Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Uniforme Set van Eisen

Versie 1.0 (15-12-2016)

Inhoudsopgave

Uniforme Set van Eisen

Uniforme Set van Eisen	
Versie	1.0
Datum deze versie	15 Dec 2016
Auteur	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Dit betreft versie 1.0 van de Uniforme Set van Eisen. Er wordt later nog functionaliteit aan toegevoegd en de eisen zullen op punten nog verder geëxpliciteerd en/of aangevuld worden, zie Nader uit te werken functionaliteit

De woorden “MOET”, “MAG NIET”, “ZOU MOETEN”, “ZOU NIET MOETEN”, en “MAG” in dit document moeten worden geïnterpreteerd gelijk aan hun Engelstalige equivalenten (“MUST", "MUST NOT / SHALL NOT", "SHOULD", "SHOULD NOT" en "MAY") als beschreven in IETF RFC 2119 (http://www.ietf.org/rfc/rfc2119.txt). Waar deze exacte termen bedoeld zijn worden ze in hoofdletters weergegeven. De betekenis van deze woorden is:

- MOET: een absolute vereiste
- MAG NIET: een absoluut verbod
- ZOU MOETEN: sterke wens, tenzij er valide reden is in specifiek geval af te wijken
- ZOU NIET MOETEN: ongewenst, tenzij er valide reden is om het in specifiek geval toe te laten
- MAG: een vrije keuze, een optie

Algemeen

Dit hoofdstuk is de algemene introductie op de Uniforme Set van Eisen. Hierin zijn de volgende zaken opgenomen:

- Voorwoord
- Leeswijzer
- Uitgangspunten
- Bereik
- Begrippenlijst

Voorwoord

Het Kabinet heeft besloten dat burgers, naast DigiD, een publiek inlogmiddel voor digitale transacties met de overheid, ook private inlogmiddelen (Authenticatiemiddelen) kunnen gebruiken om in te loggen in het Publieke domein. Het toelaten van private middelen naast een publiek middel (DigiD) staat ook wel bekend als 'multimiddelenaanpak'. Deze Uniforme Set van Eisen 1.0 bevat de eisen voor publieke en private Authenticatiemiddelen, op Betrouwbaarheidsniveau Laag, Substantieel en Hoog. Toegang tot het Publieke domein kan op termijn alleen verkregen worden op niveau Substantieel en Hoog.

Deze versie zal de basis vormen voor de aansluitvoorwaarden van het BSN koppelregister (BSNk) 2.0, dat vanaf september 2017 in productie genomen wordt. Deze aansluitvoorwaarden vormen op termijn de uitvoeringvoorschriften bij de komende Wet generieke digitale infrastructuur (Wet GDI).

De Europese eIDAS-verordening met onderliggende uitvoeringsmaatregelen, die eisen stelt aan wederzijdse erkenning van Authenticatiemiddelen, is leidend voor de opzet van de Uniforme Set van Eisen. Er worden ten opzichte van de EU-verordening wel extra eisen gesteld, onder meer vanwege het faciliteren van de multimiddelenaanpak. De Uniforme Set van Eisen richt zich met name op eisen t.a.v. veiligheid, privacy en betrouwbaarheid.

Met de brede bekendmaking van de Uniforme Set van Eisen 1.0 wordt tevens de mogelijkheid geboden op de inhoud ervan te reageren. De uitkomsten van deze consultatie zullen worden meegenomen in het traject naar de Uniforme Set van Eisen 2.0, die ook aanvullende functionaliteiten zal bevatten. De aanpak is hierbij stapsgewijs: versie 1.0 wordt verder aangescherpt. Zo zijn in versie 1.0 voor privacybescherming de aanbevelingen van de reeds uitgevoerde PIA's verwerkt, maar zal deze versie begin 2017 nogmaals aan een PIA worden onderworpen. Ook op het gebied van misbruik- en fraudebestrijding zullen, aanvullende eisen worden uitgewerkt. Op weg naar versie 2.0 zal gewerkt worden met tussenversies. De eindversie zal na een uitvoeringstoets worden vastgesteld als ministeriële regeling onder de Wet GDI.

Reageren?

Uw reactie kunt u mailen naar impulseid@logius.nl

Leeswijzer

De Uniforme Set van Eisen bevat de eisen voor erkenning van zowel publieke als private Authenticatiemiddelen, op Betrouwbaarheidsniveau Laag, Substantieel en Hoog, voor het Publieke domein.

In het hoofdstuk Algemeen staan de uitgangspunten en de begrippenlijst.

De eIDAS-verordening met onderliggende uitvoeringsmaatregelen, die eisen stelt aan wederzijdse erkenning van Authenticatiemiddelen tussen lidstaten, is leidend voor de opzet van de Uniforme Set van Eisen. In Nederland worden aanvullende eisen gesteld. Enerzijds omdat de Uniforme Set van Eisen een multimiddelenstrategie ondersteunt, wat afspraken vereist over de participanten heen, en anderzijds vanwege de specifieke nationale invulling, bijvoorbeeld het gebruik van een BSN. Deze eisen zijn opgenomen in de hoofdstukken:

- Beheer en Organisatie
- Privacy en Informatiebeveiliging
- Compliance en audit

In deze hoofdstukken zijn tabellen opgenomen, waarin links de eIDAS-eis te zien is en rechts de aanvullende eisen, wanneer deze er zijn. De eisen volgen de indeling die de eIDAS-verordening hanteert.

In het hoofdstuk Functionaliteit en Techiek is de vereiste technische invulling te vinden van de eisen. Hier is een beschrijving van de vereiste invulling van Privacy Enhancing Technology te vinden. In dit hoofdstuk staan de Rollen in de authenticatieketen en hun samenhang beschreven. Ook staan de Interface specifications met het BSNk en de Dienstverlener beschreven. Het gedeelte over Techniek is in het Engels, omdat Engels bij technische specificaties ten behoeve van ontwikkeling de de facto voertaal is.

Uitgangspunten

De Uniforme Set van Eisen is gebaseerd op een aantal uitgangspunten die kunnen worden afgeleid van drie basisuitgangspunten waaraan een Participant moet voldoen. De volgende hoofdstukken zijn dan gebaseerd op, of uitwerkingen van, deze uitgangspunten.

Doel

De uitgangspunten dienen meerdere doelen:

- Het biedt inzicht in de principes en daarmee de herleidbaarheid van de eisen uit de Uniforme Set van Eisen.
- Het biedt handvatten om de kwaliteit van de Uniforme Set van Eisen te toetsen en vormen kaders voor de doorontwikkeling van Uniforme Set van Eisen. De principes uit de Uniforme Set van Eisen maken het mogelijk om te bepalen of de uitwerking van de eisen in de Uniforme Set van Eisen voldoende is.
- Het biedt aan alle partijen die deelnemen in de authenticatieketen in het Publiek Domein inzicht in de typen afspraken uit de Uniforme Set van Eisen en de doelstelling daarvan.

Basisuitgangspunten

De Uniforme Set van Eisen is gebaseerd op drie basisuitgangspunten:

1. Betrouwbaarheid
   Betrouwbaarheid betekent niet alleen dat de Authenticatiemiddelen en technieken voldoende veilig zijn maar ook dat de binding tussen het Authenticatiemiddel en de identiteit van de burger (BSN) voldoende sterk moet zijn. Dat wil zeggen, dat identiteitdiefstal en -verwisseling niet mogelijk mag zijn. Dit stelt ook eisen aan de registratie- en verstrekkingprocessen die worden toegepast. Beide aspecten zijn geadresseerd in de eIDAS-verordening
2. Privacyvriendelijkheid
   De voorziening moet voldoen aan de principes van de Europese verordening gegevensbescherming van 27 april 2016, waaronder het principe van minimale gegevensverwerking: persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Dit principe is ook van toepassing op de Nederlandse overheid; het BSN zou alleen verwerkt moeten worden als dat noodzakelijk is. In andere gevallen moeten pseudoniemen worden gebruikt, indien een persistent identificerend kenmerk überhaupt noodzakelijk is.
3. Gebruikersvriendelijkheid
   De voorziening moet eenvoudig te gebruiken zijn, zowel voor Gebruikers als voor Dienstverleners.

Overige uitgangspunten

- De Overheid als geheel is verantwoordelijk voor het publieke arrangement dat nodig is om te borgen dat betrouwbaar en veilig kan worden ingelogd op digitale overheidsdiensten in het Publieke domein.

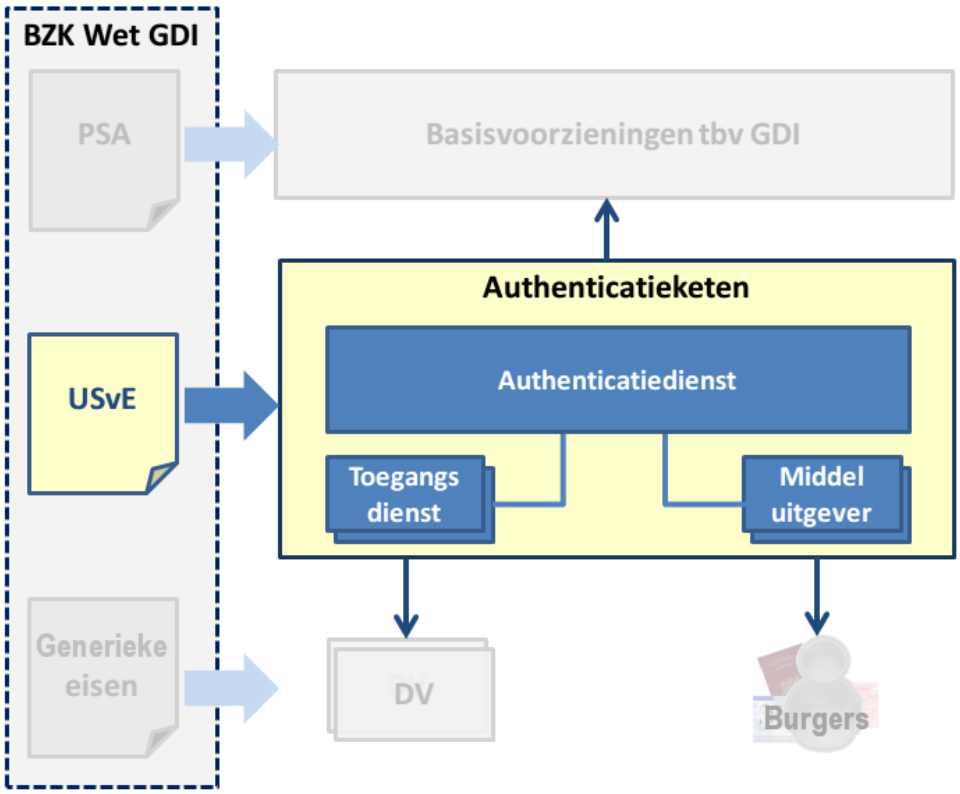
- De Uniforme Set van Eisen is verankerd in wet- en regelgeving.
- De Uniforme Set van Eisen beschrijft de minimale set eisen waaraan moet worden voldaan.
- De Uniforme Set van Eisen bevat geen eisen welke al vastgelegd zijn in andere wet- en regelgeving.
- De eIDAS-verordening vormt de basis voor de Uniforme Set van Eisen. Hiermee is de supranationale interoperabiliteit gegarandeerd.
- Voor partijen welke authenticatiedienstverlening willen leveren in het Publieke domein geldt een conformatieplicht aan de Uniforme Set van Eisen.
- 'Privacy by Design' - waarborg de privacy van gebruikers in het ontwerp, onder meer door:
  - Dataminimalisatie - zorg dat elke partij slechts de data krijgt en opslaat die nodig is voor de rol (en taken) die hij uitvoert.
  - Incident impact beperking - ga er van uit dat beveiligingsincidenten voor zullen komen en ontwerp zodanig dat de impact van een beveiligingsincident zo veel mogelijk beperkt blijft
  - Vermijd Privacy Hotspots - gerelateerd aan bovenstaande, maar ontwerp (de Rollen) ook zodanig dat het niet

nodig is om veel potentieel identificerende en vertrouwelijke informatie bij één rol neer te leggen.
    - Gebruik privacy enhancing technologies - privacy technisch afdwingen is betrouwbaarder dan te vertrouwen op procedurele afspraken
- De Uniforme Set van Eisen faciliteert een multimiddelenstrategie en richt zich op het ontstaan van meerdere Authenticatiemiddelen, op het gebruik van meerdere technologische oplossingen en op het actief zijn van meerdere leveranciers. Bij kabinetsbesluit is het ook private partijen toegestaan om Authenticatiemiddelen te leveren. Zo wordt maximaal tegemoet gekomen aan het doelen van de strategie:
    - het maximaal voorbereid zijn op nooit geheel uit te sluiten continuïteitsstoringen en/of veiligheidsincidenten bij het inloggen door burgers op digitale publieke diensten (zie ook Compartimentering).
    - ruimte voor innovatie voor de aanbieders
    - keuzevrijheid voor Gebruikers.
- Misbruik van inlogmiddelen is nooit geheel te voorkomen en het uitgangspunt is om misbruik te minimalisereren. De Uniforme Set van Eisen beschrijft maatregelen om misbruik te signaleren en te voorkomen.
- De eisen in de Uniforme Set van Eisen zijn technologie-onafhankelijk en gebaseerd op Open standaarden, waardoor er ruimte ontstaat voor innovatie. Dit draagt bij aan het borgen en vergroten van de interoperabiliteit.
- Het maximaal voorbereid zijn op nooit geheel uit te sluiten continuïteitsstoringen en/of veiligheidsincidenten en voorkomen van enkelvoudig uitgevoerde cruciale componenten.
- Het maximaal ontzorgen van de Dienstverlener.

Bereik

De Uniforme Set van Eisen beschrijft eisen aan partijen in de Authenticatieketen die burger-authenticatie in het Publieke domein verzorgen. Het betreft hier een afbakening naar doelgroep (Natuurlijke personen die over een BSN beschikken, zie Gebruiker) en niet naar partijen. Voor alle partijen die een rol spelen in de Authenticatieketen geldt, dat zij slechts deze functionaliteit mogen aanbieden indien zij aan de Uniforme Set van Eisen voldoen.

In de onderstaande figuur is het bereik van de Uniforme Set van Eisen visueel weergegeven.



Deze rollen worden verder uitgewerkt in de paragraaf Rollen.

Begrippenlijst

Binnen de Uniforme Set van Eisen wordt één begrippenlijst gehanteerd.

Authenticatie (authenticeren)

De controle (het staven) van een geclaimde identiteit van een Gebruiker.

Authenticatiedienst

Een Authenticatiedienst (AD) voert authenticatieprocedures uit waarmee Gebruikers worden geauthentiseerd daarbij gebruikmakend van elektronische Authenticatiemiddelen verstrekt door een Middelenuitgever. De Authenticatiedienst levert op basis van de authenticatieprocedure een Authenticatieverklaring aan de Toegangsdienst.

> Zie verder de rolbeschrijving.

Authenticatieketen

De Authenticatieketen bestaat uit één Authenticatiedienst en één of meerdere Toegangsdiensten en Middelenuitgevers. Gezamenlijk kunnen deze partijen een Gebruiker authenticeren ten behoeve van een Dienstverlener.

> Zie verder de rolbeschrijvingen.

Authenticatiemiddel

Een middel op grond waarvan Authenticatie van een Gebruiker kan plaatsvinden.

> In de eIDAS uitvoeringsverordening EU 2015 / 1502 wordt aan Authenticatiemiddelen gerefereerd als "elektronisch identificatiemiddel".

Authenticatieverklaring

> (Engels: Authentication assertion)

Een gestandaardiseerd elektronisch bericht (conform koppelvlakspecificaties) opgesteld en ondertekend door een Authenticatiedienst, ten behoeve van en versleuteld voor een Ontvangende Partij. De Authenticatiedienst verklaart daarmee dat hij een Gebruiker succesvol heeft geauthenticeerd als de meegeleverde Versleutelde Identiteit/Pseudoniem volgens eisen die het normenkader stelt aan betreffende Betrouwbaarheidsniveau voor een bepaalde handeling of Dienst.

Autorisatielijst BSN

De Autorisatielijst BSN is een lijst met Dienstverleners die geautoriseerd zijn voor ontvangst van het BSN, beschikbaar gesteld en ondertekend door de Beheerorganisatie BSNk. Deze Dienstverlener moet daarvoor minimaal één Dienst hebben waarvoor hij een wettelijke taak uitvoert waarbij een BSN nodig is. Een Dienstverlener moet dan aan de eisen voldoen die de Wet GDI stelt aan een Dienstverlener (onder meer op de gebieden privacy en beveiliging).

> Zie voor technische details Autorisation List BSN format

Basisregistratie Personen

De Basisregistratie Personen (BRP) is een volledig digitale voorziening die persoonsgegevens bevat van alle inwoners van Nederland (ingezetenen) en van personen die niet, of korter dan 4 maanden, in Nederland wonen maar wel een relatie met de Nederlandse overheid hebben (de niet-ingezetenen).

De wet Basisregistratie Personen is de grondslag voor het stelsel voor de registratie van persoonsgegevens in Nederland. Een aantal onderdelen van deze wet kan pas uitgevoerd worden als de Basisregistratie Personen (BRP) gereed is.

> Bron: http://www.operatiebrp.nl. Zie verder: https://www.rvig.nl/brp

Beheerorganisatie BSNk

De Beheerorganisatie BSNk (BO-BSNk) is een rol die verantwoordelijk is voor het beheer van het BSNk.

> Zie verder de rolbeschrijving.

Betrouwbaarheidsniveau

In dit kader, de mate van zekerheid die over de identiteit van een Gebruiker gegeven kan worden bij gebruik van zijn Authenticatiemiddel. De eIDAS-verordening onderscheidt de niveaus laag, substantieel en hoog. De uitvoeringsverordening EU 2015/1502 definieert de eisen aan deze betrouwbaarheidsniveaus.

BSN

Het Burgerservicenummer (BSN) is het Persoonlijke identificatie nummer van de Nederlandse overheid voor natuurlijke personen.

Herkomst

Gebaseerd op Artikel 1 sub b Wet algemene bepalingen burgerservicenummer (Wabb): het aan een natuurlijk persoon toegekende nummer.

BSN-domein

Het onderdeel binnen het Publieke domein waarin het BSN bij de interactie gebruikt wordt.

BSNk

Het BSNk is een voorziening in het kader van de Generieke Digitale Infrastructuur (GDI) die het mogelijk maakt om publieke en private authenticatiemiddelen te gebruiken in het publiek domein.

Zie verder de beschrijving.

Compartimentering

Het geheel van maatregelen bedoeld om verstoringen en (veiligheids)incidenten beperkt te houden tot de getroffen Participant.

Dienst

Een Dienst is een samenstel van elektronisch aanbod waarvoor authenticatie voorwaardelijk is.

Voorbeelden

- Het tot stand komen van een rechtsbetrekking (het nemen van een besluit of sluiten van een overeenkomst);
- Het leveren van een product of besluit;
- Het beantwoorden van een informatievraag.

De Dienst wordt aangeboden door een Dienstverlener.

Dienstverlener

Dienstverlener is een rol die elektronische Diensten aanbiedt aan Gebruikers waarvoor Authenticatie voorwaardelijk is.

> zie verder de rolbeschrijving

eIDAS-verordening

EU verordening nr. 910/2014 van het Europees Parlement en de Raad (23 juli 2014) en de Uitvoeringsverordening EU 2015/1501 en EU 2015/1502 (8 september 2015) betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

GDI

De Generieke Digitale Infrastructuur (GDI) van de overheid bestaat uit standaarden, producten en voorzieningen die gezamenlijk gebruikt worden door (alle) meerdere overheden, vele publieke organisaties en in een aantal gevallen ook door private partijen.

- De GDI is een onmisbaar deel van de (digitale) basisvoorzieningen waarmee organisaties hun primaire processen inrichten.
- De GDI is, naar zijn aard, niet organisatie-, sector- of domeinspecifiek.

De GDI bestaat uit herbruikbare digitale basisvoorzieningen, standaarden en producten die het overheden, publieke organisaties en private partijen mogelijk maken om hun primaire processen doelmatig in te richten en te blijven ontwikkelen. De GDI is een dynamisch geheel welke de komende jaren gewijzigd kan worden door de ontwikkeling van nieuwe generieke voorzieningen en standaarden of door het uit productie nemen van al opgenomen voorzieningen.

> Herkomst
>
> https://www.digitaleoverheid.nl/gdi

Gebruiker

Een Natuurlijk persoon die een Authenticatiedienst gebruikt voor Authenticatie ten behoeve van het afnemen van een Dienst bij een Dienstverlener.

HSM

Een Hardware Security Module (HSM) is een fysiek apparaat dat bescherming biedt voor de opslag, management en gebruik van cryptografisch materiaal.

Inzageregister

Een centrale rol, belegd bij de Beheerorganisatie BSNk, waarbij de status van authenticatiemiddelen wordt geregistreerd en gebruikers deze status in kunnen zien.

> Zie verder de rolbeschrijving.

Middelenuitgever

De Middelenuitgever (MU) is een rol van een Participant die een elektronisch Authenticatiemiddel verstrekt aan de Gebruiker en het middel bij het BSNk activeert voor gebruik in het Publieke domein. De Middelenuitgever biedt de Gebruiker de mogelijkheid om zijn Authenticatiemiddel(en) te beheren en zorgt ervoor dat het BSNk Inzageregister een actuele status van de Authenticatiemiddelen (of de relatie) heeft.

> Zie verder de rolbeschrijving.

Mijnoverheid

Mijnoverheid is de persoonlijke website van burgers voor overheidszaken. Via MijnOverheid kunnen zij bijvoorbeeld een herinnering krijgen als hun paspoort bijna verlopen is, controleren hoe zij bij hun gemeente geregistreerd staan of de status van hun Authenticatiemiddelen die geactiveerd zijn binnen het Publieke domein.

Misbruikbestrijdingsregister

Een centrale rol, (vooralsnog) belegd bij de Beheerorganisatie BSNk, als onderdeel van de basisvoorziening BSNk waar Middelenuitgever en Authenticatiedienst een Opmerkelijke gebeurtenis kunnen laten registreren ten behoeve van Misbruikbestrijding.

> Zie verder de rolbeschrijving.

Natuurlijk persoon

Een individueel menselijk wezen en subject van rechten en drager van plichten.

Niet-natuurlijk persoon

Hetzij een rechtspersoon, hetzij een samenwerkingsverband van natuurlijke personen en/of rechtspersonen.

OIN

Organisatie Identificatie Nummer (OIN) wordt gebruikt om een organisatie (bijvoorbeeld een Participant of Dienstverlener) te identificeren.

> Het OIN ondersteunt identificatie nummers uit meerdere registers, bijv Fiscaal nummer of Handelsregisternummer. Een OIN bestaat uit een prefix (identificeert het register), identificatienummer en een postfix (subnummer, standaard '0000').

Ontvangende Partij

Een Ontvangende Partij (OP) is vanuit een Authenticatiedienst gezien de beoogde ontvanger van een Authenticatieverklaring met een (specifiek voor deze OP) Versleutelde Identiteit/Pseudoniem (VI@OP of VP@OP) van de Gebruiker. Meestal is de Ontvangende Partij een Dienstverlener, maar het Inzageregister (of straks een Machtigingsregister of Attribuutregister) kan ook een Ontvangende Partij zijn.

> Engels: Relying party

Opmerkelijke gebeurtenis

Gebeurtenis die aantoonbaar of vermoedelijk afwijkt van het normale registratie- of gebruikspatroon (van het Authenticatiemiddel) of anderszins in het kader van misbruikbestrijding interessant is om op te merken.

> Er wordt in de Uniforme Set van Eisen geen limitatieve lijst gegeven van opmerkelijke gebeurtenissen. De interpretatie van een opmerkelijke gebeurtenis zal afgesproken en geactualiseerd worden door misbruikbestrijdings deskundigen van de diverse betrokken partijen. Dit proces staat nog niet beschreven in deze versie van de Uniforme Set van Eisen.

Participant

Een partij in de Authenticatieketen waarvan is vastgesteld door de Minister van Binnenlandse Zaken en Koninkrijksrelaties dat deze voldoet aan de eisen zoals gesteld in de Uniforme Set van Eisen.

> In de eIDAS-verordening wordt aan Participanten gerefereerd als "aanbieders".

Zie verder de rolbeschrijvingen.

Persoonsidentificatiegegevens

Gegevens die tezamen de identiteit van een Natuurlijk persoon uniek aanduiden.

Voorbeelden

Voornamen, achternaam, geboortedatum, geboorteplaats en BSN.

PKIoverheid-certificaat

PKIoverheid is de public key infrastructure (PKI) van de Nederlandse overheid. Een PKIoverheid-certificaat fungeert als een digitaal paspoort dat onder meer gebruikt wordt bij het controleren van de elektronische ondertekening van berichten en het versleutelen van informatie. PKIoverheid wordt beheerd door Logius.

Zie verder: https://www.logius.nl/diensten/pkioverheid/

Polymorfe identiteit/pseudoniem

Polymorfe Identiteit (PI) en de Polymorfe Pseudoniem (PP) zijn specifieke cryptografische elementen die op aanvraag van een Middelenuitgever door het BSNk afgeleid worden van een identiteit van de Gebruiker (BSN in geval van het Publiek Domein). De PI en PP zijn specifiek voor de aanvragende Middelenuitgever en daarom worden ze genoteerd als (voorbeeld RDW): PI@RDW en PP@RDW.

Deze PI@MU en PP@MU[1] kunnen gebruikt worden door een Authenticatiedienst om een Gebruiker te authenticeren. Dit kan als de Authenticatiedienst dezelfde partij is als de Middelenuitgever of als een Authenticatiedienst hiervoor speciaal geautoriseerd is door de betreffende Middelenuitgever (via "MU - AD affiliation" in de Metadata). In dat geval kan de Authenticatiedienst de PI@MU of PP@MU transformeren naar een Ontvangende partij specifieke Versleutelde Identiteit of Versleuteld Pseudoniem (VI@OP of VP@OP[2]).

zie verder Polymorfe encryptie en pseudonimisering

Voetnoot

1. MU is de generieke term voor een willekeurige Middelenuitgever
2. OP is de generierke term voor een willekeurige Ontvangende Partij

Publieke domein

Het domein waarbij interacties plaatsvinden tussen natuurlijke personen / niet-natuurlijke personen enerzijds en de Dienstverleners met een publieke taak anderzijds.

Een Dienstverlener is 'publiek' wanneer het een bestuursorgaan in de zin van afdeling 1.1 van de Algemene wet bestuursrecht 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 (BSN) te gebruiken.

Randomisatie

Het maken van een kopie van een polymorfe vorm (Polymorfe identiteit/pseudoniem, Versleutelde Identiteit/Pseudoniem) dat cryptografisch niet te linken is naar het origineel.

Een polymorfe vorm is technisch gezien een ElGamal versleuteld bericht en met randomisatie maakt men een nieuw versleuteld bericht met dezelfde inhoud maar dat er aan de buitenkant anders uit ziet. Voor randomisatie is geen geheime sleutel benodigd.

Omdat randomisaties ook buiten de HSM kunnen worden uitgevoerd, wordt dit in detail gespecificeerd. Een PI, PP, VI en VP bestaan elk uit drie punten op een elliptische curve, (P, Q, S). Bij randomisatie wordt een willekeurig ('random') getal r gekozen met $0 < r < q$ waar q de grootte van de elliptische groep is. De gerandomiseerde vorm is $(P + r*S, Q + r*S, S)$.

RvA

Raad van Accreditatie. Bij wet ingesteld instituut dat certificerende instellingen accrediteert. In dit kader accrediteert de RvA partijen voor de toetsing van Participanten aan de Uniforme Set van Eisen.

