start architectuur

Nationale implementatie van eIDAS
met het stelsel Elektronische Toegangsdiensten

Versie 1.2 (na PIA en risicoanalyse)
April 2017

Dit is een samenwerking van:
- Logius
- BZK
- RvIG
- EZ

Inhoud

Afbeeldingen

Opdrachtgever

Naam	Organisatie
Freek van Krevel	EZ

Opdrachtnemer

Naam	Organisatie
Mirjam Gerritsen	Logius

Auteurs

Naam	Organisatie	Rol
Michiel Dollenkamp	Logius	Architect
Ivar Vennekens	EZ	Architect
Egbert Verweij	RvIG	Architect

Documenthistorie

Versie	Document
0.8	Versie voor brede review
1.0	Verwerking reviewbevindingen Versie voor PIA, Risicoanalyse en start ontwikkeling deel PSA's
1.1	Versie na PIA en risicoanalyse
1.11	Attribuutindeling conform verordening aangepast naar: verplichte attributen, aanvullende attributen en andersoortige attributen.
1.2	Enkele opmerkingen van BZK ten aanzien van de PSA zijn verwerkt. Onderdeel hiervan is de toevoeging van een achtste beleidsmatige pijler.

Reviewers

Versie	Naam	Organisatie
0.8	Andre de Kok	BZK-RvIG
0.8	Frans Rijkers	BZK-RvIG
0.8	Esther 't Hoen	BZK
0.8	Carlo Luijten	BZK
0.8	Kick Willemse	EZ
0.8	Youssef Berrich	EZ
0.8	Jan Willem Beusink	EZ-DICTU
0.8	Henk Romein	EZ-DICTU
0.8	Marco Eikenaar	FIN-BD
0.8	Hans-Rob de Reus	FIN-BD
0.8	Eric Verheul	Stelsel eTD / Programma eID
0.8	Frans de Kok	Stelsel eTD / Programma eID
0.8	Remco Schaar	Stelsel eTD / Programma eID
0.8	Maurice Pasman	Stelsel eTD
0.8	Elles van Geest	Stelsel eTD
0.8	Johan van den Bosch	Stelsel eTD
0.8	Selman Karaman	Logius
0.8	Vincent van de Laar	ICTU

Goedkeuring

Naam	Organisatie	Akkoord
Freek van Krevel	EZ	

1 Inleiding

De ontwikkeling van één 'Digital Single Market' is een belangrijke aanjager van economische groei in de EU. Burgers en Bedrijven kunnen in de ééngemaakte interne digitale markt makkelijker, veiliger en tegen lagere kosten zakendoen over grenzen heen. Grensoverschrijdende eOverheidsdiensten verlagen de administratieve lasten voor burgers en bedrijven en bevorderen de Europese integratie. Beperkend is echter dat burgers en bedrijven de nationale toegangsmiddelen nu alleen in de eigen lidstaat kunnen gebruiken. Voor grensoverschrijdende authenticatie moeten zij de nationale toegangsmiddelen ook in andere EU-lidstaten kunnen gebruiken. De eIDAS verordening[1] regelt dit.

De Verordening (EU Nr. 910/2014) stelt verplicht dat lidstaten de eID middelen uit andere lidstaten per september 2018 van elkaar accepteren. Het aanmelden van het nationale eID middel is een keuze van de lidstaat. Een natuurlijk persoon of rechtspersoon met een EU eID middel kan toegang krijgen tot de digitale overheidsvoorzieningen in Nederland mits deze persoon inlogt met een genotificeerd/erkend eID middel. De verordening maakt het ook mogelijk dat een natuurlijk persoon of rechtspersoon met een Nederlands eID middel toegang kunnen krijgen tot de digitale overheidsvoorzieningen in andere EU-lidstaten.

De eIDAS verordening schrijft voor dat een persoon met zijn nationale toegangsmiddel in moet kunnen loggen bij publieke dienstverleners in elk van de andere Europese lidstaten, mits:

- de lidstaat zijn authenticatievoorziening / -stelsel bij de Europese Commissie genotificeerd heeft;
- het een dienst betreft die digitaal verleend wordt;
- de authenticatie op niveau substantieel of hoog plaatsvindt.

Om ervoor te zorgen dat de implementatie van de verordening in Nederland gecontroleerd verloopt en de impact op de dienstverleners, stelsels en middelen beperkt blijft, hebben het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), het Ministerie van Economische Zaken (EZ), de Rijksdienst voor Ondernemend Nederland (RVO.nl), de Belastingdienst en Logius in 2015 blauwdrukken voor grensoverschrijdende toegang opgesteld. Deze blauwdrukken beschrijven de manier waarop grensoverschrijdend inloggen via het stelsel Elektronische Toegangsdiensten (eTD) moet gaan verlopen, zowel voor (1) inloggen vanuit het buitenland in Nederland als (2) inloggen vanuit Nederland in het buitenland. En voor zowel natuurlijke personen als niet-natuurlijke personen.

1.1 Opdracht

De opdracht voor deze startarchitectuur is om de principes, richtlijnen en kaders te specificeren voor implementatie van de NL eIDAS verordening via eTD. Het specificeert daartoe de componenten die in de keten nodig zijn, de functionaliteit waarmee die uitgebreid of ontwikkeld moeten worden en de manier waarop die onderling samenhangen (koppelvlakken). Deze startarchitectuur biedt de houvast

[1] Electronic identification and trust services (UK) of Elektronische identiteiten en vertrouwensdiensten (NL).

die nodig is om vervolgens de verschillende componenten in detail uit te werken en is daarom 'overkoepelend'.

1.2 Afbakening

Deze startarchitectuur is op een aantal aspecten afgebakend:

1. De reikwijdte van de startarchitectuur is beperkt tot het onderdeel elektronische identificatie van de eIDAS verordening. De nationale implementatie van vertrouwensdiensten (zoals elektronische handtekeningen, elektronische zegels, elektronische tijdstempels, diensten voor aangetekende elektronische bezorging en elektronische certificaten voor authenticatie van websites) is buiten scope.
2. De verordening specificeert enkele verplichte en aanvullende attributen (de 'minimale dataset') en benoemt de mogelijkheid voor andersoortige attributen, zonder deze verder te specificeren. Deze startarchitectuur houdt rekening met de mogelijkheid om dergelijke andersoortige attributen uit te wisselen, maar werkt dit niet verder uit.
3. Grensoverschrijdend inloggen vindt plaats via het stelsel eTD. De architectuur sluit niet uit dat ook andere stelsels genotificeerd worden en via deze architectuur op het eIDAS netwerk aansluiten. Dit is in deze startarchitectuur echter niet verder uitgewerkt.

Merk op dat de omgeving waarin deze oplossing gespecificeerd is, sterk in beweging is. BZK stelt uniforme eisen voor toegangsdiensten in het publieke domein op, de Belastingdienst voert een pilot met iDIN uit en de besluitvorming over implementatie van een nieuwe manier van pseudonimisering (polymorf) in het stelsel eTD loopt nog. De architectuur sluit niet uit dat Europese toegang via een ander stelsel dan eTD plaats gaat vinden, maar werkt dat niet in detail uit. Indien Europese toegang op een andere manier dan via eTD plaatsvindt heeft dat mogelijk consequenties op onder meer de:

- manier waarop het eIDAS koppelpunt pseudoniemen opvraagt en ontvangt;
- attribuuttranslaties die het eIDAS koppelpunt uitvoert;
- maatregelen voor beveiliging en versleuteling van berichten;
- registratie van Europese diensten in een dienstencatalogus;
- (toestemming voor) het gebruik van het BSN-koppelregister (BSNk) voor het aan dienstverleners leveren van het BSN;
- notificatie van de Nederlandse authenticatieoplossing voor grensoverschrijdend gebruik en de bijbehorende Europese reviews;
- rol die marktpartijen kunnen en mogen leveren.

1.3 Uitgangspunten en randvoorwaarden

De architectuur is conform het huidige beleid geschreven op publieke implementatie van het eIDAS koppelpunt (eIDAS connector, eIDAS proxy service en eIDAS berichtenservice). In 2018 of daarna wordt bezien of één of meer delen van het koppelpunt zullen worden uitbesteed.

1.4 Relatie met andere ontwikkelingen

De nationale implementatie van eIDAS vindt zoveel mogelijk met bestaande voorzieningen plaats. Daarom bestaat er samenhang met de doorontwikkeling van het stelsel eTD en het eIDAS koppelpunt.

- Doorontwikkeling stelsel eTD.
  eTD is sterk in ontwikkeling. Ook de realisatie van deze startarchitectuur vereist uitbreiding van het afsprakenstelsel. De nationale implementatie van de eIDAS verordening heeft het risico dat het 'schiet op een bewegend doel'. Deze startarchitectuur baseert zich op het afsprakenstelsel 1.10[2]. Wijzigingen die voor implementatie van eIDAS in eTD nodig zijn, worden in de volgende projectfase in een aparte RFC beschreven.

- Doorontwikkeling eIDAS koppelpunt.
  Met de in gebruik name van de STORK 2 software (PEPS en V-IDP) heeft Nederland een flinke stap in implementatie van het eIDAS koppelpunt gezet. De doorontwikkeling van de software is nu in handen van DG DIGIT (eIDAS connector en eIDAS proxy service). Nieuwe implementaties hebben impact op het koppelvlak waarlangs communicatie met het koppelpunt plaatsvindt. Deze startarchitectuur baseert zich op de 1.0 specificaties van het eIDAS koppelpunt en het bijbehorende koppelvlak (en dus niet op de PEPS die momenteel nog in gebruik is). Tijdige opwaardering van de huidige PEPS naar de eIDAS connector en eIDAS proxy service is randvoorwaardelijk voor implementatie van deze startarchitectuur.

- Opstellen uniforme eisen voor authenticatie in het publieke domein.
  BZK is bezig uniforme eisen op te stellen voor de authenticatie in het publieke domein. Deze eisen betreffen ook de informatieuitwisseling met en identiteit- en toegangsmanagement voor de publieke dienstverleners en zullen aspecten als privacybescherming en misbruikbestrijding kennen. Deze startarchitectuur sorteert hier al zoveel mogelijk op voor waar raakvlakken liggen in functionaliteiten die in de scope van deze startarchitectuur liggen. Op het moment dat de eisen opgesteld zijn, is toetsing van de in deze startarchitectuur beschreven oplossing tegen de eisen nodig.

- Notificeren van het Afsprakenstelsel eTD.
  Voor notificatie van eTD voor gebruik in Europa is het nodig om de uitgifte, registratie en gebruik van middelen conform de eIDAS voorschriften te laten verlopen. Hiervoor wordt het afsprakenstelsel aangepast. Notificatie kan pas plaatsvinden na realisatie van de componenten uit deze startarchitectuur voor het verkeer naar buiten en realisatie van de wijzigingen in het afsprakenstelsel.

- Doorontwikkeling BSNk.
  De voor eIDAS vereiste wijzigingen in het BSNk kennen een andere voortbrengingsdynamiek dan de andere door BZK te realiseren wijzigingen in het kader van eIDAS. De veranderingen in het

[2] https://afsprakenstelsel.etoegang.nl/display/as/Startpagina

BSNk worden mede gedreven door de wettelijke eisen en de doorontwikkeling van het afsprakenstelsel en zullen hierdoor in een eerder stadium gerealiseerd worden. Voor de volledigheid is er gekozen om de vanuit deze startarchitectuur vereiste wijzigingen op te nemen als een programma afhankelijkheid en de vereiste aanpassing inzichtelijk te maken onder de noemer 'BSNk'.

1.5 Documentatie

De volgende documenten zijn gebruikt bij het opstellen van deze architectuur en zijn leidend voor de oplossing:

Wet- en regelgeving:
- Uitvoeringsbesluit (EU) 2015-296 van de Commissie
- Uitvoeringsbesluit (EU) 2015-1984 van de Commissie
- Uitvoeringsbesluit (EU) 20151-505 van de Commissie
- Uitvoeringsbesluit (EU) 20151-506 van de Commissie
- Uitvoeringsverordening (EU) 2015-806 van de Commissie
- Uitvoeringsverordening (EU) 2015-1501 van de Commissie
- Uitvoeringsverordening (EU) 2015-1502 van de Commissie
- Verordening (EU) nr. 9102014 van het Europees Parlement en de Raad

Architectuur en specificaties van het eIDAS netwerk:
- eidas_interoperability_architecture_v1.00
- eidas_message_format_v1.0
- eidas_saml_attribute_profile_v1.0_2
- eidas_-_crypto_requirements_for_the_eidas_interoperability_framework_v1.0

Blauwdrukken voor nationale implementatie:
- Aansluiting Idensys op eIDAS use case II-A definitief
- Aansluiting Idensys op eIDAS use case II-B definitief
- Aansluiting Idensys op eIDAS use case III-A definitief
- Aansluiting Idensys op eIDAS use case III-B definitief

Specificatie van het Afsprakenstelsel eTD:
- Afsprakenstelsel eTD 1.10

Specificatie van het Basisregister personen
- Logisch ontwerp GBA, versie 3.9

Specificatie van de Polymorfe Pseudonimisering
- https://www.idensys.nl/fileadmin/bestanden/idensys/documenten/basisdocumentatie/documentatieset/PP_Scheme_091.pdf

1.6 Verantwoording

Deze startarchitectuur is in de eerste helft van 2016 opgesteld als samenwerking van architecten van de Rijksdienst voor Identiteitsgegevens (RvIG), het ministerie van BZK, het ministerie van EZ, RVO.nl en Logius (eID programma). In de tweede helft van 2016 hebben een privacy impact assessment (PIA) en risicoanalyse op de startarchitectuur plaats gevonden. Daarnaast is de ontwerpfase gestart en heeft hierover regelmatig afstemming tussen de ontwerpteams plaatsgevonden. De verbeteringen die dit voor de startarchitectuur met zich mee heeft gebracht, zijn in versie 1.1 verwerkt.

De departementen hebben uitgesproken de in deze startarchitectuur opgenomen uitgangspunten, principes, ed. te volgen bij het ontwikkelen van de componenten die onder hun verantwoordelijkheid vallen.

De implementatie van deze startarchitectuur hoeft niet ineens plaats te vinden. De architectuur is zo ontwikkeld dat stapsgewijze implementatie mogelijk is, waarbij onderscheid gemaakt kan worden in inkomende authenticatie (met door andere lidstaten genotificeerde authenticatiemiddelen – teneinde te voldoen aan de vereisten uit de verordening) en uitgaande authenticatie (met door NL genotificeerde authenticatiemiddelen). Bijlage 2 beschrijft de faseringsmogelijkheden aan de hand van implementatievarianten.

2 Kaders

2.1 Beleidskeuzes

De startarchitectuur is gebaseerd op enkele beleidsmatige pijlers die bepalend zijn voor de uitwerking in dit document. Wijziging in één of meer pijlers moet tot herziening van de startarchitectuur leiden.

- Pijler 1: de oplossing respecteert de departementale verantwoordelijkheden alsmede wet- en regelgeving.
  De oplossing doet recht aan de verantwoordelijkheden van de departementen en de verplichting die de departementen hebben om die verantwoordelijkheid te nemen. Het ministerie van BZK is verantwoordelijk voor het – conform nationale wet- en regelgeving – registreren van natuurlijke personen in de basisregistratie persoonsgegevens en het uitgeven van het BSN. Het ministerie van EZ is beleidsverantwoordelijk voor de grensoverschrijdende toegang in het algemeen en het Nederlandse eIDAS koppelpunt in het bijzonder. De architectuur onderkent die verantwoordelijkheden en beschrijft een oplossing waarin de departementen hun verantwoordelijkheid zo autonoom mogelijk – dus onafhankelijk van de ander – kunnen nemen.

- Pijler 2: de oplossing ontzorgt Nederlandse dienstverleners.
  De architectuur volgt het principe dat de digitale toegang voor (natuurlijke- en rechts-) personen tot dienstverleners zo uniform mogelijk werkt, onafhankelijk of het nationale of Europese inlog betreft. De architectuur voorziet daarom in één koppelvlak voor zowel nationale als Europese inlog en een uniforme manier van communicatie over betrouwbaarheid van authenticatie en attributen alsmede uniform beheer op dienstinformatie. Dit minimaliseert de impact van grensoverschrijdende digitale toegang op dienstverleners.

- Pijler 3: de oplossing maakt maximaal gebruik van bestaande voorzieningen.
  De architectuur maakt maximaal gebruik van generieke en bestaande componenten, zoals bestaande authenticatiediensten, het BSNk en het eIDAS koppelpunt. De architectuur introduceert alleen nieuwe componenten indien bestaande voorzieningen daar geen passende oplossing voor bieden.

- Pijler 4: de oplossing ondersteunt alleen de betrouwbaarheidsniveaus substantieel en hoog.
  De oplossing accepteert het grensoverschrijdend inloggen (vanuit Nederland of een andere Europese lidstaat) op niveau laag dus niet. NB: dat is ook geen eis uit de eIDAS verordening.

- Pijler 5: NL zet Europese eIDAS software ongewijzigd in.
  DG DIGIT levert elk van de lidstaten een referentie-implementatie van de nationale eIDAS software (eIDAS connector en eIDAS proxy service). DG DIGIT voert hierover het changemangement en ontwikkelt de software releasegewijs door. Nederland kiest ervoor om bij implementatie van het nationale eIDAS koppelpunt gebruik te maken van deze Europese software. De software wordt voor en door Nederland geconfigureerd en operationeel beheerd, maar niet gewijzigd.

- Pijler 6: eIDAS koppelpunt initieel publiek ingevuld.
  EZ ontwikkelt en implementeert het eIDAS koppelpunt (en alle daaronder vallende componenten) in het publieke domein. Deze startarchitectuur brengt de consequenties van de private ontwikkeling van het eIDAS koppelpunt of delen daarvan niet in kaart. Verwacht wordt echter dat de consequenties vooral juridisch zijn en maar beperkt invloed hebben op de in dit document beschreven architectuur. Na 2018 zal EZ nagaan of uitbesteding van (delen van) het koppelpunt mogelijk en wenselijk is.

- Pijler 7: eIDAS koppelpunt voor publieke én private dienstverlening.
  Gebruik van het eIDAS koppelpunt is voor publieke dienstverleners verplicht. Nederland stelt het koppelpunt echter ook beschikbaar voor private dienstverlening in Nederland (authenticatie in andere lidstaat) en andere lidstaten (authenticatie in Nederland). Over financiering en een business model van private dienstverlening via het eIDAS koppelpunt zijn voor zover bekend nog geen afspraken gemaakt.

- Pijler 8: EZ draagt zorg dat de gehele authenticatieketen, voor zover binnen de reikwijdte van Nederland, voldoet aan de eisen die hieraan gesteld worden krachtens artikel 7 en 8 van de wet GDI. Dit betekent dat EZ zorgdraagt dat het eIDAS-koppelpunt (door de inzet van een ontsluitende dienst) conformeert aan de eisen die de wet GDI stelt aan de Authenticatiedienst. Verder zal EZ zich inspannen, binnen bestaande wettelijke grenzen en verantwoordelijkheden dat de door haar ingeschakelde ontsluitende dienst (binnen eTD makelaar genoemd) eveneens conformeert aan de hiervoor geldende eisen en erkend wordt door BZK.

2.2 Architectuurprincipes

Deze overkoepelende startarchitectuur hanteert – op basis van de in voorgaande beschreven beleidsbeslissingen - enkele architectuurprincipes die de individuele componenten overstijgen:

1. Nederlandse dienstverleners sluiten via het stelsel eTD - en niet direct - aan op de Nederlandse eIDAS infrastructuur. NB: dit betekent niet automatisch dat Nederlandse dienstverleners in alle gevallen zonder aanpassing in hun dienstverleningsproces diensten aan buitenlandse personen kunnen verlenen. De via het eIDAS koppelpunt verkregen attributen kunnen bijvoorbeeld afwijken van wat er nationaal beschikbaar is.

2. NL realiseert geen register of andere voorziening ter ondersteuning van een uniforme identificatie van buitenlandse rechtspersonen.

3. eTD neemt voor het inloggen bij buitenlandse dienstverleners enkele hiervoor bestemde ‘generieke’ diensten op in de stelselcatalogus. De stelselcatalogus gaat niet alle diensten van elk van de buitenlandse dienstverleners bevatten. Hiervoor ontbreekt het in eIDAS aan standaards en voorschriften. In de architectuur is wel voorzien dat voor specifieke dienstverlening (bijvoorbeeld TAXUD) Europese diensten in de stelselcatalogus opgenomen kunnen worden.

4. Op de identificatie van natuurlijke personen wordt in eTD pseudonimisering toegepast. De huidige wijze van pseudonimiseren (eTD 1.10) voldoet niet aan nationale en Europese eisen die aan privacy, vertrouwelijkheid en persistentie gesteld worden. Het stelsel eTD gaat daarom stelselbreed over tot het gebruik van Polymorfe Pseudoniemen. Tijdige formalisatie van het

besluit tot inzet van Polymorfe Pseudoniemen is randvoorwaardelijk voor implementatie van deze startarchitectuur.

5. Voor de communicatie tussen het Europese koppelpunt en eTD wordt aangesloten op de bestaande HM-AD/MR en HM-DV koppelvlakken. Deze koppelvlakken worden voor correcte implementatie van de eIDAS verordening op enkele punten aangepast (uit te werken in de RfC eTD).

6. De oplossing zorgt ervoor dat een persoon die diensten in het Nederlandse publieke (BSN) domein afneemt, herkenbaar is als één persoon met één BSN. Onafhankelijk van het land waarin en het middel waarmee authenticatie plaatsvindt. Daarvoor achterhaalt BZK in het BRP het BSN van de persoon. NB: de dienstverlener kan er voor kiezen om – indien de registratie in de BRP nog niet plaats heeft gevonden of afgerond is – de buitenlandse burger de dienst (nog) niet te verlenen. De verordening biedt die ruimte door alleen het grensoverschrijdend inloggen voor te schrijven en niet het starten van het dienstverleningsproces te verplichten.

7. De oplossing zorgt er *niet* voor dat een persoon die met authenticatiemiddelen uit verschillende lidstaten inlogt voor Nederlandse diensten buiten het publieke (BSN) domein herkenbaar is als één persoon. Die persoon wordt in deze oplossing herkend als verschillende (losstaande) identiteiten. Elk met een eigen (polymorf – onderling niet te relateren) pseudo ID.

8. BZK krijgt bij de eerste inlog van een persoon voor een BSN-dienst alle attributen die de lidstaat heeft geleverd. BZK heeft ervoor gekozen de attributen bij navolgende inlogs – na koppeling aan het BSN – niet meer te ontvangen.

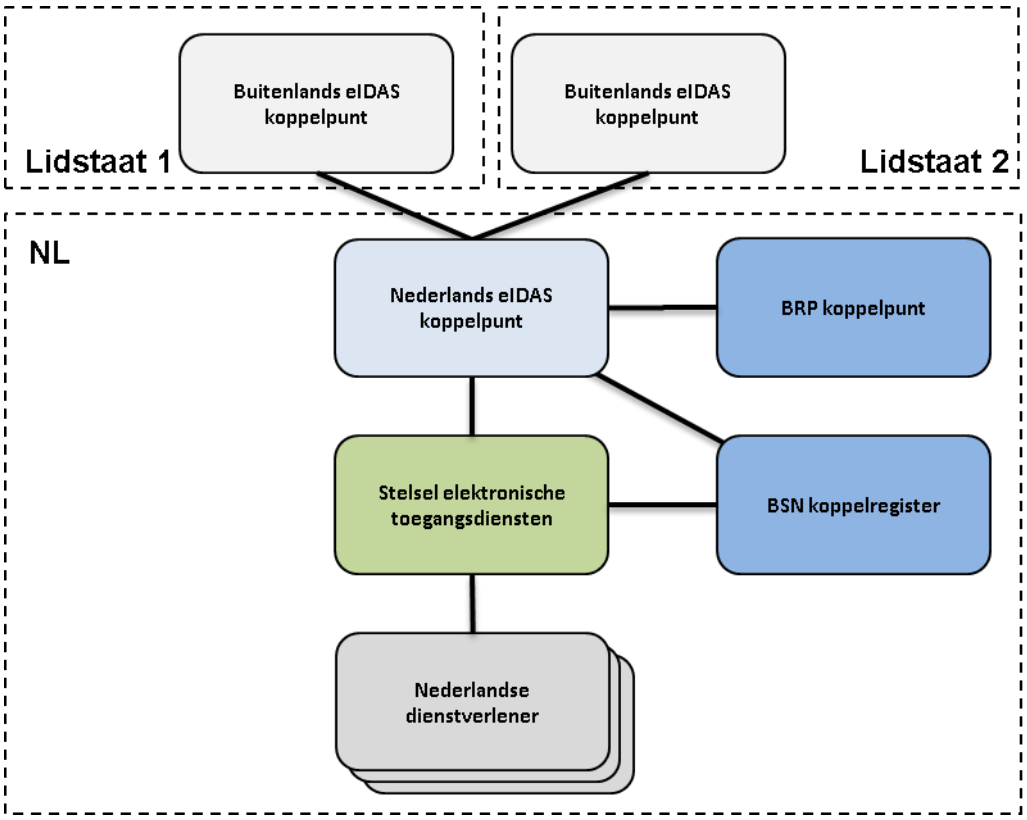
9. Het BSN is doorgaans onlosmakelijk met de persoon verbonden. Het kan in bijzondere gevallen voorkomen dat het BSN van een persoon wijzigt. Bijvoorbeeld omdat de persoon onterecht twee keer in de BRP voorkwam. De architectuur voorziet in de mogelijkheid voor BZK om een koppeling van uniquenss identifier aan een BSN te verwijderen.

10. De voorzieningen worden zo autonoom mogelijk gerealiseerd, waarbij de heldere Separation of Concerns tussen de beleidsverantwoordelijkheden gereflecteerd wordt in de te realiseren voorzieningen.

11. Er wordt gestreefd naar hergebruik van bestaande componenten, en hun werking, waar mogelijk.

2.3 Aandachtsgebieden

Voor grensoverschrijdende toegang van en naar Nederland is een samenwerking van nieuwe en bestaande functionaliteit in verschillende aandachtsgebieden nodig. De samenhang tussen deze aandachtsgebieden is hieronder afgebeeld.



Figuur 1: Context Doelarchitectuur

De Nederlandse oplossing voor grensoverschrijdende digitale toegang onderscheidt de volgende aandachtsgebieden:

- De Nederlandse dienstverlener: de organisatie die haar diensten digitaal open heeft gesteld voor dienstafnemers in Europa. Voor publieke dienstverleners is het toestaan van buitenlandse inlogs vanaf september 2018 onder voorwaarden verplicht, voor private dienstverleners optioneel.
- Het stelsel eTD: het afsprakenstelsel voor identificatie, authenticatie en machtigingen van Nederlandse (natuurlijke- en rechts-)personen en online toegangsdiensten voor Nederlandse dienstverleners.
- Het BRP koppelpunt: de voorziening die ervoor zorgt dat de attributen van natuurlijke personen worden gekoppeld aan het BSN. Dit zijn zowel ingezetenen en niet-ingezetenen.
- Het BSNk voor het (1) koppelen van authenticatiemiddelen aan het BSN en (2) het uitgeven van Polymorfe Pseudoniemen ter identificatie van natuurlijke personen.

- Het Nederlands eIDAS koppelpunt: de voorziening die ervoor zorgt dat Nederland via eTD aan de andere Europese lidstaten gekoppeld is. Het koppelpunt faciliteert enerzijds het inloggen door Europese personen bij Nederlandse dienstverleners en anderzijds het inloggen van personen met een Nederlands authenticatiemiddel bij buitenlandse dienstverleners. Daarvoor onderhoudt het koppelingen naar elk van de buitenlandse eIDAS koppelpunten en naar het stelsel eTD.
- Buitenlandse eIDAS koppelpunten. De tegenhangers van het Nederlandse eIDAS koppelpunt in elk van de andere lidstaten. De communicatie tussen de eIDAS koppelpunten is in de eIDAS interoperabiliteitsarchitectuur en bijbehorende SAML berichtspecificatie geüniformeerd.

2.4 Identificerende nummers

Centraal in de startarchitectuur staat het zorgvuldig omgaan met identificerende nummers, waarbij met name de nummers van natuurlijke personen extra aandacht behoeven. De startarchitectuur is ontwikkeld volgens *privacy by design*, zodat er geen onnodige uitwisseling van identificerende nummers en persoonskenmerken plaatsvindt. De startarchitectuur maakt veelvuldig gebruik van de volgende identifiers:

- Uniqueness identifier: dit is de identificatie die grensoverschrijdend voorgeschreven is. De identifier wordt bij authenticatie met een buitenlands middel vanuit de lidstaat waarin authenticatie plaatsvindt verstuurd en heeft een voorgeschreven formaat: land van authenticatie/land van bestemming/identifier. Bijvoorbeeld BE/NL/123243g13f. De uniqueness identifier is zo persistent mogelijk, zodat een persoon steeds aan deze identifier herkend wordt.
- PP-EU: dit is een polymorf pseudoniem waarmee de persoon bij de authenticatiedienst (incl. berichtenservice) bekend is. De PP-EU is gebaseerd op de uniqueness identifier en wordt door het BSNk gegenereerd. De PP-EU is de basis voor herkenning van de persoon bij dienstverlening in het Nederlandse private domein (niet-BSN diensten).
- PP-BSN: dit is een polymorf pseudoniem dat het BSN als basis heeft. De eIDAS berichtenservice krijgt dit pseudoniem van het BSNk als een persoon met een buitenlands middel een BSN-dienst in Nederland af wil nemen (en het BSN van de persoon bekend is). Elke authenticatiedienst krijgt een ander PP-BSN. Door het polymorfe karakter van de pseudonimisering zijn echter alle PP-BSN's van een persoon (alleen) door de dienstverlener terug te herleiden tot het BSN zelf.
- PP-PS: dit is een polymorf pseudoniem dat de basis heeft in het BSN, maar daar niet toe herleid kan worden. Het is daarom niet geschikt voor gebruik in het BSN-domein, maar wél in het private domein. Door de BSN als basis te nemen, is geborgd dat elke individu één uniek pseudoniem krijgt.
- Dienstverlener specifiek pseudoniem (EP): De PP-EU, PP-BSN en PP-PS zijn specifiek voor de eIDAS berichtenservice (of algemener: de authenticatiedienst). De berichtenservice verstrekt ze niet aan andere partijen dan het BSNk. De dienstverlener ontvangt een ander pseudoniem: het dienstverlener specifieke pseudoniem. De eIDAS berichtenservice ontvangt dit pseudoniem op basis van het PP-BSN of PP-EU van het BSNk. Dit pseudoniem is versleuteld en kan alleen door de dienstverlener ontsleuteld worden. Voor BSN-diensten leidt ontsleuteling tot het BSN van de persoon.

Onderstaande tabel toont de PP's die gebruikt worden voor dienstverlening in Nederland.

	BSN-dienst	Niet BSN-dienst
NL authenticatiemiddel	PP-BSN	PP-PS
EU authenticatiemiddel	PP-BSN	PP-EU

Voor het bepalen van de uniquenss identifier bij dienstverlening in het buitenland (inloggen met een NL authenticatiemiddel) gebruikt de eIDAS berichtenservice het PP-PS.

2.5 eIDAS attributen

De eIDAS verordening definieert de attributen van de natuurlijke en niet-natuurlijke persoon die uitgewisseld worden: de minimale dataset. De minimale dataset bestaat uit een aantal verplichte en een aantal aanvullende attributen.

