemeenten (en eventueel andere overheden) die gebruik gaan maken van de UBO oplossing voor de uitwisseling van gegevens in de verschillende usecases. De aanbeveling is om daarvoor vanuit de VNG een model DPIA ter beschikking te stellen.

Bij usecase 1 in fase 2 werken alle partijen onder (verwerkers-)verantwoordelijkheid van de gemeente (behalve het afnemersportaal van de uiteindelijke relying party). Wat betekent dit voor de inrichting van die verantwoordelijkheden? En kunnen gemeenten nog verder ondersteunt worden met aanvullende gemeenschappelijke ondersteuningsproducten (naast de technisch/functionele) en de model DPIA. Bijvoorbeeld met standaard verwerkersovereenkomsten, etc.

4.3 Openstaande punten

Vanuit het opstellen en bespreken van de DPIA door de gemeente Rijswijk kwamen de volgende vragen op die verdere analyse vragen bij uiteindelijke ontwikkeling van een model DPIA:

- De grondslag voor verwerking in de verschillende usecases verschilt mogelijk. Wat betekent dit voor de DPIA bij de gemeente op de UBO oplossing als deze voor verschillende grondslagen en doeleinden ingezet kan worden?
- Op welke manier kunnen personen hun rechten uit de AVG uitoefenen bij de gemeente, waaronder het inzien van de informatie over de bevraging van hun gegevens. Ondersteunt de UBO oplossing hierbij, bijvoorbeeld via de afspraken over logging in de FSC standaard?
- Welke gegevens precies verwerkt worden, is aan verandering onderhevig. De API definitie wordt gaandeweg verder uitgebreid met meer gegevenselementen die opvraagbaar (moeten) zijn in de verschillende usecases. Hoe ga je om met die dynamiek?
- Op welke manier kunnen gemeenten op de hoogte blijven van wijzigingen in de ketenoplossing met eventueel effect op de conclusies in de DPIA bij de gemeente zelf als onderdeel van die oplossing? Hoe sluiten eventuele evaluaties van de verschillende verantwoordelijken in de keten op elkaar aan in tijd en inhoud?
- De oplossing voor UBO vanuit de gemeente zal veelal worden geïmplementeerd door een softwareleverancier die als verwerker namens de gemeente optreedt. In veel gevallen, zoals ook in de beproeving, is dat aanvullende functionaliteit op al bestaande functionaliteit bij de gemeente. Op welke manier kunnen bestaande verwerkersovereenkomsten hier eventueel op worden aangepast met de inzichten uit de beproeving?

Adviezen voor borging en beheer

De opgedane kennis en ervaring uit de beproeving wordt ondergebracht in GBO. Hieronder volgen adviezen voor borging en beheer van de oplossing in een productiesituatie:

- Zie voor meer informatie over de gebruikte standaarden uit het Federatief Datastelsel in de oplossing voor Uniforme Bronontsluiting en de handreikingen die hiervoor beschikbaar zijn: https://www.noraonline.nl/wiki/Standaarden_in_het_Federatief_Datastelsel
- Zie voor een eerste inzicht in stappenplan implementatie voor gemeenten en QTSP's eerder in dit document. Afhankelijk van de beleidskeuzes voor in productiename van generieke functionaliteit en de toepassing van de voorgestelde standaarden kunnen deze stappenplannen verder worden uitgewerkt.
- Werken met simulatie omgeving. Gebruik van de simulatieomgeving FDS is een makkelijke manier om FSC te implementeren (in de cloudomgeving in te richten), zodat partijen voor een eerste stap van beproeven dat niet zelf hoeven te installeren, maar alleen hun API ontsluiten. Dit is mogelijk een goede manier om beproeving voor de toekomst met de oplossing voor bronontsluiting te borgen. Met de simulatieomgeving is het makkelijker om snel iets te testen in de verschillende usecases via de gepubliceerde specificaties. Het is dan niet nodig om eigen FSC managers e.a. FSC componenten te implementeren.
- Voor het beheer van de interface specificaties is het van belang te bepalen hoe die API specificaties het beste kunnen worden vormgegeven en waar de verantwoordelijkheid ligt. Bij het programma GBO wordt een voorstel uitgewerkt waarbij de bron de gegevens beschikbaar kan stellen, zoals die beschikbaar zijn. En daarmee het beheer van de specifieke schema's die nodig zijn vanuit de bevrager, neer te leggen bij de vraagkant of centraal te beheren. Dit lost mogelijk een geconstateerd probleem op uit de beproeving. Voor het beheer lijkt dit model ook handiger gezien sprake is van verschillende leveranciers en gebrek aan overstijgende standaardisatie van gegevens in alle domeinen. Door met meer partijen in andere domeinen de beproeving uit te breiden en te herhalen kunnen hieruit leerervaringen voor toekomstig beheer worden gehaald.
- Er zijn afspraken nodig over het beheren van de specificaties voor API's, de mappingsmodellen van gevraagde gegevens met aangeboden gegevens, de specificaties voor uitwisseling tussen de centrale componenten en QTSP's op basis van de ETSI standaarden en de attribuutschema's voor de gebruikte gegevens in de beproeving (en aanmelden daarvan bij EU + bewaken van samenhang met OOTS evidence types)
- Opschaling en beheer van verificatiefunctie (voor alle overheden, minimaal alle gemeenten). Als alternatief voor het (laten) realiseren van deze functie door elke authentieke bron dat zelf.
- Inzet van de basisinrichting OOTS bij RINIS voor eIDAS doeleinden borgen. Voordelen van de inzet van de (centrale) basisinrichting voor de uitwisseling met QTSPs zijn onder andere: het voorkomen van lock-ins met individuele QTSP's; het stimuleren van gelijke marktkansen binnen de EU; het overbruggen van nationale (FDS) en EU standaarden (eDelivery) voor zowel bron als QTSP; hergebruik van functionaliteit dat al gerealiseerd is en het delen van beheeractiviteiten en -kosten; gebruik maken van de mogelijkheden die de uitvoeringshandeling eIDAS biedt voor synergie tussen OOTS en de wallet; generieke functies gemeenschappelijk inrichten (ipv 342 keer).
- Verder borgen van de toepassing voor UBO binnen het FDS afsprakenstelsel, niet alleen qua techniek, maar ook voor andere eisen. Te starten met een GAP analyse ten aanzien van de bestaande afspraken.