Sleutelmateriaal

Er bestaan verschillende soorten cryptografische sleutels, ook wel sleutelmateriaal genoemd. Ruwweg bestaan sleutels voor communicatie beveiliging (PKI Overheid) en sleutels waarmee de polymorfe structuren worden gevormd. Er zijn drie soorten polymorfe sleutels. Allereerst zijn er sleutels bij BSNk ten behoeve van activatie, i.e. waarmee Polymorfe Identiteiten en Pseudoniemen worden gevormd. Ten tweede zijn er sleutels aanwezig bij Authenticatiediensten waarmee transformaties naar Versleutelde Identiteiten en Pseudoniemen kunnen worden uitgevoerd. Voor het merendeel omvat dit gedeelde sleutels. Tot slot zijn er sleutels bij Dienstverleners. Hiermee kunnen zij Versleutelde Identiteiten en Pseudoniemen ontsleutelen alsmede de authenticiteit daarvan vaststellen. De eerste twee categorieën polymorfe sleutels hebben een lange levensduur en worden (daarom) in HSMs beheerd. De laatste categorie polymorfe sleutels kunnen relatief eenvoudig worden vervangen en hoeven daarom niet in HSMs te worden beheerd.

Sleutelverstrekkingslijst

Een publiekelijk toegankelijke lijst waarin de Beheerorganisatie BSNk de Dienstverleners publiceert die sleutelmateriaal verkregen hebben van het BSNk Sleutelbeheer

> Zie voor technische details Key provisioning list format

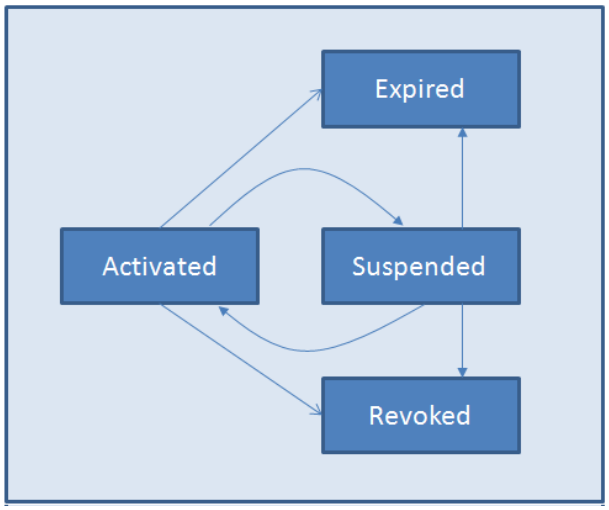
Status (van het Authenticatiemiddel)

Een Authenticatiemiddel heeft een status. Deze status bevat minimaal een geactiveerde abonnee-relatie van de

Middelenuitgever en Gebruiker of een gedeactiveerde abonnee-relatie als wijziging op de geactiveerde status. De actuele status van een middel is voor de Gebruiker altijd bij de Middelenuitgever beschikbaar.De status van de abonnee relatie wordt bij het Inzageregister geregistreerd. De volgende statussen zijn zichtbaar voor de Gebruiker:

- Activated als een middel (weer) bruikbaar is voor het Publieke domein.
- Suspended als het middel niet (meer) actief is in het Publieke domein, bijvoorbeeld omdat de Gebruiker kiest om het middel te de-activeren of omdat de Authenticatiedienst een indicatie heeft dat het middel misbruikt wordt. Een her-activatie wijzigt de status naar Activated; een permanente de-activatie wijzigt de status naar Revoked.
- Revoked als het middel zelf ingetrokken is, bijvoorbeeld omdat de Gebruiker het middel niet meer onder zijn controle heeft (kwijt, gestolen) of als de relatie tussen Gebruiker en de Authenticatiedienst is beëindigd.
- Expired als de uiterste gebruiksdatum van het middel verstreken is. Ook vanuit Expired kan een middel niet meer geactiveerd worden.

Statusovergangen zijn mogelijk als weergegeven in onderstaande figuur:



Toegangsdienst

Een Toegangsdienst (TD) verstrekt verklaringen over de identiteit van een Gebruiker aan de Dienstverlener. Op basis van deze verklaring besluit de Dienstverlener over toegang van de Gebruiker tot de Dienst. De Toegangsdienst verstrekt de verklaringen op basis van verklaringen van een Authenticatiedienst. De Toegangsdienst biedt de Gebruiker de mogelijkheid een Authenticatiedienst te kiezen.

> Zie verder de rolbeschrijving.

Versleutelde Identiteit/Pseudoniem

De Versleutelde Identiteit (VI) en het Versleutelde Pseudoniem (VP) zijn specifieke cryptografische elementen die door een Authenticatiedienst gemaakt worden door de Polymorfe identiteit/pseudoniem van een Gebruiker te transformeren voor een specifieke Ontvangende Partij. Omdat de VI en VP specifiek zijn voor deze beoogde Ontvangende Partij worden ze genoteerd als (voorbeeld Belastingdienst): VI@Belastingdienst en VP@Belastingdienst.

Een Authenticatiedienst kan slechts een Middelenuitgever specifiek Polymorfe identiteit/pseudoniem (PI@MU en PP@MU[1]) transformeren als hij dezelfde partij is als de Middelenuitgever. In alle andere gevallen moet een Authenticatiedienst speciaal geautoriseerd worden door de betreffende Middelenuitgever (via "MU - AD affiliation" in de Metadata). Pas dan kan de Authenticatiedienst de PI@MU of PP@MU transformeren naar een Ontvangende partij specifieke Versleutelde Identiteit of Versleuteld Pseudoniem (VI@OP of VP@OP[2]). De betreffende Ontvangende Partij kan op zijn beurt deze VI@OP of VP@OP gebruiken om daaruit (met het juiste Sleutelmateriaal) de Gebruiker te identificeren met een originele identiteit (BSN in geval van het Publiek Domein) of een voor de Ontvangende Partij specifiek persistent Pseudoniem[3].

Vergelijk Polymorfe identiteit/pseudoniem en zie verder Polymorfe encryptie en pseudonimisering

Voetnoot

1. MU is de generieke term voor een willekeurige Middelenuitgever
2. OP is de generieke term voor een willekeurige Ontvangende Partij
3. Een persistent Pseudoniem is altijd hetzelfde voor een combinatie van een Gebruiker en een Ontvangende Partij, ongeacht de Authenticatiedienst of het gebruikte Authenticatiemiddel. Een Pseudoniem is indirect afgeleid van de originele Identiteit (BSN in geval van het Publiek Domein of "UniquenessID" voor eIDAS) maar kan door de Ontvangende partij niet herleid worden naar diezelfde originele identiteit.

WID

Wettelijk identiteitsdocument zoals is bedoeld in de Wet op de identificatieplicht artikel 1.

Beheer en Organisatie

Dit hoofdstuk bevat vereisten aan de organisaties van de Participanten, deze eisen zijn generiek en niet afhankelijk van het betrouwbaarheidsniveau dat wordt geleverd.

De paragraafstructuur volgt de eIDAS uitvoeringsverordening EU 2015 / 1502. De tekst in de eIDAS kolom is overgenomen uit de formele Nederlandstalige versie van de uitvoeringsverordening.

- 2.4.1 Algemene bepalingen — Betreft de kaders waaraan de organisaties in de authenticatieketen moeten voldoen.
- 2.4.2 Informatie voor gebruikers — Betreft de vereisten voor informatie aan Gebruikers over processen, producten en procedures voor het informeren over wijzigingen van uitgifte/intrekkingsprocessen en leveringsvoorwaarden. Regelt een informatieplicht aan Gebruikers.
- 2.4.4 Bijhouden van de administratie — Betreft de vereisten aan de diverse administraties waaronder zakelijke overeenkomsten, registraties van identiteitsgegevens, loggings van berichtenverkeer etc. Dit met het oog op nationale regelgeving.
- 2.4.5 Faciliteiten en personeel — Deze paragraaf betreft de vereisten aan de competenties en integriteit van personeel en eisen voor de bescherming van- en toegang tot faciliteiten.

2.4.1 Algemene bepalingen

Betreft de kaders waaraan de organisaties in de authenticatieketen moeten voldoen.

Niveau betrouwbaarheid	eIDAS tekst uitvoeringsverordening	Nadere invulling en specificatie Uniforme Set van Eisen
Laag	Vereiste elementen 1. Aanbieders die een operationele dienst aanbieden die onder deze verordening valt, zijn een overheidsinstantie of een rechtspersoon die door het nationale recht van een lidstaat als zodanig wordt erkend, over een gevestigde organisatie beschikt en volledig operationeel is op alle gebieden die voor de verlening van de diensten relevant zijn. 2. De aanbieders voldoen aan al hun wettelijke verplichtingen in verband met het verrichten en leveren van de dienst, onder meer wat betreft de soorten informatie die mogen worden gevraagd, de wijze waarop het bewijs van de identiteit wordt geleverd, welke informatie mag worden bewaard en hoe lang deze mag worden bewaard. 3. De aanbieders kunnen aantonen dat zij in staat zijn het risico van de aansprakelijkheid voor schade op zich te nemen en over voldoende financiële middelen beschikken om hun activiteiten en de dienstverlening voort te zetten. 4. De aanbieders zijn verantwoordelijk voor het naleven van alle verplichtingen die zij aan andere entiteiten hebben uitbesteed en voor het voldoen aan het beleid inzake het stelsel, op dezelfde wijze als wanneer zij deze taken zelf vervulden. 5. Stelsels voor elektronische identificatie die niet volgens nationaal recht zijn opgezet, moeten over een doeltreffend beëindigingsplan beschikken. Dat plan omvat voorzieningen voor de ordelijke stopzetting van de dienstverlening of de voortzetting daarvan door een andere aanbieder, voor de wijze waarop de betrokken autoriteiten en eindgebruikers worden ingelicht, alsook voor de wijze waarop de administratie wordt beschermd, bewaard en vernietigd overeenkomstig het voor het stelsel geldende beleid.	Geen nadere invulling of specificatie

Substantieel	Zelfde als niveau laag.	Addenda bij Laag punt 5 en van toepassing op niveau Substantieel en Hoog.
		
		1. Participanten MOETEN over een plan beschikken voor het beëindigen van de dienstverlening ongeacht de intentie of oorzaak van de beëindiging. Het plan voorziet in elk geval in:
		    1. een ordelijke stopzetting van dienstverlening of;
		    2. de voortzetting van de dienstverlening door een andere erkende Participant inclusief de veilige overdracht van de identificatie-gegevens die behoren bij een Authenticatiemiddel en de loggings van informatietransacties die met deze middelen zijn gegenereerd.
		    3. het informeren van de Gebruikers en de afnemers van het voornemen en indien van toepassing, de begeleiding van de Gebruikers en afnemers bij de overgang naar een andere erkende Participant van zijn keuze;
		    4. In het geval van stopzetting van de dienstverlening MOETEN de relevante gegevens behorende bij de identiteit van de Gebruiker van Authenticatiemiddel en de loggings van informatietransacties die met Authenticatiemiddelen zijn gegenereerd onveranderd worden veiliggesteld.
		2. De erkende Participant die het voornemen heeft de dienstverlening stop te zetten of over te dragen MOET onverwijld de Toezichthouder van dat voornemen op de hoogte stellen.
		    1. De Participant MOET bij stopzetting of overdracht van de dienstverlening de aanwijzingen van de Toezichthouder opvolgen.
		    2. De Toezichthouder bepaalt bij stopzetting of overdracht of gegevens aan hem of een ander Participant MOETEN of MOGEN worden overgedragen dan wel MOETEN worden worden vernietigd.
		
		De eisen in punt 1 en 2 zijn van toepassing op alle Participanten.

Hoog	Zelfde als niveau laag.	Zelfde als niveau substantieel.

De kolom met eIDAS tekst is overgenomen uit de formele Nederlandstalige versie van de eIDAS uitvoeringsverordening EU 2015 / 1502.

Daar waar de eIDAS tekst spreekt van 'aanbieders' is in de Uniforme Set van Eisen de term 'Participant' gebruikt.

2.4.2 Informatie voor gebruikers

Betreft de vereisten voor informatie aan Gebruikers over processen, producten en procedures voor het informeren over wijzigingen van uitgifte/intrekkingsprocessen en leveringsvoorwaarden. Regelt een informatieplicht aan Gebruikers.

Niveau betrouwbaarheid	eIDAS tekst uitvoeringsverordening	Nadere invulling en specificatie Uniforme Set van Eisen
Laag	1. Er bestaat een gepubliceerde beschrijving van de dienst met alle toepasselijke voorwaarden en vergoedingen, inclusief eventuele gebruiksbeperkingen. De beschrijving van de dienst omvat een privacyverklaring. 2. Er dient te worden voorzien in passend beleid en passende procedures om de gebruikers van de dienst tijdig en op betrouwbare wijze te informeren over elke wijziging van de beschrijving van de dienst, alle toepasselijke voorwaarden en de privacyverklaring. 3. Er dient te worden voorzien in passend beleid en passende procedures om verzoeken om informatie volledig en correct te beantwoorden.	Geen nadere invulling of specificatie

Substantieel	Zelfde als niveau laag.	Addenda bij Laag punt 3 en van toepassing op niveau Substantieel en Hoog
		
		1. De Gebruiker MOET met gebruik van een geldig Authenticatiemiddel inzage worden geboden in:
		    1. de gegevens die over hem zijn vastgelegd ten behoeve van de uitgifte van een Authenticatiemiddel;
		    2. de Authenticatiemiddelen die op zijn identiteit zijn uitgegeven;
		    3. de transacties die zijn uitgevoerd met het Authenticatiemiddel dat is gekoppeld aan de identiteit van de Gebruiker. Het geboden inzicht bestaat in elk geval uit de datum en tijd van inloggen en de dienst of Dienstverlener waarop is ingelogd.
		    4. De Gebruiker MOET op laagdrempelige- en betrouwbare wijze tijdig in staat worden gesteld om op basis van het geboden inzicht met de Authenticatiedienst respectievelijk de Middelenuitgever in contact te treden met vragen en melding van fouten of vermoedens van misbruik van zijn middel.
		2. De toegang tot de informatie van de Gebruiker MOET minimaal op het betrouwbaarheidsniveau Substantieel zijn beschermd.
		3. Indien een persoon claimt niet meer over een geldig Authenticatiemiddel te beschikken of claimt dat een middel ten onrechte aan zijn identiteit is gekoppeld en online inzage niet mogelijk is, MOET fysiek inzicht gegeven worden in de gegevens genoemd onder punt 1 of de mogelijkheid worden geboden om toegang te verkrijgen met een ander Authenticatiemiddel op het zelfde betrouwbaarheidsniveau als het Authenticatiemiddel waarvan de persoon claimt dat deze er niet meer over beschikt:
		    1. Te allen tijde MOET op afdoende wijze vastgesteld worden dat inzage wordt verstrekt aan de juiste persoon.
		    2. In alle gevallen MOET een persoon die toegang tot de gegevens vraagt worden geïdentificeerd als ware het de rechtmatige Gebruiker van het geregistreerde Authenticatiemiddel. Dit betekent dat de persoon zich identificeert met zijn WID en dat de persoonsgegevens in het WID worden gevalideerd aan de hand van de door de Middelenuitgever/Authenticatiedienst geregistreerde persoonsgegevens van de Gebruiker en;
		    3. De identificatie van de persoon die fysiek toegang wordt geboden MOET plaatsvinden op het zelfde betrouwbaarheidsniveau als het geregistreerde Authenticatiemiddel.
		
		Toelichtende tekst: Met het geven van inzicht aan de Gebruiker over het gebruik van zijn middel krijgt de gebruiker de mogelijkheid van zelfcontrole. Deze zelfcontrole draagt ook bij aan het opsporen van fouten en bestrijden van misbruik van middelen door derden.
		
		Toelichting bij punt 3: Deze eis is opgenomen voor het geval dat door onvoorziene omstandigheden geen nieuw middel kan worden verstrek aan de Gebruiker. De normale gang van zaken is dat middels het verstrekken van een nieuw Authenticatiemiddel de Gebruiker weer toegang krijgt tot zijn gebruiksgegevens.
		
		De eisen in punt 1,2 en 3 zijn van toepassing op de Authenticatiedienst en de Middelenuitgever.

Hoog	Zelfde als niveau laag.	Zelfde als niveau substantieel.

2.4.4 Bijhouden van de administratie

Betreft de vereisten aan de diverse administraties waaronder zakelijke overeenkomsten, registraties van identiteitsgegevens, loggings van berichtenverkeer etc. Dit met het oog op nationale regelgeving.

Niveau betrouwbaarheid	eIDAS tekst uitvoeringsverordening	Nadere invulling en specificatie Uniforme Set van Eisen
Laag	1. Relevante informatie wordt vastgelegd en bewaard met behulp van een doeltreffend documentenbeheersysteem, met inachtneming van de toepasselijke wetgeving en goede praktijken op het gebied van gegevensbescherming en gegevensbewaring. 2. De gegevens moeten worden bewaard voor zover dat is toegestaan door het nationale recht of een andere nationale bestuurlijke regeling, en beschermd gedurende de termijn die noodzakelijk is met het oog op financiële controle en onderzoek van beveiligingsinbreuken; na afloop van de bewaringstermijn worden de gegevens veilig vernietigd.	Geen nadere invulling of specificatie
Substantieel	Zelfde als niveau laag.	Addenda bij Laag punt 1 en 2 en van toepassing op niveau Substantieel en Hoog

1. Een Participant MOET persoonsgegevens van Gebruikers bewaren in overeenstemming met de doelen zoals beschreven in de paragraaf Privacy.
2. Een Participant MOET waarborgen dat de betreffende bewaartermijn in acht wordt genomen voor de hieronder genoemde informatiecategorieën:
    1. Informatietransacties (inlog historie), de elektronische berichten die de Gebruiker met het gebruik van zijn Authenticatiemiddel gegenereerd, MOETEN gedurende 14 maanden worden bewaard ten behoeve van navraag door de Gebruiker, het aanmelding van een administratieve fout, geschil of misbruik. Het is toegestaan de gegevens zoals bedoeld in 2a op uitdrukkelijk verzoek van de Gebruiker voor een bepaalde (eindige) termijn langer te bewaren dan 14 maanden.
    2. Persoonsidentificatiegegevens van Gebruikers ten behoeve van de uitgifte van Authenticatiemiddelen MOETEN bewaard worden gedurende de geldigheid van het middel plus de bewaartermijn voor de jongste informatietransactie zoals genoemd in 2a.
    3. Loggings van activiteiten van personeel en beheerders voor toegang en beheer op systemen die zijn betrokken bij de uitgifte van Authenticatiemiddelen en systemen die de in dit kader bedoelde authenticaties met de Authenticatiemiddelen faciliteren MOETEN gedurende 14 maanden worden bewaard ter ondersteuning van onderzoek naar aanleiding van vragen van Gebruikers en aanmeldingen van een fout, geschil of misbruik.
    4. Gegevens ten behoeve van technische foutopsporing en technische foutcorrectie voor de werking van de dienst:
        1. Gegevens ten behoeve van foutopsporing over participanten heen MOETEN 14 dagen worden bewaard.
        2. Indien de bedoelde gegevens geen persoonsgegevens bevatten is er geen voorgeschreven bewaartermijn.
3. De toegang tot in elk geval de bij 2a t/m 2c genoemde gearchiveerde gegevens MOET zijn beperkt tot personeel dat hiertoe een specifieke benoemde bevoegdheid heeft. De logging van de gezochte toegang door dit personeel wordt behandeld zoals in 2c is aangegeven.
4. Een Participant MOET waarborgen dat zodra een geschil, administratieve fout of een vermoeden van misbruik wordt aangemeld door een Gebruiker, Dienstverlener, andere Participant of opsporingsinstantie de relevante gegevens zoals bedoeld in 2a t/m 2c worden veilig gesteld zolang het geschil bestaat respectievelijk zolang het onderzoek door betrokkenen naar het misbruik loopt.
5. Een Participant MOET de gegevens bedoeld in 2a en 2b zodanig archiveren dat de audit-trail van de informatietransactie tussen een Gebruiker en Dienstverlener sluitend wordt. De audit-trail MOET de reconstructie van een succesvolle authenticatie mogelijk maken zodanig dat objectief is vast te stellen dat het authenticatiemiddel is gebruikt. In elk geval MOETEN de volgende gegevens gearchiveerd worden:
    1. Een Participant MOET alle door hem ondertekende berichten of een betrouwbare samenvatting van de ondertekende berichten en alle door hem ontvangen ondertekende berichten of betrouwbare samenvatting van berichten archiveren met de bewaartermijn genoemd in 2a.
    2. Een Authenticatiedienst en een Middelenuitgever MOETEN het bewijs van de uitgifte en registratie van een Authenticatiemiddel archiveren met de bewaartermijn genoemd is 2b.
    3. Een Authenticatiedienst MOET bij een informatietransactie een referentie naar het gebruikte Authenticatiemiddel vastleggen met de bewaartermijn genoemd in 2a.
    4. Een Toegangsdienst MOET bij elk antwoordbericht aan de Dienstverlener een referentie naar de betrokken berichtenuitwisseling archiveren met de bewaartermijn genoemd in 2a.
6. Een Participant MOET waarborgen dat gearchiveerde gegevens integer bewaard blijven gedurende de genoemde termijnen.
7. Een Participant MOET waarborgen dat gearchiveerde persoonsgegevens worden vernietigd zodra er geen grondslag meer is voor het bewaren ervan.

Toelichting bij punt 2: De in 2a genoemde termijn voor gebruiksgegevens is een garantietermijn voor de Gebruiker waarmee hij 13 maanden in staat wordt gesteld om gedurende die periode fouten en afwijkingen te ontdekken. 1 maand is nodig om verwerking van verzoeken op de grens van de 13e naar de 14e maand grensgevallen zeker te stellen. Het verlengen van de termijn mag alleen na een expliciet en te archiveren verzoek daartoe van de Gebruiker plaatsvinden. De termijn MAG NIET voor onbepaalde tijd worden verlengd. NB de genoemde bewaartermijnen kunnen nog wijzigen als gevolg van nadere besluiten over de invulling van de bestrijding van misbruik en fraude.

Toelichting bij punt 4: Zodra een opsporingsinstantie in het onderzoek betrokken is zijn de regels omtrent het veiligstellen van informatie en overdracht daarvan aan de opsporingsinstantie van kracht.

Noot bij 2: Referentie ISO/IEC 27002:2013 paragraaf 18.1.3, 18.1.4

Noot bij 3, 5, 6: Referentie ISO/IEC 27002:2013 paragraaf 12.4.2,12.4.3, 12.4.4

Noot bij 4: Referentie ISO/IEC 27002:2013 paragraaf 16.1.7

		De eisen 1/m 4, 5a en 6 t/m 8 zijn van toepassing op alle participanten. De eisen in punt 5b en 5c zijn van toepassing op Authenticatiedienst en Middelenuitgever. De eis in punt 5d is van toepassing op de Toegangsdienst
Hoog	Zelfde als niveau laag.	Zelfde als niveau substantieel.

2.4.5 Faciliteiten en personeel

Deze paragraaf betreft de vereisten aan de competenties en integriteit van personeel en eisen voor de bescherming van- en toegang tot faciliteiten.

Niveau betrouwbaarheid	eIDAS tekst uitvoeringsverordening	Nadere invulling en specificatie Uniforme Set van Eisen
Laag	1. Er zijn procedures om te waarborgen dat personeelsleden en subcontractanten voldoende zijn opgeleid en gekwalificeerd en dat zij ervaren zijn in de vaardigheden die vereist zijn voor de taken die zij vervullen. 2. Er zijn voldoende personeelsleden en subcontractanten om de dienstverlening voldoende te waarborgen overeenkomstig het beleid en de procedures. 3. De voor de dienstverlening gebruikte faciliteiten staan onder permanente controle en worden permanent beschermd tegen schade door milieu-invloeden, ongeoorloofde toegang en andere factoren die de veiligheid van de dienst kunnen aantasten. 4. De voor de dienstverlening gebruikte faciliteiten zijn zodanig ingericht dat de toegang tot zones met persoonsgegevens, cryptografische gegevens en andere gevoelige informatie beperkt is tot bevoegde personeelsleden of subcontractanten.	Geen nadere invulling of specificatie
Substantieel	Zelfde als niveau laag.	Addenda bij Laag punt 1 t/m punt 4 en van toepassing op niveau Substantieel en Hoog. 1. Ad 1 Het personeel dat identificaties uitvoert ten behoeve van de uitgifte van middelen en toegang tot gebruiksgegevens MOET zijn opgeleid voor het beoordelen van de geldigheid van de relevante identiteitsdocumenten en verifiëren van persoonskenmerken. 2. Ad 1 Een Participant MOET waarborgen dat zijn personeel handelt vanuit het bewustzijn dat zij werken met persoonsgegevens. 3. Ad 1 Een Participant MOET gedurende het dienstverband de integriteit van het betrokken personeel waarborgen. 1. Een Participant MOET als voorwaarde voor het in dienst treden een vorm van screening toepasen die minimaal een vergelijkbare kwaliteit heeft als een verstrekte Verklaring Omtrent het Gedrag (VOG). 2. Een Participant MOET in dit kader bij kritieke processen het risico op samenspanning mitigeren. 4. Ad 1 t/m 4 Een Participant MOET de betreffende vereisten als beheersmaatregel opnemen in het beheerssysteem voor informatiebeveiliging. Toelichting bij punt 1: Referentie ISO/IEC 27002:2013 paragraaf Toelichting bij punt 3b: Bedoeld zijn hier in elke geval risico's in processen die bij optreden kunnen leiden tot uitgifte van middelen aan fictieve identiteiten, uitgifte van middelen op naam van bestaande identiteiten zonder dat deze daarom hebben verzocht, uitvoeren van authenticaties zonder wilsuiting van de Gebruiker, onrechtmatige toegang tot Persoonsidentificatiegegevens en gebruiksgegevens. De referentie voor kwaliteit van de opleiding is de NVVB-opleiding voor balie-ambtenaren Burgerzaken. https://publieksacademie.gemeente.nl/opleidingen/opleiding-id-en-adresfraude/ Noot bij 1: Referentie ISO/IEC 27002 paragraaf 7.2 Noot bij 2: Referentie ISO/IEC 27002 paragraaf 7.1, 7.2 Noot bij 3: Referentie ISO/IEC 27002 paragraaf 7.1, 7.2, 7.3, 6.1.2 De eisen in punt 1 zijn van toepassing op de Middelenuitgever en de Authenticatiedienst. De eisen in punt 2 t/m 4 zijn van toepassing op alle Participanten.
Hoog	Zelfde als niveau laag.	Zelfde als niveau substantieel

Functionaliteit en Techiek

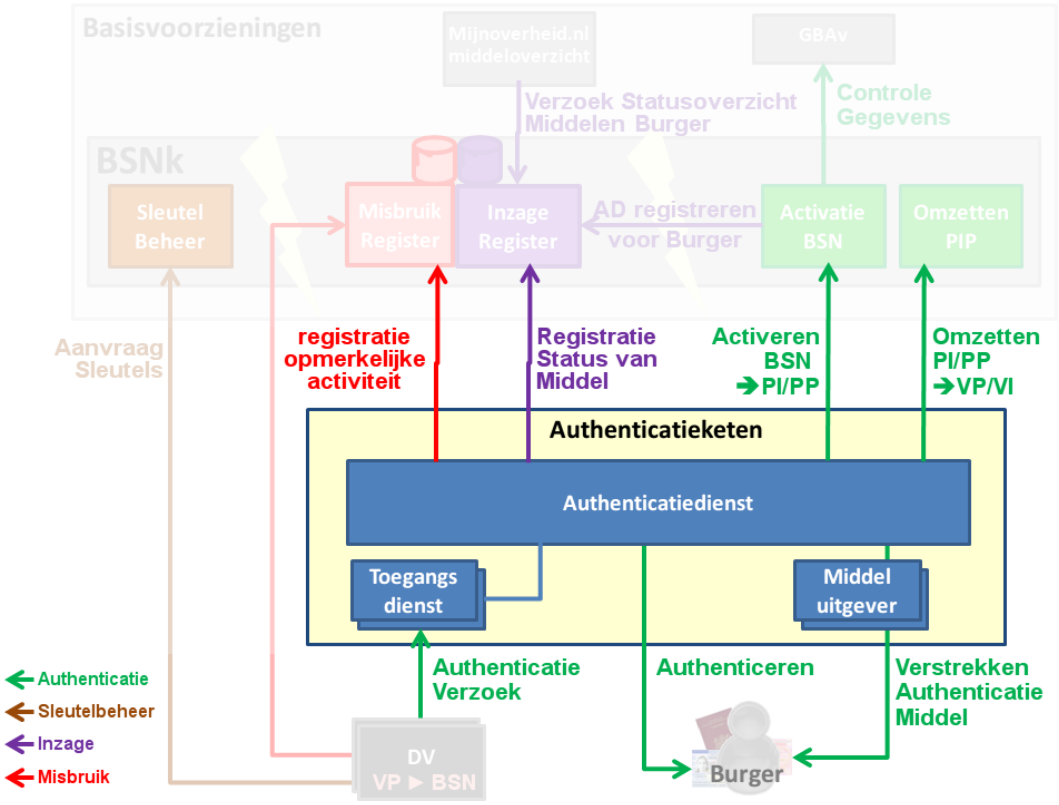
Dit hoofdstuk bevat de beschrijving van de functionaliteit en technische specificaties. Ten behoeve van de hanteerbaarheid zijn deze twee onderwerpen opgenomen in subparagrafen. De paragraaf Functionaliteit is in het Nederlands geschreven. De paragraaf Techniek is in het Engels geschreven, omdat bij technische specificaties Engels de de facto voertaal is.