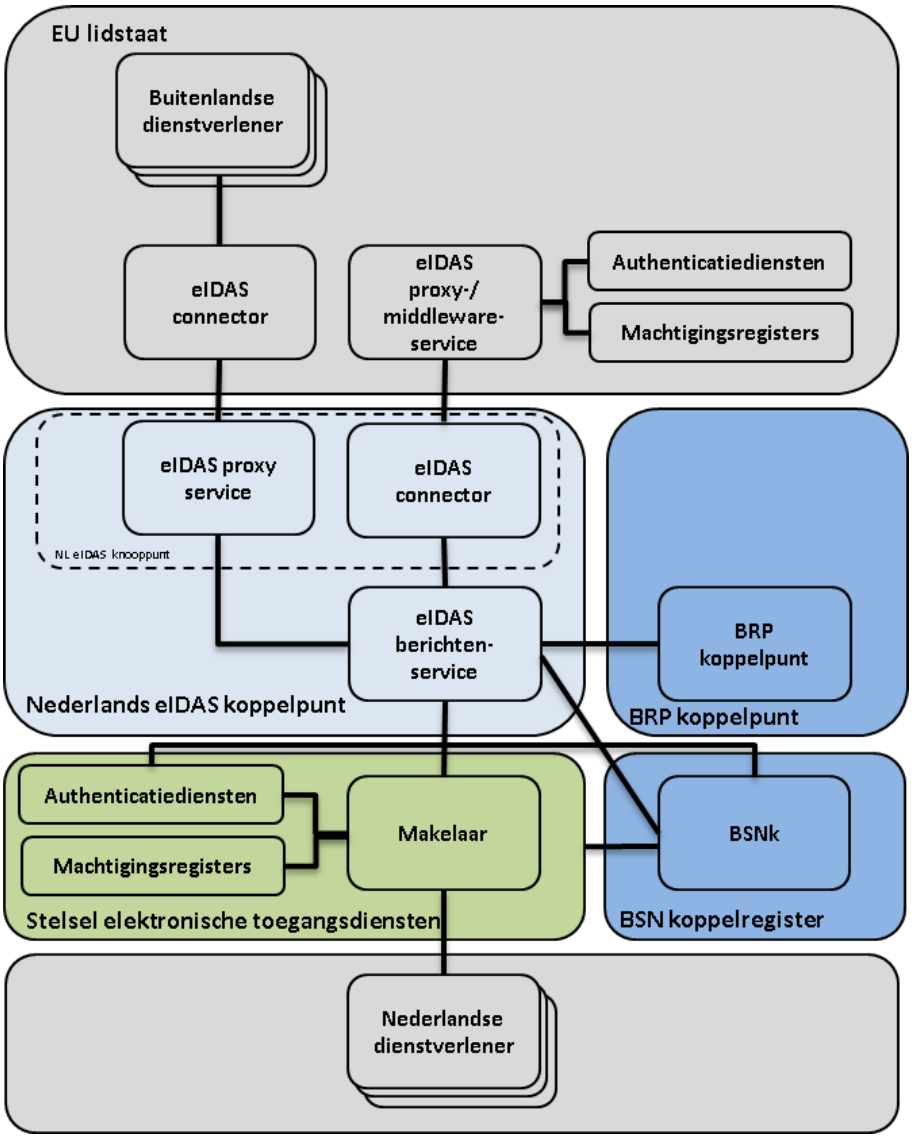
Minimale dataset voor de natuurlijke persoon:
- huidige familienaam of familienamen (verplicht)
- huidige voornaam of voornamen (verplicht)
- geboortedatum (verplicht)
- unieke identificatiecode (verplicht)
- voornaam of voornamen en familienaam of familienamen bij geboorte
- geboorteplaats
- huidig adres
- geslacht

Minimale dataset voor de rechtspersoon:
- huidige wettelijke naam (verplicht)
- unieke identificatiecode (verplicht)
- huidig adres
- btw-nummer
- fiscaal referentienummer
- de identificatiecode bedoeld in artikel 3, lid 1, van Richtlijn 2009/101/EG van het Europees Parlement en de Raad (1)
- de identificatiecode voor juridische entiteiten bedoeld in Uitvoeringsverordening (EU) nr. 1247/2012 van de Commissie (2)
- het registratie- en identificatienummer van marktdeelnemer (EORI-nr.) bedoeld in Uitvoeringsverordening (EU) nr. 1352/2013 van de Commissie (3)
- het accijnsnummer bedoeld in artikel 2, punt 12, van Verordening (EU) nr. 389/2012 van de Raad (4).

Daarnaast mogen lidstaten ervoor kiezen om andersoortige attributen uit te wisselen. Deze zijn niet in de verordening uitgewerkt.

3 Functionaliteit

Onderstaande diagram toont de componenten die binnen de verschillende aandachtsgebieden nodig zijn voor implementatie van de eIDAS verordening: de doelarchitectuur.



Figuur 2: Componenten van de doelarchitectuur

De eIDAS berichtenservice en BRP koppelpunt zijn nieuw, het BSNk wordt uitgebreid.

3.1 Nederlandse eIDAS Koppelpunt

Het Nederlandse eIDAS Koppelpunt zorgt voor de connectie naar elk van de aangesloten lidstaten enerzijds en aan het stelsel eTD anderzijds. Het eIDAS koppelpunt valt onder de departementale verantwoordelijkheid van het ministerie van EZ.

3.1.1 Beschrijving

Het Nederlandse eIDAS Koppelpunt faciliteert de interoperabiliteit tussen het Nederlandse stelsel eTD en buitenlandse eIDAS koppelpunten. Richting de buitenlandse eIDAS koppelpunten voldoet het NL koppelpunt aan de eIDAS-standaard en richting het eTD aan de daar geldende eTD-standaard. Het eIDAS koppelpunt onderhoudt de koppelingen naar elk van de andere aangesloten lidstaten en gedraagt zich naar het stelsel eTD als authenticatiedienst/machtigingregister (voor authenticatie van personen met een buitenlands middel) en dienstverlener (voor authenticatie van personen met en Nederlands middel). Het eIDAS koppelpunt bestaat uit de componenten:

- eIDAS knooppunt, bestaande uit:
    1. eIDAS connector: de functionaliteit voor koppeling aan buitenlandse authenticatiestelsels. De tegenhanger van de eIDAS connector is een buitenlandse proxy service of middleware service (Duitsland en Oostenrijk).
    2. eIDAS proxy service: de functionaliteit voor koppeling van het nationale authenticatiestelsel op buitenlandse dienstverleners. De tegenhanger van de proxy service is een buitenlandse eIDAS connector. Nederland heeft niet gekozen voor een middleware authenticatiestelsel en levert dus geen eigen eIDAS middleware service.
- eIDAS berichtenservice: de brugfunctie tussen de Europese eIDAS componenten en het nationale eTD. De berichtenservice bevat onder meer functionaliteit voor het omvormen van eIDAS berichten tot eTD berichten en omgekeerd.

3.1.2 Architectuurbeslissingen

Op het Nederlandse eIDAS koppelpunt zijn de volgende architectuurbeslissingen van toepassing:

- De belangrijkste niet-functionele eigenschappen van het eIDAS koppelpunt zijn security, efficiency, performance en ontkoppeling.
- EZ realiseert/configureert de eIDAS berichtenservice om interoperabiliteit tussen het stelsel eTD en buitenlandse eIDAS koppelpunten te realiseren.
- De eIDAS berichtenservice conformeert zich binnen Nederland aan de door het stelsel voorgeschreven gedrag van een Authenticatiedienst/Machtigingsregister, zolang dat past binnen de nationale en Europese eIDAS vereisten (verordening en wetgeving).
- De eIDAS berichtenservice is in de interactie met het stelsel eTD volgend in de actuele afspraken van het stelsel eTD, zolang dat past binnen de nationale en Europese eIDAS vereisten (verordening en wetgeving).
- Het eIDAS koppelpunt levert de buitenlandse attributen in eTD formaat aan het BRP koppelpunt voor matching en registratie. Vertaling van het eTD format naar het GBA datamodel vindt in het BRP koppelpunt plaats.

3.1.3 Eisen

De startarchitectuur stelt geen bijzondere eisen aan de eIDAS connector en eIDAS proxy service. Wél aan de eIDAS berichtenservice. De eIDAS berichtenservice:

- achterhaalt in het stelsel eTD of de Nederlandse dienstverlener een BSN vereist;
- achterhaalt in het stelsel eTD welke attributen de Nederlandse dienstverlener nodig heeft. Het eIDAS koppelpunt staat het toe dat de dienstverlener een subset van de in de catalogus bij de dienst gemarkeerde attributen vraagt. Het eIDAS koppelpunt mag het niet toestaan dat de dienstverlener meer attributen vraagt dan in de stelselcatalogus aangegeven;
- neemt de bij dienstverlener of makelaar gemaakte landenkeuze voor authenticatie over (indien beschikbaar);
- biedt de handelende persoon een landenkeuze voor authenticatie als die keuze nog niet door de dienstverlener of makelaar gemaakt is;
- achterhaalt in de eigen registratie of de persoon al eerder ingelogd was en er daarom al pseudoniemen bekend zijn;
- vormt de eIDAS attributen om naar eTD attributen en zorgt voor de daarvoor benodigde decryptie en encryptie;
- stelt bij afname van een BSN dienst de attributen van de persoon beschikbaar aan het BRP koppelpunt indien er nog geen Nederlandse identiteit is toegekend aan de elektronische identiteit;
- bevraagt indien nodig het BSNk voor het verkrijgen van de Polymorfe Pseudoniemen;
- registreert de pseudoniemen voor efficiëntie van navolgende inlogs;
- bevraagt het BSNk voor het verkrijgen van het dienstverlener specifieke pseudo ID (EP), waarbij de optie behouden blijft om in de toekomst de pseudo ID’s door de berichtenservice zelf te laten afleiden;
- honoreert de verwerkingsregels die vanuit het stelsel eTD zijn afgesproken in relatie tot het verwerken van antwoord en resultaatberichten voor zover de verordening dit toelaat.

Aan de eIDAS berichtenservice worden bij authenticatie van een persoon met een Nederlands authenticatiemiddel de volgende eisen gesteld. De eIDAS berichtenservice:

- gedraagt zich naar het stelsel eTD als dienstverlener;
- matcht het buitenlandse authenticatieverzoek naar de generieke diensten uit de eTD stelselcatalogus;
- vormt de persistente identificatie van natuurlijke personen en rechtspersonen die het van het stelsel eTD ontvangt om tot landspecifieke eIDAS uniqueness ID’s, zodat landen de identifiers niet onderling kunnen relateren;
- vormt eTD attributen om naar eIDAS attributen en zorgt voor de daarvoor benodigde decryptie en encryptie.

Tenslotte worden aan de eIDAS berichtenservice de volgende algemene eisen gesteld:

- de eIDAS berichtenservice biedt het BRP koppelpunt de mogelijkheid om koppelingen tussen de uniqueness identifier en het BSN te verwijderen als blijkt dat de koppeling onjuist is.

EZ neemt in het stelsel eTD die diensten op, die minimaal noodzakelijk zijn om use case IIIA en IIIB te ondersteunen. Het eIDAS koppelpunt stelt andere dienstverleners in staat om additionele diensten te erkennen voor grensoverschrijdende authenticatie. Daarvoor zijn aanvullende afspraken nodig over herkenning van die diensten middels andersoortige attributen in het authenticatieverzoek. De dienstverlener is hiervoor verantwoordelijk.

Use case	*Van*	*Naar*	*Type bericht*	*Protocoltranslatie*
II	eTD makelaar	eIDAS connector	NL authenticatieverzoek	eTD -> eIDAS
	eIDAS connector	eTD makelaar	EU authenticatieverklaring	eIDAS -> eTD
III	eIDAS proxy service	eTD makelaar	EU authenticatieverzoek	eIDAS -> eTD
	eTD makelaar	eIDAS proxy service	NL authenticatieverklaring	eTD -> eIDAS

3.2 Het BRP koppelpunt

Het BRP koppelpunt zorgt voor het vaststellen of een persoon die met een buitenlands middel inlogt al in de BRP bekend is. Het BRP koppelpunt is een departementsverantwoordelijkheid van het ministerie van BZK.

3.2.1 Beschrijving

Het BRP koppelpunt wordt ingeschakeld door de eIDAS berichtenservice op het moment dat een natuurlijk persoon met een buitenlands authenticatiemiddel voor de eerste keer een dienst van een Nederlandse dienstverlener af wil nemen waarvoor het BSN vereist is. Het BRP koppelpunt wordt alleen ingeschakeld indien een burger een dienst in het BSN-domein af wil nemen. Een dienst behoort tot het BSN domein als de dienstverlener voor de dienstverlening ter identificatie van de individu gebruik mag of moet maken van het BSN. Het BRP koppelpunt heeft geen rol in dienstverlening aan buitenlandse bedrijven en dienstverlening door buitenlandse dienstverleners aan personen met een Nederlands middel.
Het BRP koppelpunt geeft invulling aan de BZK verantwoordelijkheid voor registratie van natuurlijke personen. Het BRP koppelpunt registreert de koppeling tussen de uniqueness id en het BSN.

3.2.2 Architectuurbeslissingen

Op het BRP koppelpunt zijn de volgende architectuurbeslissingen van toepassing. Het BRP koppelpunt:

- vormt de van de eIDAS berichtenservice ontvangen attributen (in eTD formaat) om naar BRP attributen;
- zoekt uit of een persoon die inlogt al in de BRP geregistreerd is;
- informeert de eIDAS berichtenservice over het resultaat van dit proces: (1) de koppeling is succesvol, (2) er zijn aanvullende attributen nodig, (3) er wordt een handmatige procedure gestart wordt – eventueel met het laten legitimeren van de persoon of (4) het is niet mogelijk om een koppeling te leggen;
- verstrekt een BSN van een natuurlijke persoon die in de BRP is opgenomen. Dit gebeurt met de nu al gebruikelijke zorgvuldigheid. NB: het BRP koppelpunt staat het niet toe dat aan een persoon een BSN toegekend wordt die niet in de BRP geregistreerd is;

- koppelt de van het eIDAS koppelpunt ontvangen uniqueness ID aan het BSN;
- meldt de eIDAS berichtenservice welke koppelingen onjuist blijken te zijn;

De consequentie van deze architectuurbeslissingen is dat een BSN-dienst nog niet verleend kan worden als de registratie in de BRP nog niet plaats heeft gevonden of volledig is. Het is aan de dienstverlener om in deze situatie te besluiten om het dienstverleningsproces te blokkeren of al wel te starten zonder BSN (de dienstverlener vraagt dan in de stelselcatalogus zowel het BSN als pseudoniem). Beide alternatieven zijn niet strijdig met de eIDAS verplichtingen.

Het BRP koppelpunt gebruikt de attributen die het van het eIDAS koppelpunt ontvangt om te bepalen of de persoon al in de BRP staat dan wel om de persoon in de BRP te registreren. Mogelijk heeft het BRP koppelpunt aan de verplichte attributen uit de minimale dataset al voldoende. Indien dat niet het geval is dan:

- kan het BRP koppelpunt aanvullende attributen vragen aan het eIDAS koppelpunt;
- kan het een handmatige procedure starten om de matching te voltooien, eventueel met legitimatie van de persoon;
- Kan het BRP koppelpunt besluiten dat geen koppeling aan het BSN mogelijk is.

3.2.3 Eisen

Aan het BRP koppelpunt worden de volgende eisen gesteld. Het BRP koppelpunt:

- moet zelf de van de berichtenservice ontvangen attributen in eTD formaat omvormen tot attributen conform het GBA datamodel;
- moet vaststellen of bij een persoon een BSN bekend is;
- moet vaststellen of bij een persoon een koppeling gemaakt kan worden bij een reeds aanwezige BRP-record;
- moet foutieve koppelingen van uniqueness identifier en BSN direct melden aan de eIDAS berichtenservice.

3.3 Stelsel Elektronische Toegangsdiensten

Het stelsel eTD is een publieke-private samenwerking, onder departementale verantwoordelijkheid van het ministerie van EZ.

3.3.1 Beschrijving

Stelsel eTD richt zich op authenticatie, vertegenwoordiging en gerelateerde dienstverlening in het publieke en private domein. Voor authenticatie in het publieke domein zal eTD volgend zijn in de kaders van de wettelijk eisen onder de wet GDI, zoals opgesteld zal worden door het ministerie van BZK. Het eTD stelsel kent de volgende rollen:

- Makelaar: de functionaliteit die de dienstverlener ontzorgt ten aanzien van identificatie, authenticatie en machtigingen.
- Authenticatiedienst: de functionaliteit die zorgt voor identificatie & authenticatie van personen.

- Machtigingsregister: de functionaliteit die zorgt voor registratie en ontsluiting van informatie over de bevoegdheden van personen.

3.3.2 Architectuurbeslissingen

Op het stelsel eTD zijn de volgende architectuurbeslissingen van toepassing:

- de eIDAS verordening wordt zo transparant mogelijk gehouden voor de op het stelsel aangesloten dienstverleners;
- het stelsel voert wijzigingen in het afsprakenstelsel door, zodat personen met een buitenlands middel via het stelsel bij Nederlandse dienstverleners kunnen inloggen;
- het stelsel voert wijzigingen in het afsprakenstelsel door, zodat het in staat is om zowel de minimale dataset als eventuele andersoortige attributen te ontvangen en aan te leveren;
- het stelsel voert de wijzigingen in het afsprakenstelsel door die randvoorwaardelijk zijn voor de notificatie van het afsprakenstelsel bij de Europese Commissie;
- buitenlandse authenticaties worden, analoog aan het authenticatieverzoek van een dienstverlener richting het stelsel, middels één uitvraag gerealiseerd (in plaats van een aparte bevraging op de authenticatiedienst en op het machtigingregister zoals in het huidige afsprakenstelsel).

3.3.3 Eisen

Deze startarchitectuur stelt de volgende eisen aan eTD voor authenticatie van een persoon met een buitenlands authenticatiemiddel (use case IIA en IIB):

- Het stelsel erkent de eIDAS attributen en identiteiten binnen het stelsel, zodat deze beschikbaar gesteld kunnen worden aan de dienstverleners, eventueel naast de huidige set attributen.
- Het stelsel biedt ondersteuning voor eventuele andersoortige attributen die de lidstaten definiëren en via de eIDAS koppelpunten uitwisselen.
- Een dienstverlener moet in het authenticatieverzoek aan zijn makelaar kunnen aangeven welke lidstaat de authenticatie dient te verzorgen.
- Indien door de dienstverlener gewenst, mag de makelaar de gebruikersinteractie verzorgen voor het door de gebruiker laten kiezen van het land waarin authenticatie plaats moet vinden. De dienstverlener mag de gebruiker ook op zijn eigen website de keuze al bieden of het aan het eIDAS koppelpunt over laten.
- Voor (rechts)personen kan een dienstverlener aangeven of hij zijn dienst kan en wil openstellen op basis van de vanuit eIDAS mogelijke gegevensset.
- De dienstverlener moet voor elke dienst in de stelselcatalogus aan kunnen geven of daarvoor het BSN (1) vereist, (2) gewenst of (3) niet nodig is.
- In geval van vertegenwoordiging moet de makelaar een gecombineerd antwoord (identiteitsverklaring + bevoegdheidsverklaring) van de Berichtenservice kunnen verwerken.

Deze startarchitectuur stelt de volgende eisen aan eTD voor authenticatie van een persoon met een Nederlands authenticatiemiddel (use case IIIA en IIIB ten behoeve van de Nederlandse notificatie):

- Conformeren aan het eIDAS normenkader. Hierbij dienen in het stelsel (technische) maatregelen genomen te worden welke het mogelijk maken dat vooruitlopend op eind 2017 de individuele deelnemers reeds eerder in hun eigen tempo kunnen toetreden tot het eIDAS-compatibel normenkader, en hiermee notificatie.

- Attributen van de natuurlijke persoon worden aangeleverd vanuit stelsel en niet verrijkt door BZK.
- Het binnen het stelsel erkennen van de volledige eIDAS verplichte minimale dataset (attributen) bij natuurlijke personen.
- Het binnen het stelsel erkennen van de volledige eIDAS verplichte minimale dataset (attributen) bij niet-natuurlijke personen.
- Het binnen het stelsel erkennen van eventueel nog te definiëren andersoortige attributen die lidstaten via de eIDAS koppelpunten uitwisselen.
- Het mogelijk maken van het gelijktijdig opleveren (in het geval van vertegenwoordiging / zakelijke domein) van de eIDAS verplichte minimale dataset van natuurlijke en niet-natuurlijke personen.
- Het leveren van een unieke Identificatiecode voor natuurlijke personen die persistent is over het handelen heen. Ongeacht of de belanghebbende van dit handelen de natuurlijk persoon zelf, of een rechtspersoon is (vertegenwoordiging) en of dit met één of verschillende authenticatiediensten plaatsvindt.
- Het leveren van een persistente identificatiecode voor rechtspersonen. Het eIDAS koppelpunt gebruikt deze identifier voor communicatie over de rechtspersoon naar andere lidstaten.
- Het werken met Polymorfe Pseudoniemen.
- Het stelsel moet inzichtelijk maken of een dienst zich in het publieke domein bevindt (dit is een eIDAS verplichting).

3.4 Het BSN koppelregister

Het BSNk zorgt voor de koppeling van een authenticatiemiddel aan het BSN en het genereren van de pseudoniemen die in het stelsel nodig zijn. Het BSNk is de departementsverantwoordelijkheid van BZK.

3.4.1 Beschrijving

Het stelsel eTD biedt toegangsdiensten voor burgers en bedrijven tot zowel publieke diensten als private diensten. Private dienstverleners zijn doorgaans niet gerechtigd om het BSN het gebruiken. Om te voorkomen dat er aparte authenticatiemiddelen nodig zijn in het publieke en in het private domein is het BSNk ontwikkeld. Het BSNk koppelt de middelen aan het BSN en geeft het BSN – indien de dienstverlener daar recht toe heeft – vrij. Om de privacy te borgen, maakt het BSNk gebruik van pseudonimisering. Uitgangspunt van deze architectuur is dat BSNk en eTD (tijdig) Polymorfe Pseudonimisering implementeren. Het BSNk moet zorgen voor het genereren en uitgeven van de benodigde Polymorfe Pseudoniemen.

3.4.2 Architectuurbeslissingen

Op het BSNk zijn verschillende architectuurbeslissingen van toepassing. Het BSNk:

- is verantwoordelijk voor de uitgifte van Polymorfe Pseudoniemen (PP);
- genereert Polymorfe Pseudoniemen op basis van het BSN (PP-BSN), een van het BSN afgeleide identificatie (PP-PS) en de uniqueness ID (PP-EU);
- faciliteert de laagdrempelige adoptie van Polymorfe Pseudonimisering door het omzetten van een Polymorf Pseudoniem in een dienstverlenerspecifiek pseudoniem (Encrypted Pseudoniem, EP);

3.4.3 Eisen

Aan het BSNk worden de volgende eisen gesteld. Het BSNk moet:

- Polymorfe Pseudoniemen verstrekken;
- Polymorfe Pseudoniemen omzetten naar dienstverlenerspecifieke pseudoniemen;
- voorzien in de uitgifte van het sleutelmateriaal voor het ontcijferen van dienstverlenerspecifieke pseudoniemen door dienstverleners.

4 Proces

Dit hoofdstuk beschrijft de vier use cases die met de oplossing moeten kunnen worden gerealiseerd:

1. Use case IIA: persoon met EU middel logt in bij dienstverlener in Nederland; dienstafnemer is een natuurlijke persoon
2. Use case IIB: persoon met EU middel logt in bij dienstverlener in Nederland; dienstafnemer is een niet-natuurlijke persoon
3. Use case IIIA: persoon met NL middel logt in bij dienstverlener in andere lidstaat; dienstafnemer is een natuurlijke persoon
4. Use case IIIB: persoon met NL middel logt in bij dienstverlener in andere lidstaat; dienstafnemer is een niet-natuurlijke persoon

Onderstaande tabel laat per use case zien welke hoofdcomponenten het inschakelt.

	UC II-A	UC II-B	UC III-A	UC III-B
NL dienstverlener	x	x		
stelsel eTD	x	x	x	x
BSNk[3]	x	x	x	x
BRP koppelpunt	x[4]			
Nederlands eIDAS koppelpunt	x	x	x	x
Buitenlands eIDAS koppelpunt	x	x	x	x

4.1 Use case IIa –natuurlijk persoon met EU middel

Use case IIa beschrijft het inloggen van een natuurlijke persoon met een EU middel bij een Nederlandse dienstverlener. De use case maakt onderscheid in inloggen voor een dienst waarvoor het BSN vereist is (BSN-dienst) en een dienst waarvoor geen BSN nodig is.

[3] Waarbij buiten beschouwing is gelaten dat het in de toekomst wellicht mogelijk wordt dat authenticatiediensten (incl. berichtenservice) dor inzet van een HSM zelfstandig dienstverlenerspecifieke pseudoniemen gaan genereren.

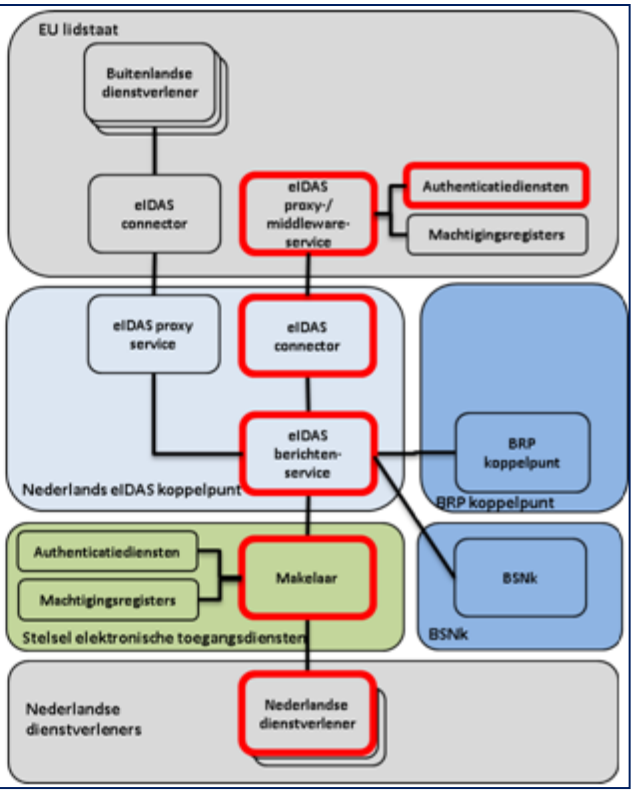
[4] Alleen indien authenticatie vereist is voor een BSN-dienst; in alle andere gevallen speelt de BRP-Koppelpunt geen rol.

Use case IIA

persoon met EU middel logt in bij dienstverlener in Nederland
dienstafnemer is een natuurlijke persoon

STAP 1: verzoek authenticatie

- Een persoon met een EU middel wil inloggen bij een NL dienstverlener. De NL dienstverlener stuurt een authenticatieverzoek naar de eTD makelaar.
- De eTD makelaar stuurt een authenticatieverzoek naar de eIDAS berichtenservice.
- De eIDAS berichtenservice bevraagt de eTD stelselcatalogus voor het vereiste betrouwbaarheidsniveau, benodigde attributen en de indicatie BSN dienst.
- De eIDAS berichtenservice vormt het eTD bericht om tot het eIDAS bericht, ondertekent het en stuurt het bericht door naar de NL eIDAS connector.
- De eIDAS connector stuurt het bericht door naar de buitenlandse eIDAS proxy- of middlewareservice.
- De buitenlandse proxy- of middleware service schakelt de buitenlandse authenticatiedienst in.
- **Voer stap 2 ontvang authenticatieresultaat uit**

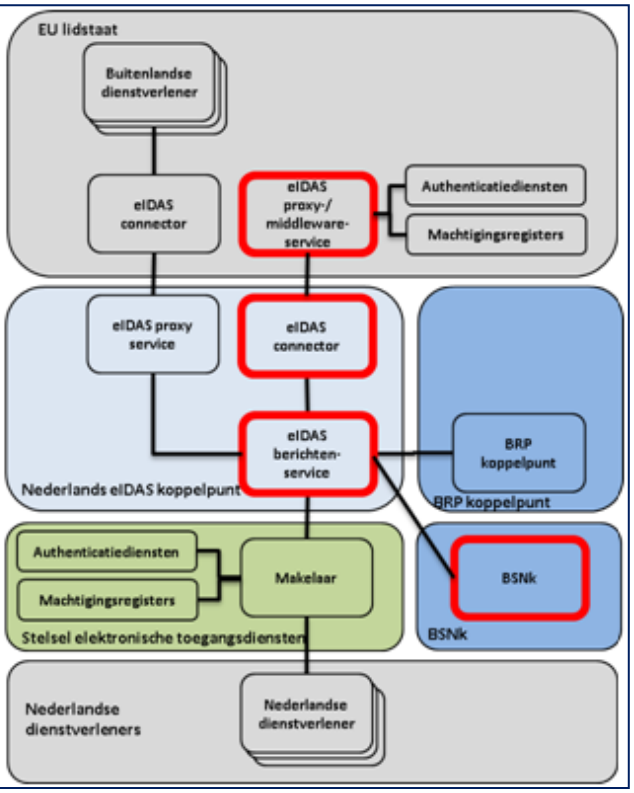


Use case IIA

persoon met EU middel logt in bij dienstverlener in Nederland
dienstafnemer is een natuurlijke persoon

STAP 2: ontvang authenticatieresultaat

- Na positieve authenticatie routeert de buitenlandse eIDAS proxy- of middlewareservice het authenticatieresultaat naar de NL eIDAS connector.
- De NL eIDAS connector stuurt het bericht door naar de eIDAS berichtenservice.
- De eIDAS berichtenservice controleert het bericht op integriteit en veiligheid.
- Als de dienst een BSN dienst is:
  - De eIDAS berichtenservice controleert of het pseudoniem (PP-BSN) behorende tot de uniquenss id van deze persoon al in de eIDAS koppeltabel voorkomt.
  - Zo ja, dan
    - de eIDAS Berichtenservice informeert de eIDAS identiteitmanager over de actuele set meegeleverde attributen.
    - De eIDAS berichtenservice Initieert **stap 4 Informeer dienstverlener**.
  - Zo nee, dan
    - initieert de eIDAS berichtenservice **stap 3 Valideer persoonsgegevens**
- Als de dienst geen BSN-dienst is:
  - De eIDAS berichtenservice controleert of het pseudoniem (PP-EU) behorende tot de uniquenss id van deze persoon al in de eIDAS koppeltabel voorkomt.
  - Zo ja, dan
    - initieert de berichtenservice **stap 4 Informeer dienstverlener**
  - Zo nee, dan
    - Vraagt de eIDAS berichtenservice het pseudoniem (PP-EU) op bij het BSNk (aan de hand van de uniquenss id)
    - Berekent het BSNk het pseudoniem
    - Levert het BSNk het pseudoniem aan de eIDAS berichtenservice
    - Registreert de eIDAS berichtenservice het pseudoniem bij de uniqueness id van de persoon in de koppeltabel
    - Initieert de eIDAS Berichtenservice **stap 4 informeer dienstverlener**.