- Samenwerking met Common Ground en aansluiten bij de verdere ontwikkeling van een gemeenschappelijke data integratielaag voor gemeenten door dit programma.
- Hoe maken we de oplossing uitlegbaar naar gemeenten (en andere overheden), burgers/bedrijven, bestuurders, e.a.?

Buiten scope geplaatst voor fase 2 (of voor vervolg)

Er zijn een aantal onderwerpen vooralsnog buiten scope geplaatst van de beproeving in fase 2:

- In de beproeving is geen gebruik gemaakt van het zogenoemde Relying Party register (RP Register) dat onderdeel moet uitmaken van het EDI stelsel. In het Relying Party register registreren de 'relying parties' (vertrouwende partijen) zichzelf en welke gegevens uit de wallet zij vragen voor hun dienstverlening. Na registratie wordt een certificaat uitgereikt aan de vertrouwende partij waarmee die zich kan identificeren als partij bij de wallet. Bovendien is het mogelijk om in een lidstaat beleid te voeren op het controleren van het geregistreerde. Met een apart certificaat voor die partij kan de wallet ook controleren voor welke gegevens de partij zich heeft ingeschreven en die vergelijken met de gegevens die worden gevraagd. Ook QTSP's zullen zich waarschijnlijk moeten registreren als vertrouwende partij en geïdentificeerd worden via een certificaat. Daarbij kan gecontroleerd worden of de QTSP is gecertificeerd en als zodanig is opgenomen op de vertrouwenslijst. Het RP Register is nog in ontwikkeling, evenals het beleid hiervoor. Bovendien ligt de focus in de beproeving vooral op het uniform kunnen ontsluiten van gegevens uit de gemeentelijke bron en minder op het gebruik daarvan in de wallet.
- In de beproeving is geen gebruik gemaakt van een gecertificeerde EUDI wallet en een check hierop door de QTSP bij uitgifte van een QEAA aan de wallet. Er bestaat nog geen certificeringsschema voor EUDI wallets in Nederland en een proces voor certificering. Er zijn dus nog geen officiële EUDI wallets beschikbaar. In de beproeving is gebruik gemaakt van de wallet (Vidua) van de deelnemende QTSP (Cleverbase). De wallet voldoet aan de afspraken, eisen en standaarden die in de laatste versie van het Architectural Reference Framework (ARF) zijn beschreven. Het ARF is de basis voor gemeenschappelijke eisen aan de componenten in het EDI stelsel voor de lidstaten. Overigens geldt hetzelfde voor de uitgifte van een QEAA. Hiervoor kunnen QTSP's nog niet worden gecertificeerd. Cleverbase geeft daarom een attribuut uit die voldoet aan de afspraken, standaarden en eisen die in de ARF staan beschreven voor een QEAA.
- In de beproeving is geen gebruik gemaakt van een PID in de wallet die is uitgegeven door RVIG, de officieel aangekondigde oplossing voor PID verstrekking in Nederland. Dit proces is nog niet ingericht. In de beproeving wordt daarom gebruik gemaakt van een PID dat is aangemaakt door Cleverbase op basis van de gegevens van de testpersoon. Hiervoor is gekeken naar de afspraken, eisen en standaarden in de ARF en het PID Rulebook.
- In de beproeving is bij alle partijen gebruik gemaakt van (kopieën van) voorzieningen in een testomgeving. In veel gevallen is in het functioneel ontwerp, en zeker in het technisch ontwerp, rekening gehouden met een omgeving dat geschikt is voor een proof of concept. Dat betekent dat de proefomgeving niet bestaat uit productiewaardige voorzieningen. Het project zal in de oplevering van de eindconclusies een inschatting maken van de activiteiten benodigd om de proefomgeving in dezelfde vorm naar een productiesituatie om te zetten.