

De attribuutverificatieservice

Specificaties Project Uniforme Bronontsluiting

Versie: 30-03-2026

Definitief voor beproeving

Inhoudsopgave

Inhoudsopgave	1
1. Attribuutverificatie	2
1.1. Use case	2
1.2. Europese voorschriften	4
1.3. UBO architectuurladers	5
1.4. Ontwerpbeslissingen	6
2. Functionele specificatie	7
2.1. Beheren attribuutmappingen	7
2.2. Beantwoorden verificatieverzoek	7
2.3. Aanvullende vereenvoudigingen voor beproeving	9

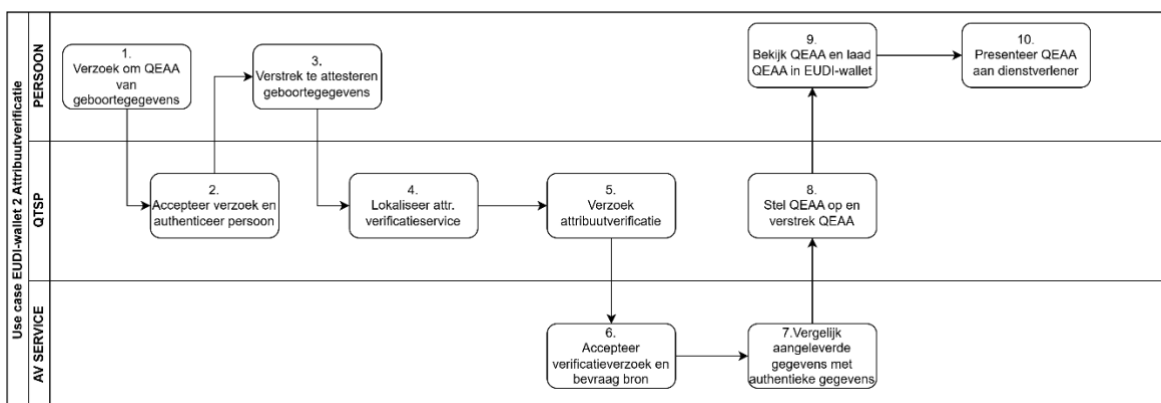
1. Attribuutverificatie

Artikel 45e van de gewijzigde eIDAS-Verordening (EU) nr. 910/2014 verplicht lidstaten om ervoor te zorgen dat QTSP's minimaal de in Bijlage VI van de Verordening vermelde attributen bij de authentieke bron kunnen verifiëren. Artikel 9 van uitvoeringsverordening (EU) 2025/1569 beschrijft dat hiervoor verificatiepunten ingericht moeten worden. Een dergelijk verificatiepunt ontvangt de attributen en de identificatiegegevens van het subject en geeft een verificatieresultaat aan de QTSP terug. Het verificatieresultaat vermeldt of het betreffende attribuut is geverifieerd of niet, en welke publieke instantie verantwoordelijk is voor de authentieke bron of, indien van toepassing, welke publieke instantie is aangewezen om namens de authentieke bron op te treden waartegen het attribuut is geverifieerd.

In het project Uniforme BronOntsluiting (UBO) correspondeert dit met "EUDI-wallet 2: attribuutverificatie". Dit document specificiert het verificatiepunt voor geboortegegevens (in dit document: de attribuutverificatieservice) die nodig is voor de beproeving van deze use-case. Het project richt de attribuutverificatieservice niet in voor gebruik door alle authentieke bronnen, maar beperkt zich nu tot ondersteuning van de use-case "verificatie van geboortegegevens in een gemeentelijke bron".

1.1. Use case

De use case start met de vraag van een persoon aan een QTSP om gegevens die de persoon al in zijn bezit heeft "te attesteren": om te zetten tot een QEAA voor zijn EUDI-wallet. Voorafgaand aan het attesteren, moet de QTSP nagaan of de door de gebruiker geleverde informatie authentiek is (overeenstemt met de actuele informatie in de authentieke bron). In tegenstelling tot de eerste use case (verstrekken van een QEAA) moet elke QTSP deze attribuutverificatiemogelijkheid krijgen, er is geen contractrelatie met een gemeente voor nodig. De attribuutverificatie zelf moet door de authentieke bron of een door de bron aangewezen instantie plaatsvinden. De QTSP gebruikt het verificatieresultaat om te bepalen of het de gegevens voor de EUDI-wallet attesteert of niet.