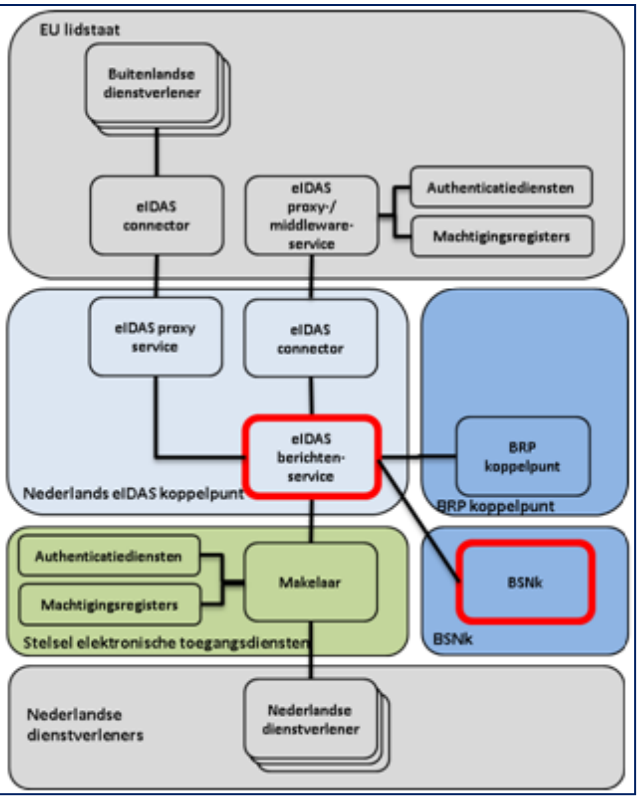


Use case IIA

persoon met EU middel logt in bij dienstverlener in Nederland dienstafnemer is een natuurlijke persoon

STAP 3: Valideer persoonsgegevens (alleen voor BSN diensten)

- De eIDAS berichtensevice stuurt de attributen van de persoon naar de eIDAS identiteitmanager
- De eIDAS Identiteitmanager bouwt een matchings/registreer verzoek op en verstuurt deze naar de BRP verificatiedienst.
- De BRP Verficatiedienst probeert op basis van de verkregen attributen te bepalen of de identiteit gematch't kan worden of moet leiden tot een nieuw voorkomen in het BRP.
- Lukt dit niet dan:
  - herhaalt stap 1 zich met een authenticatie verzoek voor de volledige dataset of
  - Informeert de eIDAS identiteitmanager de eIDAS berichtenservice dat het proces in bewerking is en gaat terug naar **stap 2 in de variant "Als de dienst geen BSN-dienst is"**.
- Lukt dit wel dan:
  - Verstrekt de BRP verificatiedienst het BSN aan de eIDAS identiteitmanager
  - Berekent de eIDAS identiteitmanager het versleuteld BSN
  - informeert de eIDAS identiteitmanager de eIDAS berichtenservice over succesvolle matching/registratie in BRP en verstrekt het versleuteld BSN.
  - Vraagt de eIDAS Berichtenservice bij het BSNk het pseudoniem (PP-BSN) behorende tot het versleuteld BSN.
  - ontsleutelt het BSNk het versleutelde BSN.
  - Genereert het BSNk obv het BSN het pseudoniem (PP-BSN) en verstrekt het aan de eIDAS berichtenservice
  - Registreert de eIDAS berichtenservice het pseudoniem (PP-BSN) bij de uniqueness id van de persoon in de koppeltabel.
  - Initieert de eIDAS berichtenservice **stap 4 informeer dienstverlener**

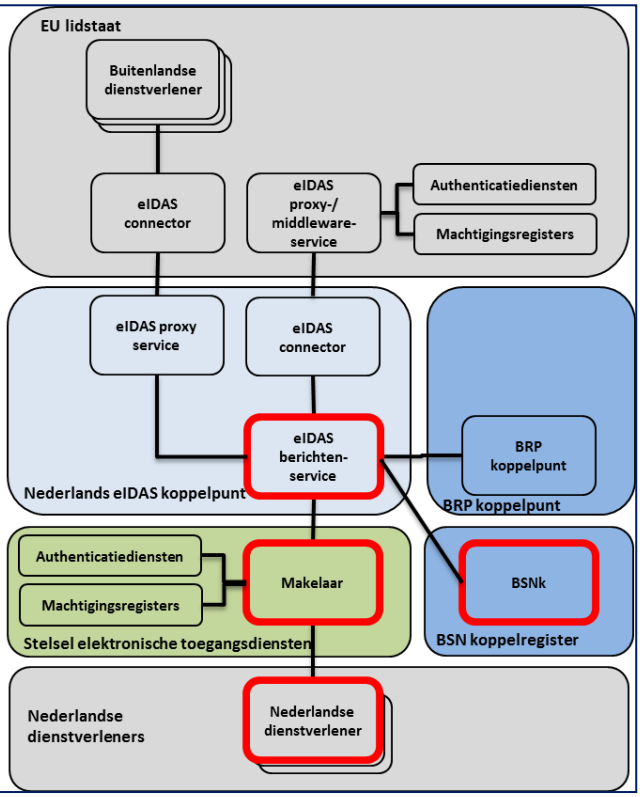


Use case IIA

persoon met EU middel logt in bij dienstverlener in Nederland dienstafnemer is een natuurlijke persoon

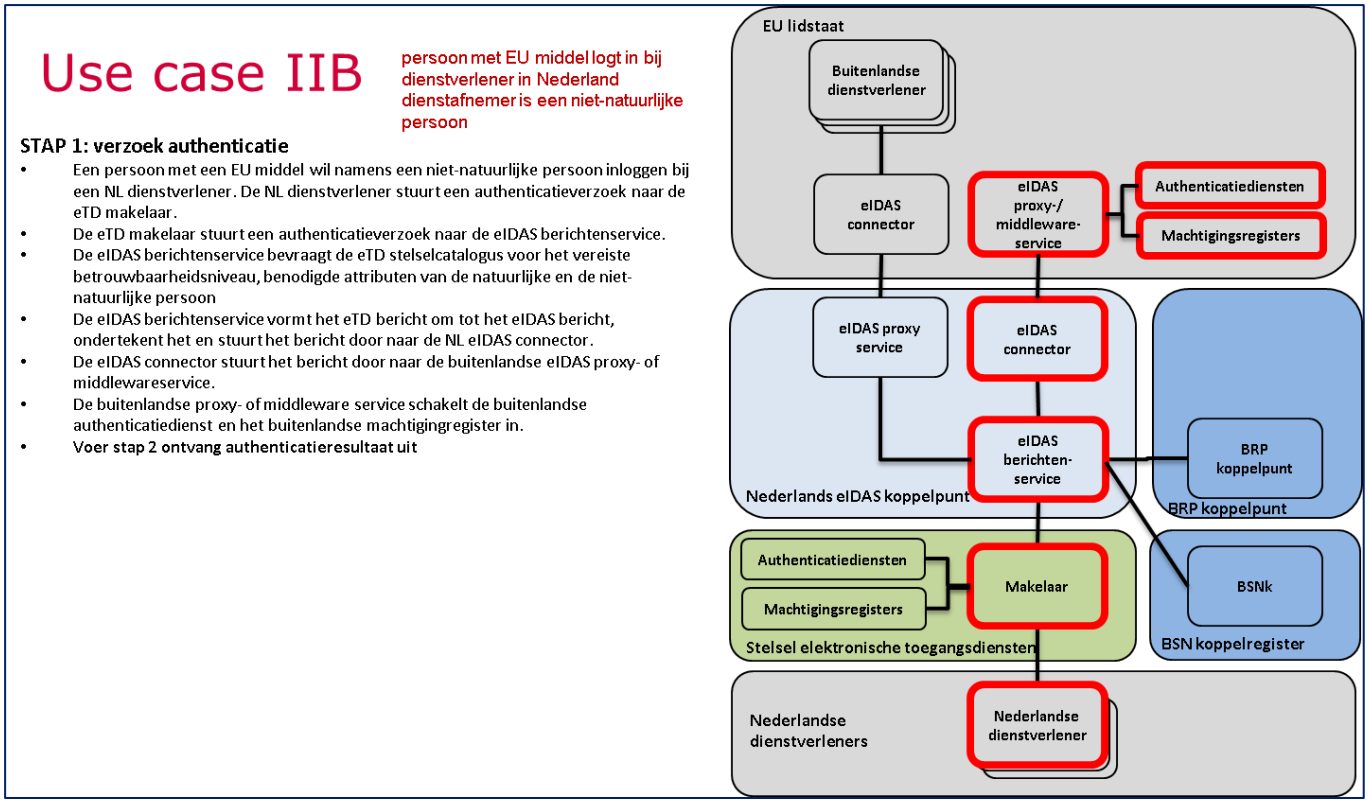
STAP 4: informeer dienstverlener

- De eIDAS berichtenservice roept het BSNk aan met het pseudoniem (PP-EU of PP-BSN).
- Het BSNk transformeert het pseudoniem in een versleuteld dienstverlenerspecifiek pseudoniem en stuurt deze terug.
- De eIDAS berichtenservice voert attribuut translatie uit (van eIDAS naar eTD)
- De eIDAS berichtenservice stelt de eTD verklaringen op, ondertekent ze en stuurt de eTD verklaring naar de eTD makelaar
- De eTD makelaar verifieert het bericht en toetst of de authenticatie voldoende betrouwbaar was (LOA)
- De eTD makelaar stuurt het bericht naar de dienstverlener
- Dienstaanbieder ontsleutelt het versleuteld dienstverlenerspecifiek pseudoniem naar een dienstverlenerspecifiek pseudoniem (niet-BSN dienst) of een BSN (BSN-dienst).



4.2 Use case IIb – rechtspersoon met EU middel

In use case IIB levert de lidstaat naast attributen van de natuurlijke persoon ook attributen van een niet-natuurlijke persoon. De natuurlijke persoon wordt conform IIA afgehandeld in de variant 'niet-BSN dienst'. Er vindt dus geen match op / registratie in BRP plaats. De attributen van de niet-natuurlijke persoon worden zo ongewijzigd mogelijk aan de dienstverlener doorgegeven.

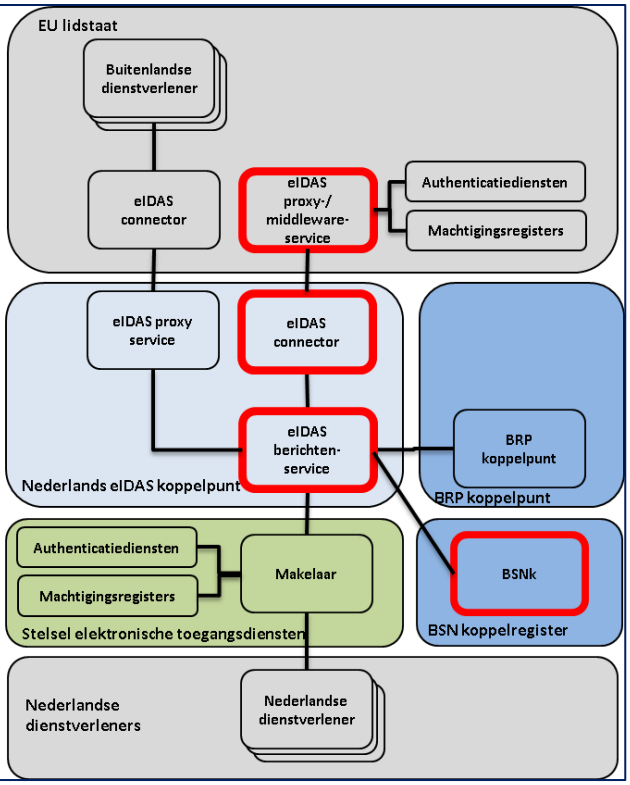


Use case IIB

persoon met EU middel logt in bij dienstverlener in Nederland dienstafnemer is een niet-natuurlijke persoon

STAP 2: ontvang authenticatieresultaat

- Na positieve authenticatie en controle van bevoegdheid routeert de buitenlandse eIDAS proxy- of middlewareservice het authenticatieresultaat naar de NL eIDAS connector.
- De NL eIDAS connector stuurt het bericht door naar de eIDAS berichtenservice.
- De eIDAS berichtenservice controleert het bericht op integriteit en veiligheid.
- De eIDAS berichtenservice controleert of het pseudoniem van de natuurlijke persoon (PP-EU) behorende tot de uniquenss id van deze persoon al in de eIDAS koppeltabel voorkomt.
- Zo ja, dan
  - initieert de berichtenservice **stap 3 Informeer dienstverlener**
- Zo nee, dan
  - Vraagt de eIDAS berichtenservice het pseudoniem (PP-EU) op bij het BSNk (aan de hand van de uniquenss id)
  - Berekent het BSNk het pseudoniem
  - Levert het BSNk het pseudoniem aan de eIDAS berichtenservice
  - Registreert de eIDAS berichtenservice het pseudoniem bij de uniqueness id van de persoon in de koppeltabel
  - Initieert de eIDAS Berichtenservice **stap 3 informeer dienstverlener**.

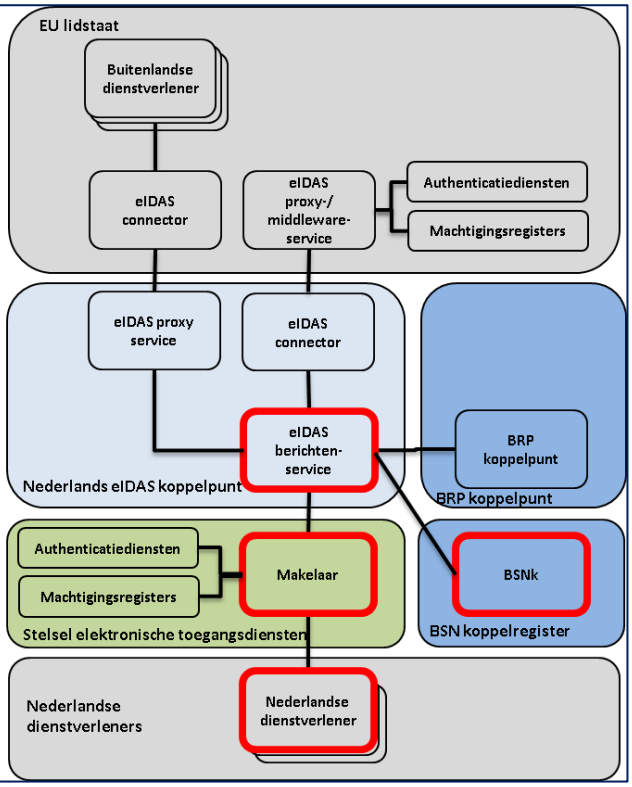


Use case IIB

persoon met EU middel logt in bij dienstverlener in Nederland dienstafnemer is een niet-natuurlijke persoon

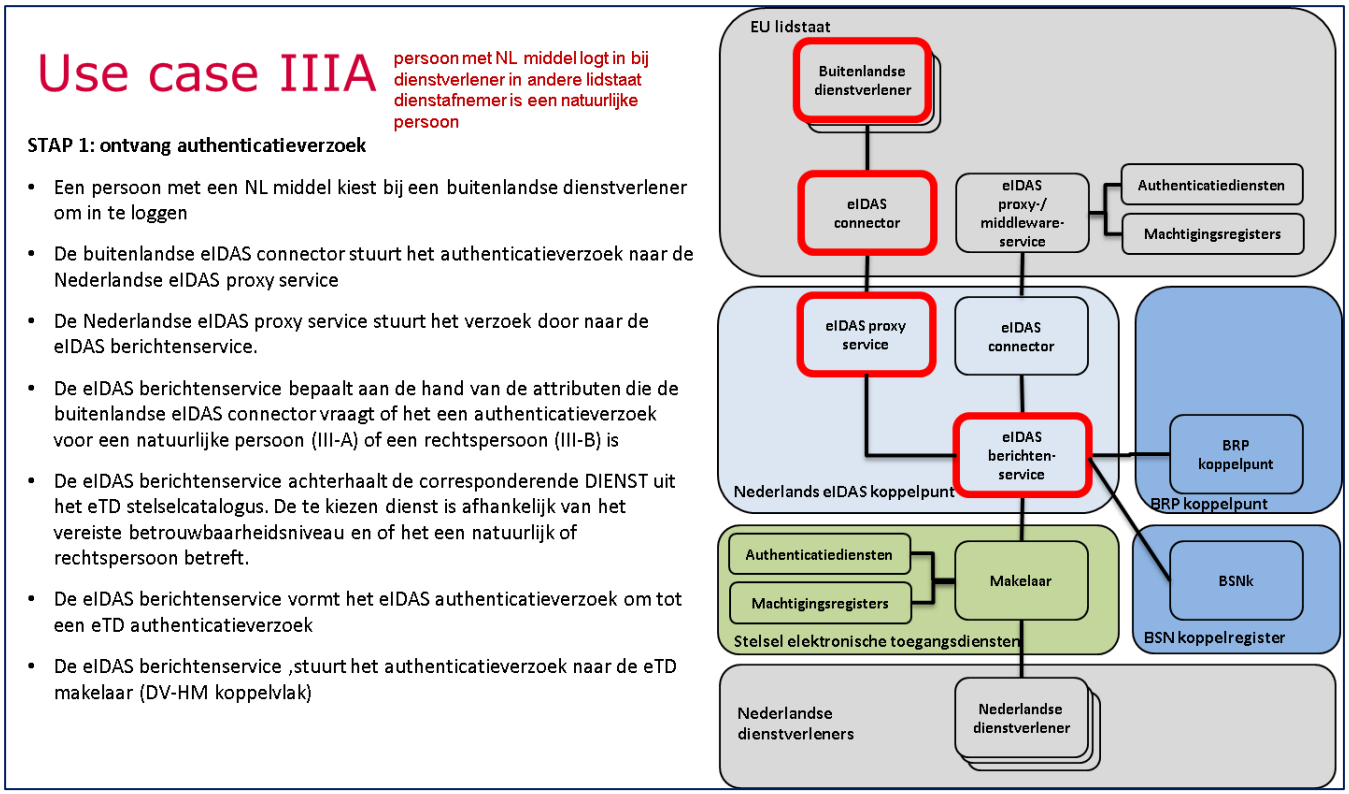
STAP 3: informeer dienstverlener

- De eIDAS berichtenservice roept het BSNk aan met het pseudoniem (PP-EU).
- Het BSNk transformeert het pseudoniem in een versleuteld dienstverlenerspecifiek pseudoniem en stuurt deze terug.
- De eIDAS berichtenservice voert attribuut translatie uit voor zowel de natuurlijke als de niet-natuurlijke persoon (van eIDAS naar eTD)
- De eIDAS berichtenservice stelt de eTD verklaringen op, ondertekent ze en stuurt de eTD verklaring naar de eTD makelaar (identiteitsverklaring én bevoegdheidsverklaring). De eIDAS berichtenservice mag er hierbij vanuit gaan dat de natuurlijke persoon bevoegd is om de dienst namens de niet-natuurlijke persoon af te nemen.
- De eTD makelaar verifieert het bericht en toetst of de authenticatie voldoende betrouwbaar was (LOA)
- De eTD makelaar stuurt het bericht naar de dienstverlener
- Dienstaanbieder ontsleutelt het versleuteld dienstverlenerspecifiek pseudoniem van de natuurlijke persoon naar een dienstverlenerspecifiek pseudoniem.



4.3 Use case IIIa - natuurlijk persoon met NL middel

In use case IIIa logt een natuurlijke persoon met een Nederlands middel in voor dienstverlening bij een buitenlandse dienstverlener. Voor deze use case is notificatie van eTD bij de Europese commissie nodig. NL levert een persistente identificatie per lidstaat, onafhankelijk van de authenticatiedienst die de persoon inschakelt. De use case maakt geen onderscheid in dienstverlening aan een persoon in de hoedanigheid als burger en in de hoedanigheid als consument. Dat onderscheid kent eIDAS immers niet.

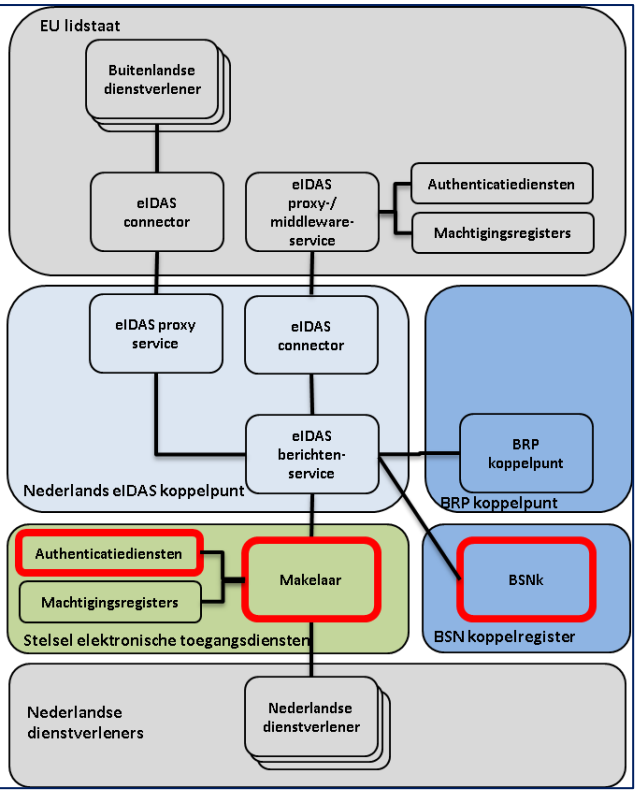


Use case IIIA

persoon met NL middel logt in bij dienstverlener in andere lidstaat dienstafnemer is een natuurlijke persoon

STAP 2: authentiseren en ophalen attributen

- De eTD makelaar laat de natuurlijke persoon via de door hem gekozen authenticatiedienst (AD) authenticeren.
- De AD toetst of de authenticatie voldoende betrouwbaar was.
- De AD vraagt het BSNk om het versleutelde dienstverlenerspecifieke pseudoniem (waarbij geldt dat de eIDAS berichtenservice als dienstverlener optreedt en de dienst altijd een niet-BSN dienst is).
- Het BSNk berekent deze.
- De eTD makelaar stuurt de eTD verklaringen naar de eIDAS berichtenservice.

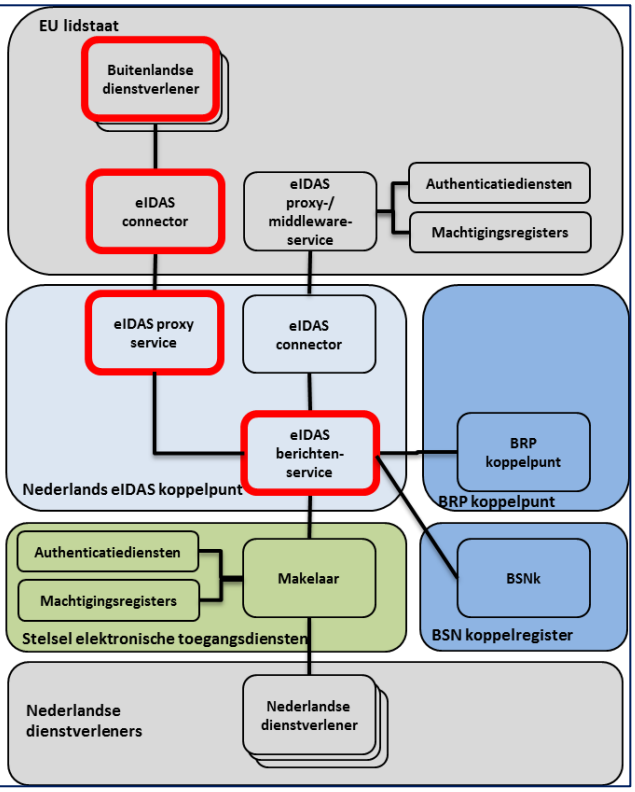


Use case IIIA

persoon met NL middel logt in bij dienstverlener in andere lidstaat dienstafnemer is een natuurlijke persoon

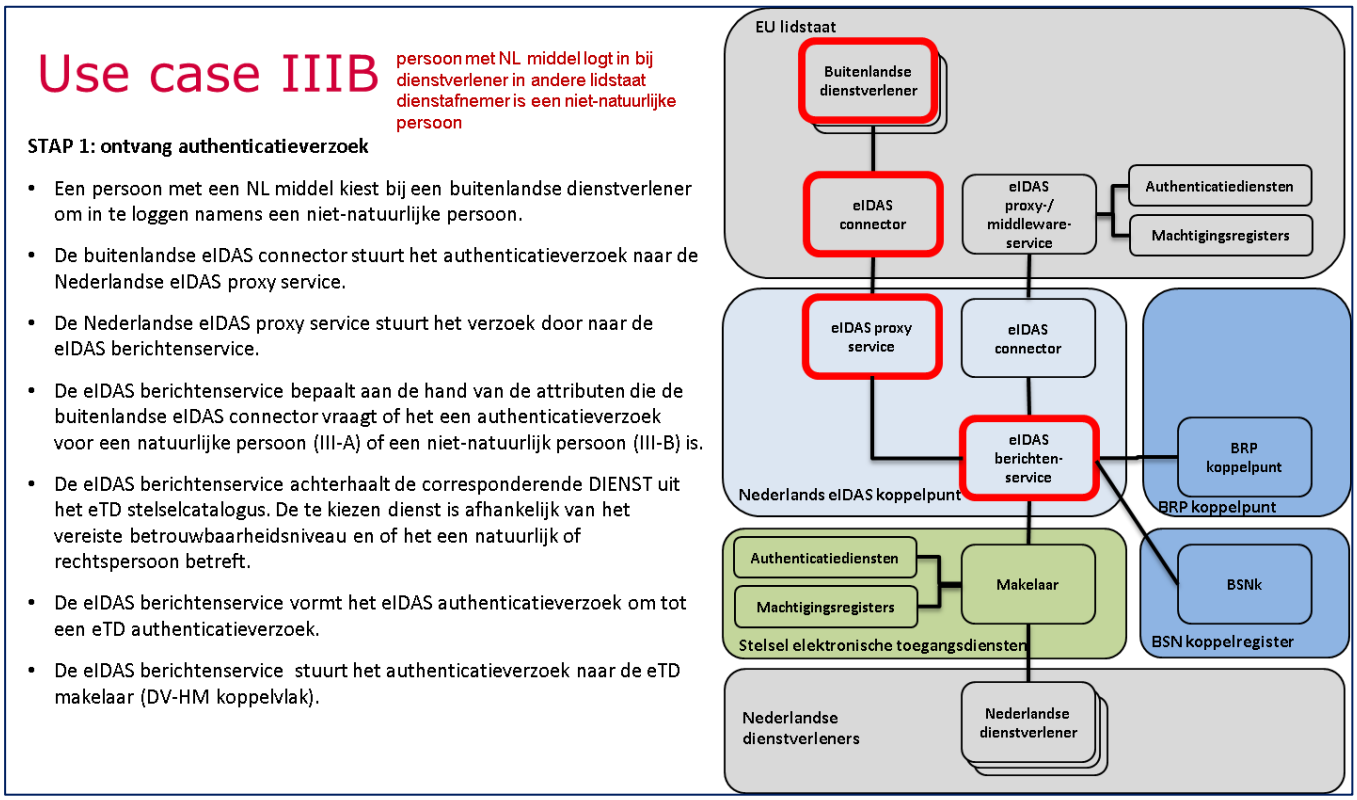
STAP 3: retourneren authenticatie

- De eIDAS berichtenservice verifieert de integriteit en veiligheid van het eTD bericht
- De eIDAS berichtenservice ontsleutelt het ontvangen versleuteld dienstverlenerspecifieke pseudoniem van de natuurlijke persoon
- De eIDAS berichtenservice berekent op basis van dit (persistente) pseudoniem de lidstaatspecifieke (persistente) uniqueness ID van de natuurlijke persoon.
- De eIDAS berichtenservice voert attribuut translatie uit (van eTD naar eIDAS).
- De eIDAS berichtenservice stelt het eIDAS berichten samen.
- De eIDAS berichtenservice ondertekent de eIDAS berichten.
- De eIDAS berichtenservice stuurt de berichten door naar de eIDAS proxy service.
- De eIDAS proxy service stuurt het bericht naar de buitenlandse eIDAS connector.
- De buitenlandse eIDAS connector informeert de buitenlandse dienstverlener



4.4 Use case IIIb - rechtspersoon met NL middel

Use case IIIb is een aanvulling op use case IIIa met attributen van de rechtspersoon. In deze use case is dus sprake van vertegenwoordiging, waarbij door eTD vastgesteld moet worden dat de natuurlijke person bevoegd is om de rechtspersoon te vertegenwoordigen. Daarvoor schakelt eTD de machtigingregisters in.

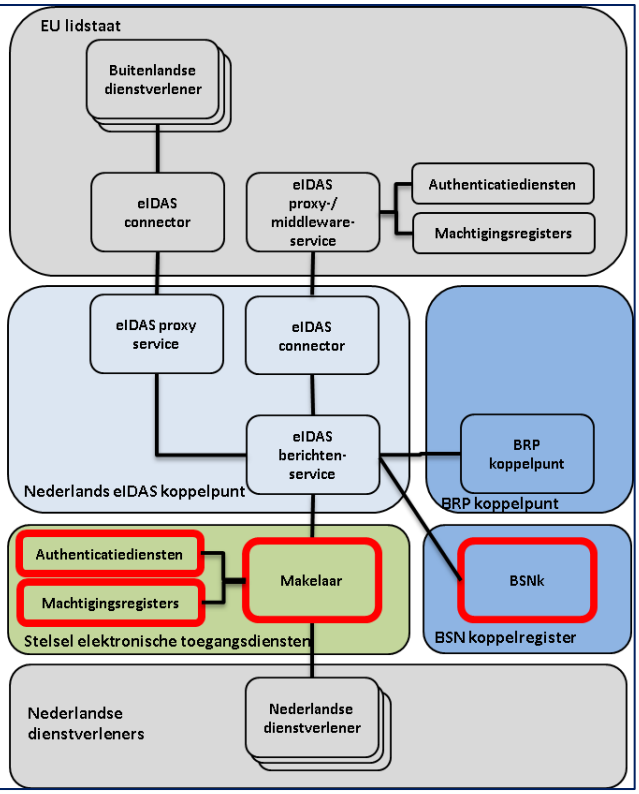


Use case IIIB

persoon met NL middel logt in bij dienstverlener in andere lidstaat dienstafnemer is een niet-natuurlijke persoon

STAP 2: authentiseren en ophalen attributen

- De eTD makelaar laat de natuurlijke persoon via de door hem gekozen authenticatiedienst (AD) authenticeren.
- De AD toetst of de authenticatie voldoende betrouwbaar was.
- De AD vraagt het BSNk om de versleuteld dienstverlenerspecifiek pseudoniem van de natuurlijke persoon (waarbij geldt dat de eIDAS berichtenservice als dienstverlener optreedt en de dienst altijd een niet-BSN dienst is).
- Het BSNk berekent deze.
- Het machtigingregister toetst of de natuurlijke persoon bevoegd is om de dienst namens de niet-natuurlijke persoon af te nemen.
- Het machtigingregister levert de attributen van de niet-natuurlijke persoon.
- De eTD makelaar stuurt de eTD verklaringen naar de eIDAS berichtenservice.

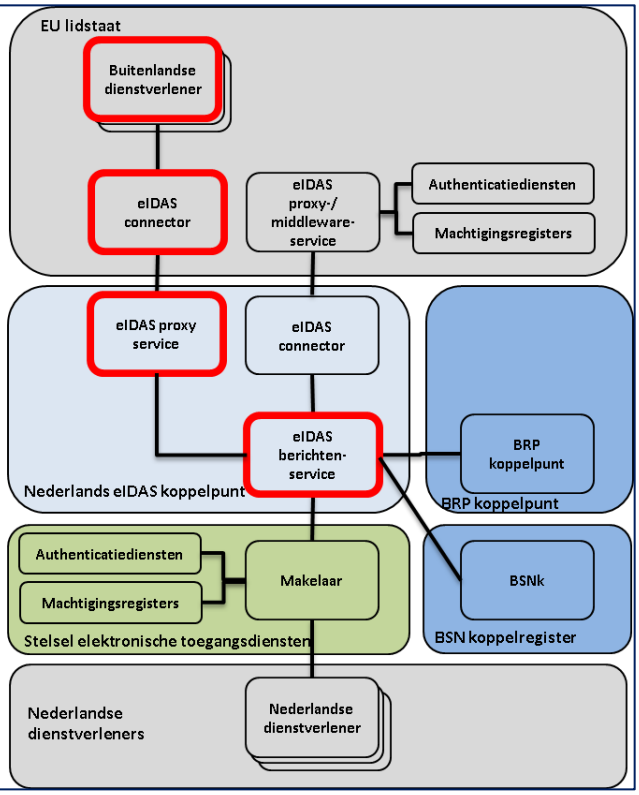


Use case IIIB

persoon met NL middel logt in bij dienstverlener in andere lidstaat dienstafnemer is een niet-natuurlijke persoon

STAP 3: retourneren authenticatie

- De eIDAS berichtenservice verifieert de integriteit en veiligheid van de eTD berichten.
- De eIDAS berichtenservice ontsleutelt het ontvangen versleuteld dienstverlenerspecifieke pseudoniem van de natuurlijke persoon.
- De eIDAS berichtenservice berekent op basis van dit (persistente) pseudoniem de lidstaatspecifieke (persistente) uniqueness ID van de natuurlijke persoon.
- De eIDAS berichtenservice voert attribuut translatie uit (van eTD naar eIDAS) voor zowel de natuurlijke als de niet-natuurlijke persoon
- De eIDAS berichtenservice stelt het eIDAS berichten samen.
- De eIDAS berichtenservice ondertekent de eIDAS berichten.
- De eIDAS berichtenservice stuurt de berichten door naar de eIDAS proxy service.
- De eIDAS proxy service stuurt het bericht naar de buitenlandse eIDAS connector.
- De buitenlandse eIDAS connector informeert de buitenlandse dienstverlener.