- Functionaliteit — Deze paragraaf beschrijft de centrale functies die de partijen in de Authenticatieketen uit moeten kunnen voeren en de koppelvlakken die daarvoor gebruikt moeten worden.
- Techniek — This chapter describes the technical requirements for Participants.

Functionaliteit

Deze paragraaf beschrijft de centrale functies die de partijen in de Authenticatieketen uit moeten kunnen voeren en de koppelvlakken die daarvoor gebruikt moeten worden.

De functies worden onderverdeeld in Authenticatie, Sleutelbeheer, Inzage en Misbruikbestrijding. De functies zijn in deze paragraaf in beschrijvende tekst en als illustratie opgenomen, zie daarvoor de onderstaande figuur. De eisen die gelden voor betreffende functionaliteit zijn opgenomen in andere paragrafen. De technische specificaties van de koppelvlakken zijn opgenomen in Techniek.



Authenticatie

Authenticatie betreft de functies die nodig zijn om een Gebruiker te kunnen authenticeren voor een Dienstverlener. Een (BSN van de) Gebruiker moet hiervoor eerst geactiveerd worden bij het BSNk en dat levert een Polymorf Identiteit/Pseudoniem (PI/PP) op die gekoppeld kan worden met een Authenticatiemiddel. Dit Authenticatiemiddel moet op zijn beurt verstrekt worden aan de Gebruiker. Vervolgens moet een Dienstverlener een authenticatieverzoek in kunnen dienen bij de (rol) Toegangsdienst, die ook door de Authenticatiedienst zelf in gevuld mag worden. De Authenticatiedienst zal de Gebruiker laten authenticeren met zijn Authenticatiemiddel en bij succes een authenticatieverklaring opstellen aan de Dienstverlener met daarin de identiteit van de Gebruiker. Hiervoor zal de Authenticatiedienst de Polymorf Identiteit/Pseudoniem (PI/PP) om moeten zetten naar een Versleutelde Identiteit/Pseudoniem als de Dienstverlener juist wel of juist geen autorisatie heeft voor het gebruik van het BSN voor betreffende Dienst. De Authenticatiedienst kan dit zelf doen als met zijn eigen HSM (met speciale toepassing en sleutelmateriaal erop) of dit door het BSNk laten doen.

De Uniforme Set van Eisen stelt eisen aan al deze authenticatie functies, op diverse Betrouwbaarheidsniveaus. Maar alleen de koppelvlakken met de Dienstverlener en met de Basisvoorziening BSNk zijn in detail voorgeschreven. Voor de invulling van interne koppelvlakken en voor de 'koppelvlakken' met de Gebruiker hebben de partijen in de Authenticatieketen meer

vrijheid. Zolang ze maar aan de eisen blijven voldoen. Hierdoor is onder andere meer innovatie mogelijk.

Sleutelbeheer

Het ontwerp dat ten grondslag ligt aan de Uniforme Set van Eisen verplicht het gebruik van PKI-Overheid certificaten en bijbehorend sleutelmateriaal. Echter met Sleutelbeheer wordt hier het beheer en gebruik van een geheel andere soort van sleutels bedoeld. Dit betreft het sleutelmateriaal dat bedoeld is voor het gebruik van de Polymorf Identiteit/Pseudoniem (PI/PP) . Wat betreft de Authenticatieketen komt alleen de rol van Authenticatiedienst in aanmerking om gebruik te maken van dergelijk sleutelmateriaal. Echter alleen in het geval dat de Authenticatiedienst gebruik gaat maken van een eigen HSM met een speciale toepassing er op voor het omzetten van Polymorf Identiteit/Pseudoniem (PI/PP) naar een Versleutelde Identiteit/Pseudoniem voor een specifiek Dienstverlener (of andere Ontvangende Partij). Het sleutelmateriaal dat nodig is voor deze Versleutelde Identiteit/Pseudoniem wordt met een formele, zeer veilige en betrouwbare procedure in de HSM gezet. Er is hier geen koppelvlak voor gespecificeerd. Dienstverleners hebben geen HSM nodig en kunnen wel van een digitaal koppelvlak gebruik maken.

Inzage

Inzage betreft de functies die nodig zijn om een Gebruiker een actueel inzicht te geven in de status van Authenticatiemiddelen die op zijn identiteit (BSN) staan. Dit betreft dus ook alleen maar de rol van Middelenuitgever. Overigens biedt inzage ook een mogelijkheid om vanuit een centraal overzicht (via Mijnoverheid) de Gebruiker richting een Middelenuitgever door te verwijzen om daar bijvoorbeeld een middel te laten deactiveren als daar iets niet mee klopt. Om dit mogelijk te maken zijn Middelenuitgevers verplicht om de status (actief, inactief, ingetrokken) van hun Authenticatiemiddelen door te geven aan het Inzageregister van het BSNk. Voor het registeren van de status van een Authenticatiemiddel is een koppelvlak gespecificeerd.

Misbruikbestrijding

Misbruik betreft de functies die nodig zijn om misbruikbestrijding effectief, efficiënt en privacyvriendelijk in te kunnen richten in een relatief complexe omgeving met meerdere rollen met meerdere partijen en een ontwerp dat gericht is op privacy en geen centraal punt heeft waar alles langs komt. De Uniforme Set van Eisen voorziet in een functie met bijbehorende koppelvlakspecificaties voor het registreren van een Opmerkelijke gebeurtenis door een Authenticatiedienst en Middelenuitgever.

Toelichting: De operationalisering van de bestrijding van misbruik wordt nog nader uitgewerkt.

Rollen

Deze paragraaf benoemt de rollen die de Uniforme Set van Eisen beschrijft.

Rollen waarvoor erkenning noodzakelijk is

De Uniforme Set van Eisen kent de volgende rollen waarvoor een erkenning noodzakelijk is. Deze worden aangeduid met de term Participanten.

- Rol Authenticatiedienst (AD) — Een Authenticatiedienst (AD) voert authenticatieprocedures uit waarmee Gebruikers worden geauthentiseerd daarbij gebruikmakend van elektronische Authenticatiemiddelen verstrekt door een Middelenuitgever. De Authenticatiedienst levert op basis van de authenticatieprocedure een Authenticatieverklaring aan de Toegangsdienst.
- Rol Middeluitgever (MU) — De Middelenuitgever (MU) is een rol van een Participant die een elektronisch Authenticatiemiddel verstrekt aan de Gebruiker en het middel bij het BSNk activeert voor gebruik in het

Publieke domein. De Middelenuitgever biedt de Gebruiker de mogelijkheid om zijn Authenticatiemiddel(en) te beheren en zorgt ervoor dat het BSNk Inzageregister een actuele status van de Authenticatiemiddelen (of de relatie) heeft.

- Rol Toegangsdienst (TD) — Een Toegangsdienst (TD) verstrekt verklaringen over de identiteit van een Gebruiker aan de Dienstverlener. Op basis van deze verklaring besluit de Dienstverlener over toegang van de Gebruiker tot de Dienst. De Toegangsdienst verstrekt de verklaringen op basis van verklaringen van een Authenticatiedienst. De Toegangsdienst biedt de Gebruiker de mogelijkheid een Authenticatiedienst te kiezen.

Overige rollen

De volgende rollen worden wel in de Uniforme Set van Eisen beschreven, maar zijn geen onderdeel van het Bereik

- Rol Dienstverlener (DV) - Dienstverlener is een rol die elektronische Diensten aanbiedt aan Gebruikers waarvoor Authenticatie voorwaardelijk is.
- Ondersteunende rollen, belegd bij het BSNk, zie Rollen BSNk.

De specificaties van de gebruikte koppelvlakken tussen de verschillende rollen staan beschreven in Koppelvlakspecificaties.

Participanten

Een Participant is gedefinieerd als: Een partij in de Authenticatieketen waarvan is vastgesteld door de Minister van Binnenlandse Zaken en Koninkrijksrelaties dat deze voldoet aan de eisen zoals gesteld in de Uniforme Set van Eisen.

Huidige rollen

Een Participant kan invulling geven aan één of meer van de volgende rollen.

- Rol Authenticatiedienst (AD)
- Rol Middelenuitgever (MU)
- Rol Toegangsdienst (TD)

Waarbij expliciet voor bovengenoemde rollen geldt dat het mogelijk is dat deze een geïntegreerde invulling kennen binnen één partij, of in een samenwerkingsverband met meerdere afzonderlijke partijen.

Toekomstige rollen

De volgende additionele Participant rollen zijn voorzien in latere versies van de Uniforme Set van Eisen:

- Machtigingsregister
- Ondertekendienst
- Attributendiensten
- SectorIDDienst

Voor deze rollen geldt dat er geen sprake kan zijn van een geïntegreerde invulling. Het blijft mogelijk voor een Participant om ook deze additionele rollen in te vullen. Deze dient dan volledig gescheiden te zijn van zijn andere dienstverlening als Participant. Eisen hieraan worden ook in toekomstige versies van de Uniforme Set van Eisen toegevoegd.

Rol Authenticatiedienst (AD)

Een Authenticatiedienst (AD) voert authenticatieprocedures uit waarmee Gebruikers worden geauthentiseerd daarbij gebruikmakend van elektronische Authenticatiemiddelen verstrekt door een Middelenuitgever. De Authenticatiedienst levert op basis van de authenticatieprocedure een Authenticatieverklaring aan de Toegangsdienst.

Het is gebruikelijk dat de partij in de rol van Authenticatiedienst ook de rol van Middelenuitgever en/of die van Toegangsdienst vervult. In federaties is de rol van Authenticatiedienst en Toegangsdienst vaak gescheiden.

De rol van de Authenticatiedienst is onder andere verantwoordelijk voor:

- Het weloverwogen authenticeren van de Gebruiker ten behoeve van een Dienstverlener die daarbij op basis van de Autorisatielijst BSN een Versleutelde Identiteit (BSN) dan wel Versleutelde Pseudoniem ontvangt in een Authenticatieverklaring (volgens de eisen aan de Betrouwbaarheidsniveaus en met behulp van GUC1 Aantonen identiteit).
- Het zorgvuldig vastleggen en ontsluiten (richting de Gebruiker) van de authenticatiehistorie (volgens eisen aan Informatiebeveiliging en Privacy)
- Indien de Authenticatiedienst en de Middelenuitgever twee verschillende partijen zijn[1], dan ook:
  - Het activeren (en de-activeren) van de relatie met de Gebruiker bij de betreffende Middelenuitgever
  - Het zorgvuldig verkrijgen van de Polymorfe identiteit/pseudoniem van deze Gebruiker aan deze Authenticatiedienst (volgens eisen aan Informatiebeveiliging en Privacy).

Voetnoot

1. Voorbeeld: RDW is Middelenuitgever van het rijbewijs dat bij de Authenticatiedienst DigiD gebruikt kan worden.

Rol Middelenuitgever (MU)

De Middelenuitgever (MU) is een rol van een Participant die een elektronisch Authenticatiemiddel verstrekt aan de Gebruiker en het middel bij het BSNk activeert voor gebruik in het Publieke domein. De Middelenuitgever biedt de Gebruiker de mogelijkheid om zijn Authenticatiemiddel(en) te beheren en zorgt ervoor dat het BSNk Inzageregister een actuele status van de Authenticatiemiddelen (of de relatie) heeft.

De rol van Middelenuitgever is onder andere verantwoordelijk voor:

- De uitgifte, beheer en intrekking van Authenticatiemiddelen aan de Gebruiker, inclusief maatregelen ter voorkoming van identiteitsfraude (volgens de eisen aan de Betrouwbaarheidsniveaus).
- Het zorgvuldig vastleggen van de daarvoor geregistreerde Persoonsidentificatiegegevens in een administratie (volgens eisen aan Informatiebeveiliging en Privacy).
- Het activeren van de relatie met de Gebruiker bij het BSNk naar aanleiding van een weloverwogen verzoek van de Gebruiker, waarbij de Middelenuitgever een Polymorfe identiteit/pseudoniem ontvangt (volgens AUC1 Activeren BSN).
- Het actueel houden van de status van een Authenticatiemiddel (of relatie) bij het BSNk Inzageregister (volgens AUC3 Aanpassen status relatie en/of authenticatiemiddel).
- Indien de Middelenuitgever andere partijen dan zichzelf in de rol van Authenticatiedienst ondersteunt[1], dan ook:
  - Het autoriseren van een Authenticatiedienst voor het gebruik van een Authenticatiemiddel (volgens "MU - AD affiliation" in de Metadata).
  - Het activeren van een relatie van een Gebruiker met een Authenticatiedienst naar aanleiding van een weloverwogen verzoek van de Gebruiker (volgens eisen aan Informatiebeveiliging en Privacy).
  - Het zorgvuldig verstrekken van de Polymorfe identiteit/pseudoniem van deze Gebruiker aan deze Authenticatiedienst (volgens eisen aan Informatiebeveiliging en Privacy).
  - Het actueel houden van (de status van) de relatie tussen deze Authenticatiedienst en de Gebruiker bij het BSNk

Inzageregister (volgens AUC3 Aanpassen status relatie en/of authenticatiemiddel).

Voetnoot

1. voorbeeld: RDW is Middelenuitgever van het rijbewijs dat bij de Authenticatiedienst DigiD gebruikt kan worden.

Rol Toegangsdienst (TD)

Een Toegangsdienst (TD) verstrekt verklaringen over de identiteit van een Gebruiker aan de Dienstverlener. Op basis van deze verklaring besluit de Dienstverlener over toegang van de Gebruiker tot de Dienst. De Toegangsdienst verstrekt de verklaringen op basis van verklaringen van een Authenticatiedienst. De Toegangsdienst biedt de Gebruiker de mogelijkheid een Authenticatiedienst te kiezen.

De rol van Toegangsdienst is onder andere verantwoordelijk voor:

- Het verstrekken van een verklaring over de identiteit van een Gebruiker op verzoek van een Dienstverlener met daarin een Authenticatieverklaring van een Authenticatiedienst en een Versleutelde Identiteit/Pseudoniem (met BSN dan wel persistent Pseudoniem) van deze Gebruiker specifiek voor deze Dienstverlener (volgens eisen aan Informatiebeveiliging en Privacy en met behulp van GUC1 Aantonen identiteit)
- Het ondersteunen van een Gebruiker om efficiënt de juiste Authenticatiedienst te kiezen (met behulp van GUC1 Aantonen identiteit)
- Het aanvragen van Sleutelmateriaal ten behoeve van de Dienstverlener bij het BSNk Sleutelbeheer (met behulp van AUC5 Verstrekken sleutelmateriaal Dienstverleners)
- Het ontzorgen van een Dienstverlener (met name in het geval van Federaties[1]) door helpen bij de technische aansluiting, het verbergen van de achterliggende complexiteit en het vereenvoudigen van diverse change en foutopsporings procesen.

Voetnoot

- Federaties zoals iDIN en Idensys;

Overige rollen

De volgende rollen vallen niet onder de noemer Participant, maar zijn wel van belang in de Uniforme Set van Eisen.

- Rol Dienstverlener (DV)
- Rollen BSNk

Rol Dienstverlener (DV)

De Dienstverlener is gedefinieerd als: Dienstverlener is een rol die elektronische Diensten aanbiedt aan Gebruikers waarvoor Authenticatie voorwaardelijk is. De Dienstverlener is geen Participant binnen de Uniforme Set van Eisen, zie paragraaf Bereik. Met andere woorden, de Uniforme Set van Eisen legt geen aanvullende eisen op aan de Dienstverlener boven de eisen die al

gesteld worden in de GDI.

Rollen BSNk

Het BSNk is een voorziening in het kader van de Generieke Digitale Infrastructuur (GDI) die het mogelijk maakt om publieke en private authenticatiemiddelen te gebruiken in het publiek domein.

Het BSNk heeft een aantal rollen:

Rol	Rolbeschrijving
Rol Inzageregister (IR)	Het BSNk stelt de Gebruiker in staat om met behulp van een inzagefunctie bij Mijnoverheid controle te houden over zijn authenticatiemiddelen.
Rol Koppeldienst (KD)	Het BSNk stelt een Authenticatiedienst (in samenwerking met een Middelenuitgever) in staat om een Authenticatiemiddel op een veilige, betrouwbare en vertrouwelijke te koppelen aan een (BSN van een) Gebruiker ten behoeve van Dienstverleners in het Publieke domein.
Rol Misbruikbestrijdingsregister (MBR)	Het BSNk vervult de rol van Misbruikbestrijdingsregister waarbij een Middelenuitgever of Authenticatiedienst een Opmerkelijke gebeurtenis vast kan laten leggen ten behoeve van misbruikbestrijding.
Rol Sleutelbeheerder (SB)	Een centrale rol, belegd bij de Beheerorganisatie BSNk die Sleutelmateriaal verstrekt aan Participanten en Dienstverleners
Rol Beheerder Metadata (BM)	De Beheerorganisatie BSNk beheert en publiceert drie soorten metadata die nodig zijn om het authenticeren van Gebruikers in het Publieke domein op een veilige en betrouwbare manier te laten werken.

Rol Inzageregister (IR)

Het Inzageregister is gedefinieerd als: Een centrale rol, belegd bij de Beheerorganisatie BSNk, waarbij de status van authenticatiemiddelen wordt geregistreerd en gebruikers deze status in kunnen zien. Het BSNk stelt de Gebruiker in staat om met behulp van een inzagefunctie bij Mijnoverheid controle te houden over zijn authenticatiemiddelen.

Ten behoeve van de rol van Inzageregister implementeert het BSNk twee use cases:

- AUC3 Aanpassen status relatie en/of authenticatiemiddel - Een Middelenuitgever is verplicht om de status van (de relatie met) elke Gebruiker die geactiveerd is voor het Publieke domein actueel te houden bij het Inzageregister van het BSNk. De registratie vindt plaats met een Inzageregister specifiek Pseudoniem van de Gebruiker (dus niet met BSN) en een identificatie en omschrijving van het betreffende relatie of Authenticatiemiddel. Het Inzageregister versleutelt de gegevens met behulp van het specifieke Pseudoniem voordat ze daadwerkelijk opgeslagen worden.
- GUC3 Inzage overzicht authenticatiemiddelen (geen onderdeel van de Uniforme Set van Eisen) - Een Gebruiker

krijgt via Mijnoverheid inzage in de status van hun Authenticatiemiddelen die (ooit) geactiveerd zijn binnen het Publieke domein. Mijnoverheid laat de Gebruiker zich authenticeren voor zichzelf en voor het Inzageregister. Hiermee verkrijgt Mijnoverheid een identiteitsverklaring waarmee hij de statusgevens van betreffende Gebruiker aan kan vragen bij het Inzageregister. Tenslotte toont Mijnoverheid deze statusgegevens in een overzicht aan Gebruiker.

Rol Koppeldienst (KD)

Het BSNk stelt een Authenticatiedienst (in samenwerking met een Middelenuitgever) in staat om een Authenticatiemiddel op een veilige, betrouwbare en vertrouwelijke te koppelen aan een (BSN van een) Gebruiker ten behoeve van Dienstverleners in het Publieke domein. Ten behoeve van de rol van Koppelregister implementeert het BSNk twee use cases:

- AUC1 Activeren BSN - Op verzoek van een Gebruiker activeert een Middelenuitgever diens BSN voor authenticatie in het Publieke domein. Hiervoor stuurt de Middelenuitgever het BSN en controlegegevens naar het BSNk. Na controle genereert en verstrekt het BSNk een Polymorfe identiteit/pseudoniem van deze Gebruiker specifiek voor betreffende Middelenuitgever. Tenslotte registreert het BSNk deze activering bij zijn eigen Inzageregister.

- AUC2 Transformeren - Een Authenticatiedienst ontvangt een authenticatieverzoek van een Dienstverlener voor een bepaalde Dienst. De Authenticatiedienst stelt vast of de gevraagde Dienst een BSN of een persistent pseudoniem nodig heeft. Indien dit eerste wordt gecontroleerd of de betreffende Dienstverlener een BSN mag ontvangen. Vervolgens transformeert de Authenticatiedienst op basis daarvan de Polymorfe identiteit/pseudoniem van de Gebruiker naar een Versleutelde Identiteit/Pseudoniem voor deze Dienstverlener. Een Authenticatiedienst kan deze transformatie door het BSNk laten doen. Een Authenticatiedienst heeft hiernaast de keuze om deze transformatie zelf uit te voeren. Hiertoe kan de Authenticatiedienst een speciaal beveiligd computer systeem (HSM) aanschaffen en speciaal Sleutelmateriaal verkrijgen van de Sleutelbeheer-functie.

Rol Misbruikbestrijdingsregister (MBR)

Het BSNk vervult de rol van Misbruikbestrijdingsregister waarbij een Middelenuitgever of Authenticatiedienst een Opmerkelijke gebeurtenis vast kan laten leggen ten behoeve van misbruikbestrijding.

Ten behoeve van de rol van Misbruikbestrijdingsregister implementeert het BSNk een use case:

- AUC4 Registreren Opmerkelijke Gebeurtenis - Een Authenticatiedienst of Middelenuitgever registreert een Opmerkelijke gebeurtenis van een Gebruiker bij het Misbruikbestrijdingsregister. De registratie vindt plaats met een Misbruikbestrijdingsregister specifiek Versleutelde Identiteit/Pseudoniem van de Gebruiker en gegevens over de Opmerkelijke gebeurtenis.

Rol Sleutelbeheerder (SB)

Een centrale rol, belegd bij de Beheerorganisatie BSNk die Sleutelmateriaal verstrekt aan Participanten en Dienstverleners

Ten behoeve van de Rol van Sleutelbeheer implementeert het BSNk twee use cases:

- AUC5 Verstrekken sleutelmateriaal Dienstverleners - Het BSNk beheert en verstrekt via een Toegangsdienst cryptografisch Sleutelmateriaal aan elke Dienstverlener die aantoonbaar beschikt over een PKIoverheid-certificaat. Indien de Dienstverlener geautoriseerd is om het BSN te verwerken verstrekt het BSNk speciaal BSN Sleutelmateriaal. De Dienstverlener ontsleutelt met dit Sleutelmateriaal het versleutelde BSN of versleutelde pseudoniem van de Gebruiker dat de Dienstverlener verstrekt.
- AUC6 Verstrekken sleutelmateriaal participanten - Het BSNk beheert en verstrekt cryptografisch Sleutelmateriaal aan Authenticatiedienst (en aan zichzelf) om opgenomen te worden in hun speciaal beveiligd computersysteem (HSM), zoals beschreven bij AUC2 Transformeren.

Rol Beheerder Metadata (BM)

De Beheerorganisatie BSNk beheert en publiceert drie soorten metadata die nodig zijn om het authenticeren van Gebruikers in het Publieke domein op een veilige en betrouwbare manier te laten werken.

- In de Metadata staan gegevens over de (erkende) Participanten.
- In de Autorisatielijst BSN staan alle Dienstverleners die geautoriseerd zijn om een BSN te ontvangen van een Gebruiker.
- In de Sleutelverstrekkingslijst staat ten behoeve van transparantie elke sleutelverstrekking door BSNk Sleutelbeheer aan Participanten en Dienstverleners.

Polymorfe encryptie en pseudonimisering

Het optimaal borgen van de privacy van Gebruiker is één van de Uitgangspunten van de Uniforme Set van Eisen. Daartoe is de toepassing van dataminimalisatie geadopteerd zoals ook vastgelegd in artikel 5c van de aankomende Europese privacy verordening: “persoonsgegevens moeten: […] adequaat en ter zake dienend zijn en beperkt blijven tot datgene wat minimaal nodig is voor de doeleinden waarvoor zij worden verwerkt; zij worden alleen verwerkt wanneer en voor zolang als de doeleinden niet zouden kunnen worden verwezenlijkt door het verwerken van andere gegevens dan persoonsgegevens”

Op deze pagina wordt beschreven hoe dataminimalisatie wordt gerealiseerd door toepassing van een Privacy Enhancing Technology genaamd polymorfe encryptie en pseudonimisering. Door toepassing hiervan voorkomt de Uniforme Set van Eisen onder meer de accumulatie van persoonsgegevens (privacy hotspots) alsmede onnodige koppeling risico’s tussen verschillende registraties. Verder wordt het Burgerservicenummer (BSN) alleen gebruikt in die situaties waarin dit strikt noodzakelijk is en wettelijk is toegestaan. In alle andere situaties wordt het gebruik van pseudoniemen voorgeschreven. In zulke gevallen faciliteert de Authenticatiedienst dus niet de verstrekking van het BSN aan een Dienstverlener, maar de verstrekking van een pseudoniem dat gebaseerd is op een Burgerservicenummer (BSN). Er wordt gesproken van ‘faciliteert’ omdat de polymorfe opzet er voor zorgt dat de Authenticatiedienst zelf geen inzage heeft in het BSN of het pseudoniem. Dat wil zeggen, de Authenticatiedienst helpt versleutelde versies van het BSN en een pseudoniem te vormen voor anderen zonder hier zelf inzage in te krijgen.

De pseudoniemen zijn daarbij Dienstverlener-specifiek, verschillende Dienstverleners kennen de Gebruiker onder een ander pseudoniem. Voor dit doel is het noodzakelijk dat pseudoniemen compatibel zijn: alle Authenticatiediensten genereren hetzelfde specifieke pseudoniem voor een Gebruiker bij een bepaalde Dienstverlener.

Het principe van dataminimalisatie wordt ook toegepast op het BSNk, i.e. de partij die faciliteert dat Authenticatiediensten het BSN, of een daarop gebaseerd pseudoniem, kunnen leveren aan een Dienstverlener. De polymorfe opzet realiseert daarbij dat de transformatiefunctie (AUC2 Transformeren) van het BSNk ‘blind’ wordt: het kan deze functie uitvoeren zonder inzicht te krijgen in de identiteit (BSN of pseudoniem) van de Gebruiker. Sterker nog, het BSNk is zelfs niet in staat om vast te stellen dat twee verzoeken van een Authenticatiedienst corresponderen met dezelfde persoon.