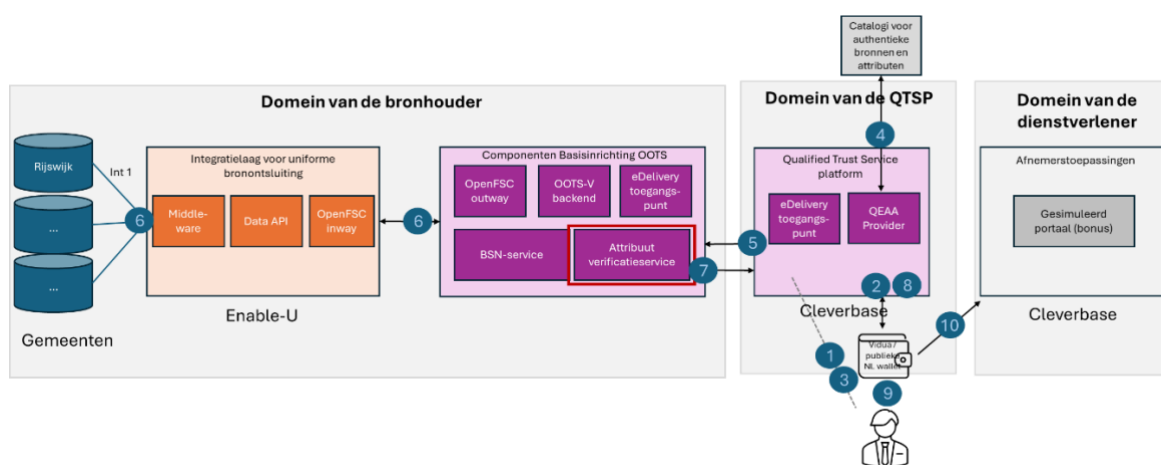


Het proces verloopt op hoofdlijn als volgt:

1. PERSON: De natuurlijk persoon benadert de QTSP met het verzoek om de geboortegegevens als QEAA aan zijn EUDI-wallet te verstrekken.
2. QTSP: De QTSP accepteert het verzoek en authenticceert de persoon met zijn EUDI-wallet.
3. PERSON: De persoon verstrek daarbij de geboortegegevens die het wil laten attesteren.

4. QTSP: De QTSP be vraagt de catalogus voor authentieke bronnen en attributen om te achterhalen welke verificatiepunt het moet aanroepen om de geboortegegevens te laten verifiëren.
5. QTSP: De QTSP verzoekt de attribuutverificatieservice om attribuutverificatie. Onderdeel van dat verzoek zijn de identificerende persoonskenmerken, waaronder het BSN van de persoon, en de geboortegegevens die geverifieerd moeten worden.
6. ATTRIBUUTVERIFICATIESERVICE: De attribuutverificatieservice ontvangt en controleert het verificatieverzoek en vraagt de bronhouder om de geboorteattributen uit de authentieke bron te leveren. De bronhouder wordt op uniforme manier bevroegd – identiek aan de bevraging in de use cases voor OOTS en EUDI-wallet use case 1 (QEAA verstrekking).
7. ATTRIBUUTVERIFICATIESERVICE: De attribuutverificatieservice vergelijkt de twee gegevenssets om te bepalen of ze overeenstemmen en informeert de QTSP over het resultaat van de vergelijking.
8. QTSP: Indien de attributen overeenstemmen – en de authenticiteit van de door de persoon geleverde informatie dus bevestigd is – verstrekt de QTSP de geboortegegevens als QEAA aan de wallet van de persoon.
9. PERSOON: De persoon bekijkt de QEAA en accepteert deze in zijn EUDI-wallet.
10. PERSOON: De persoon gebruikt de QEAA voor het aanvragen van een dienst bij een publieke dienstverlener (optioneel).

De UBO-architectuur beschrijft de componenten die nodig zijn voor de beproeving van deze flow. Die zijn opgenomen in navolgende afbeelding. De attribuutverificatieservice is daarin rood omkaderd.