5 Techniek

Dit hoofdstuk beschrijft de technische afspraken, verantwoordelijkheden en afhankelijkheden van de verschillende deelprojecten. Het schets op hoofdlijnen de samenhang, het gedrag en de kaders hierbij.

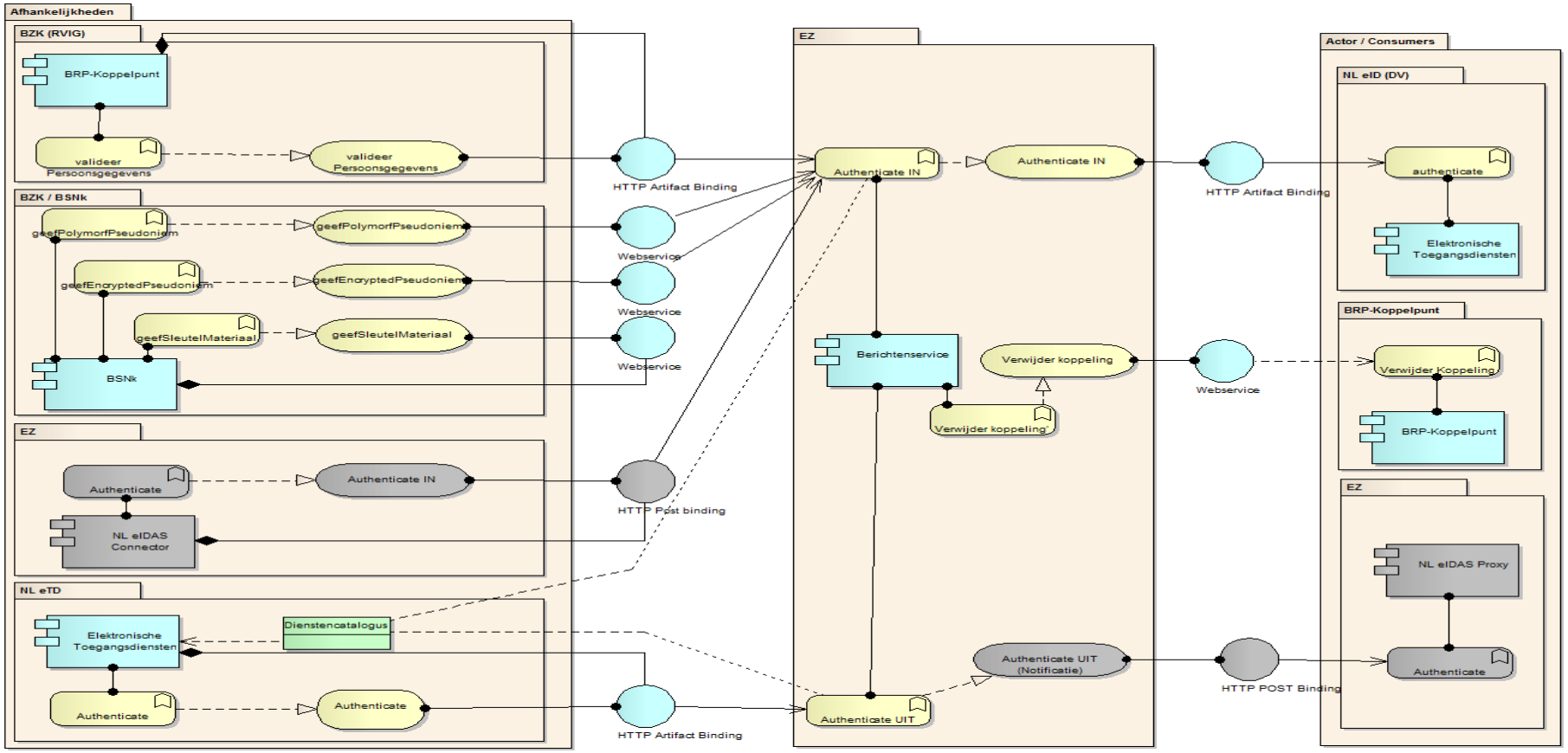
Deze architectuur gaat uit van inzet van eTD voor Europese toegangverlening. Het is niet ondenkbaar dat Europese toegang (ook) via een ander stelsel / een andere oplossing verloopt. De concepten en functies uit het vorige hoofdstuk zijn onverkort op een dergelijke situatie van toepassing (zie bijlage 1), maar de technische uitwerking in dit hoofdstuk is eTD-specifiek en moet aangepast moet worden op het moment dat de Europese toegang via een ander stelsel moet verlopen.

5.1 Gedrag eIDAS Koppelpunt (BerichtenService)

De berichtenservice verzorgt de interoperabiliteit tussen de eIDAS-nodes en het stelsel eTD.

5.1.1 Structuur BerichtenService

Onderstaand beschouwt het verandergebied binnen de scope van deze startarchitectuur vanuit het perspectief van het ministerie van EZ.



Figuur 3 Structuur Berichtenservice

5.1.2 Berichtenservice geleverde Interfaces

Onderstaande tabel geeft inzicht in het externe gedrag zoals geleverd door de Berichtenservice.

Berichtenservice Interfaces

Service Naam	consumer/ actor	objecten	Doel
Authenticate IN (HM-AD/MR)	eTD herkennings makelaar	**Input**: AuthnRequest **Output:** SAMLResponse (conform eTD specs)	Adapter Functionaliteit ten bate van de verordening De berichtenservice gedraagt zich richting het stelsel als een Authenticatiedienst/Machtigingregister en naar de eIDAS-Connector als een Dienstverlener. Door samenspel met de eIDAS-Nodes en de berichtenservice eigen applicatie logica is het resultaat van een authenticatie bij een genotificeerd MS-eID gelijk aan de interne NL-eID authenticatie. Hiermee wordt bereikt dat het voldoen aan de eIDAS verordening grotendeels transparant plaatsvindt voor op het stelsel eTD aangesloten dienstverleners en deelnemers.
Authenticate UIT (Interactie uit scope startarchitectuur)	NL eIDAS proxy service	**Input:** AuthnRequest **Output:** SAMLResponse (conform eTD spec) (NB Uit scope startarchitectur)	Adapter functionaliteit tbv notificatie De berichtenservice gedraagt zich richting het stelsel als een Dienstverlener (consumer) en richting de eIDAS proxy service als een Authenticatiedienst. Door samenspel met het stelsel eTD en de eigen adapter logica voldoet het resultaat van de authenticatie aan de eIDAS vereisten. Hiermee wordt bereikt dat het Nederlandse stelsel eTD genotificeerd kan worden, en zijn middelen bruikbaar zijn binnen de EER terwijl de wijziging grotendeels transparant is voor het stelsel deelnemers en gebruikers.
Verwijder koppeling	BRP-Koppelpunt	**Input:** SignedXML{ UniquenessID	In het geval door het BRP-koppelpunt een verkeerde koppeling is gelegd of als het BSN van een aan de eIDAS-

Service Naam	consumer/ actor	objecten	Doel
		Reason Timestamp} **Output:** SignedXML{ Confirmation-code Timestamp}	berichtendienst gemeld persoon is gewijzigd, wordt dit doorgegeven aan de EZ.Berichtenservice. De EZ.Berichtenservice zal de koppeling in de koppeltabel van de eIDAS-berichtenservice verwijderen.

5.1.3 Berichtenservice vereiste Interfaces

Hieronder volgt een opsomming van de externe interfaces welke de berichtenservice nodig heeft om de aan hem toegeschreven functionaliteit te kunnen leveren. De eIDAS berichtenservice is voor elk van de onderstaande services de consumer.

Service naam	Leverende applicatie	objecten	Doel
valideer Persoonsgegevens	eIDAS Identiteit Manager	**Input:** Encrypted & SignedXML {eIDAS-Attributes (NB in eTD syntax), UniquenessID ReturnURL Timestamp.} **Output:** Encrypted&SignedXML{ Statuscode, EncryptedBSN, Timestamp, UniquenessID}	Bij authenticatie voor het BSN-domein het matchen of toekennen van een BSN. Ter ondersteuning van de inkomende authenticaties van andere lidstaten (member states, MS) stelt de berichtenservice BZK in staat om de publieke identiteit (BSN) te bepalen bij een Europese digitale identiteit.

Service naam	Leverende applicatie	objecten	Doel
geef PolymorfPseudoniem	BSNk	**Input:** Uniqueness ID, ID Berichtensevice, EncryptedBSN **Output:** Polymorf Pseudoniemen{ PP-EU,PP-PS(opt.), PP-BSN(opt.)}	Het creeren van een stelselidentiteit Ter ondersteuning van inkomende buitenlandse authenticaties maakt de berichtenservice gebruik van BSNk om de (interne) stelselIdentiteit van de gebruiker aan te maken. Hiertoe wordt o.b.v. van de uniqueness ID (en eventueel BSN) PP's gecreeerd. Afhankelijk van BRP registratie status worden 1 of 3 PP geretourneerd
Geef SleutelMateriaal	BSNk	**Input:** Identifier Dienstverlener (EZ als dienstverlener tbv eIDAS notificatie) **Output:** Decryptiesleutel-NP Decryptiesleutel-BSN (optioneel; niet relevant voor Berichtenservice)	Het verstrekken van sleutelmateriaal waarmee de Dienstverlener (Berichtenservice) EncryptedPseudonyms kan ontsleutelen naar Pseudoniemen (of BSN's)
geef EncryptedPseudoniem	BSNk	**Input:** Identiteit BerichtenService, Identiteit beoogd Ontvanger, Polymorf Pseudoniem **Output:** EP	Ter ondersteuning van de inkomende buitenlandse authenticaties maakt de berichtenservice gebruik van BSNk om de stelselIdentiteit van de gebruiker om te zetten in een dienstverlener specifiek versleuteld pseudoniem (Encrypted Pseudoniem). Deze functionaliteit mag ook lokaal met behulp van een HSM worden gerealiseerd Afhankelijk van BSN of PseudoId authenticatie wordt respectievelijk PP-BSN of **PP-EU** gebruikt als input.

Service naam	Leverende applicatie	objecten	Doel
Authenticate	NL eIDAS Connector	**Input:** AuthnRequest **Output:** SAMLResponse (conform eTD spec)	Ter ondersteuning van de Authenticatie IN consumeert de Berichtenservice de authenticatie interface van de Nederlandse eIDAS-connector zodat het authenticatieverzoek wordt doorgezet naar de juiste (MS) eID-Service (Proxy/Adapter) Interactie buiten scope van startarchitectuur
Authenticate	eTD	**Input:** AuthnRequest **Output:** SAMLResponse (conform eTD spec) DV-HM interface	Ter ondersteuning van de Authenticatie UIT consumeert de Berichtenservice de authenticatie interface van de Nederlandse eTD-Stelsel zodat het authenticatieverzoek verder conform standaard werking binnen eTD wordt afgehandeld.
Verwijder koppeling	BRP-koppel-punt	**Input:** Encrypted&SignedXML{ UniquenessID Reason ReturnURL Timestamp} **Output:** Encrypted&SignedXML{ Confirmationcode Timestamp}	In het geval door het BRP-koppelpunt een verkeerde koppeling is gelegd of als het BSN van een aan de eIDAS-berichtendienst gemeld persoon is gewijzigd, wordt de koppeling in de koppeltabel van de eIDAS-berichtenservice verwijderd.

5.1.4 Berichtenservice Uitwerking

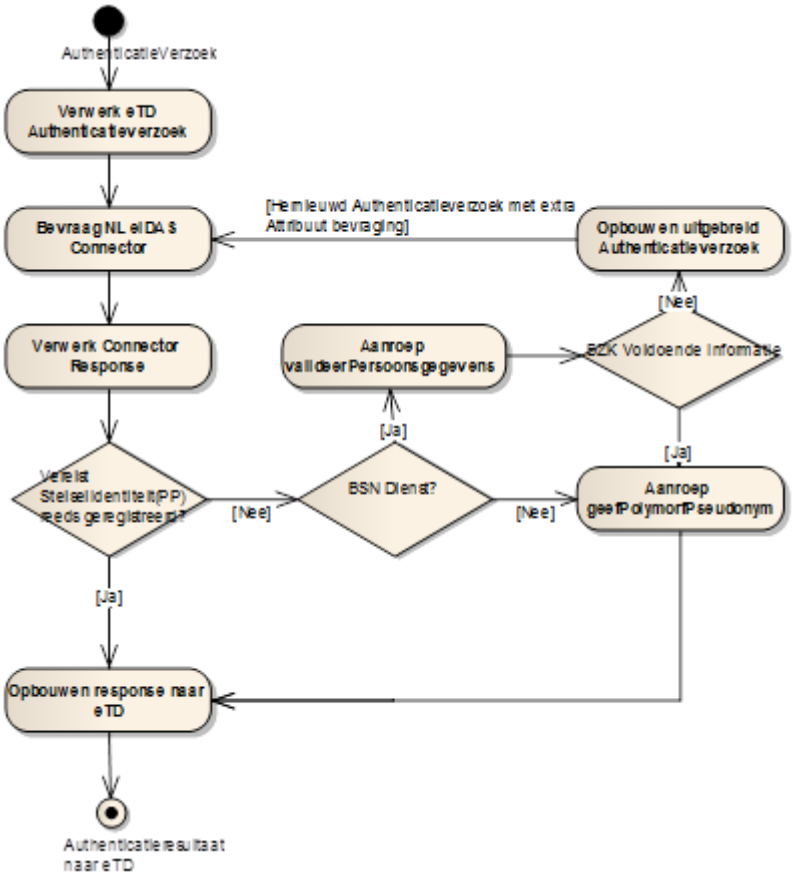
Hieronder volgen de kaders en afspraken die gehonoreerd moet worden in het realiseren van de berichtenservice bij het leveren en/of communiceren van de binnen deze startarchitectuur beschreven diensten.

5.1.4.1 *Leveren Authenticatie IN*

Leveren **Authenticatie IN**	
Doel	Door het faciliteren van adapter functionaliteit het bewerkstelligen van interoperabiliteit tussen de eIDAS-Nodes en het Nederlandse eID. Hiermee worden eID's van genotificeerde buitenlandse MS's transparant ontsloten voor op het stelsel aangesloten dienstverleners
Uitwerking	De Berichtenservice gedraagt zich richting het stelsel als een AD/AP[5]/MR en biedt hiertoe het gestandaardiseerde 'Authenticate' koppelvlak waarbij het request conform het HM-AD koppelvlak gedraagt; [https://afsprakenstelsel.etoegang.nl/display/as/Interface+specifications+HM-AD] En de response conform het DV-HM koppelvlak, in dat de originele verklaringen gewrapped worden in een summary-assertion. De processing logica voor het opbouwen van de summary-assertion hoeft echter niet gevolgd te worden [https://afsprakenstelsel.etoegang.nl/display/as/Interface+specifications+DV-HM] Bij het leveren van de service moet het volgende gedrag gerealiseerd worden.

[5] AP = attribute provider (attributendienst).

Leveren **Authenticatie IN**



Verwerk eTD Authenticatieverzoek:

- Ontvang het Authenticatie verzoek conform het gestandaardiseerde koppelvlak en voer de hierbij voorgeschreven controles uit.
- Bepaal op basis van het authenticatieverzoek en de eTD-Dienstencatalogus het vereiste betrouwbaarheidsniveau, de benodigde attributen, het identificerende kenmerk, de indicatie BSN dienst en of er reeds een keuze voor een lidstaat is gemaakt.
- Indien nog geen lidstaat gekozen is;
  Bevraag de gebruiker bij welke genotificeerde lidstaat deze zich wenst te authenticeren.

Bevraag NL eIDAS-connector:

- Schakel de NL-eIDAS-Connector in op basis van bovenstaande informatie, conform de hiervoor geldende specificaties
  [specificaties buiten scope startarchitectuur][6]

Verwerk NL eIDAS-connector response

- Ontvang het authenticatieresultaat van de NL eIDAS Connector [specificaties buiten scope startarchitectuur][7]

[6] Zie eidas_message_format_v1.0 en eidas_saml_attribute_profile_v1.0.2.

[7] Zie eidas_message_format_v1.0 en eidas_saml_attribute_profile_v1.0.2.

Leveren **Authenticatie IN**	
	• Controleer het bericht op integriteit en veiligheid. • Verifieer dat het authenticatieresultaat overeenkomt met het vereiste gevraagde uit het authenticatieverzoek. • Verifieer dat er reeds een correct stelsel Identiteit geregistreerd is bij de digitale identiteit op basis van het ontvangen uniqueness ID. Hiervoor onderhoudt de eIDAS berichtenservice is eigen registratie van PP's bij uniqueness ID. **Anders voer subflow geenStelselIdentiteit uit** Opbouwen response naar stelsel eTD: • Roep geef EncryptedPseudoniem aan met het **PP-EU** Polymorf Pseudoniem**,** tenzij de beoogde ontvanger (Dienstverlener) een BSN ***vereist*** in het authenticatieresultaat, gebruik dan het PP-BSN. NB: dit vergt een aanpassing op eTD, zodat de DV kan vragen: PP-BSN indien mogelijk, anders PP-EU. • Bouw het Authenticatieresultaat bericht op conform NL eID Specificaties, hiervoor gelden de volgende aanvullende aandachtspunten. ○ Verklaar over het serviceID in zowel de Authenticatie als eventueel bevoegdheidsverklaring op basis van de gevraagde dienst in het authenticatieverzoek ○ Transformeer de attributen zodat deze voldoen aan de actuele eTD Syntax, geef hierbij alleen de attributen door welke gevraagd zijn. Hierbij gelden de volgende afspraken; ▪ De attributen worden voorzien van een 'bron' en 'datum' conform de SAML attribute extensions specificatie https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-ext.html. Voor de datum wordt de actuele tijd van authentictie overgenomen. Als bron wordt het verklarende lidstaat overgenomen conform de 2 letterige ISO3166-1:2013 specificatie waarbij 'eIDAS' als prefix wordt opgenomen. (i.e. eIDAS:BE, eIDAS:DE, etc.) ▪ Het vanuit eIDAS ontvangen familyname voor gesplitst in eTD voorvoegsels en achternaam, conform Tabel 36 van de RVIG (http://publicaties.rvig.nl/dsresource?objectid=4793&type=pdf) ▪ Adres gegevens worden niet omgezet naar Nederlands formaat, zelfs indien het Nederlandse adressen betreft. Indien expliciet gevraagd, worden deze overgenomen in de hiervoor bestemde Internationale Adres-veld attributen, zie *Gedrag bij **consumeren Berichtenservice.Authenticate IN*** ▪ Voornaam en achternaam worden altijd meegegeven in de transliterated value. ▪ Er hoeft geen verwerking plaats te vinden op het ontvangen achternaam om hieruit het FamilyNameInfix te destilleren; deze wordt meegegeven als onderdeel binnen 'FamilyName' ▪ Indien de Dienstverlener expliciet vraagt om 'Non-

Leveren **Authenticatie IN**	
	LatinTransliterated, en indien aanwezig, worden de Non-Latin transliterated attributen meegegeven in de daarvoor erkende attributen. ▪ De geboortedatum wordt gebruikt om leeftijdsindicaties te bepalen ▪ Bij vertegenwoordiging wordt het ontvangen uniqueness ID van de rechtspersoon gecommuniceerd als het EntityConcernedType urn:etoegang:1.10:EntityConcernedID. eIDASLegalIdentifier • Verstuur het bericht naar de eTD makelaar conform de hiervoor geldende specificatie (NB. SAML-Response via Artifact binding; Stuur de gebruiker terug middels een redirect met een artifact, Faciliteer vervolgens het opvragen van het authenticatieresultaat door het stelsel middels een backchannel); Het authenticatieresultaat is grotendeels conform de actuele DV-HM interface. Sub-flow geenStelselIdentiteit: Indien er nog geen vereiste stelsel identiteit is geregistreerd bij de uniqueness ID (vereiste stelselidentiteit is PP-BSN voor BSN diensten en PP-EU voor Consumenten diensten) • Indien het authenticatie voor een BSN dienst betreft o Constateer dat er geen PP-BSN is geregistreerd o Roep valideerPersoonsgegevens ▪ Geef hierbij de ontvangen eIDAS-Attributen door zoals deze zouden worden doorgeven aan het stelsel eTD (zie boven '*Opbouwen response naar stelsel eTD'* voor verwerkingregels tav Attributen). ▪ Voeg hieraan de 'mandatoryonly' attribuut toe, met als waarde 'true' (zodat het BRP koppelpunt weet dat het meer attributen kan vragen – dit voorkomt een loop in het proces) o Bij ontvangst van response: ontsleutel het bericht en controleer het resultaat, verifieer hierbij bij een Succes dat; ▪ Het uniqueness ID overeenkomt met het verwachte uniqueness ID. ▪ Het bericht actueel is. ▪ De relatie tussen de ontvangen responsewaarden integer, en afkomstig van BZK zijn, middels handtekening validatie. o Indien er een Statuscode:Success wordt ontvangen; ▪ roep geefPolymorfPseudoniem aan ▪ Persisteer het ontvangen PP-EU,PP-PS en PP-BSN bij de digitale identiteit door registratie van de PP's bij de uniqueness ID in door de eIDAS berichtenservice. ▪ Vervolg primaire flow vanaf 'Response naar Stelsel'

Leveren **Authenticatie IN**	
	○ Indien er een Statuscode:Pending[8] wordt ontvangen; ▪ Verifieer in de dienstencatalogus dat de Authenticatie ook acceptabel is op basis van een Pseudoniem. • Indien er nog geen PP-EU is geregistreerd roep geefPolymorfPseudoniem aan en persisteer het PP-EU. • Vervolg primaire flow vanaf 'Response naar Stelsel' ▪ Indien de dienstverlener heeft aangegeven alleen met een BSN uit de voeten te kunnen. • Stuur een SAML-Response conform de 'Incorrect message (recoverable)' specificatie van eTD ○ Indien het response object middels Statuscode:RequiresRe-authentication aangeeft dat er te weinig informatie is om het proces met succes te kunnen afronden; ▪ Stel een nieuw authenticatieverzoek samen voor de NL eIDAS connector, hiervoor gelden de volgende aanvullende aandachtspunten. • De gevraagde attributen wordt uitgebreid tot de volledige minimale dataset; Inclusief de aanvullende attributen in de minimale dataset. • De 'dienst' waarvoor het authenticatieverzoek wordt gedaan wordt aangepast naar 'registratie binnen BRP' door aanpassing van de 'Serviceprovider' veld. Deze dienst wordt gemarkeerd als 'publiek'. ▪ Vervolg primaire flow vanaf Bevraag de NL eIDAS-connector • Indien authenticatie voor een niet-BSN-dienst ○ controleer dat er geen PP-EU is geregistreerd ▪ roep geefPolymorfPseudoniem aan. ▪ Constateer dat er ten minste 1 PP terugkomt, persisteer deze als het PP als PP-EU bij de digitale identiteit (uniqueness ID). ▪ Indien meegeleverd persisteer ook de PP-PS en de PP-BSN bij de digitale identiteit. ○ Vervolg primaire flow vanaf 'Response naar Stelsel'
Kenmerken	

[8] Het BRP-koppelpunt maakt interne onderscheid tussen Pending ("het proces loopt") en NotFound ("er is geen koppeling mogelijk"). Omdat er in de berichtendienst geen andere vervolgactie aan deze status hangt, retourneert het BRP koppelpunt in beide gevallen "Pending". Met dezelfde argumentatie retourneert het BRP koppelpunt de status "pending" waar het intern "RequestBusy" hanteert. Dat komt voor in situaties waarbij een tweede verzoek al binnenkomt, terwijl het eerste nog in de geautomatiseerde afhandeling zit. Dat zou kunnen gebeuren als een gebruiker met twee computers tegelijk probeert in te loggen.

Leveren **Authenticatie IN**	

5.1.4.2 *Verwijder koppeling*

Leveren Verwijder koppeling	
Doel	Deze service is bedoeld om een verkeerde koppeling tussen een Europese eID en een Nederlandse Identiteit (BSN) ongedaan te maken. Deze service wordt aangeroepen door RVIG om een koppeling te verwijderen. Zo kan worden verkomen dat een gebruiker die een nieuw BSN heeft gekregen bij een inlog via eIDAS nog steeds aan zijn oude BSN wordt gekoppeld. Maar ook eventueel verkeerde gelegde koppelingen herstelt worden.

Uitwerking	**Input:**
	Een getekend en versleuteld XML bericht, welke via een SOAP-Service wordt ontvangen.
	
	Het SOAP-Bericht bevat ten minste de volgende velden:
	• UniquenessID; van de geauthenticeerde Europese eID
	• Timestamp (format: yyyy-mm-dd hh:mm:ss)
	• Reason;
	  ○ WrongBSN; als het verkeerde BSN aan het UniquenessID is gekoppeld
	  ○ NewBSN; als de persoon een nieuw BSN heeft gekregen en het oude om die reden moet worden verwijderd.
	
	Output:
	Het resultaat van de 'Verwijder koppeling' functie wordt als response op de SOAP-call gecommuniceerd.
	Het SOAP bericht bevat de volgende velden:
	• Confirmationcode
	  ○ Success; als koppeling succesvol is verwijderd
	  ○ UID_not_found; als koppeling niet is gevonden
	• UniquenessID (zoals ontvangen in input)
	• Timestamp (format: yyyy-mm-dd hh:mm:ss)
	
	Verwerk Inputbericht:
	• De Berichtenservice controleert dat het Bericht integer en versleuteld is, en afkomstig is vanuit BZK.
	• In het koppeltabel wordt de record met overeenkomstig UniquenessID opgeschoond.
	
	Terugkoppeling response:
	• Afhankelijk van of de opschoonactie is gelukt bouwt de eIDAS berichtenservice de Confirmationcode op.
	• Het SOAP-Response wordt verzonden aan BZK.

Leveren Verwijder koppeling	
Kenmerken	

5.1.4.3 *Gedrag bij consumeren Authenticate UIT*

Gedrag bij consumeren Authenticate UIT	
Doel	Het leveren van adapter functionaliteit om interoperabiliteit bewerkstelligen tussen de eIDAS_Nodes en het Nederlandse stelsel eTD ten bate van uitgaande authenticatie. Hiermee wordt notificatie van het Nederlandse stelsel eTD gefaciliteerd.
Uitwerking	De interactie tussen de Proxy service en de Berichtenservice is uit scope van deze startarchitectuur. Ten behoeve van het kunnen leveren van deze functionaliteit aan de eIDAS Proxy gedraagt EZ zich richting het stelsel eTD echter als Dienstverlener. Voor het invullen van dit gedrag zijn de volgende verantwoordelijkheden afgesproken. Ontvangen Authenticatieverzoek: • Een ontvangen authenticatie verzoek vanuit een Europese Lidstaat wordt vertaald naar een authenticatie verzoek voor een dienst zoals eerder vastgelegd en aanwezig in de Diensten Catalogus van het stelsel eTD. o Hiertoe neemt EZ via een makelaar ten minste de diensten de volgende 4 diensten op; ▪ Authenticeer voor Europese dienstverlening op niveau Substantieel voor publieke dienst' , ▪ 'Authenticeer voor Europese dienstverlening op niveau Substantieel voor private dienst ▪ 'Authenticeer voor Europese dienstverlening op niveau Hoog voor publieke dienst' ▪ 'Authenticeer voor Europese dienstverlening op niveau Hoog voor private dienst. Deze diensten hebben elk 2 verschijningsvormen; ▪ De uitvraag voor Identiteit is het ECTA:PrivacyID. • Bij deze diensten worden de volledige minimale dataset voor natuurlijk personen opgenomen als gevraagde attributen. ▪ De uitvraag voor Identiteit is het ECTA:RSIN of ETCT:KvK • Bij deze diensten worden de volledige minimale dataset voor natuurlijk personen opgenomen als gevraagde attributen EN de volledige minimale dataset voor rechtspersonen opgenomen als gevraagde attributen. o Via het run-time meegeven van de attributen in het Authenticatieverzoek zal EZ de uitvraag van attributen verder kaderen tov de set zoals opgenomen in de dienstencatalogus; Om zo afhankelijk van het specifieke binnenkomend Europese

Gedrag bij consumeren Authenticate UIT	
	Authenticatieverzoek de juiste subset van deze attributen op te vragen vanuit het stelsel eTD. o Publieke Stakeholders mogen EZ vragen om (op basis van bv. reguliere expressies) een specifieke(re) mapping op diensten te realiseren[9]. o EZ communiceert richting het stelsel het land waarvanuit authenticatie gevraagd is, als ook de naam van de beoogde Dienstverlener, deze gegevens worden gecommuniceerd in het 'ServiceProvider' veld in het Authnrequest conform volgende syntax; ▪ Vragende lidstaat conform de 2-letterige notatie als opgenomen in de ISO3166-1:2013 specificatie. ▪ Het scheidingsteken ':'De naam van de dienstverlener zoals ontvangen in orginele Autnrequest in het veld 'ProviderName' conform sectie 2.4.1 van de eIDAS SAML over in het veld ServiceProvider. Terugsturen Authenticatieresultaat : • Als dienstverlener krijgt de Berichtenservice een over AD's heen, persistent en uniek Pseudoniem voor de natuurlijk persoon.EZ zet het ontvangen Pseudoniem om in een onderling niet relateerbaar, per land uniek, uniqueness ID • In geval van vertegenwoordiging berekent EZ het uniqueness ID voor de rechtspersoon op basis van het ontvangen RSIN; respectievelijk KVK nummer voor Eenmanszaken. • In geval van een ketenmachting verwerkt de Berichtenservice het Resultaat als ware er geen 'IntermediateEntityID' attribute aanwezig. • EZ vertaald de eTD attributen naar eIDAS attributen o Hierbij worden de eTD attributen voorvoegsels en achternaam samen tot eIDAS familyname.
Kenmerken	

5.1.4.4 *Gedrag bij consumeren geefSleutelMateriaal*

Gedrag bij consumeren GeefSleutelMateriaal	
Doel	Ophalen van sleutelmateriaal welke gebruikt wordt om de vanuit het stelsel eTD aangeleverde Encrypted Pseudoniem om te zetten in een persistent Pseudoniem.

[9] Ter illustratie; in geval van de UUM&DS project van DG-TAXUUD zal Douane meer granulariteit willen ten opzichte van de bovengenoemde standaard diensten. Hiertoe zal Douane de opname van de diensten in de dienstencatalogus van eTD op zich moeten nemen en aan EZ moeten specificeren hoe het ontvangen authenticatieverzoek aan deze gerelateerd dienen te worden.