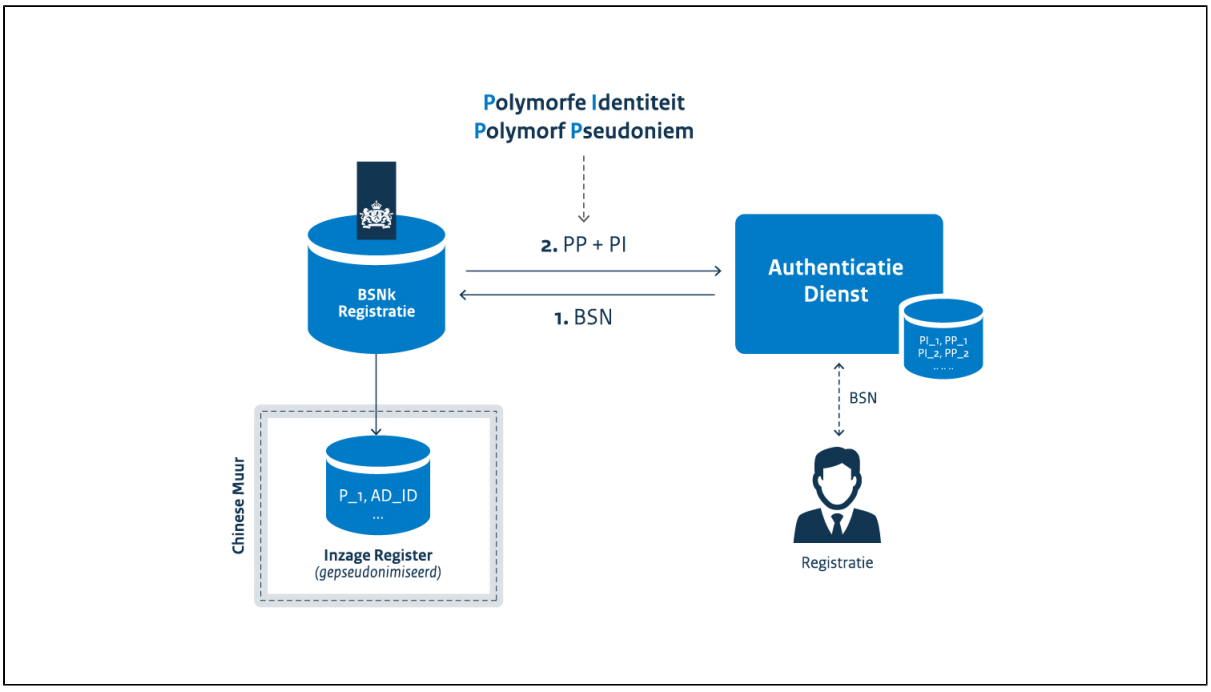
ElGamal

Polymorfe Identiteiten en Pseudoniemen zijn gebaseerd op het publieke sleutel encryptie-algoritme ElGamal dat reeds in 1985 ontwikkeld is en gebaseerd op het zogenaamde Diffie-Hellman sleutel-uitwisselingsprotocol. Het BSNk maakt gebruik van twee verschillende publieke sleutels (een voor PI en een voor PP) die in beheer zijn bij een centrale sleutelbeheerder. Dit betekent dat geen andere partij toegang heeft tot de corresponderende private sleutels. Naast de ElGamal publieke sleutel maakt de registratieservice van het BSNk gebruik van Authenticatiedienst-specifiek Sleutelmateriaal. Hiermee wordt gezorgd dat de polymorfe vormen PI en PP niet compatibel zijn. Dat wil zeggen dat een PI of PP van de ene Authenticatiedienst niet bruikbaar is voor de andere. Dit verhoogt de robuustheid van de oplossing. Tot slot merken we op dat de PI en PP digitaal ondertekend worden door het BSNk zodat een Authenticatiedienst niet zonder medewerking van BSNk zelf een PP of PI kan maken.

Het werken met polymorfe encryptie en pseudonimisering kent twee fasen: een registratie- en een gebruiksfase.

Registratiefase

In de registratiefase heeft de Authenticatiedienst de Gebruiker en zijn BSN geregistreerd. De Authenticatiedienst registreert de Gebruiker daarna in de infrastructuur door het verzenden van dit BSN naar de BSN activeringsfunctie (AUC1 Activeren BSN) BSNk. Met het BSN worden enkele andere gegevens meegestuurd waarop het BSNk enkele plausibiliteit checks uitvoert. Als deze checks succesvol afgerond worden, krijgt de Authenticatiedienst een Polymorfe Identiteit en Pseudoniem terug geleverd van het BSNk. Zie onderstaande figuur.



Figuur 1: Verstrekken van PI en PP

Hetgeen wordt teruggeleverd naar de Authenticatiedienst bestaat aldus uit twee delen:

- een Polyforme Identiteit (PI) is een versleuteling van het BSN, die de Authenticatiedienst in staat stelt het BSN van de Gebruiker te leveren aan een Dienstverlener,
- een Polymorf Pseudoniem (PP) is een versleuteling van een 'one-way' afgeleide van het BSN en die de Authenticatiedienst in staat stelt pseudoniemen van de Gebruiker te leveren aan een Dienstverlener.

De Authenticatiedienst associeert de PI en PP met het aan de Gebruiker uitgegeven Authenticatiemiddel en slaat deze relatie op in zijn registratie. Na afloop van het registratieproces is de Authenticatiedienst verplicht om het BSN van de Gebruiker te wissen zodat alleen nog diens PI en PP in de registratie van de authenticatiedienst resteren. Zoals we zullen zien, stellen deze cryptogrammen de Authenticatiedienst in staat de Gebruiker te laten aanloggen bij een Dienstverlener. De Authenticatiedienst kan uit de PI en PP zelf echter niet meer het BSN achterhalen.

Behalve dat de BSNk BSN activeringsfunctie polymorfe vormen retourneert naar de Authenticatiedienst stuurt hij ook een bericht naar het Inzageregister. Dit stelt de Gebruiker in staat te zien bij welke Authenticatiediensten hij Authenticatiemiddelen heeft geregistreerd. Op deze wijze kan de Gebruiker zelf signaleren dat er middelen op zijn naam zijn uitgegeven zonder zijn weten en toestemming, i.e. waar fraude aan ten grondslag ligt.

Vanuit het dataminimalisatie beginsel is het Inzageregister niet gebaseerd op het BSN maar op een pseudoniem gebaseerd op het BSN. De BSNk Activeren BSN functie legt geen gegevens vast en kan dit pseudoniem ten behoeve van het Inzageregister wel vormen (in versleutelde vorm) maar ken de (onversleutelde) pseudoniemen niet van Gebruikers bij het Inzageregister. Daartoe is het BSNk in staat het polymorfe pseudoniem om te zetten in een versleuteld pseudoniem voor het Inzageregister. Hier zullen we in de volgende sectie verder op ingaan. We merken op dat het belangrijk is dat functiescheiding (‘Chinese Muur’) wordt toegepast tussen de BSNk functies voor Activeren BSN en voor Inzage.

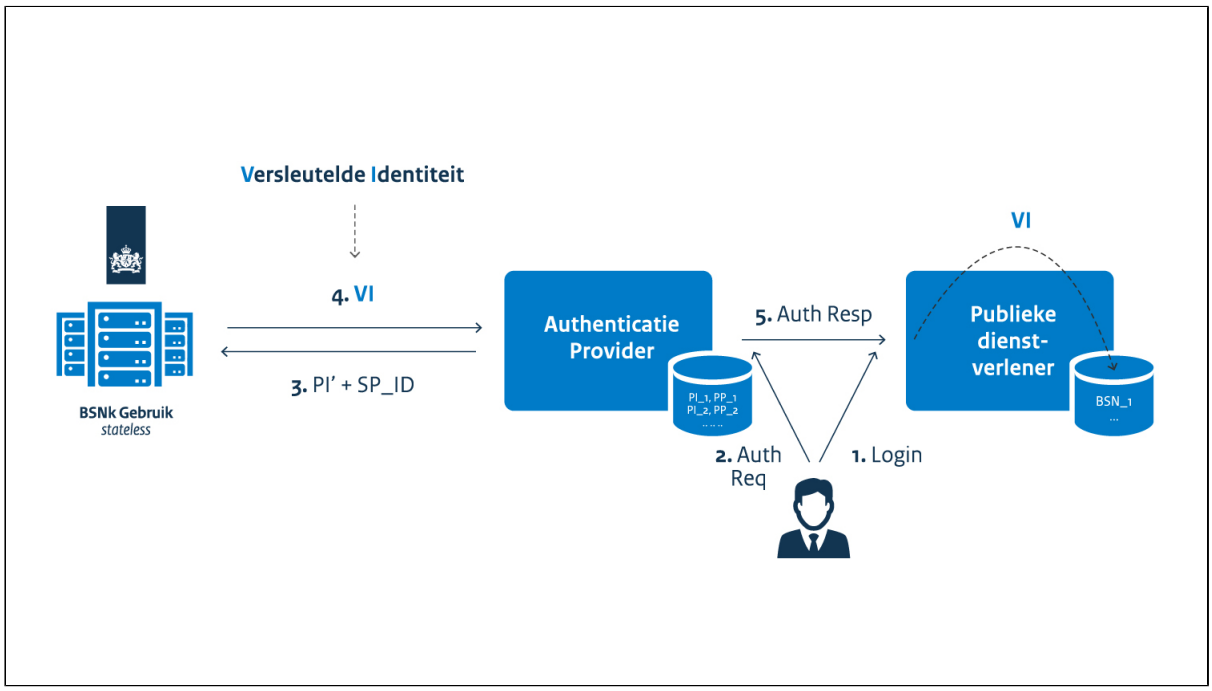
De ontsluiting van het Inzageregister geschiedt middels een standaard toepassing van de polymorfe opzet die we in de volgende sectie nader zullen toelichten.

Gebruiksfase

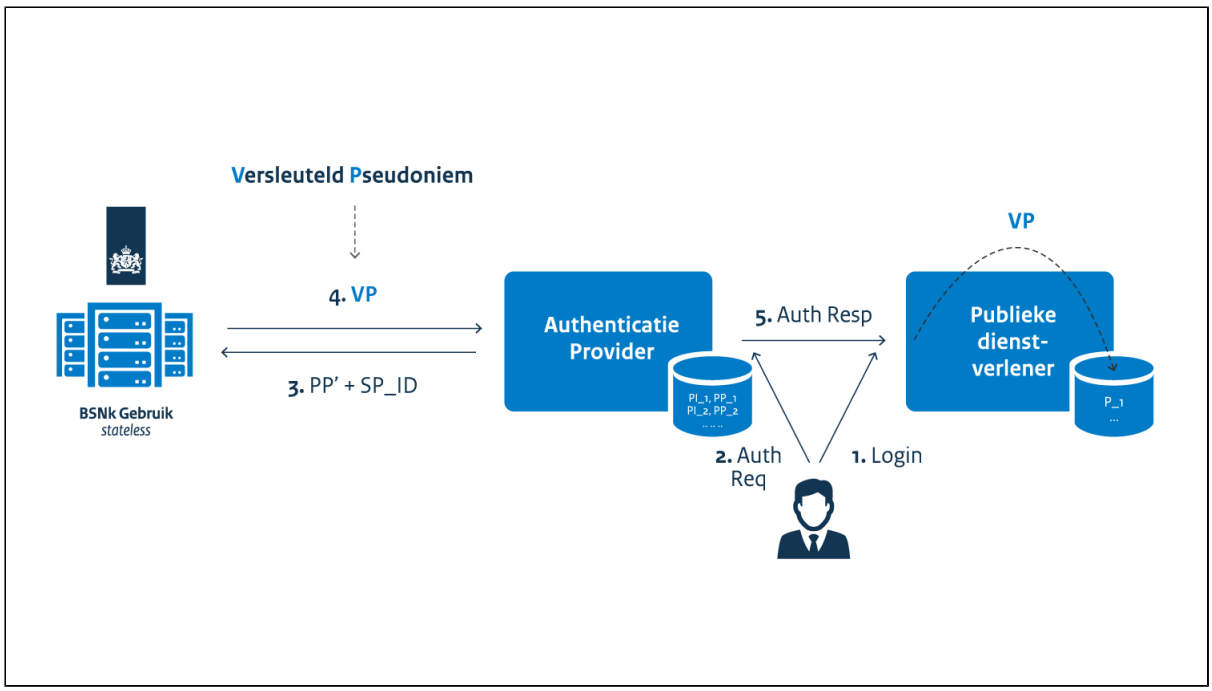
De gebruiksfase start als de Gebruiker wil inloggen bij een Dienstverlener. Dit resulteert in een authenticatieverzoek van de Dienstverlener aan de Authenticatiedienst (via de Toegangsdienst). (Stap 1 en 2 in Figuur 2 en Figuur 3). In het authenticatieverzoek wordt ook aangegeven of de Dienstverlener de Gebruiker onder zijn BSN of onder een pseudoniem wil authenticeren. Vervolgens authenticeert de gebruiker zich bij de Authenticatiedienst, gebruikmakend van het uitgegeven Authenticatiemiddel. (Stap 2 in Figuur 2 en Figuur 3). Als dit succesvol is, zoekt de Authenticatiedienst de gerelateerde Polymorfe Identiteit en Pseudoniem op. Afhankelijk van het authenticatieverzoek stuurt de Authenticatiedienst ofwel de polymorfe identiteit (Stap 4 in Figuur 2), ofwel het polymorfe pseudoniem (Stap 4 in Figuur 2 en Figuur 3) naar de BSN Transformatie functie.

De BSNk gebruik service voert vervolgens een cryptografische handeling uit op de aangeleverde polymorfe vormen. Deze handeling transformeert een Polymorfe Identiteit naar een Versleutelde Identiteit die alleen te ontsleutelen is door de bedoelde Dienstverlener die hieruit het BSN kan achterhalen. Een Polymorf Pseudoniem wordt getransformeerd tot Versleuteld Pseudoniem die ook alleen te ontsleutelen is door de bedoelde Dienstverlener die hieruit het pseudoniem kan achterhalen. Door de toepassing van de techniek van homomorfe versleuteling hebben de genoemde transformaties de bijzondere (privacy) eigenschap dat de Authenticatiedienst geen inzage krijgt in het BSN en/of pseudoniem.

Om de authenticatie te realiseren levert de Authenticatiedienst aldus de Versleutelde Identiteit en/of Versleuteld Pseudoniem aan de Dienstverlener als onderdeel van het authenticatie antwoord. Dit wordt aangegeven in onderstaande twee figuren.



Figuur 2: Authenticatie bij een Dienstverlener onder gebruikmaking van identiteit (BSN)



Figuur 3: Authenticatie bij een Dienstverlener onder pseudoniem

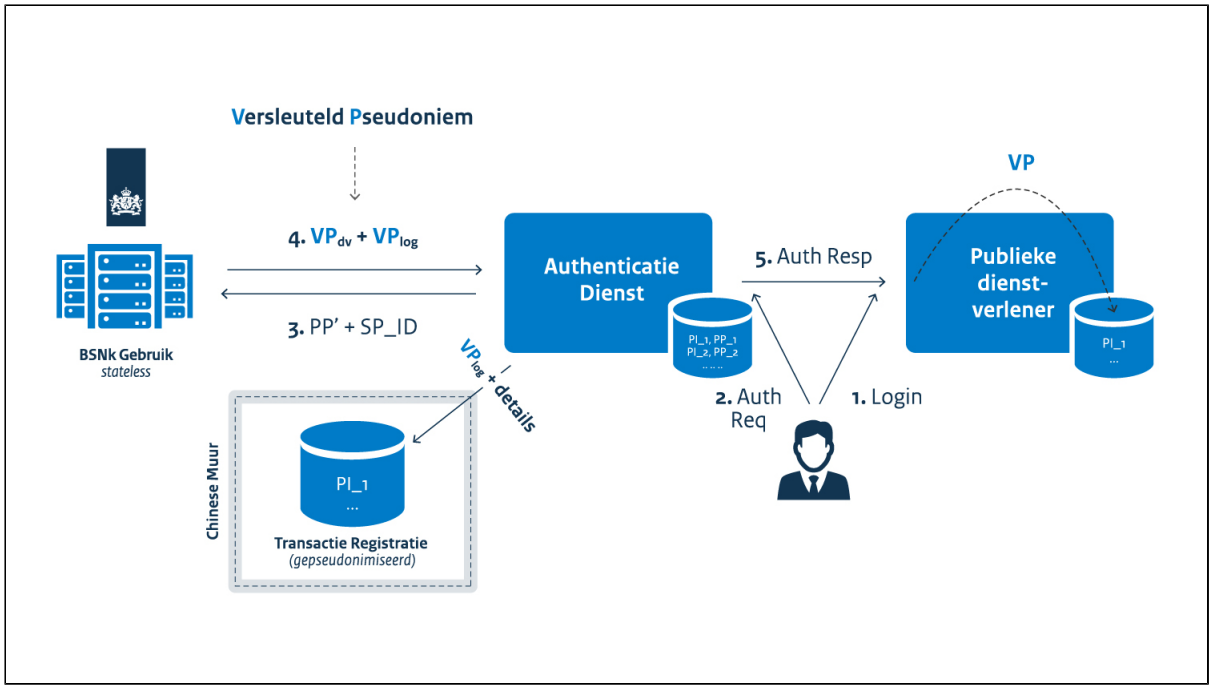
De transformatie van een Polymorfe vorm tot Versleutelde vorm door de gebruik service van BSNk vereist slechts een aantal cryptografische sleutels. Dit betekent dat gebruik service staatloos is, i.e. een protocol dat niets onthoudt. Bovendien stuurt de Authenticatiedienst niet de oorspronkelijk geleverde polymorfe vormen (PI en/of PP) maar gerandomiseerde kopieën

daarvan. Dit is aangegeven met het accent-teken in PI' en PP' in bovenstaande twee figuren.

Deze kopieën zijn functioneel/cryptografisch equivalent aan de oorspronkelijke versies maar zijn daaraan echter niet koppelbaar. Dit wordt cryptografisch afgedwongen en betekent dat BSNk fundamenteel niet in staat is aan de gerandomiseerde kopie aan het origineel te relateren en daarmee aan het BSN van de Gebruiker verstrekt tijdens registratie. Sterker nog, BSNk is zelfs niet eens in staat de gerandomiseerde kopieën aan elkaar te relateren. BSNk is aldus niet in staat om vast te stellen dat dezelfde Gebruiker tweemaal aanlogt.

Dit betekent dat de Polymorfe BSNk gebruiksdienst geen privacy hotspot vormt. De Authenticatiedienst vormt in de geschetste opzet wel een potentiele privacy hotspot; hij kent immers de identiteit van de gebruiker en weet welke Dienstverleners hij bezocht. Met andere woorden; de Authenticatiedienst kan de Gebruiker volgen. Met relatief eenvoudige, toepassing van de polymorfe opzet kan ook dit vervolgrisico worden gemitigeerd. De Authenticatiedienst kan de authenticatie detail transacties namelijk registreren onder een pseudoniem en zo een scheiding aanbrengen tussen de gebruikersregistratie (waar de Gebruiker onder volledige identiteit bekend is) en de transactieregistratie (onder pseudoniem). Deze scheiding tussen gebruikersregistratie en transactieregistratie, waarmee de privacy hotspot bij de Authenticatiedienst vermeden wordt, is een eis vanuit de Uniforme Set van Eisen, de manier waarop deze wordt gerealiseerd is vrij gelaten.

Bij de inzage door de Gebruiker van zijn authenticatietransacties gedraagt de Authenticatiedienst zich dus als een Dienstverlener. Daarbij is het belangrijk dat er een afscheiding (Chinese muur) bestaat tussen de pseudonieme registraties en de registraties waar de Gebruiker onder zijn volledige identiteit staat geregistreerd. Deze opzet is in onderstaande figuur aangegeven.

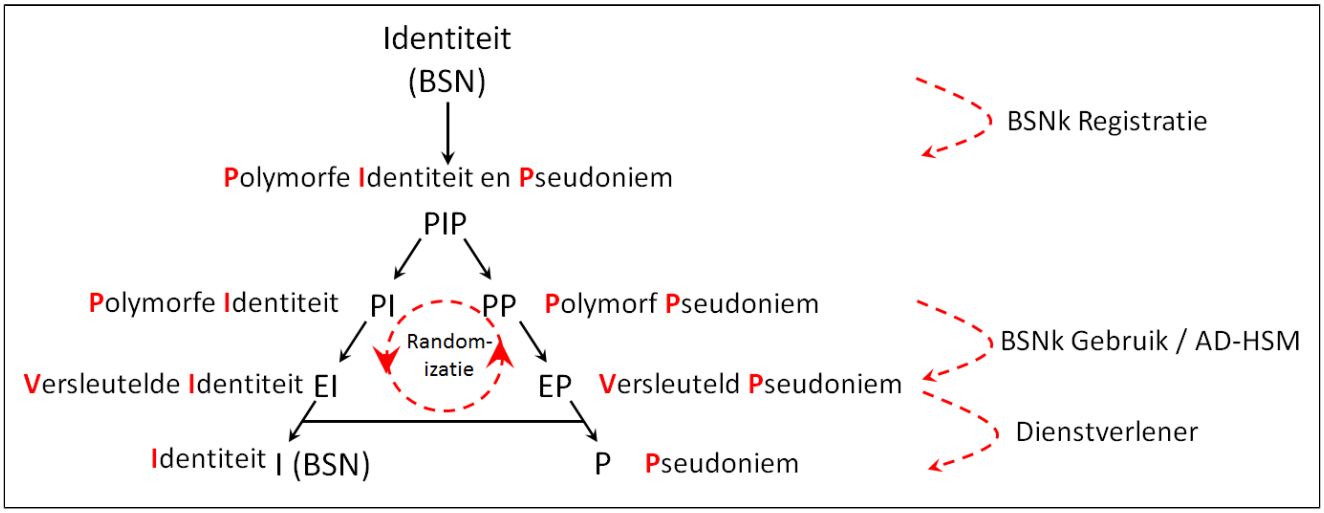


Figuur 4: Functiescheiding binnen de authenticatiedienst

In bovenstaande opzet is BSNk geen privacy hotspot, maar wel een Single Point of Failure (SPOF). Immers, als de gebruiksdienst van BSNk niet beschikbaar is, is de Authenticatiedienst niet meer in staat om een polymorfe vorm (PI/PP) te laten omzetten in een versleuteld vorm (VI/VP). Deze SPOF kan worden weggenomen door de functie van de BSNk gebruiksdienst in een zogenaamde Hardware Security Module (HSM) te plaatsen en aan te bieden aan een Authenticatiedienst. Dat wil zeggen dat de cryptografische omzetting van polymorfe vorm (PI/PP) naar versleutelde vorm (EI/EP) lokaal bij de Authenticatiedienst kan gebeuren. De fundamentele rol van de HSM is daarbij de cryptografische sleutels te beschermen. Dit omvat niet alleen zorg dragen dat de sleutels niet kunnen worden geëxporteerd uit de HSM maar ook dat alleen die cryptografische operaties mogelijk zijn die noodzakelijk zijn en ook dat geen cryptografische operaties bestaan die

delen van de sleutels kunnen prijsgeven. De opzet van HSM en de beveiliging daarvan is vastgelegd in diverse normen waarvan FIPS 140-2 de belangrijkste is.

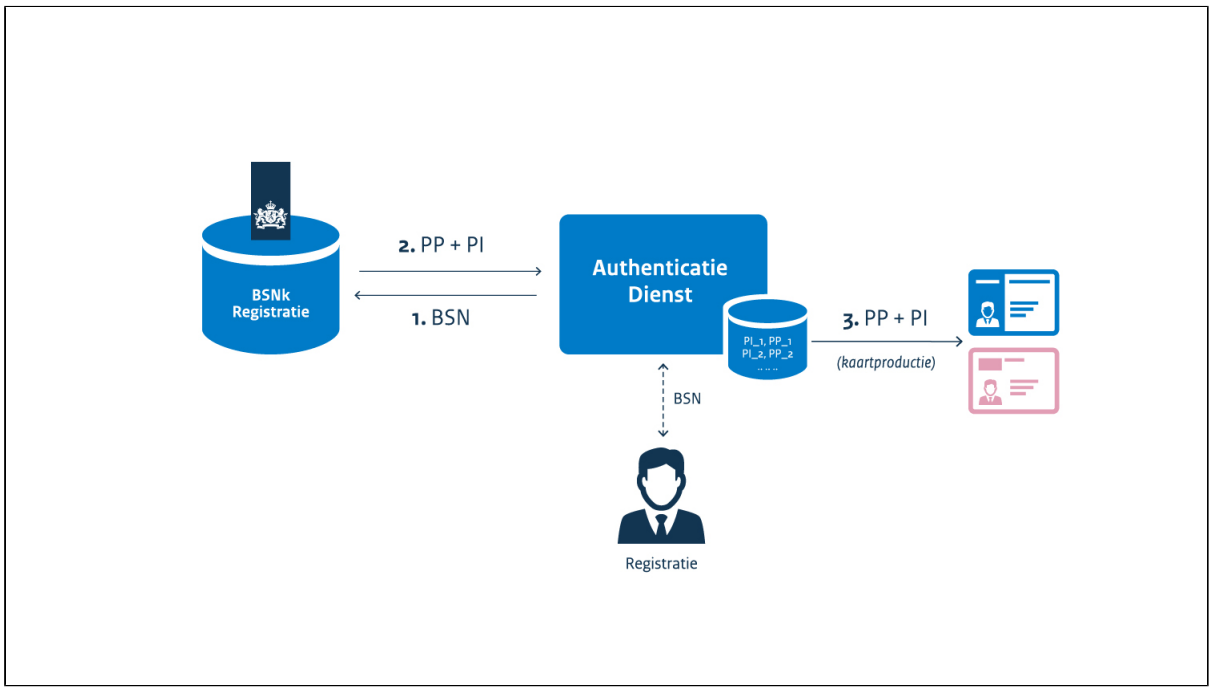
De transformatie van polymorf pseudoniem naar versleuteld pseudoniem bestaat uit drie stappen. De eerste stap is het vormen van het pseudoniem, de tweede stap het omzetten naar de publieke sleutel van de dienstverlener en de derde stap is een randomisatie. De transformatie van polymorfe identiteit naar versleutelde identiteit volgt hetzelfde principe met dit verschil dat de eerste stap achterweg moet blijven. Bij polymorfe identiteiten is het namelijk juist de bedoeling is dat elke dienstverlener hetzelfde BSN verstrekt krijgt. Dat een gerandomiseerde polymorfe vorm niet relateerbaar is aan het origineel is een klassiek resultaat rond ElGamal versleuteling. Ook Versleutelde Identiteiten (VI) en Versleutelde Pseudoniemen zijn ElGamal versleutelingen en daarmee randomiseerbaar. Tot slot, de Versleutelde Pseudoniemen die direct worden opgeleverd door het BSNk voor het Inzageregister zijn van een bijzonder vorm. Dit om te zorgen dat BSNk zelf geen inzage krijgt in deze pseudoniemen.



Figuur 5: De relatie tussen de polymorfe vormen, versleutelde vormen en finale vormen.