De architectuur kenmerkt zich door:

1. Uniformiteit in componenten en interactie met de authentieke bron door inzet van Digikoppeling API-profiel en FSC.
2. Uniformiteit in de componenten en interactie met de QTSP door inzet van eDelivery en op OOTS en ETSI TS 119 478-gebaseerde berichtmodellen voor attribuutverificatie.
3. Inzet van het intermediaire platform (“componenten Basisinrichting OOTS”) voor overbrugging van de standaarden voor bronontsluiting en de standaarden voor de EUDI-wallet en voor het leveren van algemene functionaliteit, in dit geval de attribuutverificatieservice.

1.2. Europese voorschriften

De attribuutverificatieservice heeft zijn grondslag in:

- Artikel 45 van de eIDAS-verordening over de plicht om een attribuutverificatiemogelijkheid aan te bieden:

“De lidstaten waarborgen binnen 24 maanden na de datum van inwerkingtreding van de in artikel 5 bis, lid 23, en artikel 5 quater, lid 6, bedoelde uitvoeringshandelingen dat er, ten minste voor de in bijlage VI vermelde attributen, voor zover die authentieke bronnen binnen de publieke sector gebruiken, maatregelen worden genomen zodat gekwalificeerde verleners van vertrouwensdiensten elektronische attesteringen van attributen afgeven die attributen langs elektronische weg kunnen verifiëren op verzoek van de gebruiker, overeenkomstig het Unie- of nationaal recht.”
- Annex VI van de eIDAS-verordening met de opsomming van de attributen waarvoor attribuutverificatie in ieder geval mogelijk moet worden:

“Uit hoofde van artikel 45 sexies waarborgen de lidstaten dat, indien attributen gebruikmaken van authentieke bronnen binnen de publieke sector, maatregelen worden genomen zodat gekwalificeerde verleners van elektronische attesteringen van attributen op verzoek van de gebruiker langs elektronische weg aan de hand van de relevante authentieke bron op nationaal niveau of via op nationaal niveau erkende aangewezen intermediairs, overeenkomstig Unie- of nationaal recht, de authenticiteit van de volgende attributen kunnen verifiëren: 1. adres; 2. leeftijd; 3. geslacht; 4. burgerlijke staat; 5. gezinssamenstelling; 6. nationaliteit of staatsburgerschap; 7. onderwijskwalificaties, -titels en -diploma's; 8. beroepskwalificaties, -titels en -licenties; 9. bevoegdheden en mandaten om natuurlijke of rechtspersonen te vertegenwoordigen; 10. openbare vergunningen en licenties; 11. voor rechtspersonen: financiële en bedrijfsgegevens.”
- Artikel 9 van uitvoeringsverordening 2025/1569 met nadere voorschriften voor de manier waarop de attribuutverificatie moet werken:

“Om de elektronische verificatie van de in artikel 45 sexies, lid 1, van Verordening (EU) nr. 910/2014 bedoelde attributen door gekwalificeerde verleners van vertrouwensdiensten die gekwalificeerde elektronische attesteringen van attributen afgeven, op verzoek van de gebruiker mogelijk te maken, stellen de lidstaten daartoe mechanismen en kunnen zij centrale verificatiepunten beschikbaar stellen voor de in bijlage VI bij die verordening vermelde attributen als die attributen op authentieke bronnen binnen de publieke sector berusten. De lidstaten publiceren informatie over de procedures voor het initiëren van de verificatieverzoeken en voor het ontvangen van de controleresultaten.

Het verificatiemechanisme biedt een toegangspunt waar gekwalificeerde verleners van vertrouwensdiensten die gekwalificeerde elektronische attesteringen van attributen afgeven, elektronisch kunnen verzoeken om verificatie aan de hand van authentieke bronnen of aan de hand van op nationaal niveau erkende aangewezen intermediairs van de in artikel 45 sexies, lid 1, van Verordening (EU) nr. 910/2014 bedoelde attributen. Attributen die moeten worden geverifieerd, worden op verzoek van de gebruiker door de gekwalificeerde verlener van vertrouwensdiensten aan het verificatiepunt verstrekt. De openbare instantie of de aangewezen intermediair deelt de verificatieresultaten via het verificatiepunt met de gekwalificeerde verleners van vertrouwensdiensten die gekwalificeerde elektronische attesteringen van attributen afgeven. Het verificatieverzoek bevat de attributen en de identificatiegegevens van het onderwerp van het attribuut waarvoor de gekwalificeerde verlener van vertrouwensdiensten om verificatie verzoekt. Het verificatieresultaat vermeldt uitsluitend of het attribuut al dan niet is geverifieerd en specificeert de openbare instantie die voor de authentieke bron verantwoordelijk is of, in voorkomend geval, de openbare instantie