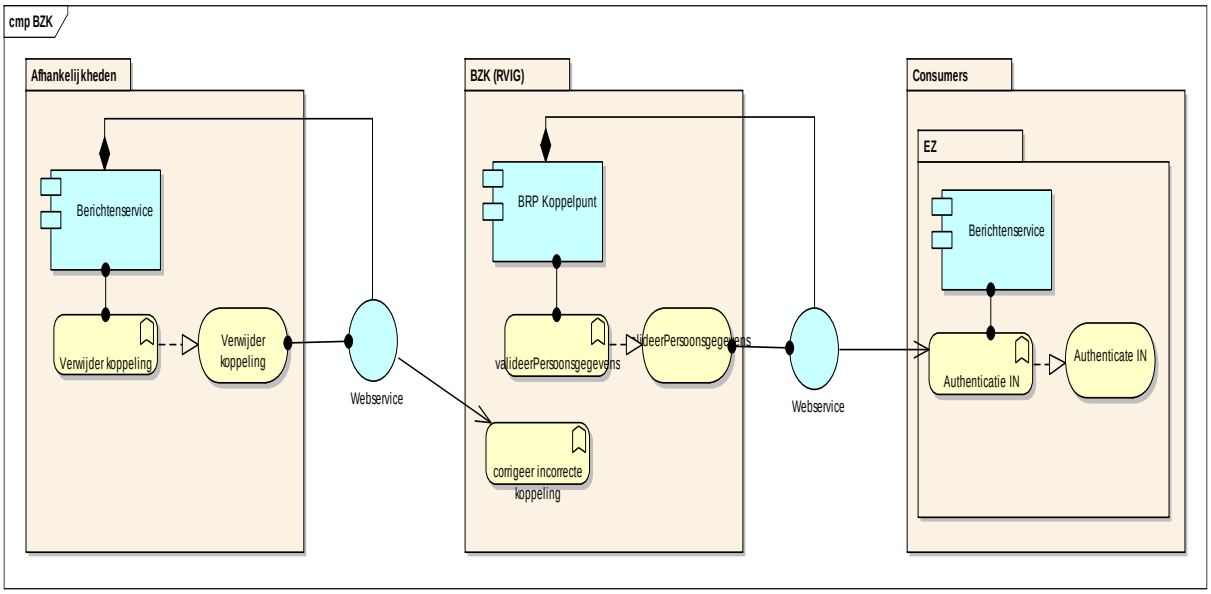
Gedrag bij consumeren GeefSleutelMateriaal	
Uitwerking	(Periodieke) beheer activiteit om de EZ-specifieke versleutelde (ont)sleutelmateriaal op te halen. Deze moet aanwezig zijn binnen de Berichtenservice om het EP om te zetten in een Pseudoniem
Kenmerken	Het sleutelmateriaal zal geautomatiseerd kunnen worden opgevraagd middels een nog te publiceren interface. De initiële invulling wordt echter via een handmatig proces ingeregeld bij de beheerorganisatie BSNk met ondersteuning van de makelaar.

5.2 Gedrag BRP-Koppelpunt

Het BRP-koppelpunt faciliteert het gebruik van BSN in (pan-European) binnenkomende digitale authenticaties zodat Nederlandse dienstverleners ontzorgd worden in hun verplichting om te voldoen aan de eIDAS verordening. De identiteitmanager is het 'aanspreekpunt' voor de eIDAS berichtenservice en zorgt onder meer voor het vertalen van de eIDAS attributen naar BRP attributen. Het BRP-Koppelpunt speelt geen rol bij binnenkomende digitale authenticaties voor rechtspersonen of consumenten domein, noch bij authenticatie met een Nederlands middel ten behoeve van een buitenlandse dienstverlener.

5.2.1 Structuur BRP-Koppelpunt

Onderstaand beschouwt het verandergebied vanuit het perspectief van BZK.



Figuur 4 Structuur BZK

5.2.2 BRP-Koppelpunt geleverde Interfaces

Onderstaande tabel geeft inzicht in het externe gedrag zoals geleverd door BZK.

Service Naam	consumer/ actor	Objecten	Doel
valideer Persoons gegevens	eIDAS Berichtenservice	**Input:** Encrypted&SignedXML { eIDAS-Attributes (NB in eID-syntax), UniquenessID ReturnURL Timestamp.} **Output:** Encrypted&SignedXML { Statuscode, EncryptedBSN, Timestamp, UniquenessID}	Bij pan-European inkomende authenticaties voor het BSN-domein het associeren of toekennen van een BSN bij de digitale Identiteit.

5.2.3 BRP-Koppelpunt vereiste interfaces

Er is voor het BRP Koppelpunt een afhankelijkheid met de EZ.Berichtenservice.**Service naam**	Leverende applicatie	objecten	Doel
Verwijder koppeling	eIDAS Berichtenservice	**Input:** SignedXML{ UniquenessID Reason Timestamp} **Output:** SignedXML{ Confirmationcode Timestamp}	In het geval door het BRP-koppelpunt een verkeerde koppeling is gelegd of als het BSN van een aan de eIDAS-berichtendienst gemeld persoon is gewijzigd, wordt dit doorgegeven aan de EZ.Berichtenservice zodat deze de koppeling in de koppeltabel van de eIDAS-berichtenservice verwijderd.

5.2.4 BRP-Koppelpunt Uitwerking

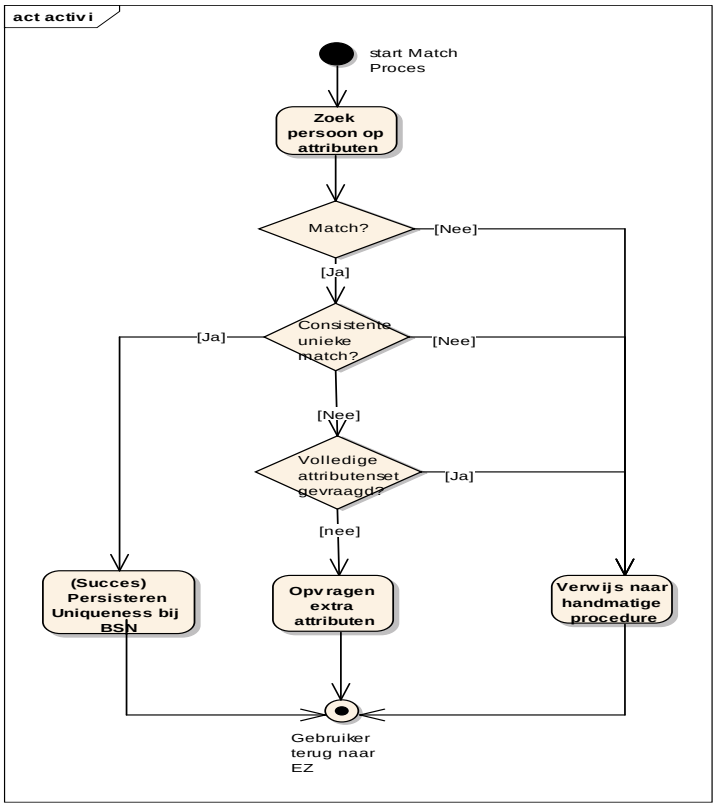
5.2.4.1 *ValideerPersoonsgegevens*

ValideerPersoonsgegevens	
Doel	Ervoor zorgdragen dat er een BSN wordt geassocieerd, of toegekend aan de ontvangen Europese digitale identiteit (eID).
Uitwerking	**Input:** Het input bericht wordt verkregen via een backchannel, waarbij via een HTML-Post of HTTP-GET variabele een verwijzing (ie. Artifact) naar dit inputbericht wordt gecommuniceerd via de user agent (browser);.. Het signed en encrypted inputobject wordt gecommuniceerd in XML formaat Deze XML bevat ten minste de volgende velden: • UniquenessID; van de geauthenticeerde Europese eID • ReturnURL; Adres waarheen gebruiker terug gestuurd kan worden richting de Berichtenservice • Timestamp (format: yyyy-mm-dd hh:mm:ss) • De attributen zoals ontvangen vanuit de memberstate in het authenticatieresultaat, conform de actuele eTD specificaties. **Output:** Het resultaat wordt middels dezelfde 'Artifact-binding' gecommuniceerd via een backchannel. Het artifact wordt via POST of GET gecommuniceerd richting de ReturnURL. Het resulterende responsebericht is een signed en encryptedresponseobject in XML formaat Deze XML bevat de volgende velden: • Statuscode (success, pending, requiresRe-authentication,error) • UniquenessID (zoals ontvangen in input) • Timestamp (format: yyyy-mm-dd hh:mm:ss) • BSN (opt. Alleen bij succes. Additioneel versleuteld voor het BSNk conform onderstaande methodiek; o De versleuteling van de BSN wordt gedaan conform XML-Encryptie http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/Overview.html#sec-eg-Element o Hiervoor worde 256bit AES sleutels gebruikt. o Voor elk bericht wordt een nieuwe AES sleutel gegenereerd door de BRP-Koppelpunt. o De AES Sleutels worden versleuteld voor een ieder van de in de BSNk metadata opgenomen publieke sleutels van het BSNk. o De versleuteling van de AES sleutels wordt uitgevoerd met RSA algoritme in combinatie met OAEP: http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p. Hierbij mag de sleutel van het BRP out-of-band gecommuniceerd worden, of gewoon een op naam van BZK PKIo certificaat zijn. Het certificaat van het BSNk kan worden gedestilleerd uit de eID-metadata. De volgende stappen die relevant zijn in het kader van deze startarchitectuur worden tenminste gerealiseerd: Ontvang Valideerpersoonsgegevens verzoek:

- Ontsleutel het verzoek, stel vast dat deze is ondertekend door de Berichtenservice en actueel is.
- Controleer daarbij dat de returnURL een beveiligde URL betreft, die is beveiligd middels een aan EZ of AZ uitgegeven certificaat.
- Stel vast dat tenminste de verplichte attributen uit de minimale dataset zijn opgeleverd.
- Stel vast dat de geleverde attributen voldoen aan de afgesproken eTD-data formaat
- Constateer dat bij de huidige uniqueness ID er nog geen registratie heeft plaatsgevonden binnen BRP (anders stuur gebruiker terug met Statuscode:Succes conform boven aangegeven interface afspraak.

Inschrijving:

- Bepaal op basis van onderstaande activiteiten de te ondernemen stappen



Retourbericht naar Berichtenservice:

- Indien er onvoldoende gegevens zijn:
  - Indien nog niet de volledige minimale dataset is gevraagd;
    - Forward de gebruiker terug naar de aangeleverde returnURL met Statuscode:RequiresRe-authentication conform afspraak, zodat duidelijk is dat de volledige minimale dataset vereist is.
      NB. Deze melding mag niet gegeven worden indien de volledig minimale dataset wel is aangevraagd, maar niet

	is aangeleverd (`fullminimumsetrequested`=true) ○ Indien de volledige dataset wel is gevraagd. ▪ Zie handmatige procedure • Indien handmatig procedure vereist is: ○ Informeer de gebruiker over de te ondernemen acties en forward de gebruiker terug naar de aangeleverde returnURL met de Statuscode:Pending conform bestaande interface afspraak. • Indien RNI inschrijving gelukt is of een bestaande BRP record gematched kan worden ○ Zorg dat het gecreëerde of geassocieerde BRP/RNI-record teruggevonden kan worden op basis van de Europese Persistente Identiteit (uniqueness ID) Forward de gebruiker terug naar de aangeleverde returnURL met de Statuscode:Success die duidelijk maakt dat de validatie succesvol verlopen is en BRP koppeling of inschrijving heeft plaatsgevonden.Hanteer hiervoor bovenstaande interface afspraak.
Kenmerken	De service wordt via een asynchroon koppelvlak geboden. Hierdoor is BZK in controle van de gebruikersinteractie en bestaat de vrijheid om de gebruiker verder te begeleiden. Bijvoorbeeld door deze te sturen naar ABO's of te informeren over de te ondernemen acties indien een handmatige procedure vereist is. De hiermee verkregen verkregen autonomiteit van het BRP-Koppelpunt reduceert de afhankelijkheid, waardoor de koppelvlakken langer stabiel kunnen blijven. De aangemaakte of geassocieerde record moet kunnen worden teruggevonden op basis van het uniqueness ID om het handmatige matching proces bij BRP te kunnen facliteren Het is een verantwoordelijkheid van BZK dat wordt voldaan aan de wettelijke eisen omtrent dataregistratie in BRP. Er mag niet vanuit worden gegaan dat hiervoor randvoorwaardelijke maatregelen bijvoorbeeld omtrent informed user consent door andere partijen in de keten reeds zijn geregeld

5.2.4.2 *Gedrag bij consumeren VerwijderKoppeling*

VerwijderKoppeling	
Doel	Omdat BRP-koppelpunt op een beperkt aantal attributen probeert een koppeling te maken met een geregistreerd BSN en omdat het streven is om tot een koppeling te komen, ook als niet 100% zeker is dat die koppeling correct is, is onvermijdelijk dat er verkeerde koppelingen worden gelegd. Deze service is bedoeld om zo'n verkeerde koppeling weer ongedaan te maken. Deze service wordt ook gebruikt om na wijziging van een BSN de bestaande koppeling te verwijderen. Daarmee wordt voorkomen dat een gebruiker die een nieuw BSN heeft gekregen bij een inlog via eIDAS nog steeds aan zijn oude BSN

	wordt gekoppeld.

Uitwerking	**Input:**
	Opsturen van het UniquenessID en de reden waarom de koppeling moet worden
	
	Deze XML bevat ten minste de volgende velden:
	• UniquenessID; van de geauthenticeerde Europese eID
	• Timestamp (format: yyyy-mm-dd hh:mm:ss)
	• Reason;
	  ○ WrongBSN; als het verkeerde BSN aan het UniquenessID is gekoppeld
	  ○ NewBSN; als de persoon een nieuw BSN heeft gekregen en het oude om die reden moet worden verwijderd.
	
	Response:
	Verwerkbevestigingvan de verwijderde koppeling. Als de verwerkbevestiging een foutmelding bevat is handmatig uitzoekwerk noodzakelijk.
	
	Deze XML bevat de volgende velden:
	• Confirmationcode
	  ○ Success; als koppeling succesvol is verwijderd
	  ○ UID_not_found; als koppeling niet is gevonden
	• UniquenessID (zoals ontvangen in input)
	• Timestamp (format: yyyy-mm-dd hh:mm:ss)

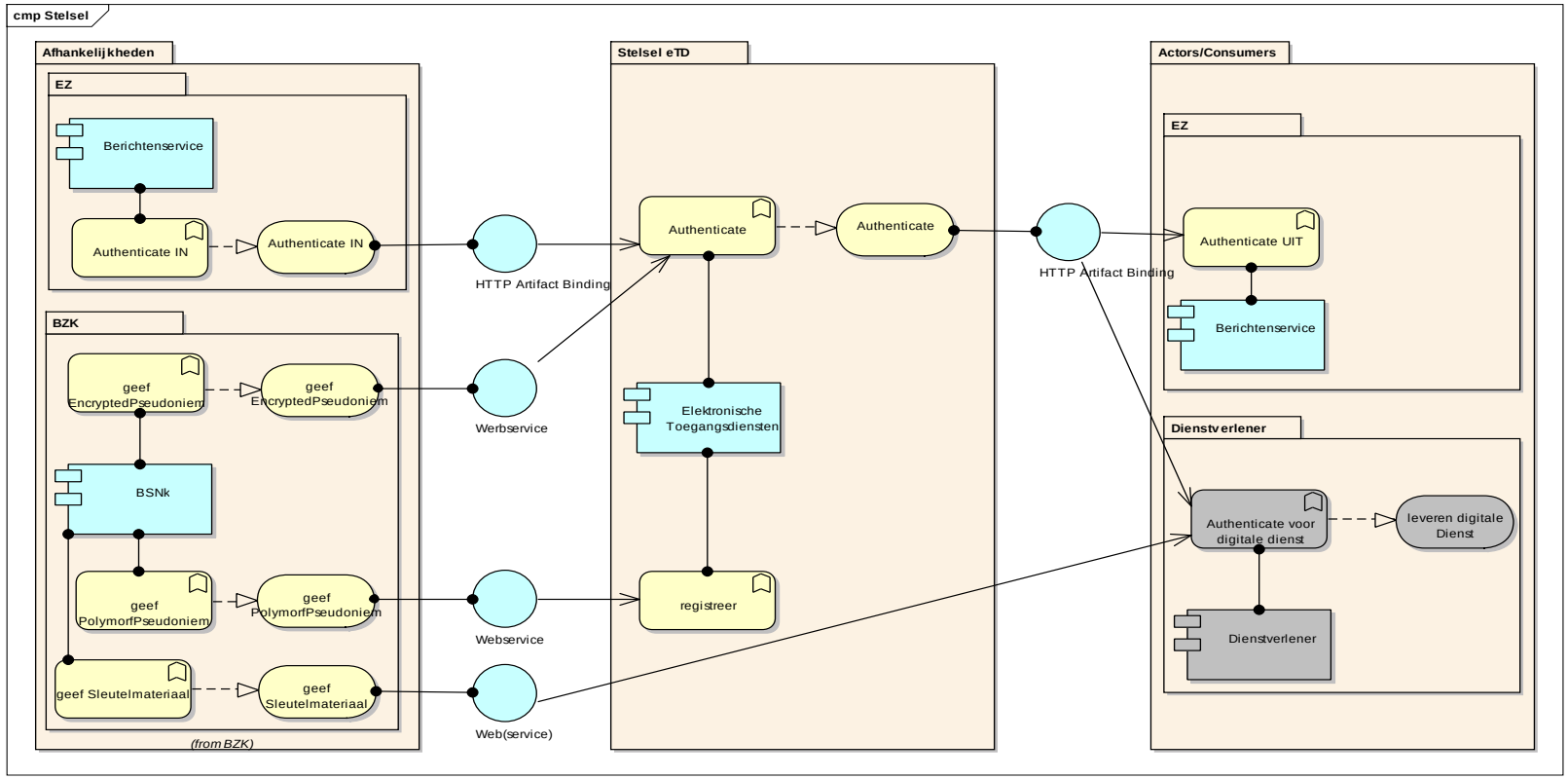
Kenmerken	De service wordt via een synchroon koppelvlak geboden.

5.3 Gedrag stelsel Elektronische Toegangsdiensten

Het Nederlandse stelsel eTD faciliteert de aansluiting van dienstverleners op eIDAS (verordening) en wordt ontsloten als eID-voorziening voor de (publieke) diensten van Europese Lidstaten (notificatie)

5.3.1 Structuur stelsel eTD

Onderstaand beschouwd het verandergebied vanuit het perspectief van eToegang.



Figuur 5 Structuur stelsel eTD

5.3.2 Stelsel eTD geleverde Interfaces

Onderstaande tabel geeft inzicht in het externe gedrag zoals geleverd door eTD.

Service Naam	consumer/ actor	Objecten	Doel
Authenticate	EZ Berichtenservice (tbv notificatie) eTD aangesloten Dienstverlener	**Input:** SAML Authnrequest **Output:** SAML Response (conform eTD spec)	Het authenticeren van een gebruiker, eventueel met vaststelling van de bevoegdheden.

5.3.3 Stelsel eTD vereiste Interfaces

Onderstaande tabel geeft inzicht in de externe vereiste interfaces die het stelsel eTD vereist om de haar toegeschreven functionaliteit te kunnen uitvoeren.

Service Naam	Leverende applicatie	Objecten	Doel
geef Encrypted Pseudoniem	BSNk	**Input:** Polymorf Pseudoniem **Output:** Encrypted Pseudoniem	Het laten omzetten van een authenticatiedienst of machtigingsregister specifiek PolymorfPseudoniem in een Dienstverlener specifiek Encryped Pseudoniem.
geef Polymorf Pseudoniem (voorheen AD-KR)	BSNk	**Input:** BSN Controlegegevens, ID-AD/MR **Output:** Polymorf Pseudoniemen{ PP-PS,PP-BSN }	Het creeeren van een stelselIdentiteit voor natuurlijke personen op basis van een uniek identificerend kenmerk van de gebruiker.

Service Naam	Leverende applicatie	Objecten	Doel
		Input: BSN Controlegegevens Pseudoniem **Output:** Bevestigingcode (DEPRECATED)	Legacy werking tbv Pilots (Uit scope startarchitectuur)
Geef SleutelMateriaal	BSNk	**Input:** Identifier Dienstverlener (EZ) **Output:** Decryptiesleutel-NP Decryptiesleutel BSN (optioneel)	Het periodiek (bijvoorbeeld eens in de drie jaar) verstrekken van sleutelmateriaal waarmee de Dienstverlener EncryptedPseudonyms kan ontsleutelen naar Pseudoniemen (of BSN's)
Authenticate IN input conform HM-AD interface output gelijkend op DV-HM interface	eIDAS berichten service	**Input:** Authnrequest **Output:** SAML Response	Ten bate van het voldoen aan de verorderning consumeert het stelsel eTD de EZ.Berichtenservice als AD /HM.

5.3.4 Stelsel eTD Uitwerking

Hieronder wordt in meer detail de vereiste wijzigingen op stelsel eTD beschreven.

5.3.4.1 *Gedrag bij leveren Authenticatie*

Gedrag bij leveren Authenticatie UIT	
Doel	Het mogelijk maken van Europees gebruik van onder het stelsel eTD tot stand gekomen authenticaties.
Uitwerking	Interface conform meeste actuele DV-HM specificatie: https://afsprakenstelsel.etoegang.nl/display/as/Interface+specifications+DV-HM+1.9 Om als stelsel genotificeerd te kunnen worden zijn de volgende wijzigingen vereist aan het authenticatie proces binnen eTD. • Conformeren aan het eIDAS normen kader. • Het bij de Authenticatie (en/of selecteren van machtiging) tonen van het land en de naam van de dienstverlener bij grensoverschrijdende authenticatie. ○ Hiertoe wordt het veld 'ServiceProvider' uit het vanuit de

<table>
<tr><td colspan="2">Gedrag bij leveren Authenticatie UIT</td></tr>
<tr><td></td><td>
EZ.Berichtenservice ontvangen Authenticatieverzoek uitgelezen. Deze is als volgt opgbouwd;

Vragende lidstaat conform de 2-letterige notatie als opgenomen in de ISO3166-1:2013 specificatie.
Het scheidingsteken ‘:’
De naam van de dienstverlener.

ie. DE:Deutsche Post

Voor de (door EZ opgenomen) Europese diensten mag geen ‘consent preferenc’ op Dienstniveau worden geboden door een AD en/of MR. Indien een AD en/of MR de gebruiker wil faciliteren in het onthouden van diens consent voorkeuren, dan moet naast de dienst hierin ook de dienstverlenersnaam en land opgenomen te worden (zoals gecommuniceerd in ‘ServiceProvider’ veld van het AuthnRequest).
Indien de dienstverlenersnaam leeg is mag geen consent preference worden gepersisteerd.
Voor de (door EZ opgenomen) Europese diensten zal voor rechtspersonen vanuit de Dienstencatalogus gevraagd worden om het ECTA.RSIN OF het ECTA.KvK. De verwerkingsregels voor MR’s hierbij is dat voor Rechtspersonen altijd het RSIN MOET worden opgeleverd, waarbij slechts voor EMZ het KvK wordt gecommuniceerd.
Het opleveren van de eIDAS verplichte minimale dataset (attributen) bij natuurlijk en niet natuurlijk personen.
NB Het stelsel ondersteunt in geval van vertegenwoordiging het gelijktijdig uitleveren van attributen van de Natuurlijk persoon en het Rechtspersoon.

Verder worden de attributen in de rechterkolom toegevoegd aan het stelsel eTD voor zover nog niet aanwezig.
<table>
<tr><td>Gegevens niet natuurlijk persoon
Verplichte dataset eIDAS</td><td>eTD-Attribute</td></tr>
<tr><td>a) huidige wettelijke naam;</td><td>CompanyName</td></tr>
<tr><td>b) unieke identificatiecode</td><td>Niet van toepassing;
Berichtenservice berekent deze o.b.v. het EntityConcernedType:RSIN voor rechtspersonen een het EntityConcernedType:KvK voor Eenmanszaken</td></tr>
<tr><td colspan="2">Aanvullende dataset</td></tr>
<tr><td>a) huidig adres</td><td>CompanyPostalCode
CompanyHouseNumer
CompanyHouseNumberSuffix</td></tr>
</table>
</td></tr>
</table>

Gedrag bij leveren Authenticatie UIT	

b) btw-nummer	VATRegistrationNumber (voor Nederlandse MR's/AP's vooralsnog altijd gevuld met RSIN zoals verkregen van KvK;)
c) fiscaal referentienummer	TaxReferenceNumber (voor Nederlandse MR's/AP's vooralsnog altijd gevuld met RSIN zoals verkregen van KvK;)
d) de identificatiecode bedoeld in artikel 3, lid 1, van Richtlijn 2009/101/EG van het Europees Parlement en de Raad (1);	ChamberOfCommerce (voor Nederlandse MR's/AP's vooralsnog altijd gevuld met KvK zoals verkregen van KvK;)
e) de identificatiecode voor juridische entiteiten bedoeld in Uitvoeringsverordening (EU) nr. 1247/2012 van de Commissie	LEI (Voor Nederlandse MR's/AP's vooralsnog altijd gevuld met LEI (Legal Entity Identifier)zoals verkregen van KvK;)
f) het registratie- en identificatienummer van marktdeelnemer bedoeld in Uitvoeringsverordening (EU) nr. 1352/2013 van de Commissie (3);	EORI (Voor Nederlandse MR's/AP's vooralsnog altijd gevuld met het economic operator registration and identification nummer zoals uitgegeven door Douane) http://ec.europa.eu/taxation_customs/dds2/eos/eori_validation.jsp
g) het accijnsnummer bedoeld in artikel 2, punt 12, van Verordening (EU) nr. 389/2012 van de Raad (4).	SEED (Voor Nederlandse MR's/AP's vooralsnog altijd gevuld System for Exchange of Excise Data | accijnsnummer, zoals uitgegeven door Douane)
h) De Standard Industrial Classification Een vier cijferige code om de bedrijfsvoering van de rechtspersoon te classificeren	SIC Standard Industrial Classification (http://www.sec.gov/info/edgar/siccodes.htm)

De gegevens voor natuurlijk persoon zijn grotendeels reeds erkend binnen het huidige versie van eTD; en laten zich als volgt mappen/opvragen

Gegevensset natuurlijk persoon Verplicht	
(a)Huidige familienaam	urn:etoegang:1.9:attribute:FamilyNameInfix urn:etoegang:1.9:attribute:FamilyName
(b)Huidigevoornaam	urn:etoegang:1.9:attribute:FirstName
(c)geboortedatum	urn:etoegang:1.9:attribute:DateOfBirth
(d)Unieke Identificatiecode	ZIE ONDER
Aanvullend	
(a)Voornaam en/of achternaam bij geboorte	urn:etoegang:1.9:attribute:FirstName urn:etoegang:1.9:attribute:FamilyNameInfix

<table>
<tr><th colspan="2">Gedrag bij leveren Authenticatie UIT</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>urn:etoegang:1.9:attribute:FamilyName</td></tr>
<tr><td>(b)geboorteplaats</td><td>urn:etoegang:1.9:attribute:PlaceOfBirth</td></tr>
<tr><td>(c)Huidige adres</td><td>urn:etoegang:1.9:attribute:PostalCode
urn:etoegang:1.9:attribute:HouseNumber
urn:etoegang:1.9:attribute:HouseNumber Suffix</td></tr>
<tr><td>(d)geslacht</td><td>urn:etoegang:1.9:attribute:Gender</td></tr>
</table>

Unieke Identificatiecode:
Het faciliteren van een stelselbrede persistent Pseudoniem voor natuurlijke personen; hiertoe worden de volgende wijzigingen aangebracht;

Het erkennen van het Identificerend Kenmerk ‘PrivacyID’, naast de huidige ECTA’s (om de nieuwe vorm van pseudonimisering o.b.v. PP aan te duiden)
In het registratie proces aansluiten op ‘leveren Polymorf Pseudoniem’.
In het authenticatieproces aansluiten op ‘leveren Encrypted Pseudoniem’ indien gevraagd wordt om het Identificerend Kenmerk ‘PrivacyID’
Het Stelsel garandeert dat ook bij vertegenwoordiging de identiteit van de natuurlijk handelend persoon in de vorm van een Encrypted Pseudonym wordt gecommuniceerd richting de BerichtenService.

Het faciliteren van een stelselbrede persistent Identifier voor niet natuurlijke personen over de verschillende Identificerende Kenmerken heen

Deze eis wordt op transparante wijze vervuld door het stelsel, doordat EZ (Berichtenservice) in rol van DV alle Pan-European diensten uitvraagt op basis van het ECTA:RSIN of het ECTA:KVK als Identiteit voor het rechtspersoon/EMZ voor alle Europese diensten. Alleen indien het een Eenmanszaak betreft zal vanuit het stelsel het KvK uitgeleverd worden. In alle andere voorkomende gevallen het RSIN.