Polymorphic Pseudonym Card Application (PPCA)

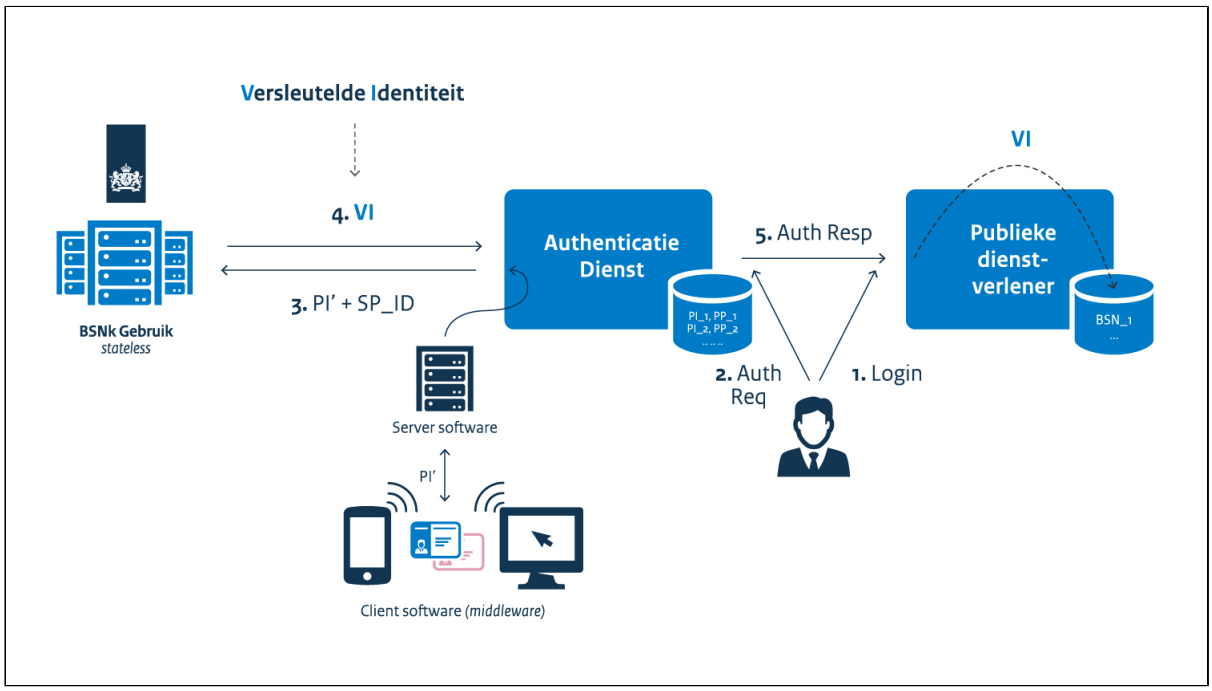
In de polymorfe opzet kan ook de privacyhotspot bij de Authenticatiedienst volledig verwijderd worden. Dit gebeurt door Polymorfe identiteit/pseudoniem in een specifieke kaartapplicatie te plaatsen die wordt verstrekt aan de Gebruiker als Authenticatiemiddel. Dat betekent dat de polymorfe vormen niet in een registratie bij de Authenticatiedienst worden geplaatst maar in een kaartapplicatie, een Polymorphic Pseudonym Card Application (PPCA). In technische zin is de plaatsing van Polymorfe identiteit/pseudoniem vergelijkbaar met de plaatsing van vingerafdrukken op elektronische paspoorten.



Figuur 6: plaatsing polymorfe vormen in kaartapplicatie

Als onderdeel van de authenticatie leest de Authenticatiedienst de polymorfe identiteiten en pseudoniemen van de kaart in plaats ze uit de Gebruikersregistratie te halen. Door de kaartapplicatie de polymorfe vormen eerst te laten randomiseren voor ze verstrekken aan de Authenticatiedienst krijgt de Authenticatiedienst geen inzicht in wie de Gebruiker is; ook zijn de verschillende PPCA authenticaties niet aan elkaar te relateren.

Het is van belang dat de Authenticatiedienst in staat is vast te stellen dat de kaart geldig is en bijvoorbeeld niet is ingetrokken door de Gebruiker. In belangrijke mate kan hiervoor gebruik worden gemaakt van de technologie die is ontwikkeld door de Duitse overheid voor de Duitse eID kaart. Door de federatieve opzet van het Nederlandse stelsel kan de geldigheid van de eenvoudiger worden vastgesteld door de Authenticatiedienst dan in de Duitse opzet. Er wordt een statusdienst ingericht die werkt op basis van pseudoniemen en waar de Authenticatiedienst (of Middelenuitgever) de status van de PPCA middelen kan registreren, i.e. of een middel 'Uitgegeven', 'Geactiveerd', 'Ingetrokken' etc. (zie Status (van het Authenticatiemiddel)) is. Bij authenticatie vormt de Authenticatiedienst op basis van het Polymorfe Pseudoniem een Versleuteld Pseudoniem bij de statusdienst en vraagt daar de status op. Als deze status wijst op geldigheid, vormt de authenticatiedienst een Versleuteld Pseudoniem voor de vragende Dienstverlener en geeft dit door als onderdeel van het authenticatieantwoord zoals al eerder is aangegeven. Zie onderstaande figuur.



Figuur 7: gebruik van PPCA

Use case beschrijvingen

De Uniforme Set van Eisen beschrijft een aantal use cases. Use case beschrijvingen tonen welke stappen doorlopen worden om een bepaald functioneel doel te bereiken. De technische details van de koppelvlakken zijn opgenomen onder Interface specifications. Het proces (en de afzonderlijke stappen daarbinnen) moeten voldoen aan de eisen die opgenomen zijn in het Normenkader, Beheer en Organisatie en Informatiebeveiliging. Use cases die door een Gebruiker doorlopen worden beginnen met een "G". Administratieve use cases hebben een "A" als voorvoegsel.

De use cases zijn onderverdeeld in een aantal hoofdcategorieën, zie Functionaliteit.

Authenticatie	De functionaliteit Authenticatie (authenticeren) valt in een aantal use cases uiteen: • AUC1 Activeren BSN — Op verzoek van een Gebruiker activeert een Middelenuitgever diens BSN voor authenticatie in het Publieke domein. Hiervoor stuurt de Middelenuitgever het BSN en controlegegevens naar het BSNk. Na controle genereert en verstrekt het BSNk een Polymorfe identiteit/pseudoniem van deze Gebruiker specifiek voor betreffende Middelenuitgever. Tenslotte registreert het BSNk deze activering bij zijn eigen Inzageregister. • AUC2 Transformeren — Een Authenticatiedienst ontvangt een authenticatieverzoek van een Dienstverlener voor een bepaalde Dienst. De Authenticatiedienst stelt vast of de gevraagde Dienst een BSN of een persistent pseudoniem nodig heeft. Indien dit eerste wordt gecontroleerd of de betreffende Dienstverlener een BSN mag ontvangen. Vervolgens transformeert de Authenticatiedienst op basis daarvan de Polymorfe identiteit/pseudoniem van de Gebruiker naar een Versleutelde Identiteit/Pseudoniem voor deze Dienstverlener. Een A • GUC1 Aantonen identiteit — De Gebruiker wil een Dienst afnemen bij een Dienstverlener in het Publieke domein. De Dienstverlener stuurt de Gebruiker via zijn Toegangsdienst met een authenticatieverzoek naar een Authenticatiedienst . De Authenticatiedienst stelt op het gevraagde Betrouwbaarheidsniveau de identiteit vast van de Gebruiker en verklaart hierover in een Authenticatieverklaring met behulp van een Dienstverlener specifieke Versleutelde Identiteit/Pseudoniem. • GUC2 Revocatie middel — In deze Use Case wil een Gebruiker (de geldigheid van) een Authenticatiemiddel intrekken zodanig dat deze niet meer bruikbaar is, bijvoorbeeld na het constateren van (een vermoeden van) misbruik.
Inzage	De functionaliteit Inzage wordt mede met onderstaande Use Case gefaciliteerd. • AUC3 Aanpassen status relatie en/of authenticatiemiddel — Een Middelenuitgever is verplicht om de status van (de relatie met) elke Gebruiker die geactiveerd is voor het Publieke domein actueel te houden bij het Inzageregister van het BSNk. De registratie vindt plaats met een Inzageregister specifiek Pseudoniem van de Gebruiker (dus niet met BSN) en een identificatie en omschrijving van het betreffende relatie of Authenticatiemiddel. Het Inzageregister versleutelt de gegevens met behulp van het specifieke Pseudoniem voordat ze daadwerkelijk opgeslagen w
Misbruikbestrijding	De Gebruiker en Dienstverlener moeten beschermd worden tegen misbruik, de volgende use cases draagt hier aan bij: • AUC4 Registreren Opmerkelijke Gebeurtenis — Een Authenticatiedienst of Middelenuitgever registreert een Opmerkelijke gebeurtenis van een Gebruiker bij het Misbruikbestrijdingsregister. De registratie vindt plaats met een Misbruikbestrijdingsregister specifiek Versleutelde Identiteit/Pseudoniem van de Gebruiker en gegevens over de Opmerkelijke gebeurtenis.

Sleutelbeheer	De functionaliteit Sleutelbeheer valt in een aantal use cases uiteen: • AUC5 Verstrekken sleutelmateriaal Dienstverleners — Het BSNk beheert en verstrekt via een Toegangsdienst cryptografisch Sleutelmateriaal aan elke Dienstverlener die aantoonbaar beschikt over een PKIoverheid-certificaat. Indien de Dienstverlener geautoriseerd is om het BSN te verwerken verstrekt het BSNk speciaal BSN Sleutelmateriaal. De Dienstverlener ontsleutelt met dit Sleutelmateriaal het versleutelde BSN of versleutelde pseudoniem van de Gebruiker dat de Dienstverlener verstrekt. • AUC6 Verstrekken sleutelmateriaal participanten — Het BSNk beheert en verstrekt cryptografisch Sleutelmateriaal aan Authenticatiedienst (en aan zichzelf) om opgenomen te worden in hun speciaal beveiligd computersysteem (HSM), zoals beschreven bij AUC2 Transformeren.

Authenticatie

De functionaliteit Authenticatie (authenticeren) valt in een aantal use cases uiteen:

- AUC1 Activeren BSN — Op verzoek van een Gebruiker activeert een Middelenuitgever diens BSN voor authenticatie in het Publieke domein. Hiervoor stuurt de Middelenuitgever het BSN en controlegegevens naar het BSNk. Na controle genereert en verstrekt het BSNk een Polymorfe identiteit/pseudoniem van deze Gebruiker specifiek voor betreffende Middelenuitgever. Tenslotte registreert het BSNk deze activering bij zijn eigen Inzageregister.
- AUC2 Transformeren — Een Authenticatiedienst ontvangt een authenticatieverzoek van een Dienstverlener voor een bepaalde Dienst. De Authenticatiedienst stelt vast of de gevraagde Dienst een BSN of een persistent pseudoniem nodig heeft. Indien dit eerste wordt gecontroleerd of de betreffende Dienstverlener een BSN mag ontvangen. Vervolgens transformeert de Authenticatiedienst op basis daarvan de Polymorfe identiteit/pseudoniem van de Gebruiker naar een Versleutelde Identiteit/Pseudoniem voor deze Dienstverlener. Een A
- GUC1 Aantonen identiteit — De Gebruiker wil een Dienst afnemen bij een Dienstverlener in het Publieke domein. De Dienstverlener stuurt de Gebruiker via zijn Toegangsdienst met een authenticatieverzoek naar een Authenticatiedienst . De Authenticatiedienst stelt op het gevraagde Betrouwbaarheidsniveau de identiteit vast van de Gebruiker en verklaart hierover in een Authenticatieverklaring met behulp van een Dienstverlener specifieke Versleutelde Identiteit/Pseudoniem.
- GUC2 Revocatie middel — In deze Use Case wil een Gebruiker (de geldigheid van) een Authenticatiemiddel intrekken zodanig dat deze niet meer bruikbaar is, bijvoorbeeld na het constateren van (een vermoeden van) misbruik.

AUC1 Activeren BSN

Op verzoek van een Gebruiker activeert een Middelenuitgever diens BSN voor authenticatie in het Publieke domein. Hiervoor stuurt de Middelenuitgever het BSN en controlegegevens naar het BSNk. Na controle genereert en verstrekt het BSNk een Polymorfe identiteit/pseudoniem van deze Gebruiker specifiek voor betreffende Middelenuitgever. Tenslotte registreert het BSNk deze activering bij zijn eigen Inzageregister.

Stap	Actie	Omschrijving

	Initiële staat	De Gebruiker heeft bij een Middelenuitgever een registratieproces doorlopen dat minimaal voldoet aan de eisen die het normenkader stelt aan betrouwbaarheidsniveau substantieel, inclusief het vaststellen van het BSN van Gebruiker. Vervolgens heeft de Gebruiker een weloverwogen keuze gemaakt om diens BSN te laten activeren voor authenticatie in het Publieke domein.
1.1	BSNk ontvangt een activatie aanvraag	Het BSNk ontvangt een activatie aanvraag van een Middelenuitgever voor een Gebruiker met de BSN, geboortedatum en naam (voorletter + achternaam) met behulp van Interface spec BSNk: activate.
1.2	BSNk valideert de aanvraag	Het BSNk controleert dat de Middelenuitgever gemachtigd is om een Gebruiker te activeren voor het Publieke domein en of de aanvraag daadwerkelijk en ongewijzigd van de Middelenuitgever afkomstig is. Vervolgens controleert het BSNk de aangeleverde gegevens bij de Basisregistratie Personen.
1.3	BSNk genereert de PI@MU en PP@MU	Het BSNk genereert een Polymorfe identiteit/pseudoniem specifiek voor de Middelenuitgever op basis van de BSN van de Gebruiker (PI@MU en PP@MU).
1.4	BSNk verstrekt de PI@MU en PP@MU aan de Middelenuitgever	Het BSNk verstrekt de Polymorfe Identiteit en Polymorfe Pseudoniem aan de betreffende Middelenuitgever, die beide zodanig bewaart dat ze betrouwbaar zijn gekoppeld aan de Gebruiker.
1.5	BSNk registreert de activering bij het Inzageregister	Het BSNk genereert op basis van het BSN het Versleuteld Pseudoniem ten behoeve het Inzageregister (VP@IR) en registreert daarmee vervolgens de relatie tussen Middelenuitgever en de Gebruiker bij het Inzageregister[1].
	Finale staat	De Middelenuitgever is in staat om een Authenticatiedienst de Gebruiker te laten identificeren voor diensten in het Publieke domein.

Voetnoten

1. Dit betreft dus het registreren van de relatie tussen de Middelenuitgever en de Gebruiker door het BSNk zelf, terwijl AUC3 Aanpassen status relatie en/of authenticatiemiddel gaat over het actueel houden van de relatie door de Middelenuitgever zelf.

AUC2 Transformeren

Een Authenticatiedienst ontvangt een authenticatieverzoek van een Dienstverlener voor een bepaalde Dienst. De Authenticatiedienst stelt vast of de gevraagde Dienst een BSN of een persistent pseudoniem nodig heeft. Indien dit eerste wordt gecontroleerd of de betreffende Dienstverlener een BSN mag ontvangen. Vervolgens transformeert de Authenticatiedienst op basis daarvan de Polymorfe identiteit/pseudoniem van de Gebruiker naar een Versleutelde

Identiteit/Pseudoniem voor deze Dienstverlener. Een Authenticatiedienst kan deze transformatie door het BSNk laten doen. Een Authenticatiedienst heeft hiernaast de keuze om deze transformatie zelf uit te voeren. Hiertoe kan de Authenticatiedienst een speciaal beveiligd computer systeem (HSM) aanschaffen en speciaal Sleutelmateriaal verkrijgen van de Sleutelbeheer -functie.

Nr.	Actie	Omschrijving
	Initiële staat	De Authenticatiedienst heeft als onderdeel van AUC1 Activeren BSN of GUC1 Aantonen identiteit toegang tot de Polymorfe identiteit/pseudoniem van de Gebruiker. Verder is bekend voor welke Ontvangende Partij de Gebruiker geïdentificeerd moet worden en voor welke Dienst (in verband met bepaling van identiteitstype: BSN of Pseudoniem).
2.1	Authenticatiedienst kiest PI@MU of PP@MU van de Gebruiker	De Authenticatiedienst kiest op basis van het identiteitstype (BSN of Pseudoniem) behorend bij de beoogde Dienst het benodigde Polymorfe identiteit/pseudoniem (PP@MU of PI@MU)
2.2	Authenticatiedienst verzorgt transformatie PI@MU VP@OP of PP@MU PI@OP	Indien de Authenticatiedienst de transformatie niet zelf doet maar gebruik maakt van de BSNk Transformatie dienst, ga verder bij AUC2.2 Authenticatiedienst gebruikt BSNk transformatie functie
2.3		De Authenticatiedienst transformeert met eigen HSM de Polymorfe identiteit/pseudoniem met behulp van de identiteit van de Ontvangende Partij naar een Versleutelde Identiteit/Pseudoniem: (PP@MU VP@OP of PI@OP VI@OP). Ga verder bij AUC2.3 HSM transformatie.
	Finale staat	De Authenticatiedienst kan de Gebruiker identificeren bij de betreffende Ontvangende Partij

AUC2.2 Authenticatiedienst gebruikt BSNk transformatie functie

Alternatieve Flow op stap 2.2 van AUC2 Transformeren

Stap	Actie	Omschrijving
	Initiële staat	De Authenticatiedienst heeft de benodigde Polymorfe Identiteit/Pseudoniem (PP@MU of PI@MU) van de authenticerende Gebruiker en weet ten behoeve van welke Ontvangende Partij het authenticatieverzoek is gedaan.
2.2.1	Authenticatiedienst randomiseert PI@MU of PP@MU	De Authenticatiedienst randomiseert de Middelenuitgever specifieke Polymorfe identiteit/pseudoniem (PP@MU of PI@MU) zodat het BSNk deze niet meer kan herkennen.

2.2.2	Authenticatiedienst vraagt het BSNk om de PI@MU of PP@MU te transformeren	De Authenticatiedienst stuurt de gerandomiseerde Middelenuitgever specifieke Polymorfe identiteit/pseudoniem (PP@MU of PI@MU) samen met de identiteit (OIN) van de beoogde Ontvangende Partij naar het BSNk volgens Interface spec BSNk: transform
2.2.3	BSNk valideert de aanvraag	Het BSNk controleert dat de aanvragende partij geautoriseerd is als Authenticatiedienst en of de aanvraag daadwerkelijk en ongewijzigd van die partij afkomstig is. Indien de Middelenuitgever niet dezelfde partij is als de Authenticatiedienst, dan controleert het BSNk ook nog of de betreffende Authenticatiedienst volgens de Metadata (MU - AD affiliation) geautoriseerd is om het Authenticatiemiddel van betreffende Middelenuitgever te gebruiken.
2.2.4	BSNk transformeert de PI@MU VI@OP of PP@MU VP@OP	Het BSNk transformeert met zijn HSM de Middelenuitgever specifieke Polymorfe Identiteit/Pseudoniem met behulp van de identiteit (OIN) van de Ontvangende Partij naar een specifieke Versleutelde Identiteit/Pseudoniem (PP@MU VP@OP of PI@MU VI@OP).
2.2.5	BSNk verstrekt de VI@OP of VP@OP aan de Authenticatiedienst	Het BSNk verstrekt de Ontvangende Partij specifieke Versleutelde Identiteit/Pseudoniem (VP@OP of VI@OP) aan de Authenticatiedienst en logt de aanvraag ten behoeve van audit-doeleinden.
	Finale staat	De Authenticatiedienst kan de Gebruiker identificeren voor de betreffende Ontvangende Partij.

AUC2.3 HSM transformatie

NB Deze interface naar de HSM wordt door de HSM leverancier vastgelegd.

Nr.	Actie	Omschrijving
2.3.1	HSM valideert de aanvraag	Het HSM controleert of de aanvraag correct gespecificeerd is.
2.3.2	HSM genereert het VP@OP of VI@OP	De HSM transformeert de Middelenuitgever specifieke Polymorfe identiteit/pseudoniem met behulp van de identiteit van de Ontvangende Partij naar een Ontvangende Partij specifieke Versleutelde Identiteit/Pseudoniem (PP@MU VP@OP of PI@MU VI@OP).

2.3.3	HSM verstrekt het VP@OP of VI@OP	De HSM verstrekt de Ontvangende Partij specifieke Versleutelde Identiteit/Pseudoniem (VP@OP of VI@OP) aan de aanvrager en logt de aanvraag ten behoeve van auditing.

Voetnoten

1. De HSM van een Authenticatiedienst kan alleen Polymorfe identiteit/pseudoniem transformeren van een Middelenuitgever waarmee hij een relatie heeft. Via AUC6 Verstrekken sleutelmateriaal participanten zal de Authenticatiedienst per Middelenuitgever waarmee hij een relatie heeft (dat wil zeggen wiens Authenticatiemiddel hij mag gebruiken) specifiek Sleutelmateriaal voor zijn HSM aan moeten vragen.

GUC1 Aantonen identiteit

De Gebruiker wil een Dienst afnemen bij een Dienstverlener in het Publieke domein. De Dienstverlener stuurt de Gebruiker via zijn Toegangsdienst met een authenticatieverzoek naar een Authenticatiedienst . De Authenticatiedienst stelt op het gevraagde Betrouwbaarheidsniveau de identiteit vast van de Gebruiker en verklaart hierover in een Authenticatieverklaring met behulp van een Dienstverlener specifieke Versleutelde Identiteit/Pseudoniem.

Nr.	Actie	Omschrijving
	Initiële staat	Dienstverlener wil een Gebruiker authenticeren voor een bepaalde Dienst en voor deze Gebruiker is eerder AUC1 Activeren BSN afgerond.
1.1	Dienstverlener stuurt een authenticatieverzoek via een Toegangsdienst naar een Authenticatiedienst	Een Dienstverlener stuurt een authenticatieverzoek naar een Authenticatiedienst om een Gebruiker te authenticeren voor een (of optioneel meerdere) bepaalde Dienst met daaraan verbonden een minimaal betrouwbaarheidsniveau en Identificatietype (BSN of Pseudoniem). De Toegangsdienst helpt daarbij de Gebruiker om zijn Authenticatiedienst te kiezen.
1.2	Gebruiker authenticeert zich bij de Authenticatiedienst	De Authenticatiedienst laat de Gebruiker een authenticatieproces doorlopen dat minimaal voldoet aan de eisen die het normenkader stelt aan het vereiste betrouwbaarheidsniveau. De Gebruiker maakt daarbij een weloverwogen keuze om zich voor Dienst van de betreffende Dienstverlener(s) te authenticeren. Voor een beschrijving van foutsituaties, zie GUC1.2 Foutsituatie bij authenticeren.
1.3	Authenticatiedienst controleert of de Dienstverlener geautoriseerd is voor het BSN	Als het een aanvraag voor BSN betreft dan controleert de Authenticatiedienst of de betreffende Dienstverlener(s) geautoriseerd is voor ontvangst van een BSN aan de hand van de Autorisatielijst BSN.
1.4	Authenticatiedienst valideert het Authenticatiemiddel	De Authenticatiedienst valideert dat het gebruikte Authenticatiemiddel nog 'actief' is voor het publieke domein.

1.5	Authenticatiedienst stelt de VI@DV of VP@DV vast	De Authenticatiedienst gebruikt de Polymorfe identiteit/pseudoniem van de Gebruiker om deze (met AUC2 Transformeren) per Dienstverlener (dan wel andere Ontvangende Partij) te transformeren naar een specifieke Versleutelde Identiteit/Pseudoniem (VP@DV of VI@DV) .
1.6	Authenticatiedienst stelt een Authenticatieverklaring op.	Authenticatiedienst stelt een Authenticatieverklaring op met elke Versleutelde Identiteit/Pseudoniem (VP@DV of VI@DV) van de Gebruiker versleuteld met publieke sleutel uit het PKIoverheid-certificaat van de betreffende Ontvangende Partij.
1.7	Authenticatiedienst verstrekt de Authenticatieverklaring aan de Dienstverlener	De Authenticatiedienst verklaart met behulp van een Authenticatieverklaring over de Versleutelde Identiteit/Pseudoniem van de Gebruiker via de Toegangsdienst richting de vragende Dienstverlener. De Toegangsdienst ontvangt de Authenticatieverklaring van de Authenticatiedienst en stuurt deze door naar de Dienstverlener in een antwoordbericht.
1.8	Dienstverlener ontvangt en controleert het antwoordbericht	De Dienstverlener ontvangt het antwoordbericht en controleert met behulp van de Metadata of de verklarende Authenticatiedienst erkend is en controleert of de Authenticatieverklaring daadwerkelijk en ongewijzigd van de betreffende Authenticatiedienst afkomstig is en een voldoende betrouwbaarheidsniveau heeft. De Dienstverlener controleert ook of deze Authenticatieverklaring geldig en correct is.
1.9	Dienstverlener haalt de BSN of pseudoniem uit de Authenticatieverklaring	De Dienstverlener haalt de Versleutelde Identiteit/Pseudoniem (VP@DV of VI@DV) van de Gebruiker uit de Authenticatieverklaring en controleert of deze geldig en correct is. Vervolgens gebruikt de Dienstverlener het verstrekte (cryptografische) sleutelmateriaal om het BSN dan wel het Pseudoniem uit Versleutelde Identiteit/Pseudoniem (VP@DV of VI@DV) te halen.
	Finale staat	De Dienstverlener beschikt over de Identiteit (BSN) of Pseudoniem van een Gebruiker op het gevraagde betrouwbaarheidsniveau.

GUC1.2 Foutsituatie bij authenticeren

Tijdens de GUC1 Aantonen identiteit kan het voorkomen dat een validatie niet succesvol is, of dat er benodigde gegevens niet beschikbaar zijn. In dit geval levert dit een fout situatie op, deze situaties worden allemaal op dezelfde manier afgehandeld:

- De Participant ZOU de Gebruiker MOETEN informeren dat voor de dienst een BSN nodig is, maar dat zijn BSN nog niet geactiveerd is voor het Publieke domein.
- De Participant ZOU de Gebruiker op het scherm op de hoogte MOETEN stellen van de reden van het mislukken van het aantonen.
- De Participant MAG de Gebruiker aanbieden met een ander Authenticatiemiddel bij een andere Authenticatiedienst opnieuw te proberen (waarvoor wel een BSN is geregistreerd voor deze Gebruiker).
- De Participant MOET de Gebruiker de mogelijkheid bieden te annuleren.

GUC2 Revocatie middel

In deze Use Case wil een Gebruiker (de geldigheid van) een Authenticatiemiddel intrekken zodanig dat deze niet meer bruikbaar is, bijvoorbeeld na het constateren van (een vermoeden van) misbruik.

De verschillende acties worden hier in meer detail beschreven.

Stap	Actie	Omschrijving
	Initiële staat	Een Gebruiker wil zijn middel revoceren, dat wil zeggen: wil de geldigheid van het middel intrekken. Een Authenticatiemiddel heeft de status 'Activated' bij het Inzageregister.
2.1	De Gebruiker authenticeert zich bij de Middelenuitgever	De Middelenuitgever laat de Gebruiker een authenticatieproces doorlopen dat minimaal voldoet aan de eisen die het normenkader stelt aan het vereiste betrouwbaarheidsniveau.
2.2	De Gebruiker selecteert de Middelenuitgever	De Gebruiker selecteert het Authenticatiemiddel waarvan de geldigheid ingetrokken moet worden aan de hand van een herkenbaar volgnummer en/of einddatum (jaar+maand).
2.3	De Gebruiker geeft aan dat van het geselecteerde Authenticatiemiddel de geldigheid ingetrokken moet worden.	De Gebruiker geeft met een expliciete handeling aan dat van het geselecteerde Authenticatiemiddel de geldigheid ingetrokken moet worden.
2.4	De Gebruiker bevestigt zijn keuze	De Gebruiker bevestigt zijn keuze en geeft zo definitief akkoord voor de wijziging.
2.5	De Middelenuitgever stuurt de nieuwe status naar het Inzageregister	De Middelenuitgever meldt de nieuwe status (zie Status (van het Authenticatiemiddel))van het Authenticatiemiddel aan bij het Inzageregister conform AUC3 Aanpassen status relatie en/of authenticatiemiddel
	Finale staat	De geldigheid van het Authenticatiemiddel is ingetrokken en dit is bekend bij het Inzageregister

Inzage

De functionaliteit Inzage wordt mede met onderstaande Use Case gefaciliteerd.