die is aangewezen om op te treden namens de authentieke bron aan de hand waarvan het attribuut is geverifieerd. De lidstaten kunnen toegangscontroles of andere verificatiemechanismen opleggen die de integriteit, de authenticiteit en de vertrouwelijkheid bieden om te bepalen of de verzoeker een gekwalificeerde verlener van vertrouwensdiensten is en op verzoek van een legitieme gebruiker optreedt. De lidstaten kunnen ook controlemechanismen opleggen voor het gebruik van de verificatiemethoden, indien zij dit passend achten, met inachtneming van relevante factoren, waaronder de vraag of de authentieke bronnen vertrouwelijke persoonsgegevens of gevoelige gegevens bevatten. Indien de lidstaten deze controlemechanismen instellen, publiceren zij informatie over de reikwijdte van de controlemechanismen als onderdeel van de in lid 1 bedoelde informatie.”

- Artikel 10 van uitvoeringsverordening 2025/1569 over hergebruik van de OOTS common services en de daarmee verbonden nationale componenten:
“Voor de toepassing van de artikelen 3 tot en met 9 kunnen de lidstaten verwijzen naar de gemeenschappelijke diensten van het in artikel 14 van Verordening (EU) 2018/1724 bedoelde technische systeem en de daarmee verbonden nationale componenten en die hergebruiken. Bij de vaststelling van het beveiligde aanmeldingssysteem en de lijst van openbare instanties als bedoeld in de artikelen 5 en 6 en de catalogi als bedoeld in de artikelen 7 en 8 verwijst de Europese Commissie, in voorkomend geval, naar de gemeenschappelijke diensten van het technische systeem overeenkomstig Verordening (EU) 2018/1724 en hergebruikt die.”.

1.3. UBO architectuurkaders

Dit ontwerp is opgesteld binnen de architectuurkaders die de UBO-architectuur voor de beproeving van deze use-case heeft geformuleerd:

1. De beproeving maakt gebruik van de in de eerste fase reeds benutte datadefinitie voor geboortegegevens.
2. De interactie tussen de verificatieservice en de QTSP wordt ingericht op basis van het OOTS berichtenmodel en ETSI TS 119 478 v1.1.1 (ISO 15000-variant)¹.
3. De QTSP gebruikt voor deze beproeving versie 2.0 van de OOTS Common Services (de componenten Data Service Directory en Semantic Repository) op de User Acceptance Testing (UAT)-omgeving van de DG DIGIT.
4. In de beproeving levert de QTSP het BSN van de natuurlijk persoon in het attribuutverificatieverzoek. De UBO-architectuur schetst ook drie andere opties waarlangs het BSN in de verificatieketen beschikbaar kan komen (herauthenticatie in het intermediaire platform van de authentieke bron, ontsleutelen van een versleuteld BSN in de EUDI-wallet en het uitvoeren van identiteitsmatching). Het is bij het opstellen van dit ontwerp nog niet duidelijk welke juridische kaders gaan gelden en of hiervoor nationale richtlijnen opgesteld worden. Het project werkt daarom vanuit de veronderstelling dat de QTSP het BSN voor attribuutverificatiedoeleinde mag opvragen en aan de verificatieservice levert.
5. Om het BSN in het verificatieverzoek mee te kunnen leveren, moet de QTSP het BSN van de EUDI-wallet kunnen lezen. Dat vereist dat het BSN op de EUDI-wallet staat. Dit is naar verwachting alleen bij EUDI-wallets het geval met een Nederlandse PID. Buitenlandse EUDI-wallets worden in deze beproeving niet ondersteund².

¹ Uitvoeringsverordening 2025/1569 wordt momenteel aangepast om inzet van deze ETSI standaard voor attribuutverificatie wettelijk voor te schrijven.

² BZK bereidt de ontwikkeling van een koppelvoorziening waar, waarbij de PID's van buitenlandse wallets gekoppeld kan worden aan het BSN, zodat personen met een buitenlandse PID ook in kunnen loggen op BSN-diensten. Deze voorziening is nog niet beschikbaar.