</td></tr>
<tr><td>Kenmerken</td><td></td></tr>
</table>

5.3.4.2 *Gedrag bij consumeren Berichtenservice.Authenticate IN*

Gedrag bij consumeren Berichtenservice.Authenticate IN	
Doel	Om te voldoen aan de eIDAS verordening zal het eTD Stelsel de Berichtenservice erkennen als ware deze een Authenticatiedienst binnen het stelsel. Hiermee worden Europese genotificeerde eID’s grotendeels

Gedrag bij consumeren Berichtenservice.Authenticate IN	
	transparant ontsloten voor op het stelsel eTD aangesloten Dienstverleners.
Uitwerking	Om de aansluiting van Berichtenservice als AD/MR binnen het stelsel mogelijk te maken zijn de volgende wijzigingen binnen het stelsel vereist: • Het mogelijk maken van het meegeven van een Landkeuze vanuit de Dienstverlener in het DV-HM koppelvlak als functionaliteit. Het staat een makelaar vrij om deze keuze vervolgens ook functioneel te ondersteunen (middels het doorgeven van dit veld richting de Berichtenservice). • Het meeleveren van de dienstverleners naam in het autenticatieverzoek in het 'ServiceProvider' veld. • Het kunnen bieden van een landenkeuze scherm bij de makelaar o Waarvoor de templates opgeleverd worden van uit de beheerorganisatie. Het staat de makelaar vrij om deze functionaliteit te ondersteunen als optionele functionaliteit. Indien de gebruiker nog geen land keuze bij DV of HM heeft gemaakt wordt de landkeuze geboden door de berichtenservice. • Vasthouden bij dienst of deze zich in het publieke domein bevindt o Eventueel door de oude semtnische waarde aan IsPublic in ere te herstellen, of een additioneel veld in de DC te erkennen • 1 gecombineerd antwoord accepteren van de Berichtenservice o De makelaar bevraagt de EZ-Berichtenservice als een 'normale' Authenticatiedienst en verwerkt het response als ware deze een DV-HM response. • Er zal een additioneel Identiteit voor Rechtspersonen erkend worden naast de huidige KVK en RSIN. Hiertoe neemt het afsprakenstelsel urn:etoegang:1.10:EntityConcernedID. eIDASLegalIdentifier op. De waarde van dit veld bevat een zo persistent mogelijke Identifier van het rechtspersoon, maar is binnen de context van eTD verder betekenisloos. • In de Dienstencatalogus kan middels het (mede) uitvragen van de ECTA eIDASLegalIdentifier worden aangegeven dat buitenlandse rechtspersonen in principe toegang kunnen krijgen tot de dienst. • De volgende additionele attributen worden toegevoegd aan de attribuut catalogus van het stelsel eTD zodat dienstverleners in staat worden gesteld buitenlandse adressen te ontvangen; o urn:etoegang:1.10:Attribute:EU- PoBox o urn:etoegang:1.10:Attribute:EU-LocatorDesignator o urn:etoegang:1.10:Attribute:EU-LocatorName o urn:etoegang:1.10:Attribute:EU-CVaddressArea o urn:etoegang:1.10:Attribute:EU-Thoroughfare o urn:etoegang:1.10:Attribute:EU-PostName o urn:etoegang:1.10:Attribute:EU-AdminunitFirstline o urn:etoegang:1.10:Attribute:EU-AdminUnitSecondline o urn:etoegang:1.10:Attribute:EU-PostCode

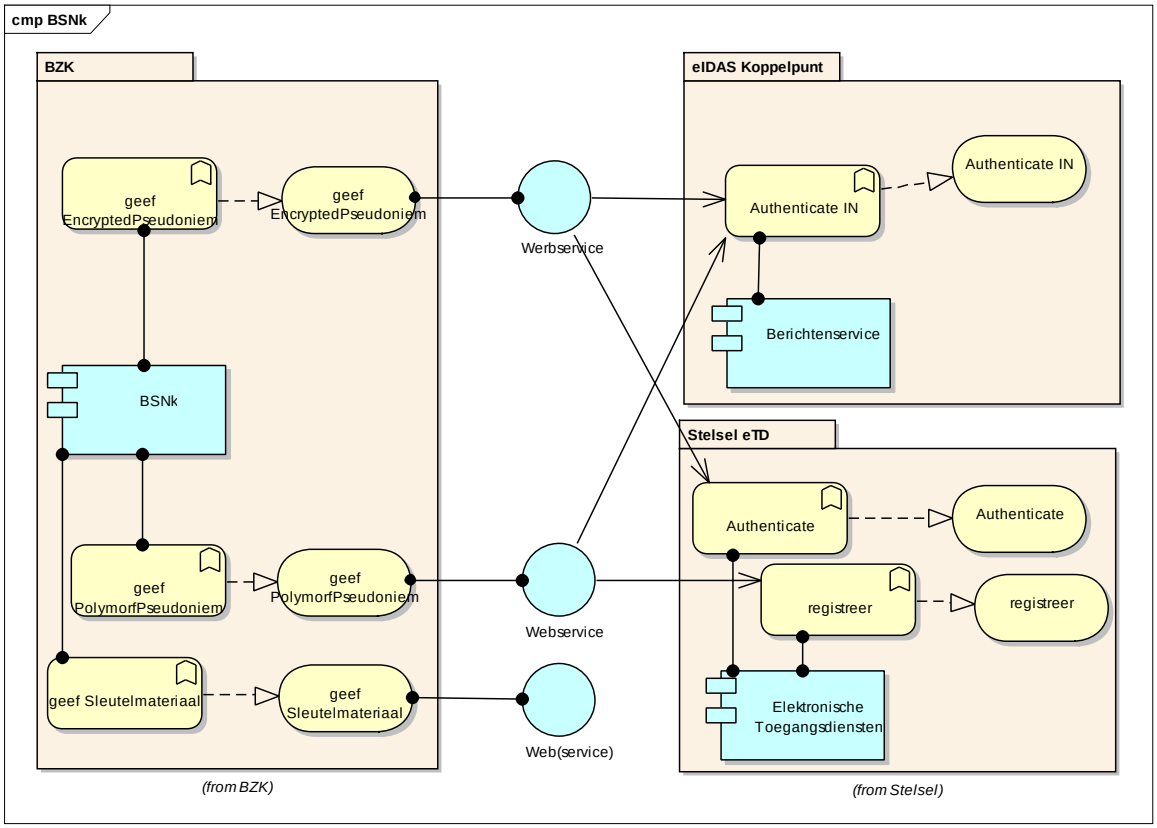
Gedrag bij consumeren Berichtenservice.Authenticate IN	
	• De volgende additionele attributen worden erkend binnen eTD zodat dienstverleners in staat worden gesteld namen van bedrijven in hun originele schrijfwijze te ontvangen; ○ urn:etoegang:1.10:Attribute:Non- transliterated- CompanyName • De volgende additionele attributen worden erkend binnen eTD zodat dienstverleners in staat worden gesteld namen van gebruikers in hun originele schrijfwijze te ontvangen; ○ urn:etoegang:1.10:Attribute:Non-T transliterated-Firstname ○ urn:etoegang:1.10:Attribute:Non- transliterated-FamilyName • De volgende additionele attributen worden erkend binnen eTD ○ urn:etoegang:1.10:Attribute:Birthname ○ urn:etoegang:1.10:Attribute:Non- transliterated-Birthname
Kenmerken	

5.4 Gedrag BSN koppelregister

Het BSNk faciliteert het gebruik van een persistent digitale identiteit.

5.4.1 Structuur BSNk

Onderstaand beschouwt het verandergebied vanuit het perspectief van BSNk.



Figuur 6 Structuur BSNk

5.4.2 BSNk geleverde Interfaces

Onderstaande tabel geeft inzicht in het externe gedrag zoals geleverd door BSNk.

Service Naam	consumer/ actor	objecten	Doel
Geef Polymorf Pseudoniem	stelsel eTD	**Input**: Identiteit AD/MR, BSN, ControleGegevens **Output:** Statuscode, Polymorf Pseudoniemen (PP-PS, PP-BSN)	Ter ondersteuning van de authenticatie creeert BSNk een stelsel identiteit. Deze heeft de vorm van een PolymorfPseudoniem en kent 3 gebruiksvormen. 1 direct gebaseerd op het BSN voor het BSN-Domein. Het PP-BSN. 1 indirect gebaseerd op het BSN (PP-PS), of indirect gebaseerd op het uniqueness ID(PP-EU), voor gebruik waarbij de identiteit moet leiden tot een Pseudoniem.
	eIDAS berichtenservice	**Input:** Identiteit berichtenService, uniqueness ID, EncryptedBSN **Output:** Polymorf Pseudoniemen(PP-EU, PP-PS (opt.), PP-BSN (opt.))	
	Stelsel eTD (Reeds gerealiseerd tbv legacy implementaties tijdelijk handhaven!)	**Input**: Identiteit AD, BSN, ControleGegevens **Output:** Bevestigingscode	
Geef Encrypted Pseudoniem	stelsel eTD eIDAS berichtenservice (in rol van eID AD)	**Input:** Identiteit AD/MR, Identiteit beoogd Ontvanger, Polymorf Pseudoniem **Output:** Encrypted Pseudoniem	Het faciliteren van het inlog proces middels een centrale service. Ter ondersteuning van het authenticatieproces levert BSNk een centrale dienst die een PolymorfPseudoniem omzet in een EncryptedPseudoniem.

Service Naam	consumer/ actor	objecten	Doel
Geef Sleutel Materiaal	eIDAS berichtenservice tbv Authenticate UIT Dienstverleners die gebruik maken van het stelsel eTD	**Input:** Identifier Dienstverlener **Output:** Decryptiesleutel NP[10] Decryptiesleutel BSN (optioneel)	Het verstrekken van sleutelmateriaal waarmee de Dienstverlener EncryptedPseudonyms kan ontsleutelen naar Pseudoniemen (of BSN's)

5.4.3 BSNk vereiste Interfaces

De BSNk vereist van het BRP-Koppelpuntdat op basis van het uniqueness ID gezocht kan worden op een BSN.

5.4.4 BSNk Uitwerking

5.4.4.1 *geefPolymorfPseudoniem*

geefPolymorfPseudoniem	
Doel	Het uitleveren van Polymorfe Pseudoniemen op basis van BSN en/of uniqueness ID.
Uitwerking	**Input:** BSN met controle gegevens OF uniqueness ID en versleuteld BSN Identiteit aanvrager **Output:** PolymorfPseudoniem(en) Ontvang het geefPolymorfPseudoniem verzoek. • Controleer of het verzoek is gedaan door een daartoe geautoriseerde partij op basis van matching op een entry in de BSNk geaggregeerde metadata set. Aanroep met BSN • Volg de standaard verwerking zoals gerealiseerd voor de legacy (Introductieplateau) 'Registratieproces'. Sla na voltooiing echter niet het BSN op, maar bereken op basis van deze een PP-BSN en een PP-PS.

[10] De decryptiesleutel PS wordt gebruikt voor het ontsleutelen van EP's die moeten leiden tot een Pseudoniem, het speelt hierbij geen rol of deze gecreëerd zijn op basis van PP-PS of PP-EU.

geefPolymorfPseudoniem	
	Aanroep met uniqueness ID en versleuteld BSN • Controleer dat het bericht afkomst is van EZ.Berichtenservice middels msg-lvl signature validatie. • Bereken het PP-EU op basis van de uniqueness ID. • Ontsleutel het BSN en bereken op basis van dit BSN ook een PP-BSN en op basis van een afgeleide van het BSN een PP-PS Response • Retourneer de berekende Polymorfe Pseudoniem(en).
Kenmerken	Het BSNk kent momenteel reeds een registratie functie (AD-KR https://afsprakenstelsel.etoegang.nl/display/as/Interface+specifications+AD-KR+1.9). Deze huidige functie waarbij een registratie wordt vastgelegd blijft (vooralsnog) gehandhaafd naast de nieuwe functies. De interface van de hierboven beschreven 2 nieuwe functies komen zoveel mogelijk overeen met bovengenoemde reeds gerealiseerde interface. Dit is een SOAP call. Deze startarchitectuur abstraheert de 3 verschijningsvormen naar 1 interface, in de detail uitwerking is het BSNk/BZK vrij om te bepalen hoe de interfaces worden gerealiseerd (als aparte diensten of geaggregeerd).

5.4.4.2 *geefEncryptedPseudoniem*

geefEncryptedPseudoniem	
Doel	Het uitleveren van een Dienstverleners specifiek Encrypted Pseudoniem op basis van het ontvangen Polymorf Pseudoniem.
Uitwerking	**Input:** Identiteit aanroeper (middels PKIo certificaat) Identiteit beoogde ontvanger (o.b.v. OIN) Het aanroeper specifiek Polymorf Pseudoniem. **Output:** Encryped Pseudodniem Ontvang het geefEncryptedPseudoniem verzoek. • Controleer of het verzoek is gedaan door een daartoe geautoriseerde partij op basis van matching op een entry in de BSNk geaggregeerde metadata set. • Controleer of het inputbericht volledig is. • Zet het ontvangen PP om in de EP voor gecommuniceerde beoogde

	ontvangende partij (NB dus andere dan de requester) • Stuur het berekende EP terug naar de aanroeper.
Kenmerken	De Identiteit van de aanroepende partij dient te worden vastgesteld op basis van een PKIo-certificaat; die te relateren moet zijn aan een entry in de geaggregeerde metadata van het BSNk. Vaststellen van identiteit van de aanroepende partij mag zowel op transport als berichtniveau worden gerealiseerd. De aanroepende partij MOET zorg dragen dat het PP gerandomiseerd wordt aangeleverd. BSNk hoeft *geen* technische controle in te bouwen om deze maatregel af te dwingen.

5.4.4.3 *geefSleutelMateriaal*

geefSleutelMateriaal	
Doel	Het uitleveren van een Dienstverleners specifiek sleutelmateriaal op basis waarvan de Dienstverlener een EncryptedPseudoniem ontsleuteld kan worden naar een dienstverlener specifiek persistent Pseudoniem (of BSN indien het een overheisdienstverlener betreft een een Encrypted Pseudoniem o.b.v. PP-BSN is aangemaakt)
Uitwerking	**Input:** Identiteit ontvanger op basis van een PKIo. **Output:** Sleutelmateriaal • Bepaal op basis van het in de dienstencatalogus gepubliceerde PKIo-certificaat de identiteit van de Dienstverlener in OIN-formaat. • Bereken op basis van deze identiteit het sleutelmateriaal. • Versleutel het resultaat met het publieke certificaat. • Verstrek deze aan de dienstverlener
Kenmerken	De Dienstverlener sleuteluitgifte verloopt via een Web(service) van het BSNk. De meeste actuele procedure zoals opgenomen vanuit het programma eID / BO BSNk is hiervoor leidend.

6 Privacy en informatiebeveiliging

Deze startarchitectuur is ontwikkeld met privacy by design, dataminimalisatie en passende informatieveiligheid. In dat licht hebben een privacy impact assessment en een risicoanalyse plaatsgevonden. Naar aanleiding van beide zijn maatregelen gedefinieerd die betrekking hebben op:

1. Dataminimalisatie
2. Logging & audit trail
3. Preventie van ongeautoriseerde toegang tot componenten
4. beschikbaarheid
5. Pseudonimisering
6. Versleuteling & integriteit

6.1 Kaderstelling

Wetgeving en voorschriften:

- eIDAS-verordening en Uitvoeringsverordeningen 2015/1501 en 2015/1502. Deze bevatten een aantal bepalingen die relevant zijn vanuit het oogpunt van privacy.
- Wet elektronisch berichtenverkeer belastingdienst, Besluit verwerking persoonsgegevens generieke digitale infrastructuur, Regeling voorzieningen GDI. Deze bevatten een grondslag voor en stellen regels aan (de verwerking van persoonsgegevens door) het BSNk. De toelichting bij het Besluit gaat ook in op de verwerkersrol die authenticatiediensten hebben ten aanzien van het BSN.
- Voorschrift Informatiebeveiliging Rijksdienst (VIR)
- Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie 2013 (VIR-BI 2013). Het VIR-BI 2013 geeft aan dat maatregelen proportioneel, efficiënt en effectief zijn in relatie tot de belangen. In de praktijk betekent dit doorgaans dat een risico analyse aan de basis van keuzes ligt.
- Wet Bescherming Persoonsgegevens (WBP). Hoe om te gaan met WBP is verder toegelicht in CBP Richtsnoeren Beveiliging van Persoonsgegevens (rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf).
- Algemene verordening gegevensbescherming (AVG)

Richtlijnen en normenkaders:

- Baseline Informatiebeveiliging Rijksdienst (BIR)
- NCSC ICT-Beveiligingsrichtlijnen voor webapplicaties
- ISO 27001 / 27002

De maatregelen waarmee privacy en informatieveiligheid gebord worden hebben ook betrekking op onderwerpen die buiten de reikwijdte van deze startarchitectuur vallen, zoals governance op de eIDAS keten. Dit hoofdstuk benoemt alleen de maatregelen op de implementatie van de verordening met de softwarecomponenten, gegevensbestanden en koppelingen die in deze startarchitectuur opgenomen zijn.

6.2 Dataminimalisatie

Deze startarchitectuur is ontwikkeld volgens het principe van dataminimalisatie: elke component in de oplossing krijgt alleen die informatie die nodig is voor correcte werking van de keten. Hiervoor sluit de startarchitectuur onder meer aan op de polymorfe pseudonimisering die in de volgende versie van eTD geïmplementeerd moet worden. Dit levert adequate afscherming van het BSN door gebruik van een slim pseudoniem en maskering van persoonsgegevens voor alle componenten die er niets mee hoeven te doen.

Extra aandacht gaat uit naar de verplichte attributen uit de minimale dataset. De eIDAS verordening schrijft voor dat bij elke inlog de verplichte attributen uit de minimale dataset geleverd worden. Oók als de dienstverlener niet alle attributen nodig heeft. Om te voorkomen dat attributen onnodig tussen componenten uitgewisseld worden, verwijdert de eIDAS berichtenservice de attributen die de Nederlandse dienstverlener niet nodig heeft uit het bericht.

Voor de matching en registratie van een persoon in het BRP krijgt het BRP koppelpunt alléén de verplichte attributen uit de minimale dataset van de natuurlijke persoon. Indien het BRP koppelpunt aanvullende attributen nodig heeft, dan stelt het daartoe specifiek een authenticatieverzoek op voor de eIDAS berichtenservice. Het BRP koppelpunt krijgt nooit attributen van de rechtspersoon. Dit voorkomt dat er onnodig attributen tussen de eIDAS berichtenservice en het BRP koppelpunt uitgewisseld worden.

Bij elke navolgende inlog voor een BSN dienst krijgt het BRP koppelpunt géén attributen van de natuurlijke persoon. Omdat de attributen niet van een ‘versheidsdatum’ zijn voorzien, kan niet worden beoordeeld of het attribuut een wijziging is ten opzichte van de geregistreerde waarde of dat het juist een oude waarde betreft. Bovendien wordt zo voorkomen dat het BRP koppelpunt attributen krijgt waarmee zij niet in alle gevallen wat doet. Nadeel is dat de BRP geen mogelijkheid heeft om via deze route de persoonsregistratie bij te werken op het moment dat persoonsgegevens (zoals de achternaam bij huwelijk) volautomatisch te wijzigen.

De Nederlandse dienstverlener mag binnen eTD niet meer attributen vragen dan het wettelijk recht op heeft. De benodigde attributen markeert hij per dienst in de eTD stelselcatalogus. Hierbij wordt per attribuut een doelbinding opgegeven zodat de gebruiker in staat is een ‘informed consent’ te geven. eTD stelt de Autoriteit Persoonsgegevens in staat om controle uit te oefenen op de gevraagde attributen in relatie tot de te verlenen dienst.

Het eIDAS knooppunt (eIDAS connector en eIDAS proxy) slaan geen gegevens op, anders dan voor logging & audittrail doeleinden. Logfiles worden voldoende sterk versleuteld om ongeautoriseerd gebruik ervan te voorkomen.

De eIDAS berichtenservice zorgt volgens dezelfde regels voor adequate logging & mogelijkheid tot audit trail. In aanvulling daarop registreert de eIDAS berichtenservice per UID de polymorfe pseudoniemen: PP-BSN, PP-PS en PP-EU). Waarbij de PP-BSN en PP-PS alleen van toepassing zijn indien de persoon minimaal ééns voor een BSN-dienst heeft ingelogd. Deze registratie is technisch

noodzakelijk, zodat het BSNk niet bij elke inlog opnieuw polymorfe pseudoniemen hoeft te berekenen. Het BSNk is niet ontwikkeld om deze pseudoniemen bij élke inlog te berekenen. Het niet beschikbaar zijn van deze functionaliteit in het BSNk zou direct betekenen dat grensoverschrijdend inloggen niet meer mogelijk is. Dat is een extra en ongewenste afhankelijkheid. Tevens heeft dit naar verwachting een stevige impact op de gebruikservaring vanwege langere doorlooptijden in elk inlogproces. De startarchitectuur beschouwt het opslaan van de pseudoniemen in de eIDAS berichtenservice daarom als technisch best passende oplossing.

Voor correcte werking van de eIDAS berichtenservice heeft het momenteel alleen de PP-EU (niet-BSN-dienst) en PP-BSN nodig (BSN-dienst). Tóch slaat de eIDAS berichtenservice bij afname van een BSN dienst de PP-PS op. Deze opslag wordt gerechtvaardigd door het (verwachte) voorschrift uit de uniforme set van eisen (wet GDI in wording) dat het PP-PS gebruikt moet worden om de gebruiker inzage te geven in het gebruik van zijn authenticatiemiddel. Dit moet misbruik sneller detecteerbaar maken en geeft de gebruiker meer inzicht en vertrouwen, terwijl zijn privacy gewaarborgd blijft. Het alternatief om met terugwerkende kracht per eID een PP.PS te laten bereken en persisteren zou onevenredig grote inspanningen en kosten met zich meebrengen.

De eTD componenten in deze architectuur volgen de eTD principes en afspraken voor dataminimalisatie. Deze worden hier niet verder toegelicht.

6.3 Logging & audit trail

De verschillende componenten in deze startarchitectuur kennen vanzelfsprekend elk een adequate logging en audit trail. Logfiles moeten adequaat versleuteld zijn. Elke wijziging in configuratie en data is inzichtelijk. Logfiles kunnen niet gewijzigd worden. Logfiles worden voor een passende periode bewaard en daarna vernietigd. Hierbij zal worden aangesloten op de kaders zoals wettelijk geborgd in de Uniforme set van Eisen.

6.4 Preventie van ongeautoriseerde toegang

Voor elk van de componenten is adequate toegangsbeveiliging belangrijk. De componenten moet in ieder geval voldoen aan de volgende eisen:

- de component draait op een adequaat beveiligde omgeving.
- de toegang is voorbehouden tot vooraf benoemde en daartoe geautoriseerde beheerders.
- de toegang van beheerders tot componenten kan direct ingetrokken worden.
- elke toegang – en elke wijziging in configuratie of data – is achteraf traceerbaar.

Hierbij geldt additioneel als specifieke maatregel voor het sleutelmateriaal:

- Gevoelig sleutelmateriaal, zoals de privé sleutels waarmee de NL eIDAS Knooppunt zich authenticeert richting de andere MS's zal, tijdig voor verplichtend karakter van de verordening in effect is, gepersisteerd zijn in een HSM van tenminste FIPS 140-2 Level 3.

6.5 Beschikbaarheid

De beschikbaarheidseisen aan de componenten is hoog. Elk van de componenten moet 7x24 beschikbaar zijn . Voor de eIDAS berichtenservice betekent dit:

1. Volledig dubbele uitvoering
2. Aansluiting op twee eTD makelaars, om onbeschikbaarheid van een makelaar te ondervangen

6.6 Pseudonimisering

Eén van de binnen deze startarchitectuur beschreven wijzigingen op het afsprakenstelsel eTD is de overgang naar Polymorfe Pseudoniemen als Pseudonimiseringsvorm. Polymorfe Pseudoniemen zorgen ervoor dat partijen met elkaar kunnen communiceren over personen op een betrouwbare, veilige, vertrouwelijke manier. Polymorfe Pseudoniemen zijn gebaseerd op een beproefde versleutelings technologie. De technologie zelf kan nagelezen worden in o.a. het volgende document; [https://www.idensys.nl/fileadmin/bestanden/idensys/documenten/basisdocumentatie/documentatieset/PP_Scheme_091.pdf]. Hieronder volgt een korte functionele beschrijving van de werking;

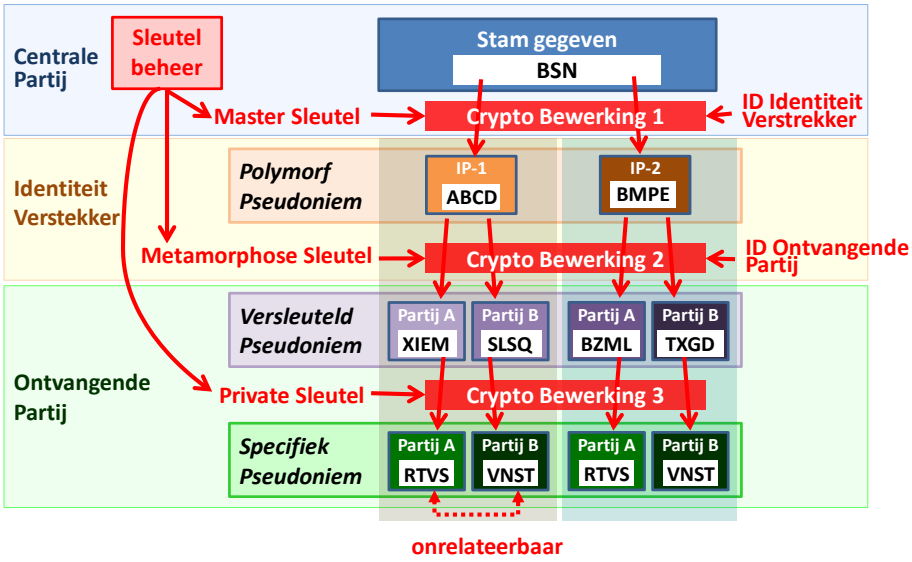
Ontwerp op basis van Polymorfe Pseudoniemen
Praktisch gezien krijgt elke partij voor elke persoon die hij kent een eigen Pseudoniem. Dit pseudoniem is alleen bekend bij deze partij zelf, en door geen enkele andere partij. Zelfs niet de authenticatiedienst die over dit pseudoniem verklaard of afgeeft. Daarbij zal dit Pseudoniem ongeacht de gerandomiseerde verschijningsvormen van Polymorf en Encrypted Pseudoniem, of de hierbij gebruikte Authenticatiedienst altijd de zelfde waarde bevatten binnen het domein van een ontvangende partij.

Identiteit Verstrekker
Om het voorgaande mogelijk te maken is er een centrale partij nodig die op basis van een unieke identiteit een *'Polymorf Pseudoniem'* van een persoon kan maken. Deze Centrale Partij kan dat doen op verzoek van een partij die de taak heeft om de Identiteit van een persoon te verstrekken aan andere partijen. Zo'n Identiteit Verstrekker zal meestal een Authenticatiedienst zijn, maar het kan ook een andere rol hebben, zoals bijvoorbeeld een Machtigingsregister.

Polymorf Pseudoniem
De Polymorf Pseudoniem is versleuteld en gerandomiseerd en hij is alleen bruikbaar door de Identiteit Verstrekker die hem heeft aangevraagd. Daar bovenop bezit het Polymorf Pseudoniem de eigenschap dat deze met een cryptografische bewerking specifiek gemaakt worden voor een derde Ontvangende Partij. Het Polymorfe Pseudoniem moet dus als het ware nog een cryptografische metamorfose ondergaan om van zijn a-specifieke vorm naar een Ontvangende Partij specifieke Versleutelde Pseudoniem te transformeren.

Andere partijen (dan de Identiteit Verstrekker) kunnen niet zelf een Versleutelde Pseudoniem maken voor een derde partij, maar zij kunnen die wel aanvragen bij zo'n Identiteit Verstrekker. Zo kan partij_A bij een authenticatie van een Gebruiker behalve zijn eigen versleutelde Pseudoniem_A ook een Versleutelde Pseudoniem_B ten behoeve van partij_B aanvragen, liefst met gebruikers

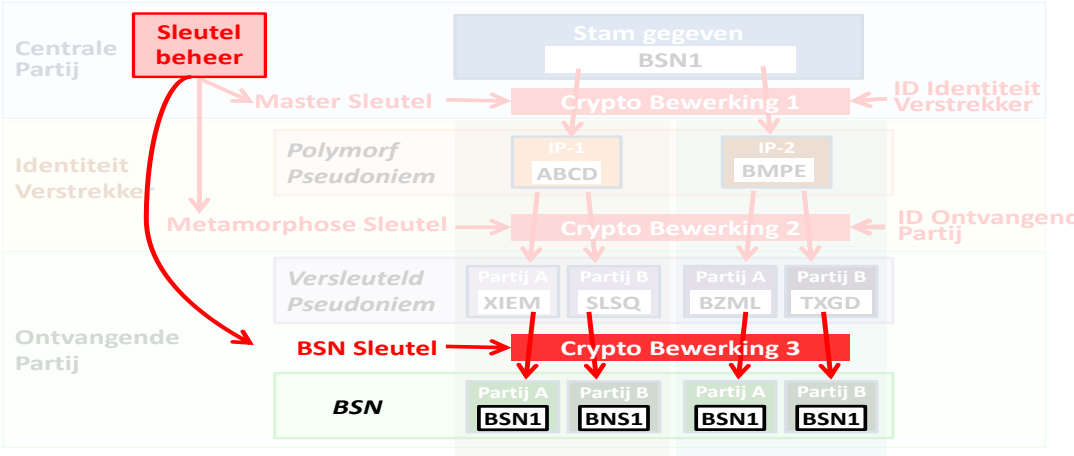
instemming. Daarmee kan hij met partij_B over deze persoon communiceren zonder het (onversleutelde) Specifieke Pseudoniem van partij_B te kennen[11].



Figuur 7: (functionele) Werking versleuteling voor Polymorfe Pseudoniemen

Overheid en Polymorfe Pseudoniemen

Een typische eigenschap van een Polymorfe Pseudoniem is dat er ook een BSN in 'verstopt' kan zitten (PP-BSN). Dit BSN zit dan ook in de daarvan afgeleide gerandomiseerde versleutelde pseudoniem. Een partij die geautoriseerd is voor een BSN kan dan met speciaal sleutelmateriaal een BSN uit het Versleutelde Pseudoniem halen in plaats van een specifiek Pseudoniem. Het is deze architectuur welke naar alle waarschijnlijk voorgeschreven zal gaan worden als wettelijke uniforme eisen door BZK voor het gebruik van authenticatiemiddelen in het publieke domein.



Figuur 8: Werking Polymorfe Pseudoniemen in BSN domein

[11] *Elke partij kan een persoon aanwijzen bij een andere partij zonder dat deze partijen daarover eerst een afspraak hebben gemaakt en zonder dat een partij daarbij een identificerende persoonskenmerk onthult of een nieuwe ontstaat.*

Noodzaak voor (gegarandeerd BSN-loze) Pseudoniemen
Echter binnen de overheidssector zijn ook situaties waarbij geen BSN nodig is of waar privacy zelfs zodanig gevoelig is dat een partij perse geen BSN mag kunnen halen uit de Versleutelde Pseudoniem. Een voorbeeld hiervan is de in deze startarchitectuur beschreven noodzaak voor het opleveren van een over AD's persistent pseudoniem aan de EZ-eIDAS Berichtenservice ten bate van het ondersteunen van een persistente uniqueness ID.

Andere voorbeelden zijn o.a. privacy gevoelige diensten die een Gebruiker moeten kunnen herkennen en toch garanderen dat hij niet in de echte wereld geïdentificeerd kan worden via zijn BSN of andere persoonsgegevens. Bijv referenda, enquêtes, inspraak, petities of meldpunten. Of voorzieningen tbv misbruikbestrijding als inzagediensten.
Ook voor de inzet van bredere functionaliteit als bevoegdheden o.b.v. machtigingen of rol (arts, apotheker, advocaat, leraar) is er een noodzaak voor de Dienstverlener om gebruik te maken van persistente pseudoniemen.

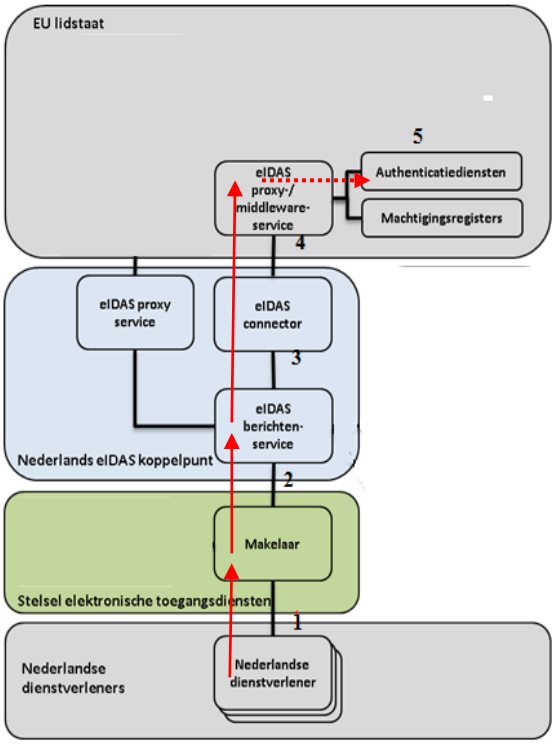
6.7 Versleuteling & integriteit

De eIDAS berichtenservice registreert de polymorfe pseudoniemen bij de UID's van personen die met een buitenlands middel ingelogd hebben. De UID's als een hash opgeslagen, zodat de UID niet uit de registratie te herleiden is. Als een persoon voor een tweede maal inlogt, dan wordt conform hetzelfde hashingmechnisme dezelfde hash berekend, zodat de eIDAS berichtenservice het bijbehorende pseudoniem uit kan lezen. Alle attributen in de tabel worden voorts versleuteld opgeslagen.