- AUC3 Aanpassen status relatie en/of authenticatiemiddel — Een Middelenuitgever is verplicht om de status van (de relatie met) elke Gebruiker die geactiveerd is voor het Publieke domein actueel te houden bij het Inzageregister van het BSNk. De registratie vindt plaats met een Inzageregister specifiek Pseudoniem van de Gebruiker (dus niet met BSN) en een identificatie en omschrijving van het betreffende relatie of Authenticatiemiddel. Het Inzageregister versleutelt de gegevens met behulp van het specifieke Pseudoniem voordat ze daadwerkelijk opgeslagen w

AUC3 Aanpassen status relatie en/of authenticatiemiddel

Een Middelenuitgever is verplicht om de status van (de relatie met) elke Gebruiker die geactiveerd is voor het Publieke domein actueel te houden bij het Inzageregister van het BSNk. De registratie vindt plaats met een Inzageregister specifiek Pseudoniem van de Gebruiker (dus niet met BSN) en een identificatie en omschrijving van het betreffende relatie of Authenticatiemiddel. Het Inzageregister versleutelt de gegevens met behulp van het specifieke Pseudoniem voordat ze daadwerkelijk opgeslagen worden.

Stap	Actie	Omschrijving
	Initiële staat	Een Authenticatiemiddel heeft een status bij het Inzageregister of de status wordt voor het eerst geregistreerd. Zie Status (van het Authenticatiemiddel) voor meer informatie over mogelijke statussen.
3.1	De Middelenuitgever identificeert het Authenticatiemiddel en de Gebruiker	De Middelenuitgever identificeert (al dan niet samen met de Gebruiker) het Authenticatiemiddel waarvan een nieuwe status geregistreerd moet worden aan de hand van een herkenbaar volgnummer en/of einddatum (jaar+maand).
		Indien de Middelenuitgever nog geen Inzageregister specifiek Versleuteld Pseudoniem van de Gebruiker (VP@IR) heeft dan dient als alternatieve flow eerst AUC2 Transformeren doorlopen worden. Daar wordt het (niet naar BSN te herleiden) Versleuteld Pseudoniem van het Inzageregister Misbruikbestrijdingsregister vastgesteld (VP@IR).
3.2	De Middelenuitgever stuurt de nieuwe status naar het Inzageregister	De Middelenuitgever meldt de nieuwe Status (van het Authenticatiemiddel) aan bij het Inzageregister met het zojuist verkregen Versleuteld Pseudoniem van de Gebruiker (VP@IR) en het volgnummer en/of einddatum van het Authenticatiemiddel.
3.3	Inzageregister valideert de aanvraag	Het Inzageregister controleert of de Middelenuitgever gemachtigd is om een Gebruiker te activeren voor het overheidsdomein en of de aanvraag daadwerkelijk en ongewijzigd van de Middelenuitgever afkomstig is en ontsleutelt de Inzageregister specifieke pseudoniem van de Gebruiker uit de Versleutelde Pseudoniem (VP@IR).
3.4	Inzageregister versleutelt en registreert de nieuwe status	Het Inzageregister versleutelt zowel het specifieke pseudoniem (P@IR) als de overige gegevens (met een sleutel afgeleid van dit pseudoniem) en registreert de nieuwe status voor de combinatie van specifieke pseudoniem van de Gebruiker, de Authenticatiedienst en het volgnummer en/of einddatum van het Authenticatiemiddel. Deze registratie gaat met Interface Spec BSNk: registerStatusEIM.

		Indien de betreffende status wijziging als een Opmerkelijke gebeurtenis gekwalificeerd moet worden start de Middelenuitgever AUC4 Registreren Opmerkelijke Gebeurtenis voor het registreren van de statuswisseling.
	Finale staat	Het Authenticatiemiddel heeft een nieuwe status bij het Inzageregister en (eventueel) een Opmerkelijke gebeurtenis is vastgelegd bij het Misbruikbestrijdingsregister

Voetnoten

- In het geval dat een Middelenuitgever een andere partij is dan de Authenticatiedienst, dan dient de Middelenuitgever de ook de activering van Authenticatiemiddel voor betreffende Authenticatiedienst te registreren bij het Inzageregister. Dat gebeurt via bovenstaande proces waarbij de identiteit van de Authenticatiedienst als extra gegeven aan het registratieverzoek wordt toegevoegd. De Middelenuitgever moet daarbij garanderen dat een Authenticatiedienst het middel slechts kan gebruiken na de registratie bij de Middelenuitgever en na een weloverwogen toestemming van de Gebruiker.
- De identiteit van het Authenticatiemiddel (volgnummer en/of einddatum) dient zo weinig mogelijk uniek te zijn. De Gebruiker moet zijn eventuele meerdere authenticatiemiddelen van één Middelenuitgever kunnen onderscheiden, maar hoe minder onderscheidend hoe beter privacy bij het Inzageregister geborgd kan worden

Misbruikbestrijding

De Gebruiker en Dienstverlener moeten beschermd worden tegen misbruik, de volgende use cases draagt hier aan bij:

- AUC4 Registreren Opmerkelijke Gebeurtenis — Een Authenticatiedienst of Middelenuitgever registreert een Opmerkelijke gebeurtenis van een Gebruiker bij het Misbruikbestrijdingsregister. De registratie vindt plaats met een Misbruikbestrijdingsregister specifiek Versleutelde Identiteit/Pseudoniem van de Gebruiker en gegevens over de Opmerkelijke gebeurtenis.

AUC4 Registreren Opmerkelijke Gebeurtenis

Een Authenticatiedienst of Middelenuitgever registreert een Opmerkelijke gebeurtenis van een Gebruiker bij het Misbruikbestrijdingsregister. De registratie vindt plaats met een Misbruikbestrijdingsregister specifiek Versleutelde Identiteit/Pseudoniem van de Gebruiker en gegevens over de Opmerkelijke gebeurtenis.

Stap	Actie	Omschrijving
	Initiële staat	De Authenticatiedienst[1,2] constateert een Opmerkelijke gebeurtenis.
4.1	De Authenticatiedienst classificeert de opmerkelijke activiteit	De Authenticatiedienst classificeert de Opmerkelijke gebeurtenis en identificeert de Gebruiker die daarbij betrokken is. Optioneel wordt ook het Authenticatiemiddel geïdentificeerd dat daarbij gebruikt is.

		Indien de Authenticatiedienst nog geen Misbruikbestrijdingsregister specifiek Versleutelde Pseudoniem van de Gebruiker heeft dan dient als alternatieve flow eerst AUC2 Transformeren doorlopen worden om een Versleutelde Pseudoniem van de Gebruiker bij het Misbruikbestrijdingsregister (VP@MBR) vast te stellen.
4.2	De Authenticatiedienst stuurt gegevens over de Opmerkelijke gebeurtenis naar het Misbruikbestrijdingsregister	De Authenticatiedienst meldt de Opmerkelijke gebeurtenis aan bij het Misbruikbestrijdingsregister met het zojuist verkregen Versleutelde Pseudoniem van de Gebruiker (VP@MBR) en indien van toepassing de identiteit van het Authenticatiemiddel (meestal volgnummer en/of einddatum)
4.3	Misbruikbestrijdingsregister valideert de aanvraag	Het Misbruikbestrijdingsregister controleert dat de Authenticatiedienst gemachtigd is om een activiteit te registreren in het Publieke domein en of de aanvraag daadwerkelijk en ongewijzigd van de Authenticatiedienst afkomstig is.
4.4	Misbruikbestrijdingsregister legt de Opmerkelijke gebeurtenis vast	Het Misbruikbestrijdingsregister legt de Opmerkelijke gebeurtenis vast met behulp van de combinatie van Authenticatiedienst, Versleutelde Pseudoniem van de Gebruiker en de identiteit van het Authenticatiemiddel (meestal het volgnummer en/of einddatum).
	Finale staat	Het Misbruikbestrijdingsregister heeft een Opmerkelijke gebeurtenis vastgelegd.

Voetnoten

1. Om de privacy en veiligheid van de Gebruiker te waarborgen dienen er activiteiten te worden ontplooid voor Misbruikbestrijding. De verwachting is dat met het faciliteren van de hier beschreven functionaliteit, een optimum gevonden kan worden tussen behoud van privacy en het bieden van informatiebeveiliging aan de burger. De exacte invulling van misbruikbestrijding en eventueel hieruit voortkomende verplichtingen voor Participanten zullen in volgende versies verder ingevuld worden.
2. Indien gesproken wordt over Authenticatiedienst in deze Use Case, lees dan Authenticatiedienst of Middelenuitgever

Sleutelbeheer

De functionaliteit Sleutelbeheer valt in een aantal use cases uiteen:

- AUC5 Verstrekken sleutelmateriaal Dienstverleners — Het BSNk beheert en verstrekt via een Toegangsdienst cryptografisch Sleutelmateriaal aan elke Dienstverlener die aantoonbaar beschikt over een PKIoverheid-certificaat. Indien de Dienstverlener geautoriseerd is om het BSN te verwerken verstrekt het BSNk speciaal BSN Sleutelmateriaal. De Dienstverlener ontsleutelt met dit Sleutelmateriaal het versleutelde BSN of versleutelde pseudoniem van de Gebruiker dat de Dienstverlener verstrekt.
- AUC6 Verstrekken sleutelmateriaal participanten — Het BSNk beheert en verstrekt cryptografisch Sleutelmateriaal aan Authenticatiedienst (en aan zichzelf) om opgenomen te worden in hun speciaal beveiligd computersysteem (HSM), zoals beschreven bij AUC2 Transformeren.

AUC5 Verstrekken sleutelmateriaal Dienstverleners

Het BSNk beheert en verstrekt via een Toegangsdienst cryptografisch Sleutelmateriaal aan elke Dienstverlener die aantoonbaar beschikt over een PKIoverheid-certificaat. Indien de Dienstverlener geautoriseerd is om het BSN te verwerken verstrekt het BSNk speciaal BSN Sleutelmateriaal. De Dienstverlener ontsleutelt met dit Sleutelmateriaal het versleutelde BSN

of versleutelde pseudoniem van de Gebruiker dat de Dienstverlener verstrekt.

Stap	Actie	Omschrijving
	Initiële staat	Een Dienstverlener heeft Sleutelmateriaal nodig om de identiteit (bijv BSN) en/of pseudoniem uit de Versleutelde Identiteit/Pseudoniem te halen en vraagt zijn Toegangsdienst om dit voor hem te regelen.
5.1	De Toegangsdienst valideert het verzoek.	De Toegangsdienst valideert dat het verzoek afkomstig is van de Dienstverlener, of een door deze geautoriseerde persoon.
5.2	De Toegangsdienst stuurt een aanvraag naar het Sleutelbeheer	De Toegangsdienst stuurt een aanvraag voor Sleutelmateriaal naar het BSNk Sleutelbeheer met daarin het PKIoverheid-certificaat van betreffende Dienstverlener.
5.3	Sleutelbeheer valideert de aanvraag	BSNk Sleutelbeheer controleert of de aanvraag daadwerkelijk en ongewijzigd van een erkende Toegangsdienst afkomstig is en of het meegeleverde PKIoverheid-certificaat van de Dienstverlener geldig is.
5.4	Sleutelbeheer controleert of Dienstverlener BSN mag ontvangen	BSNk Sleutelbeheer controleert of het OIN van de Dienstverlener zoals deze op het meegeleverde PKIoverheid-certificaat voorkomt op de Autorisatielijst BSN en ook Sleutelmateriaal mag ontvangen om een BSN te ontsleutelen.
5.5	Sleutelbeheer genereert Sleutelmateriaal	BSNk Sleutelbeheer genereert het Sleutelmateriaal voor het OIN van de Dienstverlener inclusief het BSN-Sleutelmateriaal indien diens OIN inderdaad voorkomt op de Autorisatielijst BSN
5.6	Sleutelbeheer versleutelt Sleutelmateriaal	BSNk Sleutelbeheer versleutelt Sleutelmateriaal met de publieke sleutel op het meegeleverde PKIoverheid-certificaat van de Dienstverlener
5.7	Sleutelbeheer verstrekt Sleutelmateriaal aan de Toegangsdienst en registreert de verstrekking	BSNk Sleutelbeheer verstrekt Sleutelmateriaal ten behoeve van de Dienstverlener aan de aanvragende Toegangsdienst en registreert de verstrekking in een publiekelijk toegankelijke Sleutelverstrekkingslijst .
5.8	Toegangsdienst verstrekt Sleutelmateriaal aan de Dienstverlener	De Toegangsdienst verstrekt Sleutelmateriaal aan de betreffende Dienstverlener.
5.9	Dienstverlener ontsleutelt en installeert Sleutelmateriaal	De Dienstverlener ontsleutelt Sleutelmateriaal en installeert dit op zijn toegangssystemen.
	Finale staat	De Dienstverlener kan BSN en Pseudoniem uit een Versleutelde Identiteit/Pseudoniem halen. En de sleutelverstrekking is geregistreerd in het Sleutelverstrekkingslijst

AUC6 Verstrekken sleutelmateriaal participanten

Het BSNk beheert en verstrekt cryptografisch Sleutelmateriaal aan Authenticatiedienst (en aan zichzelf) om opgenomen te worden in hun speciaal beveiligd computersysteem (HSM), zoals beschreven bij AUC2 Transformeren.

Nader uit te werken functionaliteit

Zie paragraaf Functionaliteit voor de beschrijving van de functionaliteit in deze versie van de Uniforme Set van Eisen.

In opvolgende versies van de Uniforme Set van Eisen komen hier de volgende functionaliteiten en diensten bij:

- Attribuutverstrekking: Verstrekken van aanvullende, gevalideerde persoonsgegevens (attributen) op verzoek van de gebruiker zoals initialen, geboortedatum/plaats en voldoen aan leeftijdsgrens.
- Machtigingen: de bevoegdheid aantonen om te kunnen handelen namens iemand die jou gemachtigd heeft (bijvoorbeeld ten bate van minder digivaardigen of rechtspersonen), maar ook machtigen voor onder curatele stelling, voogdij, en gezagvoering.
- Ondertekenen: Het digitaal ondertekenen van stukken om zo de wilsverklaring vast te leggen.
- Dienstbemiddeling: het ondersteunen van de situatie dat een partij een dienst van een Dienstverlener verzorgt, bijvoorbeeld het invullen van de belastingaangifte in de software van een tussenpartij
- Multi-channel: het geautomatiseerd ondersteunen van additionele kanalen naast het webkanaal (bijvoorbeeld voor mobiele platformen, Application-to-Application, Machine-to-Machine)

Dit brengt nieuwe rollen met zich mee, zie ook Participanten.

Techniek

This chapter describes the technical requirements for Participants.The following subjects are detailed below:

- Open standards
- Generic technical requirements — For consistency and interoperability, various generic technical requirements apply to all interfaces for all Participants.
- Technical security requirements — The following technical security requirements apply to all interfaces for all Participants.
- Interface specifications
- Metadata specifications

Open standards

Because of interoperability, security, robustness and prevention of lock-in, the Uniforme Set van Eisen requires open standards where applicable and possible. The list of required open standards, maintained by the Forum Standaardisatie is used as a reference. Dutch governmental organisations are obliged to use the relevant open standards for digital information exchange on this list.

Generic technical requirements

For consistency and interoperability, various generic technical requirements apply to all interfaces for all Participants.

- Character encoding
- Error handling
- Synchronize system clocks
- Web services

Character encoding

UTF-8 MUST be used as character encoding.

Error handling

This topic describes how errors MUST be handled within the network, to ensure that both users as well as Participants will be appropriately informed and serviced. The main principal concerning error handling is that the error should be dealt with, there where it occurs within the network.

Cancellation

In any normal user flow the user can choose to abort the request by pressing a cancel button. If a user does so, the Participant MUST send the user back to the originating party, with a valid SAML message. This SAML message SHALL contain a StatusCode.Value=AuthnFailed, and a statusMessage SHOULD be included (i.e. ‘Authentication Cancelled’).

Wrongly formatted messages

Whenever a party receives a wrongly formatted message, that party SHOULD immediately abort the process.
Wrongly formatted messages include messages that contain invalid XML, have an invalid Signature or use an unsupported SAML or Scheme version. The receiving party MUST report to the user that an unrecoverable error has occurred. The receiving party SHOULD start an investigation, and SHOULD inform the sending party that an error has occurred. When informed the sending party MUST investigate the occurred incident.

Functionally incorrect messages

A message can also be invalid because it contains functional errors, for instance because a wrong issuer is supplied. Whenever a party receives a message that does not comply with the specification on a functional level that party MUST abort the process. The receiving party MUST send the user back to the requester. The receiving party SHOULD respond with a valid SAML message, containing a SAML status code 'Requester', and a firstlevel status code 'RequestDenied', as well as a SAML status message to indicate why the message has been denied (i.e. 'missing or unknown issuer'). As an exception, a receiving Service Provider receiving an incorrect response MAY abort the process and provide the User with an alternative.

Also a message could be sent, that the receiving party is unable to answer. For instance, because the requested Level of Assurance is not supported by the Identity Provider in question. When a party receives a message that, from a functional perspective, it is unable to handle, that party MUST abort the process. The receiving party MUST send the user back to the original requester. The receiving party SHOULD transmit a valid SAML message, with a SAML status code 'Responder', and a first level status code 'RequestUnsupported' including a SAML status message that indicates the arisen problem (e.g. 'level not supported').

When a party receives a message that is too ‘old’, or when it receives a message that is unexpected at that moment in the user flow (for instance unknown InResponseTo) that party MUST abort the process. The user SHOULD be sent back to the requester with a valid SAML message, with SAML status code 'Responder', and a first level status code 'RequestDenied'. The receiver SHOULD include a SAML status message indicating the problem (i.e. ‘message invalid’).

The requester MUST investigate the arisen error. The requester informs the user of the reason of failure. The requester MAY offer the user an alternative.

Synchronize system clocks

Each Participant and service provider MUST synchronize the system with a reliable and precise time source so the system time never deviates more than 2 seconds either way.

All time stamps in messages MUST be formatted as yyyy-mm-ddThh:mm:ssZ. The T(time) and Z(zulu) are fixed values.

Web services

When web services are used within Uniforme Set van Eisen, the web service standards as defined in DigiKoppeling/Forum Standaardisatie "pas toe of leg uit" (comply or explain) are adhered to. The '2W-be' profile is to be applied, effectively resulting in:

- the web service MUST conform to WS-I Basic Profile 1.1. This implies the use of SOAP 1.1, WSDL 1.1 and XML 1.0 (second edition).
- the web service MUST use WS-Addressing as per WS-I Basic Profile 1.2.
- the web service MUST conform to WS-I Simple SOAP Binding Profile Version 1.0.
- the connection MUST be secured using (mutual authenticated) TLS, with the parameters as defined under Secure

connection (TLS).

Web services

All interfaces, except Interface Dienstverlener - Toegangsdienst, are implemented as web services. All Technical security requirements (e.g. Secure connection (TLS)) apply, unless specified otherwise. When using a HSM to realize the transformation functionality, only the Requirements on HSMs performing polymorphic transformations at authentication providers apply.

Message level security

The body of both request and response MUST be signed with a WS-Security header containing an XML Signature based on the PKIo certificate. The WS-Security signature MUST include the KeyInfo in the signature, as per WS-Security X.509 Certificate Token Profile 1.0, §3.3.3. The certificate referenced MUST be listed in the Metadata for participants in a KeyDescriptor of the Authenticatiedienst marked for the use "signing" (or without use, the default includes signing).

Both the certificate used for the WS-Security signature as well as the certificate used for the TLS connection to the web service MUST contain the OIN of the requesting Authenticatiedienst (or Middelenuitgever).

> Note: a PKI-overheid certificate with the OIN of the Authenticatiedienst (or Middelenuitgever) MUST be used.

Technical security requirements

The following technical security requirements apply to all interfaces for all Participants.

- DNSSEC — Every Participant MUST publish DNSSEC records for their domains registered for use. Every Participant SHOULD verify DNSSEC records when communicating with peers. For Service Providers it is RECOMMENDED to publish and verify DNSSEC records.
- Secure connection (TLS) — All connections between systems MUST be secured using Transport Layer Security (TLS) conforming to the following requirements.
- XML Digital Signature — To guarantee authenticity, integrity and non-repudiation, each message described MUST be provided with a digital signature from the message sender.
- (SAML) Encryption — To prevent the users attributes and identifiers from being readable by unintended parties, encryption MUST be used to guarantee confidentiality.

DNSSEC

Every Participant MUST publish DNSSEC records for their domains registered for use. Every Participant SHOULD verify DNSSEC records when communicating with peers. For Service Providers it is RECOMMENDED to publish and verify DNSSEC records.

Secure connection (TLS)

All connections between systems MUST be secured using Transport Layer Security (TLS) conforming to the following requirements.

- All connections between Participants, between Participants and Service Providers or between Participants and other peers like BSNk MUST use TLS 1.2.
- All connections between Participants and a user's browser/application MUST use TLS 1.0, TLS 1.1 or TLS 1.2.
- A Participant MUST NOT use or accept TLS compression, Insecure Renegotiation and Client-initiated Renegotiation.
- A new, cryptographically sound, generated random MUST be used for each connection.

PKIoverheid certificates

For all TLS connections:

- A Participant MUST use a PKIoverheid G2, PKIoverheid G3 or PKIoverheid EV SSL certificate. The (extended) key usage of the used certificate MUST allow use for TLS.
- A public service provider MUST use a PKIoverheid G2, PKIoverheid G3 or PKIoverheid EV SSL certificate.
- For communication over direct connections between Participants or between Dienstverlener and Participants (e.g. back-channel requests), TLS with mutual authentication using certificates MUST be used, and:
  - the server-certificate Subject.CommonName MUST match the contacted endpoint's hostname.
  - the client-certificate(s) used MUST be listed in the metadata.

Cipher suites

For all TLS connections, the following requirements with regards to cipher suites apply:

- A Participant MUST use and accept one or more of the cipher suites that are categorized "adequate" in the cipher suite table below.
- A Participant SHOULD use and accept one or more of the cipher suites that are categorized "good" in the cipher suite table below.
- A Participant MUST follow the order of the cipher suite list, as it is ordered by strength/level of security, with the strongest/most secure cipher suite on top.

Cipher suites marked "good":

IANA format	OpenSSL format	GnuTLS format
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	TLS_ECDHE_ECDSA_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	TLS_ECDHE_ECDSA_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_AES_128_GCM_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	ECDH-ECDSA-AES256-GCM-SHA384	-
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	ECDH-ECDSA-AES128-GCM-SHA256	-
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	ECDH-RSA-AES256-GCM-SHA384	-
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	ECDH-RSA-AES128-GCM-SHA256	-
TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384	TLS_RSA_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256	TLS_RSA_AES_128_GCM_SHA256

Cipher suites marked "adequate":

IANA format	OpenSSL format	GnuTLS format
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	TLS_ECDHE_ECDSA_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	TLS_ECDHE_ECDSA_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	TLS_ECDHE_ECDSA_AES_256_CBC_SHA1
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	TLS_ECDHE_ECDSA_AES_128_CBC_SHA1
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	TLS_ECDHE_ECDSA_3DES_EDE_CBC_SHA1
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_AES_256_CBC_SHA1
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_AES_128_CBC_SHA1
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	TLS_ECDHE_RSA_3DES_EDE_CBC_SHA1
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	ECDH-ECDSA-AES256-SHA384	-
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	ECDH-ECDSA-AES128-SHA256	-
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	ECDH-ECDSA-AES256-SHA	-
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	ECDH-ECDSA-AES128-SHA	-
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDH-ECDSA-DES-CBC3-SHA	-
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	ECDH-RSA-AES256-SHA384	-
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	ECDH-RSA-AES128-SHA256	-
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	ECDH-RSA-AES256-SHA	-
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	ECDH-RSA-AES128-SHA	-
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	ECDH-RSA-DES-CBC3-SHA	-
TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256	TLS_RSA_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256	TLS_RSA_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	TLS_RSA_AES_256_CBC_SHA1
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	TLS_RSA_AES_128_CBC_SHA1
TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	TLS_RSA_3DES_EDE_CBC_SHA1

The tables above with a qualification of TLS-ciphersuites is based on the recommendation of NCSC.

The WS-I Basic Security Profile mentions cipher suites that are discouraged. These cipher suites SHALL NOT be used.

The requirements above are a realization of 2.4.6 Technische controles, LoA Substantial, item 4.

XML Digital Signature

To guarantee authenticity, integrity and non-repudiation, each message described MUST be provided with a digital signature from the message sender.

The message recipient MUST validate all of the digital signatures in the message before processing it.

- The recipient MUST check that the message is signed with a valid digital signature that envelopes the whole message with Enveloped Signature Transform.
- The recipient MUST NOT process the message if it contains parts that are not signed with a valid digital signature.

The following requirements apply to generating digital signatures:

- The digital signature is embedded in the message content with Enveloped Signature Transform http://www.w3.org/2000/09/xmldsig#enveloped-signature.
- Canonicalization MUST be carried out according to the exclusive c14n method without comments, as identified by ' http://www.w3.org/2001/10/xml-exc-c14n#' (see http://www.w3.org/TR/xml-exc-c14n/)
- Digests MUST be calculated with the SHA256 algorithm.
- The SignatureValue MUST be calculated with the RSA-SHA256 algorithm.
- The sender MUST sign messages with a PKIoverheid (G2, G3 or newer, or a PKIo EV) certificate with a key length of at least 2048 bits.
    - The (extended) key usage of the used certificate MUST allow use for signing.
    - The Subject.serialNumber of the PKIoverheid certificate MUST contain the OIN of the holder of the certificate.
- In case of signing metadata, the <Signature> element MUST contain only an <X509Data> element with an <X509Certificate> element.
- In all other cases the <Signature> element MUST identify the certificate used for the signature. To this end the <Signature> MUST contain a <KeyInfo> element that:
    - MAY contain a <KeyName>, this <KeyName> MUST match the <KeyName> stated in the officially exchanged metadata of the sender and uniquely reference the certificate in the context of the Signing entity.
    - MAY contain a <X509Data> element with either a <X509Certificate> element that contains the certificate used or a <X509IssuerSerial> that references the certificate.
- The Reference MUST refer to the signed element via an ID attribute in the local document or use the empty (URI="") to reference the direct enclosing node-set.

The requirements above are a realization of 2.4.6 Technische controles, LoA Substantial, item 4.

(SAML) Encryption

To prevent the users attributes and identifiers from being readable by unintended parties, encryption MUST be used to guarantee confidentiality.For the encryption the following requirements apply;

- Encryption of the attributes/identifier will be based on a 256 bit AES key.
- The block encryption algorithms identified by the following URI in conjunction with the use of XML Encryption MUST be used: http://www.w3.org/2001/04/xmlenc#aes256-cbc
- A new, cryptographically sound randomly generated symmetric key MUST be used per encrypted element (and EncryptedID).
    - The @Recipient of the resulting <EncryptedKey> MUST be set to the EntityID of the recipient (intended public ServiceProvider).
    - XML contents in the encrypted element MUST have all relevant namespace definitions.