1.4. Ontwerpbeslissingen

Voor de attribuutverificatie zijn verder de volgende ontwerpbeslissingen genomen:

1. Doorgifte van het BSN van QTSP naar verificatieservice gebeurt in het PID attribuut “personal administrative number”. Dit is identiek aan de manier waarop het BSN ook voor EUDI-wallet use case 1 (verstrekking van een QEAA) door de QTSP gecommuniceerd wordt.
2. De verificatie moet plaatsvinden op elk attribuut, zodat de verificatieservice per attribuut reageert met een verificatieresultaat (Match, NoMatch). Er is echter niet eenduidig gedefinieerd hoe smal of breed een “attribuut” is. Annex VI van de eIDAS-verordening maakt een mix variërend van elementaire attributen (leeftijd) tot volledige sets (onderwijskwalificaties, financiële en bedrijfsgegevens). Het gebrek aan eenduidigheid is ook terug te lezen in ETSI TS 119 478. Deze standaard laat alle ruimte om een attribuut heel smal of juist heel breed te definiëren.

De beproeving gaat daarom van het volgende uit:

- Het Geboortebewijs wordt beschouwd als één attribuut waarvoor de QTSP verificatie vraagt.
 - Het attribuutverificatieverzoek bevat de te verifiëren gegevenselementen (zoals geboortedatum en geboorteplaats) van het geboortebewijs.
 - Verificatie vindt plaats op elk van de opgenomen gegevenselementen.
 - Als een gegevenselement niet in het verificatieverzoek opgenomen is dan betreft de attribuutverificatieservice het niet in het matchingsproces.
 - Er komt één verificatieresponse op het verzoek met één uitspraak (Match/NoMatch) voor het Geboortebewijs als geheel.
4. De verificatieservice heeft functionaliteit nodig om voor de gegevenselementen waarvoor een verificatie gevraagd is te bepalen welke bron bevraagd moet worden. Hierbij kan bijvoorbeeld van de namespaces van het attribuut of de onderliggende gegevenselementen gebruik gemaakt worden om te bepalen binnen welke context (“welke dataset”) de attribuutverificatie uitgevraagd wordt³.
 5. Het is goed denkbaar dat de waarden van gegevenselementen op verschillende manieren vastgelegd kunnen zijn, denk aan verschillend gebruik van dakrieten, karaktersets, non-latinscript en nationale verschillen, zoals de typisch Nederlandse gewoonte om het tussenvoegsel van de naam te scheiden van de achternaam. De kans dat de waarden niet 1-op-1 overeenkomen is dan ook reëel. ETSI TS 119 478 biedt de mogelijkheid om de waarden met “fuzzy matching” met elkaar te vergelijken. Het resultaat van de matching kan dan “MatchWithVariation” worden. De beproeving maakt geen gebruik van fuzzy matching en ondersteunt dit verificatieresultaat niet. Door gebruik van voor gedefinieerde test sets borgt het project dat – in geval van een match – de waarden identiek zijn.
 6. ETSI TS 119 478 biedt de mogelijkheid om – net zoals in het OOTS – op een verzoek te reageren met de mededeling dat er tijd nodig is om tot een antwoord te komen (“deferred response”). De QTSP kan het verificatieverzoek op een ander aangegeven moment dan opnieuw indienen. Deze optie wordt niet beproefd.
 7. Bij elk attribuutverificatieverzoek moet gecontroleerd worden of het door een geaccrediteerde QTPS is ingediend. Het UBO-project veronderstelt dat er voor attribuutverificatie een Europees eDelivery netwerk ingericht wordt, waarbij op Europees niveau toetreding en

³ Hiermee wordt per gegevenselement duidelijk binnen welke context (en dus met welke gegevensset) de verificatie moet plaatsvinden. Het verificatieresultaat voor het element “adres” is bijvoorbeeld anders als het gaat over het adres bij geboorte of het huidige adres.

uittreding van QTSP's plaatsvindt. De attribuutverificatieservice richt daarom geen eigen controles op de identiteit en accreditatie van de QTSP in.

2. Functionele specificatie

De attribuutverificatieservice geeft uitvoering aan de volgende processen:

1. Beheren attribuutmappingen
2. Beantwoorden verificatieverzoek

2.1. Beheren attribuutmappingen

De gegevenselementen die in het attestatieschema gedefinieerd zijn voor de uit te geven QEAA kunnen afwijken van de elementen die de bron aanbiedt. De naam van een element kan afwijken, het formaat kan verschillen en de toegestane waarden zijn mogelijk anders. De attribuutverificatieservice heeft functionaliteit nodig om de QEAA-elementen te relateren aan de elementen die de bronhouder aanbiedt: de attribuutmapping.