Voor de communicatie tussen de componenten wordt allereerst aangesloten bij het voorgeschreven eIDAS interoperabiliteitsnetwerk (voor grensoverschrijdende communicatie) en de vereisten van het eTD stelsel. Daarnaast wordt - daar waar binnen deze twee kaders toegestaan – voor communicatie tussen componenten steeds gebruik gemaakt van een artefict resolve via een backchannel. Navolgende geeft inzicht in de gebruikte communicatievorm en integriteit/endpoints over de componenten heen bij grensoverschrijdende authenticatie;

Authenticatie met een Europees eID voor een Nederlandse Dienstverlener

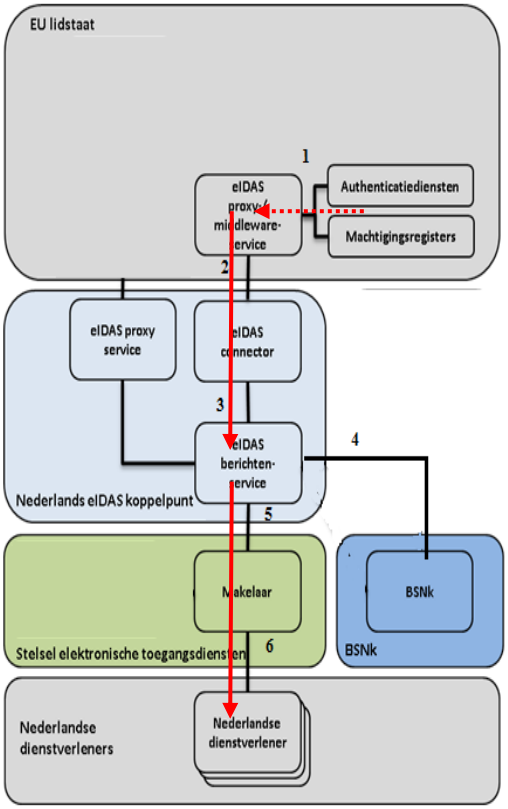
Authenticatieverzoek



Rode pijlen tonen E2E encryptie/integriteit

#	Gedrag
1	Nederlandse Dienstverlener stuurt gebruiker met authenticatieverzoek naar makelaar (middels Artifact binding)
2	Makelaar zet het authenticatieverzoek door naar de EZ-eIDAS Berichtenservice; als ware deze een Authenticatiedienst (Artifact binding)
3	De EZ eIDAS-Berichtenservice zet het Authenticatieverzoek door naar de NL-eIDAS-Connector (Artifact Binding)
4	De NL-eIDAS-Connector zet het bericht door naar de MS-eIDAS-Proxy of Middleware service. (Post-binding)
5	De MS-eIDAS Service set het authenticatieverzoek door naar het nationale eID-Stelsel. (MS-specifiek)

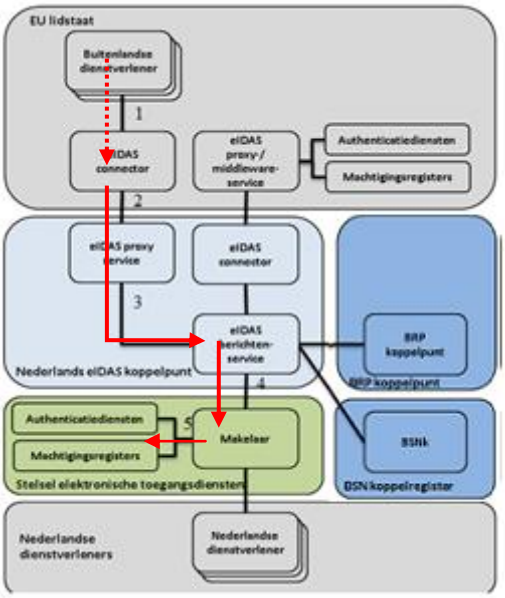
Authenticatieresultaat



#	Gedrag
1	MS-eID stuurt gebruiker met het Authenticatieresultaat naar MS-Proxy/ Middleware service (MS-specifiek)
2	MS-Proxy/Middleware service stuurt gebruiker met authenticatieresultaat door naar NL eIDAS-Connector (Post binding)
3	De EZ eIDAS-Connector stuurt gebruiker met authenticatieresultaat door naar BerichtenService (Artifact Binding)
4	De BerichtenService roept geefEP aan bij BSNk om het PP in een DV-specifiek EP om te laten zetten. (backchannel)
5	De BerichtenService stuurt de gebruiker met het authenticatieresultaat door naar de makelaar (Artifact binding)
6	De makelaar stuurt de gebruiker met het authenticatieverzoek door naar dienstverlener (Artifact binding)

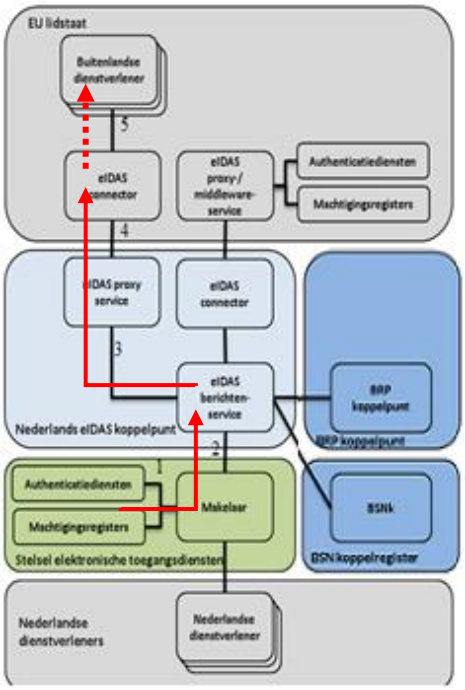
Authenticatie met een Nederlands eID voor een Europese Dienstverlener

Authenticatieverzoek



#	Gedrag
1	MS Dienstverlener stuurt gebruiker met authenticatieverzoek naar MS-eIDAS Connector (MS-Keuze)
2	MS eIDAS Connector stuurt gebruiker met authenticatieverzoek naar NL eIDAS-Proxy (POST-Binding))
3	NL-eIDAS Proxy stuurt gebruiker met Authenticatieverzoek naar eIDAS-Berichtenservice (Artifact Binding)
4	eIDAS berichtenservice stuurt gebruiker naar Makelaar (Artifact-binding)
5	Makelaar stuurt gebruiker naar AD of/en naar de MR

Authenticatieresultaat



#	Gedrag
1	De Authenticatiedienst (of en MR) stuur de gebruiker met Authenticatieresultaat naar Makelaar (Artifact binding)
2	De Makelaar stuurt gebruiker met authenticatieresultaat naar Berichtenservice (Artifact-binding)
3	De Berichtenservice stuurt gebruiker met AuthResultaat naar NL-eIDAS Proxy (Artifact Binding)
4	De NL eIDAS Proxy stuurt gebruiker naar MS-Connector (Post-Binding)
5	De MS-Connector stuurt gebruiker met Authenticatie resultaat naar MS-Dienstverlener (Keuze MS)

7 Beheer & exploitatie

Aandachtspunt voor de realisatie van de benoemde componenten is dat deze in samenhang moeten voldoen aan de eisen die worden gesteld aan de functionaliteit welke ze gedeeld uitvoeren. Dit geldt voor het geheel als incidentmanagement, changemanagement en monitoren. Vooral dient er een maximale inspanning geleverd te worden om de benoemde service niveau overeenkomsten zoals opgenomen in het afspraken stelsel eTD te kunnen leveren[12].

Voor de realisatie en exploitatie betreft het hier met name de aspecten performance en beschikbaarheid. Doordat functionaliteit gezamenlijk door meerdere componenten wordt geleverd zal hier een verdeelsleutel bepaald moeten worden.
Deze detaillering zal later worden uitgewerkt zodat de exacte eisen voor elke van de afzonderlijke componenten SMART gemaakt kunnen worden. Voor de uitwerking wordt nu volstaan met het uitgangspunt dat in realisatie en exploitatie afwegingen de non-functional performance en availability zwaar dienen te wegen. Er moet in alle redelijkheid gestreefd worden naar snelle, hoog-beschikbare realisaties.

[12] Er dient gestreefd te worden dat de gebruikersbeleving ondanks de vele schakels acceptabel blijf. De gemiddelde response tijd voor de gebruiker tussen (zichtbare) schermen zou in de meeste gevallen niet meer dan 3 seconden, en tenminste ij 99% van de gevallen niet langer dan 5 seconden moeten duren. Indien het moment tussen voor de gebruiker zichtbare interactie deze waarden overschrijdt zou de gebruiker geïnformeerd moeten worden over het onderhanden proces

8 Begrippenlijst

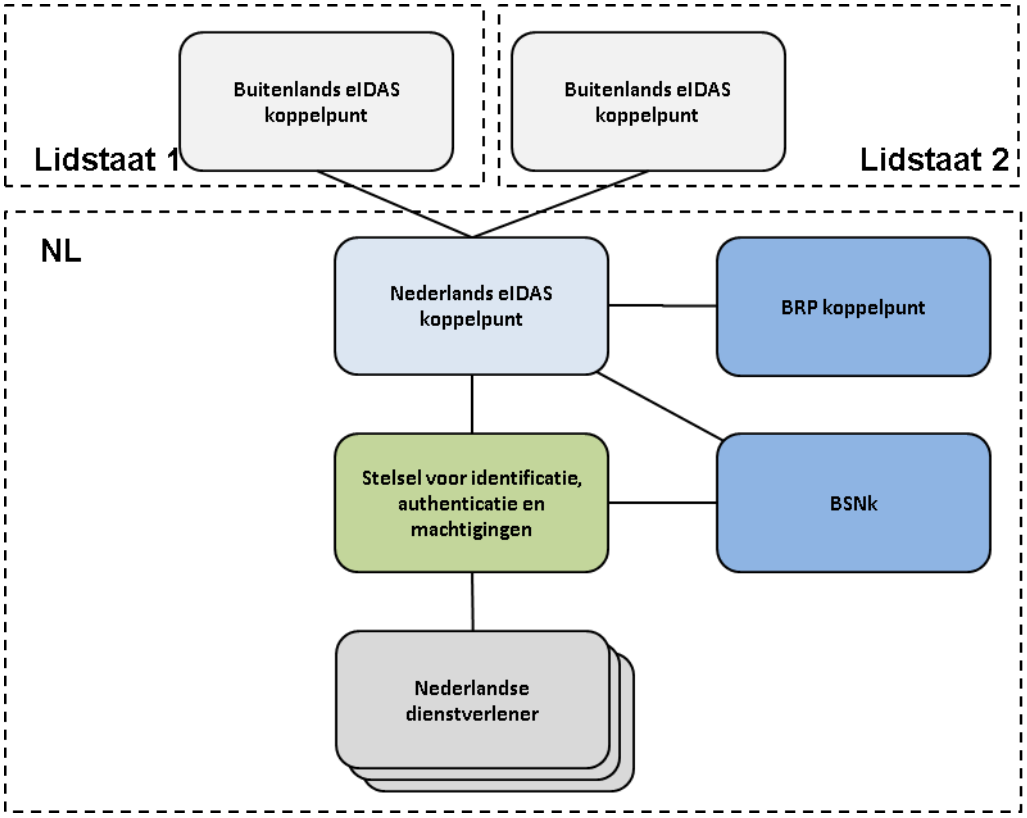
Begrip	Omschrijving
eIDAS Berichtenservice	De berichtenservice functioneert als adapter tussen de eIDAS nodes en het Nederlandse eID stelsel. Hiermee wordt gefaciliteerd dat voor beide componenten de integratie (grotendeels) transparant is. De berichtenservice gedraagt zich als Authenticatiedienst richting het stelsel en als dienstverlener richting de Nodes voor authenticatie met een buitenlands middel. Voor authenticatie met een Nederlands middel gedraagt de berichtenservice zich als Dienstverlener richting het stelsel en als Authenticatiedienst richting de eIDAS Nodes.
BRP-Koppelpunt	Het BRP-Koppelpunt faciliteert het matchen op of toekennen van, een Nederlandse identiteit (BSN) aan een Europese burger.
BSNk	Het BSN-Koppelregister is een publieke voorziening geleverd door BZK die faciliteert in de uitgifte en communicatie van het de elektronische identiteit voor natuurlijke personen.
BSN dienst	Een dienst waarvoor de dienstverlener wettelijk het recht heeft om het BSN te verwerken. De dienstverlener kan een publieke of private organisatie zijn. Een dienstverlener is publiek wanneer het een bestuursorgaan in de zin van artikel 1:1 Awb betreft, maar ook wanneer het andere overheidsorganen alsmede natuurlijke en rechtspersonen, niet zijnde overheidsorganen betreft, die vanwege het uitoefenen van een publieke taak gerechtigd zijn het burgerservicenummer te gebruiken. Het si de verantwoordelijkheid van de dienstverlener om in de eTD dienstencatalogus aan te geven of een dienst een publieke dienst is en of de dienst een BSN-dienst is. De dienstverlener onderbouwt dat met een verwijzing naar de relevante wetsartikelen.
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
EER	Europese Economische Ruimte
EP	Zie Encrypted Pseudoniem
EU	Europese Unie
eTD	Afsprakenstelsel Elektronische Toegangsdiensten

EZ	Ministerie van Economische Zaken
MS	Member State (een Europese lidstaat)
MS Dienstverlener	Een Member State Dienstverlener biedt elektronische diensten aan waarvoor een genotificeerd stelsel gebruikt kan worden als Toegangsdienst.
MS eID	Een Member State eID is een genotificeerd eID waarvan de authenticatieresultaten door Nederlandse (publieke) diensten herkend dienen te worden.
MS eID Connector	Een MS-eID Connector geeft het Authenticatieverzoek van een buitenlandse dienstverlener door aan de NL eIDAS Proxy om te faciliteren dat er via het stelsel eTD toegang verleend kan worden
MS eID Service	Een MS-eID Service heeft de verschijningsvorm van een Proxy of Middleware en geeft het Authenticatieresultaat van een buitenlandse eID door aan de NL eID Connector om te faciliteren dat er via een genotificeerd lidstaat eID-stelsel toegang verleend kan worden tot Nederlandse diensten.
NL Dienstverlener	Een entiteit die digitale diensten aanbiedt waarvoor authenticatie vereist en die is aangesloten op het stelsel eTD voor deze authenticatie.
NL eIDAS-Connector	Een component die Nederland inzet om het authenticatieverzoek vanuit een Nederlandse Dienstverlener door te zetten richting de beoogde MS eIDAS Service (Proxy/middelware)
NL eIDAS-proxy Service	De NL eIDAS Proxy waaraan een MS eIDAS Connector het authenticatieverzoek van een lokale lidstaat kan delegeren
NL eIDAS knooppunt	Het samenstel van de eIDAS proxy service en de eIDAS connector.
NL eTD Stelsel	Het Nederlandse Stelsel, Elektronische toegangsdiensten.
PP	Zie Polymorf Pseudoniem
Polymorf Pseudoniem	Een AuthenticatieDienst en/of Machtigingsregister specifiek bouwblok waaruit een ontvanger specifiek Encrypted Pseudoniem kan worden berekend. Een Polymorf Pseudoniem is randomiseerbaar waardoor relateerbaarheid tussen verschillende transacties vermeden kan worden

Encrypted Pseudoniem	Een voor een specifieke dienstverlener versleuteld pseudoniem, op basis van een Polymorf Pseudoniem. Ontsleuteling levert, afhankelijk van de gebruiksscenario een BSN of pseudoniem op. Een Encrypted Pseudoniem is randomiseerbaar waardoor relateerbaarheid tussen verschillende transacties vermeden kan worden
Pseudoniem	Een permant identificerend kenmerk van de uitvoerend natuurlijk persoon. Een pseudoniem is uniek per combinatie ontvangende partij en persoon, maar gelijk ongeacht de gebruikte authenticatie en machtigingsdienst

Bijlage 1 Context en doelarchitectuur – stelselonafhankelijk

Deze bijlage beschrijft de context en doelarchitectuur op een stelselonafhankelijke wijze.



Figuur 9: Context Doelarchitectuur (stelsel onafhankelijk)

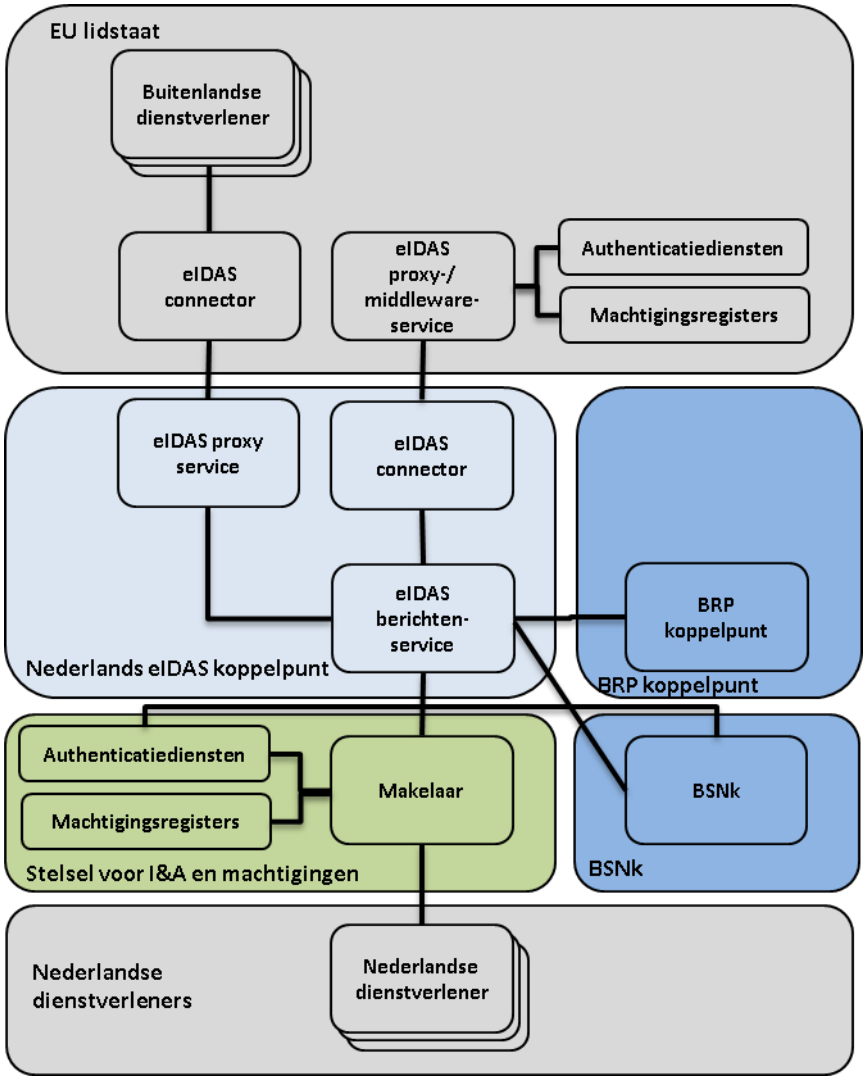
De Nederlandse oplossing voor grensoverschrijdende digitale toegang onderscheidt de volgende hoofdcomponenten:

- De Nederlandse dienstverlener: de organisatie die haar diensten digitaal open heeft gesteld voor dienstafnemers in Europa. Voor publieke dienstverleners is het toestaan van buitenlandse inlogs vanaf september 2018 onder voorwaarden verplicht, voor private dienstverleners optioneel.
- Stelsel voor identificatie, authenticatie en machtigingen: de oplossing die aan Nederlandse dienstverleners toegangsfunctionaliteit levert en Nederlandse authenticatiediensten en machtigingenregisters ontsluit voor het Nederlandse eIDAS koppelpunt.
- Het BRP koppelpunt: de voorziening die ervoor zorgt dat koppeling van natuurlijke personen aan een BSN plaatsvindt. Dit zijn zowel ingezetenen en niet-ingezetenen.
- Het BSNk voor het (1) koppelen van authenticatiemiddelen aan het BSN en (2) het uitgeven van Polymorfe Pseudoniemen ter identificatie van natuurlijke personen.
- Het Nederlands eIDAS koppelpunt: De voorziening die ervoor zorgt dat Nederland aan de andere Europese lidstaten gekoppeld is. Het koppelpunt faciliteert enerzijds het inloggen door Europese personen bij Nederlandse dienstverleners en anderzijds het inloggen van personen met een

Nederlands authenticatiemiddel bij buitenlandse dienstverleners. Daarvoor onderhoudt het koppelingen naar elk van de buitenlandse eIDAS koppelpunten en naar de functie voor identificatie, authenticatie en machtigingen.

- Buitenlandse eIDAS koppelpunten. De tegenhangers van het Nederlandse eIDAS koppelpunt in elk van de andere lidstaten. De communicatie tussen de eIDAS koppelpunten is in de eIDAS interoperabiliteitsarchitectuur en bijbehorende SAML berichtspecificatie geüniformeerd.

Navolgende componentdiagram geeft inzicht in de implementatie van de eIDAS Verordening. Het contextdiagram visualiseert het aandachts- en verandergebied.



Figuur 10: Componenten van de doelarchitectuur (stelsel onafhankelijk)

Het stelsel voor identificatie, authenticatie en machtigingen omvat de deelfuncties:

- Makelaar: de functionaliteit die de dienstverlener ontzorgt ten aanzien van identificatie, authenticatie en machtigingen.

- Authenticatiedienst: de functionaliteit die zorgt voor identificatie & authenticatie van personen.
- Machtigingsregister: de functionaliteit die zorgt voor registratie en ontsluiting van informatie over de bevoegdheden van personen.

Bijlage 2 Implementatievarianten en fasering

De implementatie van deze startarchitectuur hoeft niet ineens plaats te vinden. Deze bijlage beschrijft langs welke deelimplementaties de architectuur gerealiseerd kan worden. Daarbij is wordt opgemerkt dat de fasering niet dwingend is. Het is niet nodig om elke implementatievariant te implementeren. Er mogen varianten overgeslagen worden indien een grotere stap op dat moment haalbaar wordt geacht. De indeling in implementatievarianten heeft tot doel om besluitvorming te ondersteunen over gecontroleerde en beheerste implementatie.

De faseringsmogelijkheden zijn gescheiden voor use case 2 (inkomende authenticatie) en use case 3 (uitgaande authenticatie). Er is vanuit architectuur geen strikte noodzaak om beide te implementeren of beide gelijktijdig te implementeren.

De fasering is opgebouwd naar toenemende complexiteit van de oplossing en toenemende afhankelijkheid tussen de componenten onderling. Er is geen rekening gehouden met politieke, bestuurlijke of projectmatige ambities.

De componenten en koppelingen die in scope zijn van een uitvoeringsvariant zijn rood en vetgedrukt weergegeven.

Use case 2: authenticatie door een persoon met een buitenlands middel bij een NL dienstverlener

Implementatievarianten:

1. Implementatie zonder BSN
2. implementatie met BSN voor reeds geregistreerde personen
3. Implementatie met BSN voor nog onbekende personen

IN Variant 1

Implementatie zonder BSN

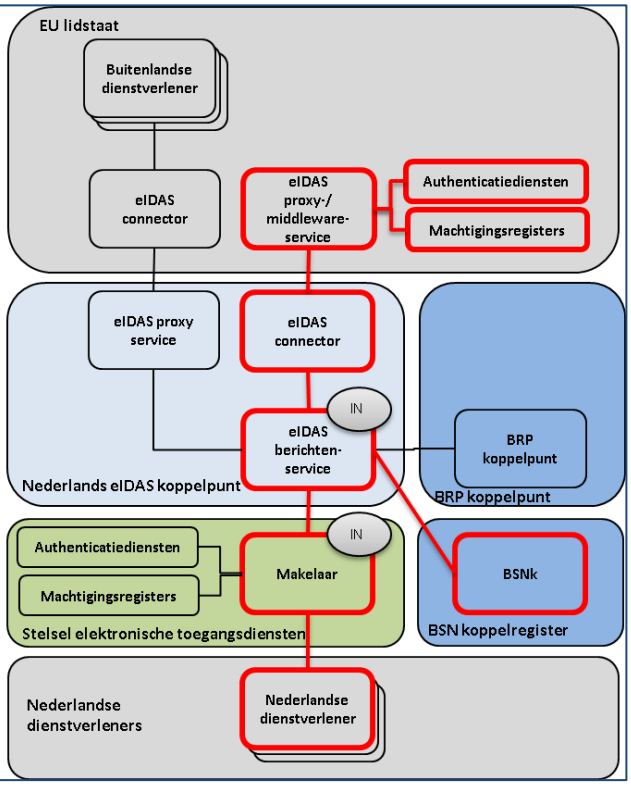
Voldoen aan de vereisten uit de verordening. Volgens de regel van de verordening.

Beperking:

- Levert geen BSN voor publieke diensten

Inzetbaar voor:

- Alle inlogs met een EU middel
- Waarbij in geval van een BSN-dienst de dienstverlener zelf het BSN moet achterhalen of laten registreren.



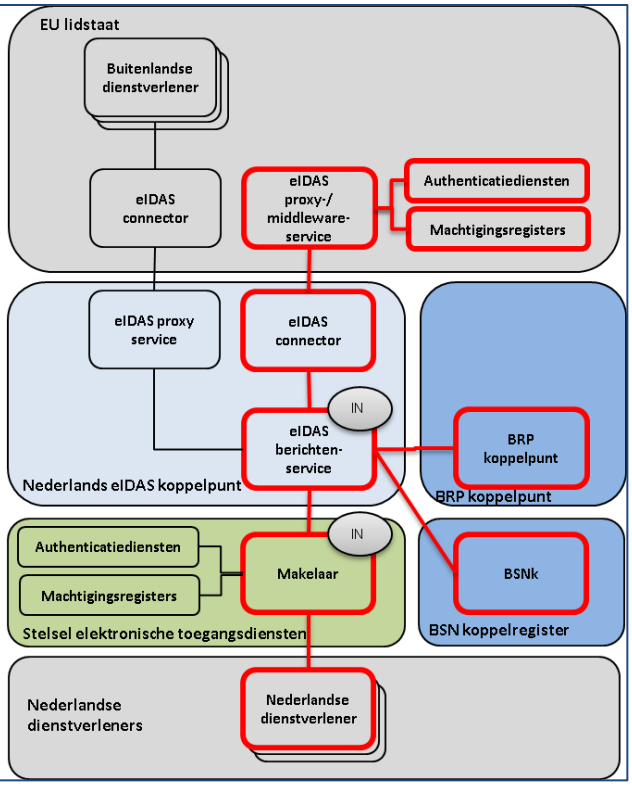
IN Variant 2

Implementatie met BSN voor reeds geregistreerde personen

Faciliteren van het inloggen van burgers op BSN diensten voor zover de persoon die inlogt al in het BRP geregistreerd is.

Beperking:
- Zorgt niet voor centrale registratie van onbekende personen.

Inzetbaar voor:
- Alle inlogs met een EU middel
- Waarbij de dienstverlener zelf moet zorgen voor opname van de buitenlandse persoon in BRP indien die persoon een BSN-dienst wil afnemen en nog niet in BRP staat.



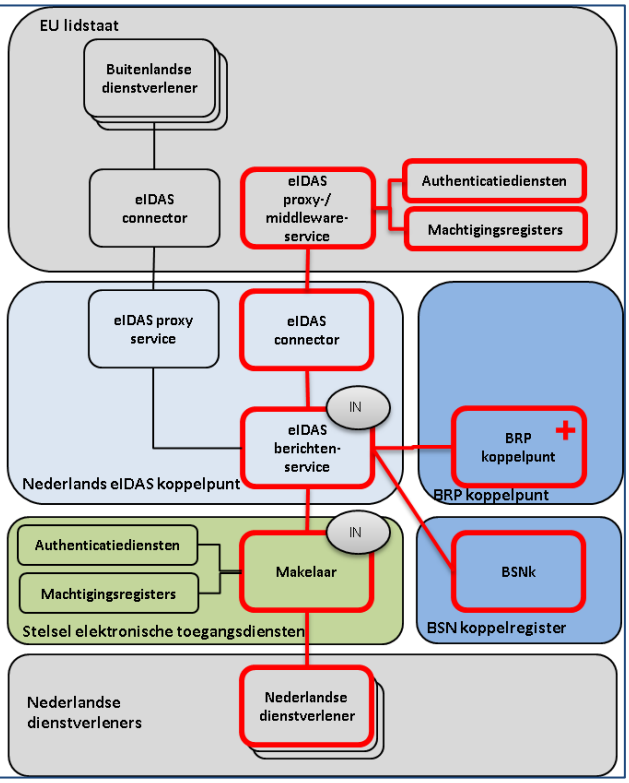
IN Variant 3

Implementatie met BSN voor nog onbekende personen

Leveren van volledige ondersteuning voor het inloggen van personen met een buitenlands middel.

Beperking:
- geen

Inzetbaar:
- Volledig voor burgers en bedrijven
- Volledig voor publieke én private dienstverleners
- Volledig voor BSN diensten en niet-BS diensten
- Volledig voor al in BRP geregistreerde personen
- Volledig voor nog niet in BRP geregistreerde personen

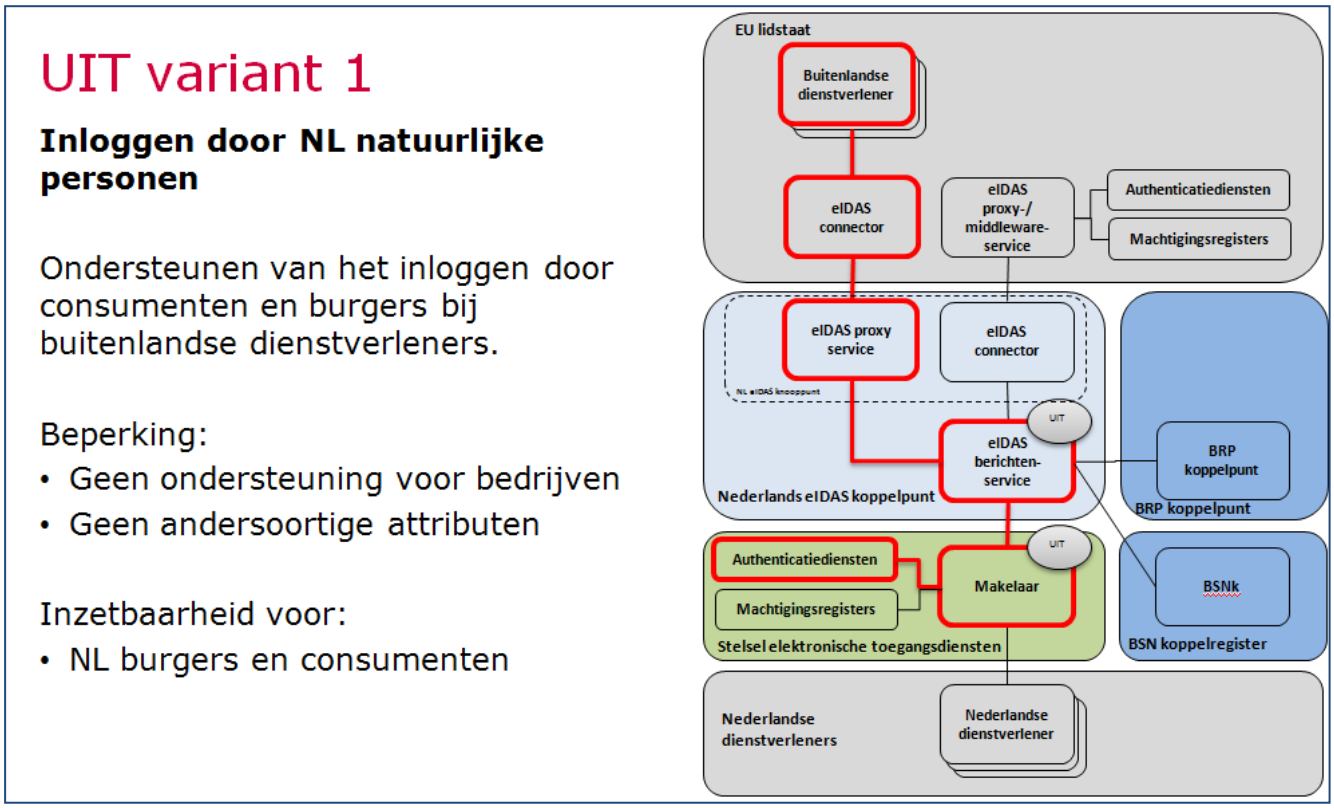


Use case 3: authenticatie door een persoon met een NL middel bij een buitenlandse dienstverlener

Implementatievarianten:

1. Inloggen door NL natuurlijke personen
2. Inloggen door NL natuurlijke personen en rechtspersonen
3. Uitbreiding met levering van andersoortige attributen

NB: voor implementatie van de TAXUD pilot voldoet alleen de implementatievariant 3.