For asymmetric encryption, used to encrypt keys, the RSA algorithm in combination with OAEP padding and a SHA-1 digest MUST be used, as described at http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/Overview.html#rsa-oaep-mgf1p. These algorithms are identified as

- http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p
- http://www.w3.org/2000/09/xmldsig#sha1

Multiple certificates

SAML and XML-encryption allow for multiple 'recipients' of the same encrypted element. The construct for this is specified in more detail in errata E43 of SAML 2.0 errata 05.
This feature MAY be used to help facilitate a certificate change at the Service Provider, by (temporarily) allowing both the old and/or the new certificate to be used. The following additional requirements than apply.

- each EncryptedKey MUST have a CarriedKeyName equal to the KeyName used in the KeyInfo of the EncryptedData.
- each EncryptedKey SHOULD have a ReferenceList, referring back to the data encrypted with the symmetric key contained.

The requirements above are a realization of 2.4.6 Technische controles, LoA Substantial, item 4.

Interface specifications

The Uniforme Set van Eisen specifies the following interfaces:

- Interface Dienstverlener - Toegangsdienst
- Interfaces Authenticatiedienst/Middelenuitgever - BSNk
- Interfaces Middelenuitgever - BSNk
- Interface Toegangsdienst - BSNk Sleutelbeheer: provideDVKeys
- Polymorphic Pseudonymization Notation

Interface Dienstverlener - Toegangsdienst

The interface described is used to implement the use case GUC3 Aantonen identiteit and MUST be offered by every Toegangsdienst.

Request

The authentication request MUST be communicated within a SAML AuthnRequest.
The SAML AuthnRequest itself MAY be wrapped in additional container (e.g., but not limited to, a SAML ArtifactResolve).
The SAML AuthnRequest MUST conform to the specifications as listed below:

Element/@Attribute	0..n	Content
@ID	1	Unique message characteristic. MUST identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.

@Version	1	Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	1	Time of issuing of the request.
@Destination	0..1	MAY be present. When present MUST match the URL of the intended recipient.
@Consent	0..1	MAY be present. SHALL be ignored.
@ForceAuthn	0..1	MAY be present. MUST be “true” if present.
@IsPassive	0..1	MAY be present. MUST be “false” if present.
@ProtocolBinding	0..1	Specifies the used binding. MUST only be used when an @AssertionConsumerServiceURL is used. MUST NOT be used in combination with an @AssertionConsumerServiceIndex.
@AssertionConsumerServiceIndex	0..1	MAY be present. When present this index MUST refer to an endpoint of an AssertionConsumerServiceas as recorded in the 'Dienstverlener' 'Toegangsdienst' bilateral metadata. MUST NOT be present when @AssertionConsumerServiceURL is present.
@AssertionConsumerServiceURL	0..1	MAY be present. When present MUST be used to communicate the return URL of the Dienstverlener. MUST NOT be present when @AssertionConsumerServiceIndex is present.
@ AttributeConsumingServiceIndex	0..1	MAY be present. When present MUST refer to a service identification as agreed upon by the Dienstverlener and Toegangsdienst, to request the authentication-data 'by reference' (i.e Level of Assurance, attributes etc.).
@ProviderName	0..1	MAY be present; when present SHOULD match formal registered name.
Issuer	1	MUST contain the Identity of the Dienstverlener.
@NameQualifier	0	MUST NOT be present.
@SPNameQualifier	0	MUST NOT be present.
@Format	0	MUST NOT be present.
@SPProvidedID	0	MUST NOT be present.

Signature	0..1	MAY be present, when present MUST contain the Digital signature of the DV for the enveloping message (i.e. http://www.w3.org/TR/xmldsig-core/#sec-EnvelopedSignature transform) MAY be omitted. When omitted the dienstverlener MUST guarantee the integrity of the AuthnRequest at a higher container level (e.g. on ArtifactResolve-level).
Extensions	0..1	MAY be present.
Subject	0	MUST NOT be present.
NameIDPolicy	0	MUST NOT be present.
Conditions	0..1	MAY be present.
RequestedAuthnContext	0..1	MAY be present, when present MUST specify the required Level of Assurance. When not present the required Level of Assurance MUST be communicated by reference through means of the AttributeConsumingServiceIndex referencing the agreed upon bilateral metadata.
@Comparison	1	MUST be: 'minimum'.
AuthnContextClassRef	1	MUST specify the required level of assurance (eIDAS Subtantial of High).
Scoping	0..1	MAY be present.

Response

A successful authentication result MUST be communicated as a SAML AuthnResponse, the SAML response MUST be transmitted through a backchannel.
The SAML AuthnResponse MAY be wrapped in an additional container (e.g. wrapped in an ArtifactResolve message)

The AuthnResponse MUST conform to the specifications as listed below:

Element/@Attribute	0..n	Content
@ID	1	Unique message characteristic. MUST identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.
@InResponseTo	1	Unique attribute of the AuthnRequest for which this Response message is the answer.

@Version	1	Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	1	Time of issuing of the response
@Destination	0..1	MAY be present. When present MUST match the the endpoint of the Dienstverlener to which the message is offered
@Consent	0..1	MAY be present, SHALL be ignored by the Dienstverlener.
Issuer	1	MUST contain the identity of the issuer of the response message (Toegangsdienst).
@NameQualifier	0	MUST NOT be present.
@SPNameQualifier	0	MUST NOT be present.
@Format	0	MUST NOT be present.
@SPProvidedID	0	MUST NOT be present.
Signature	0..1	MAY be present, when present MUST contain the Digital signature of the Issuer (Toegangsdienst) for the enveloping message (i.e. http://www.w3.org/TR/xmldsig-core/#sec-EnvelopedSignature transform) MAY be omitted. When omitted the Dienstverlener MUST guarantee the integrity of the AuthnResponse at a higher container level (e.g. on ArtifactResolve level).
Extensions	0	MUST NOT be present.
Status	1	MUST be present.
StatusCode	1	MUST be present.
@Value	1	MUST be: “urn:oasis:names:tc:SAML:2.0:status:Success” when indicating a successful authentication.
StatusCode	0..1	MUST be present.
@Value	1	SHOULD be present, SHOULD provide insight as to why authentication has failed.

StatusMessage	0..1	MUST NOT be present on a successful authentication.
StatusDetail	0	MUST NOT be present
Assertion	0..1	MUST be present when the authentication was successful (see below).
EncryptedAssertion	0	MUST NOT be present.

The authentication Response MUST (assuming a successful authentication) contain an Assertion declaring about the authentication process.

In case of a collaboration between different parties for the roles of 'Toegangsdienst' and 'Authenticatiedienst' a 'Toegangsdienst' MAY create the following assertion.
When the 'Toegangsdienst' signs the assertion, that assertion MUST contain an additional Assertion under the Advice element, which MUST be signed by the party who authenticated the user.
A 'Dienstverlener' MUST be able to reliably and easily verify both Assertions declare about the same Principal.

Otherwise the Assertion MUST be created by the party who authenticated the user (Authenticatiedienst).

Element/@Attribute	0..n	Description
@ID	1	Unique message characteristic. MUST identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.
@Version	1	Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	1	Time of creation of the Assertion.
Issuer	1	MUST contain the Identity of the 'Authenticatiedienst' (or Toegangsdienst, see above).
@NameQualifier	0	MUST NOT be present.
@SPNameQualifier	0	MUST NOT be present.
@Format	0	MUST NOT be present.
@SPProvidedID	0	MUST NOT be present.

Signature	1	MUST be present to guarantee the integrity of the Assertion, MUST be signed with a certificate that can be matched with the above Issuer.
Subject	1	MUST be present.
BaseID	0	MUST NOT be present.
NameID	0	MUST NOT be present.
EncryptedID	1	MUST be present. Contains the NameID element in encrypted form, according to the SAML specification. The NameID itself consists of an encrypted identity or encrypted pseudonym conform the specification of the Uniforme Set van Eisen; see Polymorphic Pseudonymization Notation
SubjectConfirmation	1	MUST be present: Contain SubjectConformation according to the WebSSO profile.
Conditions	1	MUST be present.
@NotBefore	1	MUST be present: Contains DateTime at which the Assertion was created.
@NotOnOrAfter	0..1	MAY be present.
Condition	0	MUST NOT be present.
AudienceRestriction	1	MUST be present
Audience	1..n	Contains an URI which identifies the intended audience (i.e. Dienstverlener) to receive and process the Assertion.
OneTimeUse	0..1	MAY be present, SHALL be ignored.
ProxyRestriction	0	MUST NOT be present.
Advice	0..1	MUST NOT be present when the Authenticatiedienst signed the assertion. When present MUST contain a signed Assertion by the 'Authenticatiedienst'. The principal in this underlying assertion must strongly match the principal in its parents Assertion.
AssertionIDRef	0	MUST NOT be present.
AssertionURIRef	0	MUST NOT be present.

Assertion	0..1	MAY be present (see above).
EncryptedAssertion	0	MUST NOT be present.
AuthnStatement	1	MUST NOT be present.
@AuthnInstant	1	MUST be present; DateTime at which the authentication took place.
@SessionIndex	0..1	MAY be present.
AuthnContext	1	MUST be present.
AuthnContextClassRef	1	MUST be present. MAY be 'urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified' to indicate that authentication has occured at, at least, the requested level of assurance. Otherwise MUST contain either http://eidas.europa.eu/LoA/substantial or http://eidas.europa.eu/LoA/high in accordance with the level of assurance of the authentication proces.
AttributeStatement	1	MUST be present. Contains the following required information in plain text SAML <Attribute>; • ServiceID: contains the ServiceID for which authentication took place. • Level of Assurance: contains the level of assurance at which authentication took place. and the following optional information in <EncryptedAttribute> (see Technical security requirements) • DeprecatedID: identifier previously associated with the user (when applicable).

Interfaces Authenticatiedienst/Middelenuitgever - BSNk

The BSNk shall expose web services containing the operations listed below for Authenticatiediensten / Middelenuitgevers and publish the corresponding WSDL document.

- Interface spec BSNk: transform — This interface between an Authenticatiedienst or Middelenuitgever and BSNk transforms a given Polymophic Pseudonym to a Relying Party specific Encrypted Pseudonym or Polymorphic Identity to an Encrypted Identity. An Authenticatiedienst uses this interface after authenticating an User.
- Requirements on HSMs performing polymorphic transformations at authentication providers
- Interface spec BSNk: registerRemarkableEvents — Authenticatiedienst and Middelenuitgever use this interface to register a Remarkable authentication or Registration Event at the BSNk Misbruikbestrijdingsregister.

Interface spec BSNk: transform

This interface between an Authenticatiedienst or Middelenuitgever and BSNk transforms a given Polymophic Pseudonym to a Relying Party specific Encrypted Pseudonym or Polymorphic Identity to an Encrypted Identity. An Authenticatiedienst uses this interface after authenticating an User.

The interface described may be used to implement the use case AUC2 Transformeren and can be implemented by every Authenticatiedienst or Middelenuitgever.

WSDL transform

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<wsdl:definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
                  xmlns:bsnk="urn:nl-gdi-eid:1.0:webservices"
                  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
                  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata"
                  name="BSNk_transform"
                  targetNamespace="urn:nl-gdi-eid:1.0:webservices">

    <wsdl:types>
        <xsd:schema targetNamespace="urn:nl-gdi-eid:1.0:webservices"
                    attributeFormDefault="unqualified"
                    elementFormDefault="qualified">
            <xsd:element name="ProvideEPRequest" type="bsnk:ProvideEncryptedRequestType">
                <xsd:annotation>
                    <xsd:documentation>Request message to provide an encrypted
                        pseudonym of a user for a specific relying party
                        (service provider).
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:element name="ProvideEIRequest" type="bsnk:ProvideEncryptedRequestType">
                <xsd:annotation>
                    <xsd:documentation>Request message to provide an encrypted
                        identity of a user for a specific relying party
                        (service provider).
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:complexType name="ProvideEncryptedRequestType">
                <xsd:complexContent>
                    <xsd:extension base="bsnk:BSNkProvideRequestBasetype">
                        <xsd:sequence>
                            <xsd:element name="RelyingParty" type="bsnk:OINType" />
                            <xsd:element name="RelyingPartyKeySetVersion" type="bsnk:KeyVersionType" />
                            <xsd:element name="PolymorphicPseudonym"
type="bsnk:PolymorphicPseudonymType" />
                            <xsd:element name="Role" type="bsnk:RoleType" minOccurs="0" />
                            <xsd:element name="TransactionID" type="bsnk:TransactionIDType"
minOccurs="0" />
                        </xsd:sequence>
                    </xsd:extension>
                </xsd:complexContent>
            </xsd:complexType>
            <xsd:complexType name="BSNkProvideRequestBasetype" abstract="true">
                <xsd:sequence>
                    <xsd:element name="Requester" type="bsnk:OINType" />
                </xsd:sequence>
                <xsd:attribute name="DateTime" type="xsd:dateTime" use="required" />
                <xsd:attribute name="RequestID" type="xsd:ID" use="required" />
            </xsd:complexType>
            <xsd:complexType name="PolymorphicPseudonymType">
                <xsd:simpleContent>
                    <xsd:extension base="xsd:base64Binary"/>
                </xsd:simpleContent>
            </xsd:complexType>
            <xsd:simpleType name="KeyVersionType">
                <xsd:annotation>
                    <xsd:documentation>Key(set) version type.</xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:positiveInteger"/>
            </xsd:simpleType>
            <xsd:simpleType name="OINType">
                <xsd:annotation>
                    <xsd:documentation>OIN type.
                    </xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:string">
                    <xsd:length value="20" />
                </xsd:restriction>
            </xsd:simpleType>
            <xsd:simpleType name="RoleType">
                <xsd:annotation>
                    <xsd:documentation>Role type.
                    </xsd:documentation>
                </xsd:annotation>
```

```
            <xsd:restriction base="xsd:integer"/>
        </xsd:simpleType>
        <xsd:simpleType name="TransactionIDType">
            <xsd:annotation>
                <xsd:documentation>TransactionID Type.
                </xsd:documentation>
            </xsd:annotation>
            <xsd:restriction base="xsd:string">
                <xsd:length value="128" />
            </xsd:restriction>
        </xsd:simpleType>

        <xsd:element name="ProvideEPResponse" type="bsnk:ProvideEncryptedResponseType">
            <xsd:annotation>
                <xsd:documentation>
                    Response to a ProvideEPRequest.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:element name="ProvideEIResponse" type="bsnk:ProvideEncryptedResponseType">
            <xsd:annotation>
                <xsd:documentation>
                    Response to a ProvideEIRequest.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:complexType name="ProvideEncryptedResponseType">
            <xsd:complexContent>
                <xsd:extension base="bsnk:BSNkProvideResponseBasetype">
                    <xsd:sequence>
                        <xsd:element name="EncryptedPseudonym" type="bsnk:EncryptedPseudonymType"
/>
                    </xsd:sequence>
                </xsd:extension>
            </xsd:complexContent>
        </xsd:complexType>
        <xsd:complexType name="BSNkProvideResponseBasetype" abstract="true">
            <xsd:attribute name="DateTime" type="xsd:dateTime" use="required" />
            <xsd:attribute name="ResponseID" type="xsd:ID" use="required" />
            <xsd:attribute name="InResponseTo" type="xsd:NCName" use="required" />
        </xsd:complexType>
        <xsd:simpleType name="EncryptedPseudonymType">
            <xsd:restriction base="xsd:base64Binary" />
        </xsd:simpleType>
        <xsd:element name="ProvideEncryptedFault" type="bsnk:ProvideEncryptedFaultType">
            <xsd:annotation>
                <xsd:documentation>
                    Fault response to a ProvideEPRequest of ProvideEIRequest.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:complexType name="ProvideEncryptedFaultType">
            <xsd:sequence>
                <xsd:element name="FaultReason" type="bsnk:ProvideEncryptedFaultReasonType" />
                <xsd:element name="FaultDescription" type="bsnk:FaultDescriptionType"
maxOccurs="unbounded" />
            </xsd:sequence>
        </xsd:complexType>
        <xsd:simpleType name="ProvideEncryptedFaultReasonType">
            <xsd:union memberTypes="bsnk:FaultReasons bsnk:ProvideEncryptedFaultReasons" />
        </xsd:simpleType>
        <xsd:simpleType name="FaultReasons">
            <xsd:restriction base="xsd:string">
                <xsd:enumeration value="NotFound">
                    <xsd:annotation>
                        <xsd:documentation>Provided information results in
                            zero matches.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="AuthorizationError">
                    <xsd:annotation>
                        <xsd:documentation>Authentication invalid or access denied.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="SyntaxError">
                    <xsd:annotation>
                        <xsd:documentation>Request invalid.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="TemporarilyUnavailable">
                    <xsd:annotation>
                        <xsd:documentation>Request could temporarily not be
                            processed. A new request for provisioning MAY be
                            send at a later moment by the requesting party.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
            </xsd:restriction>
        </xsd:simpleType>
```

```
            <xsd:simpleType name="ProvideEncryptedFaultReasons">
                <xsd:restriction base="xsd:string">
                    <xsd:enumeration value="ProvisioningRefused">
                        <xsd:annotation>
                            <xsd:documentation>Transformation refused for other
                                (non-disclosed) reason.
                            </xsd:documentation>
                        </xsd:annotation>
                    </xsd:enumeration>
                </xsd:restriction>
            </xsd:simpleType>
            <xsd:complexType name="FaultDescriptionType">
                <xsd:simpleContent>
                    <xsd:extension base="xsd:string">
                        <xsd:attribute name="lang" type="xsd:language" />
                    </xsd:extension>
                </xsd:simpleContent>
            </xsd:complexType>
        </xsd:schema>
    </wsdl:types>

    <wsdl:message name="BSNk_ProvideEPRequest">
        <wsdl:part name="in" element="bsnk:ProvideEPRequest" />
    </wsdl:message>

    <wsdl:message name="BSNk_ProvideEIRequest">
        <wsdl:part name="in" element="bsnk:ProvideEIRequest" />
    </wsdl:message>

    <wsdl:message name="BSNk_ProvideEPResponse">
        <wsdl:part name="out" element="bsnk:ProvideEPResponse" />
    </wsdl:message>

    <wsdl:message name="BSNk_ProvideEIResponse">
        <wsdl:part name="out" element="bsnk:ProvideEIResponse" />
    </wsdl:message>

    <wsdl:message name="BSNk_ProvideEncryptedFault">
        <wsdl:part name="fault" element="bsnk:ProvideEncryptedFault" />
    </wsdl:message>

    <wsdl:portType name="BSNk_Transform_Port">
        <wsdl:operation name="BSNk_ProvideEP">
            <wsdl:input message="bsnk:BSNk_ProvideEPRequest"
wsam:Action="urn:nl-gdi-eid:1.0:webservices:ProvideEPRequest" />
            <wsdl:output message="bsnk:BSNk_ProvideEPResponse"
wsam:Action="urn:nl-gdi-eid:1.0:webservices:ProvideEPResponse" />
            <wsdl:fault message="bsnk:BSNk_ProvideEncryptedFault" name="BSNk_ProvideEncrypted_Fault"/>
        </wsdl:operation>
        <wsdl:operation name="BSNk_ProvideEI">
            <wsdl:input message="bsnk:BSNk_ProvideEIRequest"
wsam:Action="urn:nl-gdi-eid:1.0:webservices:ProvideEIRequest" />
            <wsdl:output message="bsnk:BSNk_ProvideEIResponse"
wsam:Action="urn:nl-gdi-eid:1.0:webservices:ProvideEIResponse" />
            <wsdl:fault message="bsnk:BSNk_ProvideEncryptedFault" name="BSNk_ProvideEncrypted_Fault"/>
        </wsdl:operation>
    </wsdl:portType>

    <wsdl:binding name="BSNk_Transform_SOAP" type="bsnk:BSNk_Transform_Port">
        <soap:binding style="document"
            transport="http://schemas.xmlsoap.org/soap/http" />
        <wsdl:operation name="BSNk_ProvideEP">
            <soap:operation soapAction="urn:nl-gdi-eid:1.0:webservices:ProvideEPRequest" />
            <wsdl:input>
                <soap:body use="literal" />
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal" />
            </wsdl:output>
            <wsdl:fault name="BSNk_ProvideEncrypted_Fault">
                <soap:fault name="BSNk_ProvideEncrypted_Fault" use="literal" />
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="BSNk_ProvideEI">
            <soap:operation soapAction="urn:nl-gdi-eid:1.0:webservices:ProvideEIRequest" />
            <wsdl:input>
                <soap:body use="literal" />
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal" />
            </wsdl:output>
            <wsdl:fault name="BSNk_ProvideEncrypted_Fault">
                <soap:fault name="BSNk_ProvideEncrypted_Fault" use="literal" />
            </wsdl:fault>
        </wsdl:operation>
    </wsdl:binding>

    <wsdl:service name="BSNk_Transform_Service">
        <wsdl:port binding="bsnk:BSNk_Transform_SOAP" name="BSNk_Transform">
            <soap:address location="https://.../TODO/Transform" />
        </wsdl:port>
```