Het beheer van de attribuutmappingen omvat het bijhouden van:

1. de registratie van brongegevens: het bekend zijn met de voor attribuutverificatie bekende authentieke bronnen, de datasets die zij publiceren en de bronelementen waaruit die sets bestaan.
2. de registratie van QEAA-gegevens: het bekend zijn met de QEAA's waarvoor attribuutverificatie mogelijk is en de gegevenselementen waaruit de QEAA's bestaan.
3. de mapping tussen de voorgaande twee, zodat de twee met elkaar vergeleken kunnen worden.

Vereenvoudigingen voor beproeving:

Voor de beproeving gaat de attribuutverificatieservice uit van de volgende vereenvoudigingen:

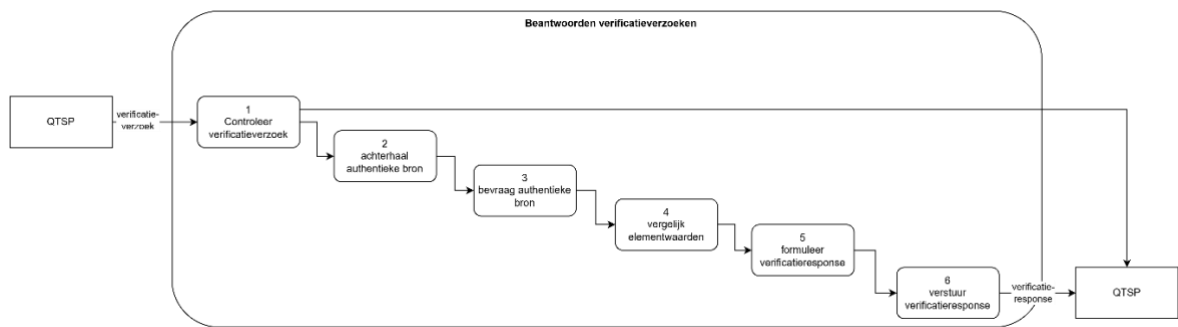
- De gegevenselementen uit de attestatie zijn 1-op-1 te herleiden tot de elementen uit de bron.
- De gegevenselementen uit de bron en uit de attestatie hanteren voor de beproeving hetzelfde formaat en dezelfde toegestane waarden. Er is geen omvorming van waarden nodig om tot zinvolle vergelijking te komen.
- Er wordt geen gebruik gemaakt van complexe gegevenselementen (elementen met één of meer onderliggende elementen of andersoortige relaties tussen elementen).

Automatiseringsverwachting

Het beheer van attribuutmappingen is een proces dat door een gegevensbeheerder door middel van een configuratiebestand uitgevoerd wordt. Het configuratiebestand bevat initieel alleen de mapping voor de geboortegegevens. Er wordt geen grafische userinterface (schermen) ontwikkeld voor de beproeving en er worden geen maatregelen voor interne controle toegepast, zoals het vier-ogen-principe. Er vindt geen logging plaats op wijzigingen die in de attribuutmapping aangebracht worden.

2.2. Beantwoorden verificatieverzoek

Onderstaande afbeelding toont de procesflow voor het beantwoorden van de verificatieverzoeken die QTSP's aan de verificatieservice doen.



Toelichting:

1. Controleer verificatieverzoek: in deze stap neemt de verificatieservice het verzoek van de QTSP in ontvangst en controleert of het verzoek aan de vereisten voldoet. Het verzoek hoort in ieder geval te bevatten:
 - a. Het versienummer van de toegepaste berichtspecificatie
 - b. Een unieke identificatie van het verzoek
 - c. De datum & tijdstip van het verzoek
 - d. De verzoekende QTSP (de requester)
 - e. De instantie die om verificatie wordt gevraagd (de provider: de aanbieder van de verificatieservice)
 - f. De bevestiging van het verzoek van de gebruiker om de verificatie uit te laten voeren
 - g. De identiteitsgegevens van de persoon wiens attributen het betreft, inclusief het BSN in "personal administrative number" dat onderdeel is van de PID.
 - h. De identificatie van het te verifiëren attribuut (het geboortebewijs)
 - i. De identificatie van de gegevenselementen waarvoor verificatie gevraagd wordt.
 Indien het verzoek niet aan de vereisten voldoet dan informeert de attribuutverificatieservice de QTSP daarover in een foutbericht.
2. Achterhaal authentieke bron: de attribuutverificatieservice bepaalt in deze stap aan de hand van de gegevenselementen die in het verzoek opgesomd zijn, welke aangesloten bron(nen) bevrage moet(en) worden en welke dataset(s) opgevraagd moet(en) worden om de verificatie uit te kunnen voeren. De verificatieservice maakt in deze stap gebruik van de eigen attribuutmapping.
3. Bevrage authentieke bron: in deze stap haalt de attribuutverificatieservice aan de hand van het ontvangen BSN de benodigde gegevens bij de bronhouder(s) op. Het maakt gebruik van de standaard interactie die UBO-breed toegepast wordt: eDelivery API profiel met FSC. De attribuutverificatieservice treedt binnen FSC op als consumer en verwijst naar het FSC contract met de properties:
 - a. AVG grondslag = taak van algemeen belang
 - b. Verwerkingsrelatie = wettelijke taak
 - c. Kanaal = QEAA
4. Vergelijk elementwaarden: de attribuutverificatieservice voert in deze stap per gegevenselement een vergelijking uit tussen de waarde uit het verificatieverzoek en de van de bronhouder verkregen waarde. De attribuutverificatiedienst formuleert na uitvoering van de vergelijking één resultaat: indien alle waarden overeenkomen dan kent de attribuutverificatieservice het resultaat "Match" toe. Indien één of meer waarden afwijken dan wordt het resultaat "NoMatch".

5. Formuleer verificatieresponse: de attribuutverificatieservice stelt het antwoordbericht op voor de QTSP. Het bericht bevat na succesvolle verificatie in ieder geval:
- a. Het versienummer van de toegepaste berichtspecificatie
 - b. Een uniek nummer van het antwoord
 - c. Het unieke nummer van het verzoek waarop gereageerd wordt
 - d. De status van het antwoord (Success)
 - e. De datum & tijdstip van het antwoord
 - f. De verzoekende QTSP (de requester)
 - g. De instantie die om verificatie is gevraagd (de provider – de aanbieder van de verificatieservice)
 - h. Het verificatieresultaat (Match / NoMatch)
 - i. Een opsomming van de gegevenselementen die in de vergelijking betrokken zijn, de identificatie van de authentieke bron waartegen de verificatie plaats heeft gevonden en optioneel de waarde uit de authentieke bron (indien de waarde overeenstemde met de waarde die de QTSP heeft verstrekt).

Vereenvoudigingen voor beproeving:

Voor de beproeving gaat de attribuutverificatieservice uit van de volgende vereenvoudigingen:

- De waarden voor de gegevenselementen zijn 1-op-1 te vergelijken. Er wordt geen rekening gehouden met bewerkingen, omvormingen, diakrieten, concatenaties, spatiegebruik, non-latin script, ed. In de voorbereiding op de uitvoering van de beproeving zorgt het project ervoor dat de waarden volledig overeenstemmen.
- De attribuutvergelijking wordt in de beproeving alleen uitgevoerd voor de voorgedefinieerde set geboortegegevens.
- De beproeving ondersteunt de situatie niet waarin de QTSP meer gegevenselementen ter verificatie voorlegt dan de authentieke bron kan leveren.

Automatiseringsverwachting

Het beantwoorden van een verificatieverzoek gebeurt geautomatiseerd, zonder tussenkomst van medewerkers. Elke request-reponse flow wordt gelogd.

2.3. Aanvullende vereenvoudigingen voor beproeving

Voor de UBO beproeving zijn enkele aanvullende vereenvoudigingen mogelijk (over te besluiten afhankelijk van implementatie-inspanningen:

- Hard-coded attribuutmapping voor het geboortebewijs in plaats van een configuratie van attribuutmappingen.
- Hard-coded attribuutvergelijking voor het geboortebewijs in plaats van een dynamische vergelijkingsfunctie die voor alle attributen kan werken.

Auteurs

Indra Henneman
Aleksandar Simsic
Ivar Vennekens

VNG Realisatie

Nassaulaan 12
2514 JS Den Haag
070 373 80 08