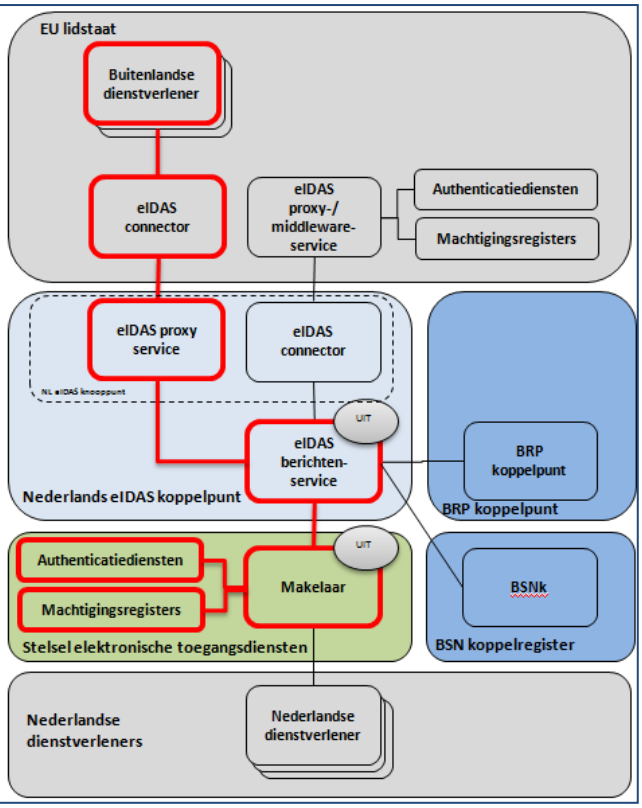
UIT variant 2

Inloggen door NL rechtspersonen

Ook ondersteunen van het inloggen door (medewerkers van) NL bedrijven bij buitenlandse dienstverleners.

Beperking:
- Geen andersoortige attributen

Inzetbaarheid voor:
- NL burgers en consumenten
- NL bedrijven



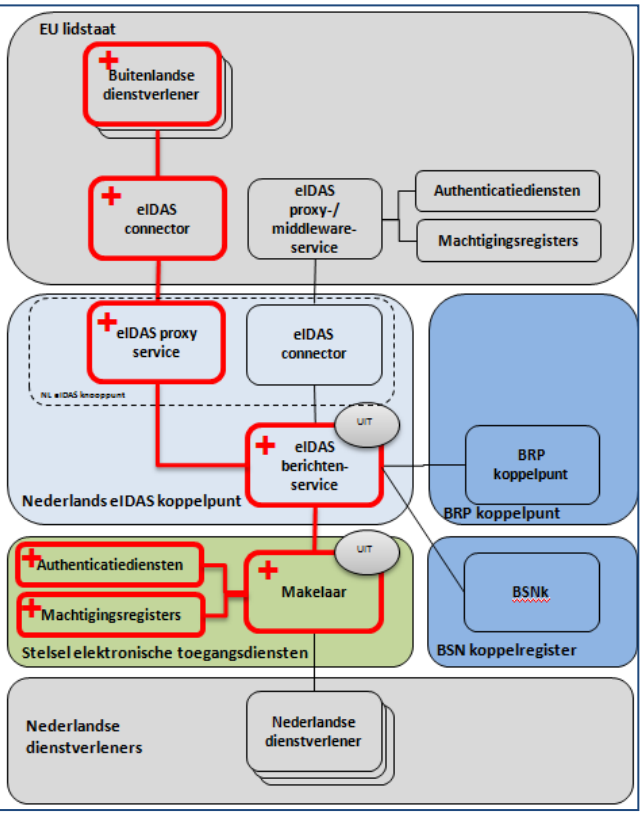
UIT variant 3

Ook andersoortige attributen

Extra attributen leveren aan buitenlandse dienstverlener.

Beperking:
- Geen

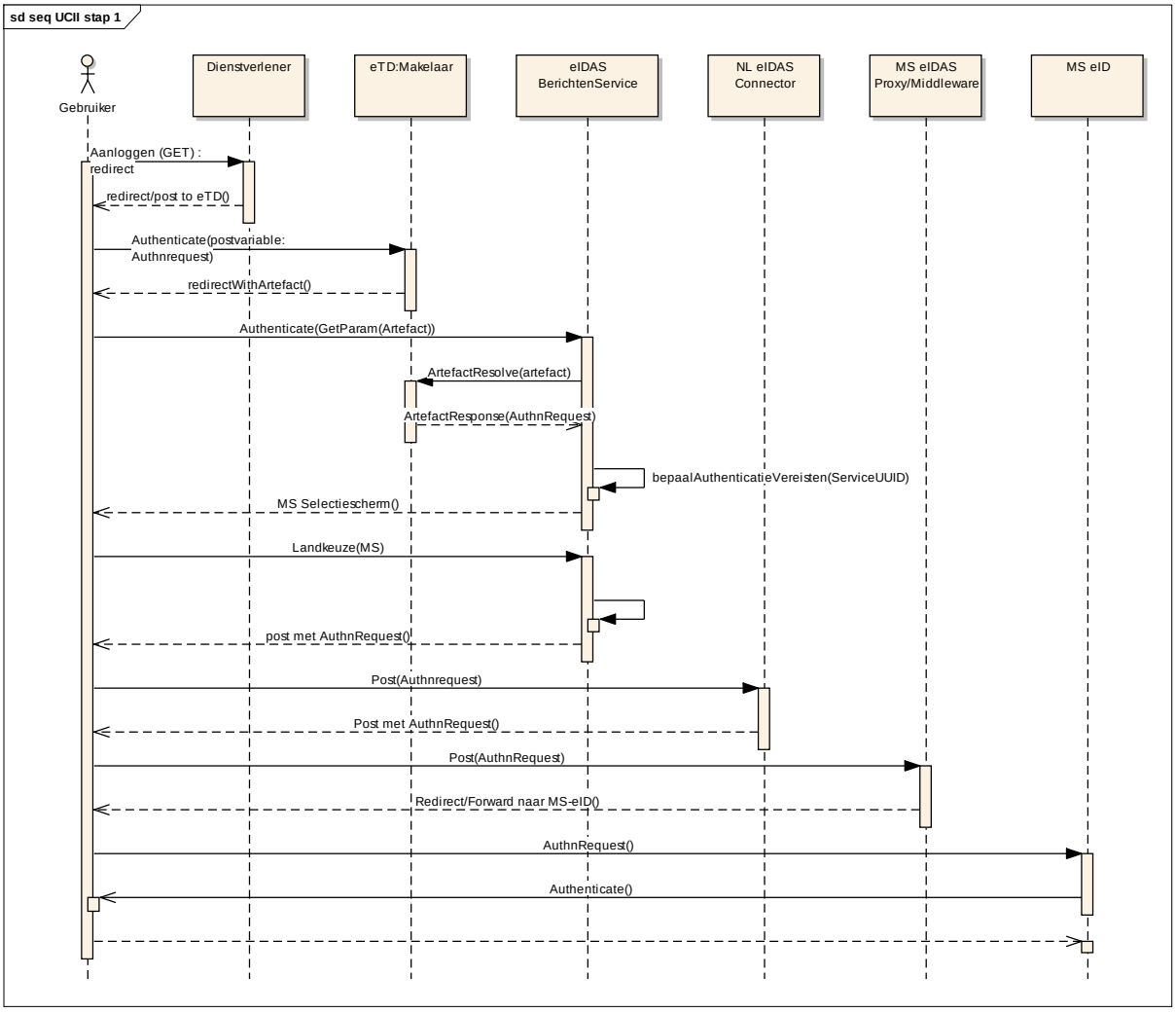
Inzetbaarheid voor:
- NL burgers en consumenten
- NL bedrijven



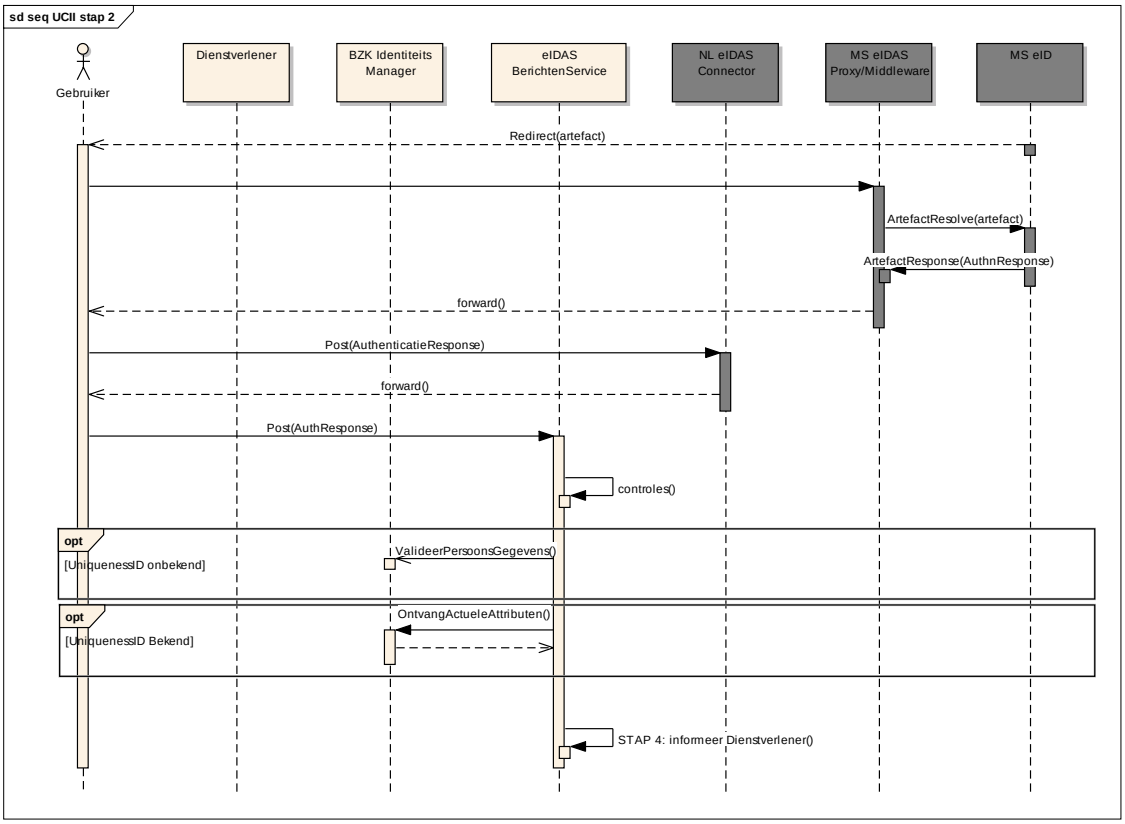
Bijlage 3 Interactie Flow bij Use Cases

Use case IIA: EU / EER ingezetene logt in bij dienstverlener in Nederland

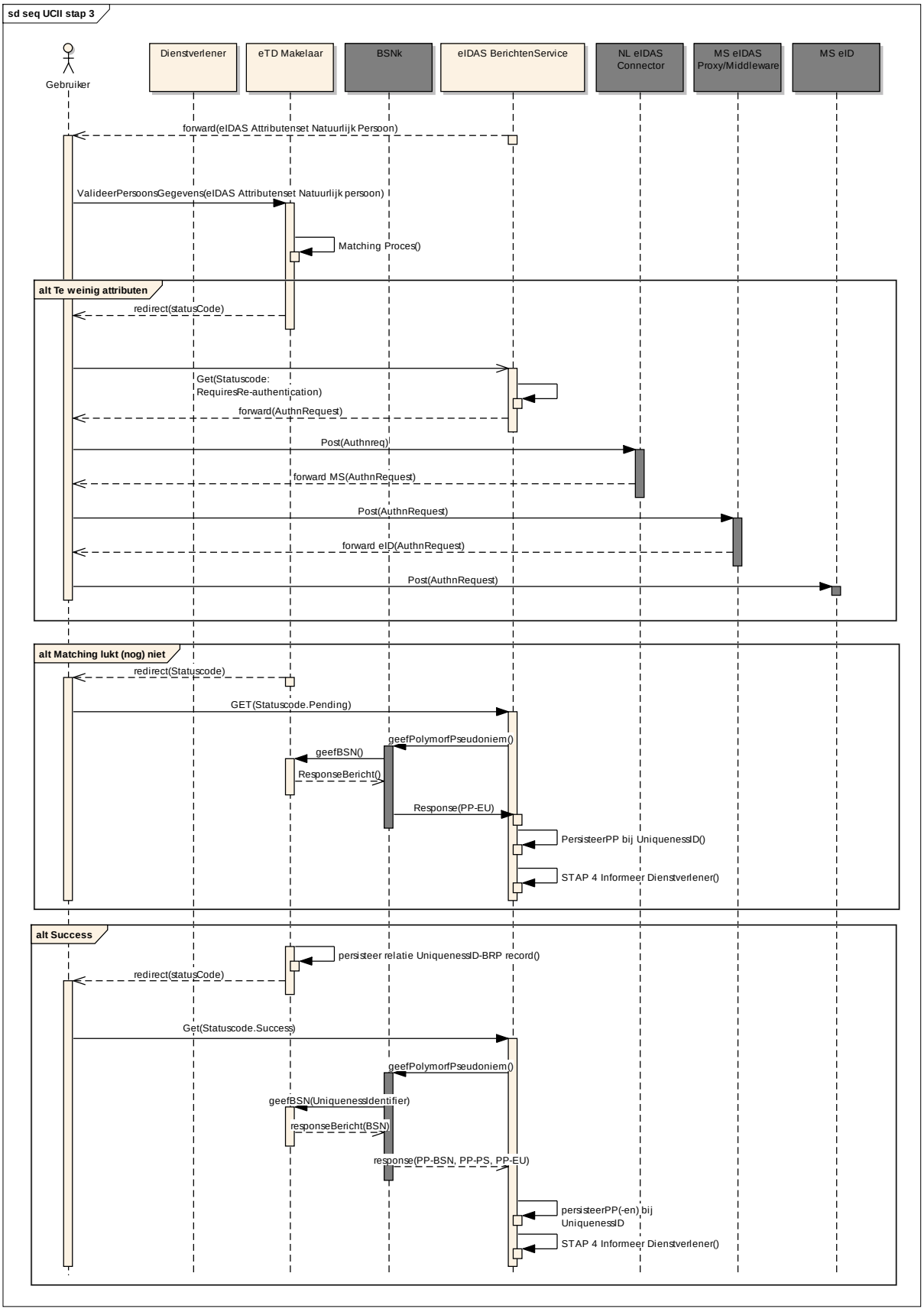
Use case IIA Stap 1: Interactie



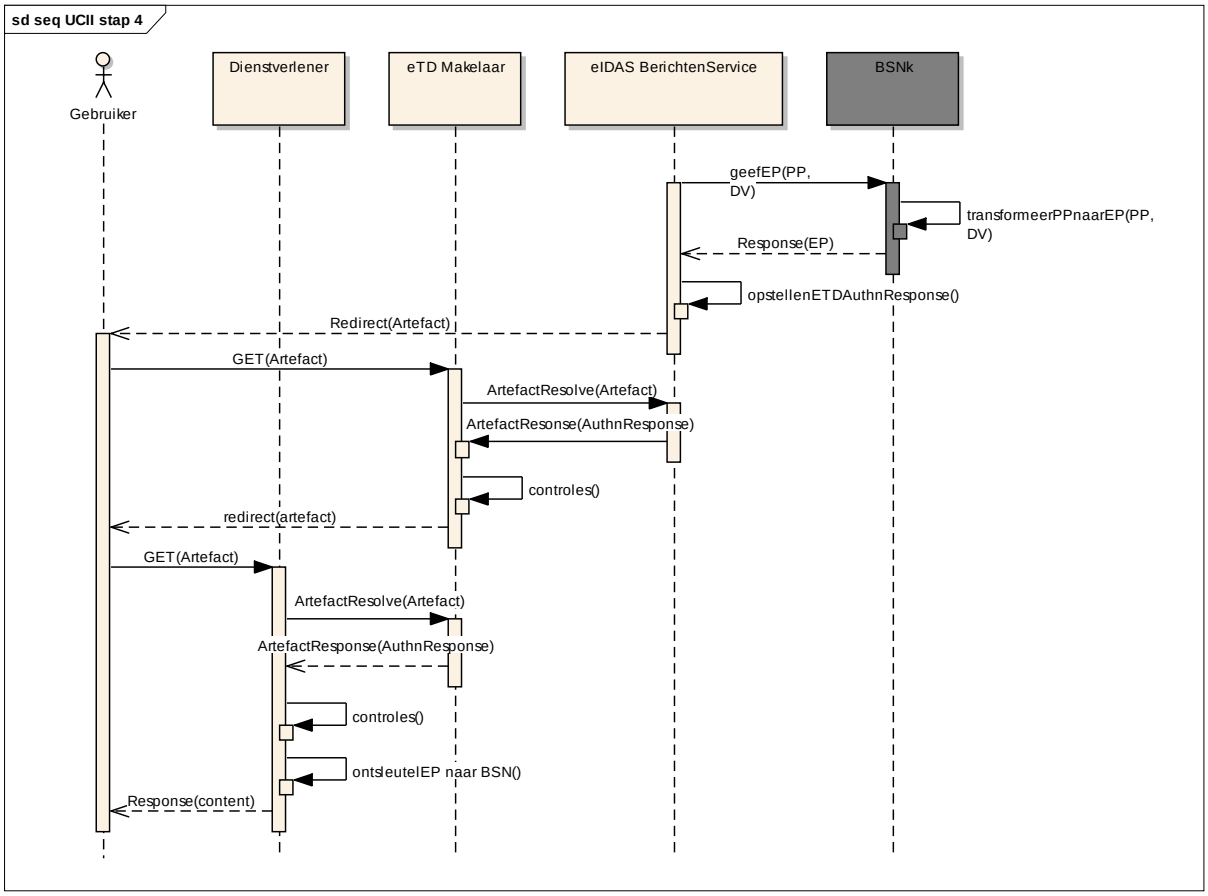
Use Case II A Stap 2 – Interactie



Use Case II A Stap 3 – Interactie

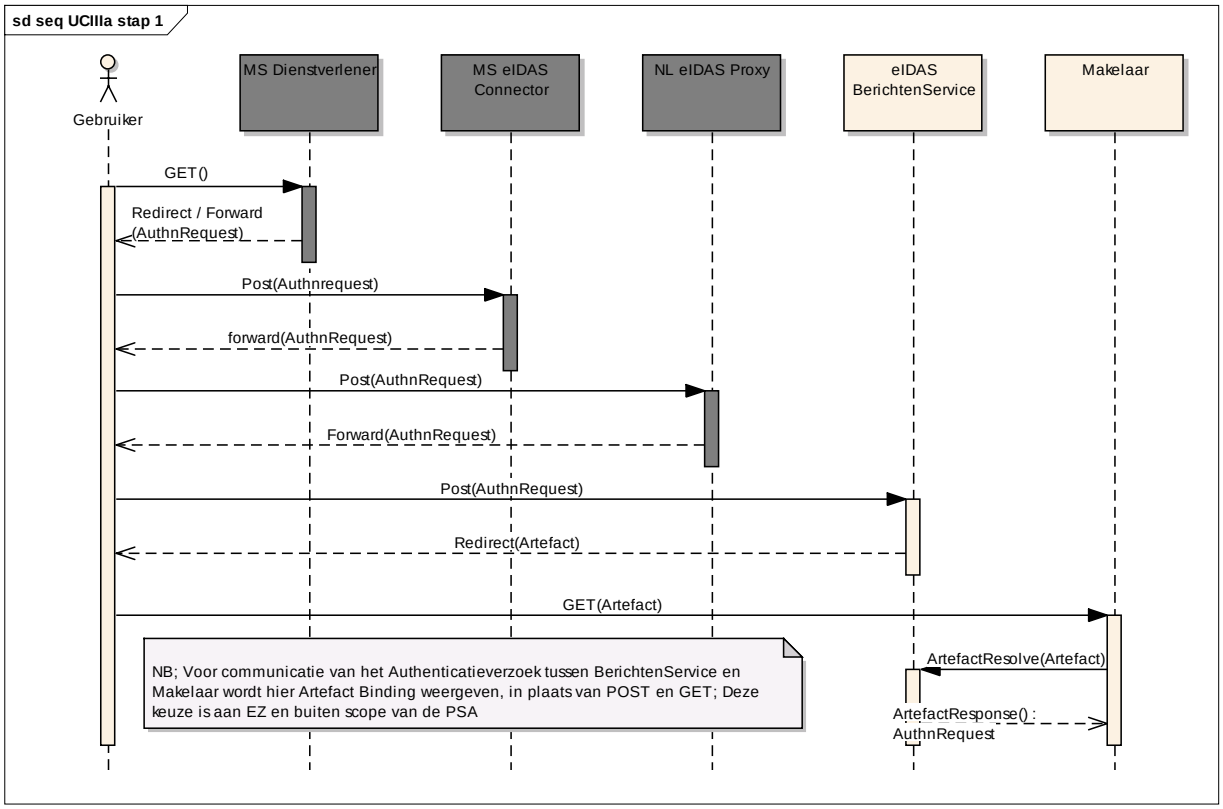


Use case IIA stap 4 Interactie

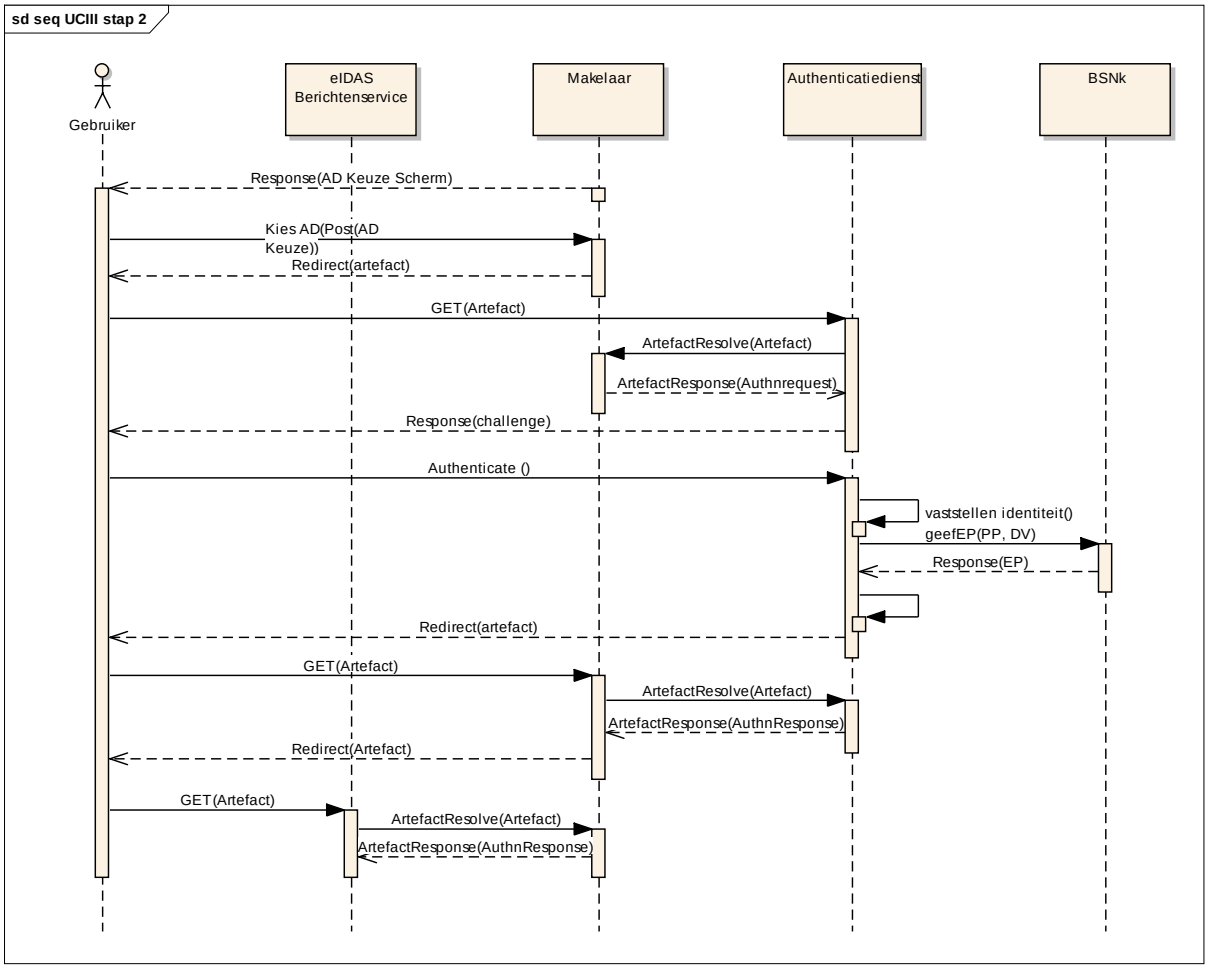


Use case IIIA: Persoon met Nederlands eID logt in bij dienstverlener in andere lidstaat

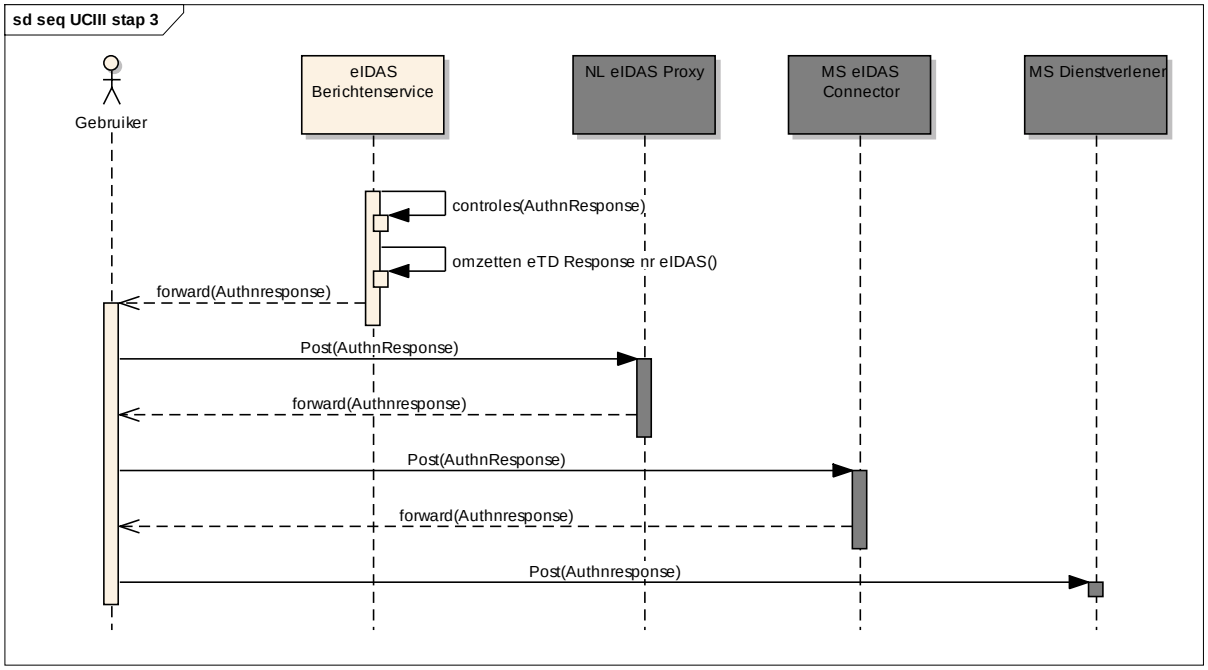
Use case IIIA Stap 1: Interactie



Use case IIIA Stap 2: Interactie



Use case III Stap 3: Interactie



Bijlage 4 wijzigingen t.o.v. 1.0 versie

Beleidsbeslissing:

- De mogelijkheid tot toevoegen van persoonsgegevens aan de BRP verwijderd (inclusief de registratie van een nog onbekend persoon en uitgifte van een nieuw BSN), met uitzondering van bijlage 2.

Bron werkgroep ontwerp & bouw:

- Procesflows vanuit de bijlage naar het hoofddocument verplaatst ten gunste van de leesbaarheid.
- Procesflows aangescherpt.
- RfC van ICTU op opvragen polymorfe pseudoniemen bij BSNk doorgevoerd: de eIDAS berichtenservice ontvangt versleuteld BSN en levert die aan BSNk voor opvragen van PP-BSN en PP-PS. Het BSNk bevraagt niet langer zelf de eIDAS identiteitmanager voor het BSN.
- eIDAS identiteitmanager & verificatiedienst zijn in elkaar geschoven. De resulterende component heet nu "BRP koppelpunt".
- De eIDAS berichtenservice levert aan de eTD makelaar bij attributen in de bronvermelding ook het land: "eIDAS:BE", "eIDAS: DE", etc.
- De eIDAS berichtenservice geeft in het authenticatieverzoek aan de makelaar real-time mee welke attributen de dienstverlener vraagt.
- De berichtenservice splitst de eIDAS familyname in eTD voorvoegstels en achternaam, conform Tabel 36 (use case II).
- De berichtenservice voegt de eTD voorvoegsels en achternaam samen tot eIDAS familyname (use case III).
- Het BRP koppelpunt krijgt van de eIDAS berichtenservice attributen in eTD format in plaats van eIDAS format.
- De bijlage met attribuutmappingen is verwijderd na besluit om dit in het ontwerp op te nemen i.v.m. onderhoudbaarheid van de mappingen.
- Functionaliteit toegevoegd voor het vanuit het BRP koppelpunt uit de koppeltabel van de eIDAS berichtenservice kunnen verwijderen van entries indien de koppeling aan het BSN onjuist bleek of het BSN is gewijzigd.
- Voor organisaties die geen RSIN hebben (bijvoorbeeld eenmanszaken) wordt het KvK nummer gebruikt als basis voor de eIDAS UID.

Bron PIA (onder voorbehoud van definitieve rapport en de bespreking daarvan):

- Toegevoegd dat de eIDAS connector en de eIDAS proxy service samen het eIDAS knooppunt vormen. Het eIDAS koppelpunt is het eIDAS knooppunt plus de eIDAS berichtenservice.
- Het BRP koppelpunt ontvangt niet bij iedere inlog op een BSN dienst de persoonsattributen. De functie "ontvangActueleAttributen" vervalt daarom.
- Argumentatie voor het opslaan van PP-PS in de koppeltabel van de eIDAS berichtenservice toegevoegd.

Bron: risicoanalyse (onder voorbehoud van definitieve rapport, de nog op te stellen netto risicoanalyse en de risico-acceptatie):

- Betrouwbaarheid attributen: aanpassing Source/time, zodat de dienstverlener weet dat de attributen vanuit het buitenland zijn geleverd.
- Grofmazigheid machtiging: Verdere erkenning van diensten van 4 naar 8 (onderscheid tussen publieke en private diensten toegevoegd).

- Vanuit NL-stelsel de "Dienstverlener" meegeven, zodat de buitenlandse authenticatiedienst die bij het inlogproces aan de gebruiker kan tonen.
- Vanuit eIDAS Berichtenservice indien mogelijk naam meegeven. Eis aan eTD toegevoegd om deze te tonen.
- Wijzigingsprocedure toegevoegd voor koppelingen UID aan BSN.
- IB hoofdstuk: Artifact gebruiken voor communicatie tussen componenten.
- IB Hoofdstuk: Gegevens in de eIDAS koppeltabel versleuteld/hashed opslaan.
- Misbruik eisen vanuit USvE IB Hoofdstuk (PP-PS) (voetnoot bij uitwerking in 5)
- Toetsing op gevraagde attributen vooraf door Autoriteit Persoonsgegevens. Advies toegevoegd om hier actief op te toetsen
- Beschikbaarheid: Inzetten 2de makelaar op de erIDAS berichtenservice in IB hoofdstuk toegevoegd
- Consent per lidstaat: aandachtspunt eTD hoofdstuk 5 toegevoegd.
- Inzet HSM voor eIFDAS berichtenservice in 2018 in IB hoofdstuk toegevoegd.

Tenslotte diverse wijzigingen naar aanleiding van interne kwaliteitscontrole.