```
    </wsdl:service>
</wsdl:definitions>
```

Request

Consists of a transformation request message <ProvideEPRequest> or <ProvideEIRequest> in the SOAP body of the request message. SOAP should be implemented accoording to the Web services requirements .

Element/@Attribute	0..n	Description
@DateTime	1	Time of issuing of the request.
@RequestID	1	Unique identifier for this request.
<Requester>	1	EntityID (OIN) of the requesting Authenticatiedienst.
<RelyingParty>	1	EntityID (OIN) of the intended relying party.
<RelyingPartyKeySetVersion>	1	Key set version to be used for relying party.
<PolymorphicPseudonym>	1	Polymorphic Pseudonymization structure for the user to be transformed to an encrypted pseudonym. Only one Polymorphic Pseudonym MUST be present.
<Role>	0..1	Optional "persoonsrol". Reserved for future use where the same user can act in different roles, e.g. private, volunteer and employee.
<TransactionID>	0..1	Optional "transactie ID". Reserved for future use where privacy prohibits use of a persistent pseudonym. TransactionID can be used to create a transaction-, session- or case- specific pseudonym. Also for guarantees for the 4-eyes principle, TransactionID can be used in combination with the default Role (otherwise a person could break a 4-eyes signature by using two different Roles). Another example is eIDAS that requires a pseudonym per EU country, for which a countryID can be used als TransactionID to make the resulting pseudonym specific and persistent per country.

Rules for processing a Transformation Request

A requesting Authenticatiedienst:

- MUST authenticate a User at the requested Level of Assurance before requesting a transformation.
- MUST check the relying party is listed in the Autorisatielijst BSN as authorized before requesting transformation of a PI.
- MUST only provide a PP for a <ProvideEPRequest> and MUST only provide a PI for a <ProvideEIRequest>.
- SHOULD randomize the PP/PI to be transformed before requesting a transformation, to enhance the privacy of the User.

Response

Consists of a response message <ProvideEPResponse> or <ProvideEIResponse> in the SOAP body of the response message, containing an Encrypted Pseudonym or Encrypted Identity for the requested Relying Party.
In case an error occurs a SOAP fault will be used. The SOAP fault will contain error codes as <FaultReason> as described below, with one (or more) (localized) <FaultDescription>s.

Element/@Attribute	0..n	Description
@DateTime	1	Time of issuing of the response.
@ResponseID	1	Unique identifier of the Response
@InResponseTo	1	Unique identifier of the Request this is a response to (@RequestID of request)
<EncryptedPseudonym>	1	One (signed) Encrypted Pseudonym structure for the User for the RelyingParty.

For encoding of the Encrypted Pseudonym (or Encrypted Identity), see Polymorphic Pseudonymization Notation.

FaultReasons

The following response codes are used to indicate the status of a response.

ResponseCode	Description
ProvisioningRefused	Request rejected. Transformation of a Polymorphic Pseudonym refused for non-disclosed reason.
AuthorizationError	Request rejected. Authentication invalid or access denied. A HTTP 403 status response MAY be given instead of a SOAP-fault with this response.
SyntaxError	Request rejected. Request invalid.
TemporarilyUnavailable	Request could temporarily not be processed. A new request for transformation of a Polymorphic Pseudonym MAY be sent at a later moment by the requesting party.

Requirements on HSMs performing polymorphic transformations at authentication providers

Authentication providers can make use of a Hardware Security Module (HSM) to transform polymorphic forms to encrypted forms, i.e. independently of the Interface spec BSNk: transform. This removes the dependency of the authentication provider (or Middelenuitgever) on the availability of the BSNk transformation service. A HSM is a security system providing both logical as physical protection to cryptographic keys. In short, a HSM facilitates that keys can be used but cannot be exported out of the HSM or the HSM cloned. For the polymorphic transformation a HSM combines several cryptographic operations using different keys that are provided by BSNk Key Management in a controlled fashion. Basic HSM security requirements are:

- Access to the transformation operation MUST be adequately controlled, i.e. it is technically enforced that only authorized applications within the authentication provider are able to perform the operation.
- Only the transformation operation is exposed to the authentication provider; the individual cryptographic operations the transformation is composed of MUST NOT be exposed or available.
- All keys within the HSM MUST be physically and logically protected; a high attack potential attacker shall not be able

to extract these keys from the HSM nor shall be able to run the individual cryptographic operations the transformation is composed of.
- All communication between requesting application and HSM MUST be secured to ensure confidentiality and integrity.
- The authentication provider MUST provide an independent conformity assessment report to BSNk Sleutelbeheer that the HSM meets the above requirements in its operational environment.

FIPS 140-2 level 3 certification or equivalent provides assurance that the HSM meets the requirements on key protection.

Interface spec BSNk: registerRemarkableEvents

Authenticatiedienst and Middelenuitgever use this interface to register a Remarkable authentication or Registration Event at the BSNk Misbruikbestrijdingsregister. The interface described here is used to implement use case AUC4 Registreren Opmerkelijke Gebeurtenis and should be implemented by every Authenticatiedienst or Middelenuitgever that services the domain.

Request

Consists of a registration request message <registerRemarkableEventRequest> in the SOAP body of the request message. SOAP should be implemented according to the Web services requirements .

Element/@Attribute	0..n	Description
@DateTime	1	Time of issuing of the request.
@RequestID	1	Unique identifier for this Request.
<Requester>	1	EntityID (OIN) of the requesting Authenticatiedienst (or Middelenuitgever).
<EncryptedPseudonym>	1	Encrypted Pseudonym of the user to be transformed to a pseudonym of the BSNk Misbruikbestrijdingsregister
<DeprecatedEP>	0..1	Optional previous Encrypted Pseudonym of the user to be transformed to a previous pseudonym of the BSNk Misbruikbestrijdingsregister, used for instance when Misbruikbestrijdingsregister changes from Beheerorganisatie BSNk to another party.
<Qualification>	1	String max 20 chars. A qualification of the remarkable event, e.g. "Sign" (could be part of ID-Fraud) or "Presumption" (presumed to be part of ID-Fraud).
<EventIndicator>	1	String max 20 chars. Indicator identifying which type of remarkable event
<CollectionID>	0..1	Base64 encoded SHA256 HASH of a Authenticatiedienst (or Middelenuitgever) specific Collection-identifier for remarkable activities. This CollectionID is only used to link multiple activities at a single Authenticatiedienst that are considered remarkable as a Collection.

<MeansType>	0..1	String max 30 chars. Value that represents a human-readable version of the type of Electronic Identification Means, involved in the remarkable event, e.g. for a government-issued document possible values are "NL-Paspoort", "NL-Identiteitskaart" and "NL-Rijbewijs".
<SequenceNr>	0..1	Number or Date. SequenceNr identifies a specific Electronic Identification Means. For privacy reasons this SequenceNr MUST have a low entropy. preferably 01, 02 ...09. In case of a date, for example, only use one weekday in a week for every means issued that week. In XML-schema a choice between 'number', 'date', 'gYear' or 'gYearMonth' format. MUST be present together with <MeansType>.
<RelyingParty>	0..1	EntityID (OIN) of the Relying Parties that the user is authenticating for.
@InResponseTo	0..1	Unique ID of request of the RelyingParty. MUST be present together with <RelyingParty>.
@IDAssertion	0..1	Unique ID of assertion sent to the RelyingParty. MUST be present together with <RelyingParty>.
<EventDateTime>	0..1	DateTime of remarkable event, MUST not be after @DateTime of this request.
<DeviceFingerprint>	0..1	Base64 encoded SHA256 HASH of the device fingerprint involved in the remarkable event. The exact construction of the device fingerprint for different scenarios will be defined by the Beheerorganisatie BSNk. The device fingerprint should provide enough entropy and stability (>day) to be usable for matching devices. The BSNk Inzageregister will apply a private one way function (HMAC) before registering the DeviceFingerprint for enhanced privacy (protection against third party replaying DeviceFingerprint on their users). The exact basic browserfingerprint (user-agent, OS, plugins, fonts) will be defined by the Beheerorganisatie BSNk.
<AnonimisedIP>	0..1	Base64 encoded SHA256 HASH of the user's IP-address and a basic passive browser fingerprint (without obvious querying of the client machine: user-agent, OS, plugins, fonts) involved in the remarkable event. This AnonimisedIP provides a privacy friendly alternative for matching IP-addresses over different parties. The browser fingerprint should provide enough entropy to protect the Anonimised-IP against rainbowtable attacks and it should provide enough stability for matching an AnonimisedIP over time (>week) for different parties. Note, when javascript is turned off the entropy of the browser fingerprint will be quite limited (possibly only user agent information), but this percentage is too small to be a risk. The BSNk Inzageregister will apply a private one way function (HMAC) before registering the AnonimisedIP for enhanced privacy (protection against third party replaying FingerprintIP on their users). The exact basic browser fingerprint (user-agent, OS, plugins, fonts) will be defined by the Beheerorganisatie BSNk.
<GeoLocation>	0..1	ISO 3166 alpha-3 Country Code of the used IP-address for this remarkable event, e.g. based on GeoIP database.
<ReadableText>	0..1	String max 120 chars. Human readable additional description of the remarkable event.

Processing rules for registerRemarkableEventRequest

A requesting Authenticatiedienst or Middelenuitgever:

- MUST await a successful response or retry to send the request. Requests MUST be buffered and retried during 7 days.
- MUST log and investigate failures.

Response

Consists of a response message <registerRemarkableEventResponse> in the SOAP body of the response message. In case a response is received, the request resulted in a registered remarkable authentication event. In case an error occurs a SOAP fault message will be used. The SOAP fault will contain error response codes as FaultReason as described below, with one (or more) localized FaultDescription.

Element/@Attribute	0..n	Description
@DateTime	1	Time of issuing of the response.
@ResponseID	1	Unique identifier of the response.
@InResponseTo	1	Unique identifier of the request this is a response to (@RequestID of request).

FaultReasons

The following response codes are used to indicate the status of a response.

ResponseCode	Description
NotFound	Request rejected. Provided information resulted in zero matches.
RegistrationRefused	Request rejected. Registration of event refused for other non-disclosed reason.
AuthorizationError	Request rejected. Authentication invalid or access denied. A HTTP 403 status response MAY be given instead of a SOAP-fault with this response.
SyntaxError	Request rejected. Request invalid.
TemporarilyUnavailable	Request could temporarily not be processed. A new request for registering the event MAY be sent at a later moment by the requesting party.

Interfaces Middelenuitgever - BSNk

The BSNk shall expose web services containing the operations listed below for Middelenuitgevers and publish the

corresponding WSDL document.

- Interface spec BSNk: activate — This interface between a Middelenuitgever and BSNk is used to activate a user's social security number (BSN) for government related electronic services. The activation requires a BSN and validation data and will result in the provision of one or more Polymorphic Pseudonymization structures (e.g. Polymorphic Identity and Polymorphic Pseudonym) by the BSNk.
- Interface Spec BSNk: registerStatusEIM — Middelenuitgever uses this interface to register a status for an Electronic Identification Means at the BSNk Inzageregister, for a new (first time) or a changed status.

Character set

As specified under Character encoding, UTF-8 MUST be used as character encoding.
As a character set for the Interface spec BSNk: activate interface, only values in the GBA-V (Teletex) character set MUST be used in the request attributes, as specified in "Logisch Ontwerp GBA 3.9", §II.2.

Interface spec BSNk: activate

This interface between a Middelenuitgever and BSNk is used to activate a user's social security number (BSN) for government related electronic services. The activation requires a BSN and validation data and will result in the provision of one or more Polymorphic Pseudonymization structures (e.g. Polymorphic Identity and Polymorphic Pseudonym) by the BSNk.

The interface described in this document is used to implement the use case "AUC1 Activeren BSN" (activate BSN) and MUST be implemented by every Middelenuitgever.

WSDL

WSDL activate

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<wsdl:definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
                  xmlns:bsnk="urn:nl-gdi-eid:1.0:webservices"
                  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
                  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata"
                  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                  name="BSNK_activate"
                  targetNamespace="urn:nl-gdi-eid:1.0:webservices">

    <wsdl:types>
        <xsd:schema targetNamespace="urn:nl-gdi-eid:1.0:webservices"
                    attributeFormDefault="unqualified"
                    elementFormDefault="qualified">

            <xsd:import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
schemaLocation="saml-schema-assertion-2.0.xsd"/>

            <xsd:element name="ProvidePPRequest" type="bsnk:ProvidePolymorphicRequestType">
                <xsd:annotation>
                    <xsd:documentation>Request message to provide PP for a
                        specific user, for future use via ProvideEP queries.
                        The 'BSNk' will generate one or more
                        polymorphic pseudonym(s) for the identified user.
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:element name="ProvidePP_PPCAOptimizedRequest"
type="bsnk:ProvidePolymorphicRequestType">
                <xsd:annotation>
                    <xsd:documentation>Request message to provide PP for a
                        specific user, for future use via ProvideEP queries.
                        The 'BSNk' will generate one or more
                        polymorphic pseudonym(s) for the identified user. This
                        request will result in one-or-more polymorphic
                        pseudonyms in a form optimized for usage as a PPCA.
                    </xsd:documentation>
                </xsd:annotation>
```

```
            </xsd:element>
            <xsd:complexType name="ProvidePolymorphicRequestType">
                <xsd:complexContent>
                    <xsd:extension base="bsnk:BSNkProvideRequestBasetype">
                        <xsd:sequence>
                            <xsd:element name="RequesterKeySetVersion" type="bsnk:KeyVersionType" />
                            <xsd:choice>
                                <xsd:element name="BSN" type="bsnk:BSNType" />
                                <xsd:element name="EncryptedBSN" type="bsnk:EncryptedBSNType"/>
                                <xsd:element name="EncryptedIdentity" type="bsnk:EncryptedIdentityType"
/>
                                <xsd:sequence>
                                    <xsd:element name="eIDAS-UniquenessID"
type="bsnk:eIDAS-UniquenessIDType"/>
                                    <xsd:element name="EncryptedBSN" type="bsnk:EncryptedBSNType"
minOccurs="0"/>
                                </xsd:sequence>
                            </xsd:choice>
                            <xsd:element name="DocumentType" type="bsnk:DocumentTypeType" minOccurs="0"
/>
                            <xsd:element name="DocumentID" type="bsnk:DocumentIDType" minOccurs="0" />
                            <xsd:element name="GivenNames" type="bsnk:GivenNamesType" minOccurs="0" />
                            <xsd:element name="SurName" type="bsnk:SurNameType" minOccurs="0" />
                            <xsd:element name="DateOfBirth" type="bsnk:BirthDateType" minOccurs="0" />
                            <xsd:element name="PlaceOfBirth" type="bsnk:PlaceOfBirthType" minOccurs="0"
/>
                        </xsd:sequence>
                    </xsd:extension>
                </xsd:complexContent>
            </xsd:complexType>
            <xsd:complexType name="BSNkProvideRequestBasetype" abstract="true">
                <xsd:sequence>
                    <xsd:element name="Requester" type="bsnk:OINType" />
                </xsd:sequence>
                <xsd:attribute name="DateTime" type="xsd:dateTime" use="required" />
                <xsd:attribute name="RequestID" type="xsd:ID" use="required" />
            </xsd:complexType>
            <xsd:simpleType name="KeyVersionType">
                <xsd:annotation>
                    <xsd:documentation>Key(set) version type.</xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:positiveInteger"/>
            </xsd:simpleType>
            <xsd:simpleType name="BSNType">
                <xsd:annotation>
                    <xsd:documentation>In case a BSN consists of a number of
                       only 8 digits, the BSN shall be padded with a preceding
                       '0' (digit zero).
                    </xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:string">
                    <xsd:length value="9" />
                </xsd:restriction>
            </xsd:simpleType>
            <xsd:simpleType name="EncryptedIdentityType">
                <xsd:annotation>
                    <xsd:documentation>Identity encrypted as an EncryptedIdentity
                        according to Polymorphic Pseudonimization.
                    </xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:base64Binary" />
            </xsd:simpleType>
            <xsd:simpleType name="eIDAS-UniquenessIDType">
                <xsd:annotation>
                    <xsd:documentation>To be used only in eIDAS context.
                    </xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:string" />
            </xsd:simpleType>
            <xsd:complexType name="EncryptedBSNType">
                <xsd:annotation>
                    <xsd:documentation>BSN encrypted in the form of a
                        SAML2 EncryptedID.
                    </xsd:documentation>
                </xsd:annotation>
                <xsd:sequence>
                    <xsd:element ref="saml2:EncryptedID" />
                </xsd:sequence>
            </xsd:complexType>
            <xsd:simpleType name="OINType">
                <xsd:annotation>
                    <xsd:documentation>OIN type.
                    </xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:string">
                    <xsd:length value="20" />
                </xsd:restriction>
            </xsd:simpleType>
            <xsd:simpleType name="DocumentIDType">
                <xsd:annotation>
                    <xsd:documentation>Document ID as appearing on the Identity
                        Document referenced
```

```
                </xsd:documentation>
            </xsd:annotation>
            <xsd:restriction base="xsd:string">
                <xsd:maxLength value="15" />
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="DocumentTypeType">
            <xsd:annotation>
                <xsd:documentation>Type of Identity Document referenced.
                </xsd:documentation>
            </xsd:annotation>
            <xsd:restriction base="xsd:string">
                <xsd:enumeration value="NL-Paspoort" />
                <xsd:enumeration value="NL-Identiteitskaart" />
                <xsd:enumeration value="NL-Rijbewijs" />
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="GivenNamesType">
            <xsd:annotation>
                <xsd:documentation>Given names as these appear on the
                    Identity Document referenced. If given names are not
                    fully known than must contain all known initials.
                </xsd:documentation>
            </xsd:annotation>
            <xsd:restriction base="xsd:string">
                <xsd:maxLength value="200" />
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="SurNameType">
            <xsd:annotation>
                <xsd:documentation>Surname as appears on the
                    Identity Document referenced.
                </xsd:documentation>
            </xsd:annotation>
            <xsd:restriction base="xsd:string">
                <xsd:maxLength value="210" />
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="BirthDateType">
            <xsd:union>
                <xsd:simpleType>
                    <xsd:restriction base="xsd:date" />
                </xsd:simpleType>
                <xsd:simpleType >
                    <xsd:restriction base="xsd:gYearMonth" />
                </xsd:simpleType>
                <xsd:simpleType >
                    <xsd:restriction base="xsd:gYear" />
                </xsd:simpleType>
            </xsd:union>
        </xsd:simpleType>
        <xsd:simpleType name="PlaceOfBirthType">
            <xsd:annotation>
                <xsd:documentation>For Dutch places of birth this value
                    must correspond to the exact value as listed in table
                    33 of the logic design of the BRP. MUST NOT be used for
                    foreign places of birth.
                </xsd:documentation>
            </xsd:annotation>
            <xsd:restriction base="xsd:string">
                <xsd:maxLength value="40" />
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:element name="ProvidePPResponse" type="bsnk:ProvidePolymorphicResponseType">
            <xsd:annotation>
                <xsd:documentation>
                    Response to a ProvidePPRequest or
                    ProvidePP_PPCAOptimizedRequest.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:element name="ProvidePP_PPCAOptimizedResponse"
type="bsnk:ProvidePolymorphicResponseType">
            <xsd:annotation>
                <xsd:documentation>
                    Response to a ProvidePP_PPCAOptimizedRequest.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:complexType name="ProvidePolymorphicResponseType">
            <xsd:complexContent>
                <xsd:extension base="bsnk:BSNkProvideResponseBasetype">
                    <xsd:sequence>
                        <xsd:element name="PolymorphicPseudonym"
type="bsnk:PolymorphicPseudonymType" maxOccurs="unbounded" />
                    </xsd:sequence>
                </xsd:extension>
            </xsd:complexContent>
        </xsd:complexType>
        <xsd:complexType name="BSNkProvideResponseBasetype" abstract="true">
            <xsd:attribute name="DateTime" type="xsd:dateTime" use="required" />
            <xsd:attribute name="ResponseID" type="xsd:ID" use="required" />
```

```
            <xsd:attribute name="InResponseTo" type="xsd:NCName" use="required" />
        </xsd:complexType>
        <xsd:complexType name="PolymorphicPseudonymType">
            <xsd:simpleContent>
                <xsd:extension base="xsd:base64Binary" />
            </xsd:simpleContent>
        </xsd:complexType>
        <xsd:element name="ProvidePolymorphicFault" type="bsnk:ProvidePolymorphicFaultType">
            <xsd:annotation>
                <xsd:documentation>
                    Fault response to a ProvidePPRequest or
                    ProvidePP_PPCAOptimizedRequest.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:complexType name="ProvidePolymorphicFaultType">
            <xsd:sequence>
                <xsd:element name="FaultReason" type="bsnk:ProvidePolymorphicFaultReasonType" />
                <xsd:element name="FaultDescription" type="bsnk:FaultDescriptionType"
maxOccurs="unbounded" />
            </xsd:sequence>
        </xsd:complexType>
        <xsd:simpleType name="ProvidePolymorphicFaultReasonType">
            <xsd:union memberTypes="bsnk:FaultReasons bsnk:ProvidePolymorphicFaultReasons" />
        </xsd:simpleType>
        <xsd:simpleType name="FaultReasons">
            <xsd:restriction base="xsd:string">
                <xsd:enumeration value="NotFound">
                    <xsd:annotation>
                        <xsd:documentation>Provided information results in
                            zero matches.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="AuthorizationError">
                    <xsd:annotation>
                        <xsd:documentation>Authentication invalid or access denied.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="SyntaxError">
                    <xsd:annotation>
                        <xsd:documentation>Request invalid.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="TemporarilyUnavailable">
                    <xsd:annotation>
                        <xsd:documentation>Request could temporarily not be
                            processed. A new request for activation MAY be send
                            at a later moment by the requesting party.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="ProvidePolymorphicFaultReasons">
            <xsd:restriction base="xsd:string">
                <xsd:enumeration value="NotEnoughInfo">
                    <xsd:annotation>
                        <xsd:documentation>Provided information may resolve
                            to a unique match, but not enough assurance
                            (e.g. against typos) can be established.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="NotUnique">
                    <xsd:annotation>
                        <xsd:documentation>Provided information results in
                            more than one match.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="DocumentRejected">
                    <xsd:annotation>
                        <xsd:documentation>Document not accepted.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="ProvisioningRefused">
                    <xsd:annotation>
                        <xsd:documentation>Activation refused for other
                            (non-disclosed) reason.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:complexType name="FaultDescriptionType">
            <xsd:simpleContent>
                <xsd:extension base="xsd:string">
                    <xsd:attribute name="lang" type="xsd:language" />
```

```
                    </xsd:extension>
                </xsd:simpleContent>
            </xsd:complexType>
        </xsd:schema>
    </wsdl:types>

    <wsdl:message name="BSNK_ProvidePPRequest">
        <wsdl:part name="in" element="bsnk:ProvidePPRequest" />
    </wsdl:message>

    <wsdl:message name="BSNK_ProvidePP_PPCAOptimizedRequest">
        <wsdl:part name="in" element="bsnk:ProvidePP_PPCAOptimizedRequest" />
    </wsdl:message>

    <wsdl:message name="BSNK_ProvidePPResponse">
        <wsdl:part name="out" element="bsnk:ProvidePPResponse" />
    </wsdl:message>

    <wsdl:message name="BSNK_ProvidePP_PPCAOptimizedResponse">
        <wsdl:part name="out" element="bsnk:ProvidePP_PPCAOptimizedResponse" />
    </wsdl:message>

    <wsdl:message name="BSNK_ProvidePolymorphicFault">
        <wsdl:part name="fault" element="bsnk:ProvidePolymorphicFault" />
    </wsdl:message>

    <wsdl:portType name="BSNK_Activate_Port">
        <wsdl:operation name="BSNK_ProvidePP">
            <wsdl:input message="bsnk:BSNK_ProvidePPRequest"
wsam:Action="urn:nl-gdi-eid:1.0:webservices:ProvidePPRequest" />
            <wsdl:output message="bsnk:BSNK_ProvidePPResponse"
wsam:Action="urn:nl-gdi-eid:1.0:webservices:ProvidePPResponse" />
            <wsdl:fault message="bsnk:BSNK_ProvidePolymorphicFault"
name="BSNK_ProvidePolymorphic_Fault"/>
        </wsdl:operation>
        <wsdl:operation name="BSNK_ProvidePP_PPCAOptimized">
            <wsdl:input message="bsnk:BSNK_ProvidePP_PPCAOptimizedRequest"
wsam:Action="urn:nl-gdi-eid:1.0:webservices:ProvidePP_PPCAOptimizedRequest" />
            <wsdl:output message="bsnk:BSNK_ProvidePP_PPCAOptimizedResponse"
wsam:Action="urn:nl-gdi-eid:1.0:webservices:ProvidePP_PPCAOptimizedResponse" />
            <wsdl:fault message="bsnk:BSNK_ProvidePolymorphicFault"
name="BSNK_ProvidePolymorphic_Fault"/>
        </wsdl:operation>
    </wsdl:portType>

    <wsdl:binding name="BSNK_Activate_SOAP" type="bsnk:BSNK_Activate_Port">
        <soap:binding style="document"
            transport="http://schemas.xmlsoap.org/soap/http" />
        <wsdl:operation name="BSNK_ProvidePP">
            <soap:operation soapAction="urn:nl-gdi-eid:1.0:webservices:ProvidePPRequest" />
            <wsdl:input>
                <soap:body use="literal" />
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal" />
            </wsdl:output>
            <wsdl:fault name="BSNK_ProvidePolymorphic_Fault">
                <soap:fault name="BSNK_ProvidePolymorphic_Fault" use="literal" />
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="BSNK_ProvidePP_PPCAOptimized">
            <soap:operation soapAction="urn:nl-gdi-eid:1.0:webservices:ProvidePP_PPCAOptimizedRequest"
/>
            <wsdl:input>
                <soap:body use="literal" />
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal" />
            </wsdl:output>
            <wsdl:fault name="BSNK_ProvidePolymorphic_Fault">
                <soap:fault name="BSNK_ProvidePolymorphic_Fault" use="literal" />
            </wsdl:fault>
        </wsdl:operation>
    </wsdl:binding>

    <wsdl:service name="BSNK_Activate_Service">
        <wsdl:port binding="bsnk:BSNK_Activate_SOAP" name="BSNK_Activate">
            <soap:address location="https://.../TODO/Activate" />
        </wsdl:port>
```

```
    </wsdl:service>
</wsdl:definitions>
```

Request

Consists of a registration request message <ProvidePPRequest> in the SOAP body of the request message. SOAP should be implemented according to the Web services requirements. An identical <ProvidePP_PPCAOptimizedRequest> request exists for Middelenuitgevers that implement optimized versions of PPCA.

Element/@Attribute	0..n	Description
@DateTime	1	Time of issuing of the request.
@RequestID	1	Unique identifier for this Request
<Requester>	1	EntityID (OIN) of the requesting Middelenuitgever.
<RequesterKeySetVersion>	1	Key set version of the requesting Middelenuitgever.
<BSN>	0..1	Sector ID for Dutch citizens. String of 9 characters, in case a BSN consists of a number of only 8 digits, the BSN shall be padded with a preceding '0' (digit zero). As verification data at least DocumentID and one or more other identity supporting elements (those other than DocumentType) MUST be provided. Either a BSN, EncryptedBSN, EncryptedIdentity or eIDAS-uniquenessID MUST be provided.
<EncryptedBSN>	0..1	An encrypted BSN. This BSN MUST be encrypted using XML-encryption, as per (SAML) Encryption. Either a BSN, EncryptedBSN, EncryptedIdentity or eIDAS-uniquenessID MUST be provided.
<EncryptedIdentity>	0..1	Identity (typically BSN) encrypted as EncryptedIdentity under Polymorphic Pseudonimization. Either a BSN, EncryptedBSN, EncryptedIdentity or eIDAS-uniquenessID MUST be provided.
<eIDAS-UniquenessID>	0..1	An eIDAS uniquenessID. For exclusive use by an eIDAS-berichtenservice. Either a BSN, EncryptedBSN, EncryptedIdentity or eIDAS-uniquenessID MUST be provided.
<EncryptedBSN>	0..1	An eIDAS uniquenessID MAY be accompanied by an encrypted BSN. For exclusive use by an eIDAS-berichtenservice.
<DocumentType>	0..1	String max 20 chars. Value represents the type of government-issued document that was used. Possible values are "NL-Paspoort", "NL-Identiteitskaart" and "NL-Rijbewijs".
<DocumentID>	0..1	String max 15 chars. Value represents the ID of a government-issued document that was used. MUST be present together with <DocumentType>.

<GivenNames>	0..1	String max 200 chars. Must contain all given names, if given names are not fully known than MUST contain all known Initials. MUST be present together with <SurName>. An empty value can be used to specify the current subject has not registered a given name in the BRP.
<SurName>	0..1	String max 210 chars. Surname including prefixes, as stated on the Identity Document. MUST be present together with <GivenName>.
<DateOfBirth>	0..1	Date of birth of the user. In XML-schema a choice between 'date', 'gYear' or 'gYearMonth' format. In case the specific day or month is unknown (also expressed as 1900-00-00 or 1900-03-00), the value MUST be expressed as a gYear or gYearMonth.
<PlaceOfBirth>	0..1	String max 40 chars. NB For Dutch places of birth this value MUST correspond to the exact value as listed in table 33 of the logic design of the BRP. MUST NOT be used for foreign places of birth.

N.B. Only providing the BSN is not deemed to identify a subject with sufficient assurance, additional information must be provided for verification. In general: the more information is provided in the request, the more chance of a unique match with sufficient assurance.

Response

Consists of a response message <ProvidePPResponse> in the SOAP body of the response message, containing one or more Polymorphic Pseudonyms. In case a response is received, the request resulted in a unique and valid match and the cryptographic transformation of the specified BSN to a Polymorphic Pseudonym and/or Polymorphic Identity. An identical <ProvidePP_PPCAOptimizedResponse> is provided that will return a PIP (and PP) for PPCA optimized implementations. In case an error occurs a SOAP fault will be used. The SOAP fault will contain error codes as <FaultReason> as described below, with one (or more) localized <FaultDescription>s.

Element/@Attribute	0..n	Description
@DateTime	1	Time of issuing of the response.
@ResponseID	1	Unique identifier of the Response
@InResponseTo	1	Unique identifier of the Request this is a response to (@RequestID of request)
<PolymorphicPseudonym>	1..n	One or more (signed) Polymorphic Pseudonymization structure(s) for the User. At least one structure MUST be provided.

For encoding of the PolymorphicPseudonym, see Polymorphic Pseudonymization Notation.

FaultReasons

The following response codes are used to indicate the status of a response.

ResponseCode	Description
NotEnoughInfo	Request rejected. Provided information may resolve to a unique match, but not enough assurance (e.g. against typos) can be established.
NotUnique	Request rejected. Provided information results in more than one match.
NotFound	Request rejected. Provided information results in zero matches.
DocumentRejected	Request rejected. Document not accepted.
ProvisioningRefused	Request rejected. Activation refused for other non-disclosed reason.
AuthorizationError	Request rejected. Authentication invalid or access denied. A HTTP 403 status response MAY be given instead of a SOAP-fault with this response.
SyntaxError	Request rejected. Request invalid.
TemporarilyUnavailable	Request could temporarily not be processed. A new request for activation MAY be sent at a later moment by the requesting party.

Interface Spec BSNk: registerStatusEIM

Middelenuitgever uses this interface to register a status for an Electronic Identification Means at the BSNk Inzageregister, for a new (first time) or a changed status. The interface described in this document is used to implement the use case AUC6 Registreren BSN (register BSN) and MUST be implemented by every Middelenuitgever.

WSDL registerStatusEIM

```
<wsdl:definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
                  xmlns:bsnk="urn:nl-gdi-eid:1.0:webservices"
                  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
                  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata"
                  name="BSNK_registerStatusEIM"
                  targetNamespace="urn:nl-gdi-eid:1.0:webservices">

    <wsdl:types>
        <xsd:schema targetNamespace="urn:nl-gdi-eid:1.0:webservices"
                    attributeFormDefault="unqualified"
                    elementFormDefault="qualified">

            <xsd:element name="RegisterStatusEIMRequest" type="bsnk:RegisterStatusEIMRequestType">
                <xsd:annotation>
                    <xsd:documentation>Request message to register a EIM status.
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:complexType name="RegisterStatusEIMRequestType">
                <xsd:complexContent>
                    <xsd:extension base="bsnk:BSNkProvideRequestBasetype">
                        <xsd:sequence>
                            <xsd:element name="EncryptedPseudonym" type="bsnk:EncryptedPseudonymType"
/>
                            <xsd:element name="DeprecatedEP" type="bsnk:EncryptedPseudonymType"
minOccurs="0"/>
                            <xsd:element name="MeansType" type="bsnk:MeansType" />
                            <xsd:element name="LevelofAssurance" type="bsnk:LevelOfAssuranceType" />
                            <xsd:element name="SequenceNr" type="bsnk:SequenceNrType" />
                            <xsd:element name="Status" type="bsnk:StatusType" />
                            <xsd:element name="IDP" type="bsnk:OINType" minOccurs="0" />
                            <xsd:element name="StatusDateTime" type="xsd:dateTime" />
                            <xsd:element name="ReadableCardID" type="bsnk:ReadableCardIDType"
minOccurs="0" />
                            <xsd:element name="RevocationURL" type="bsnk:RevocationURLType"
minOccurs="0" />
```

```
                </xsd:sequence>
            </xsd:extension>
        </xsd:complexContent>
    </xsd:complexType>
    <xsd:complexType name="BSNkProvideRequestBasetype" abstract="true">
        <xsd:sequence>
            <xsd:element name="Requester" type="bsnk:OINType" />
        </xsd:sequence>
        <xsd:attribute name="DateTime" type="xsd:dateTime" use="required" />
        <xsd:attribute name="RequestID" type="xsd:ID" use="required" />
    </xsd:complexType>
    <xsd:simpleType name="MeansType">
        <xsd:restriction base="xsd:string">
            <xsd:maxLength value="25" />
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="LevelOfAssuranceType">
        <xsd:restriction base="xsd:anyURI">
            <xsd:maxLength value="128" />
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="SequenceNrType">
        <xsd:restriction base="xsd:string">
            <xsd:maxLength value="16" />
            <xsd:pattern value="[0-9]+"></xsd:pattern>
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="StatusType">
        <xsd:restriction base="xsd:string">
            <xsd:maxLength value="64" />
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="EncryptedPseudonymType">
        <xsd:annotation>
            <xsd:documentation>Pseudonym encrypted as an EncryptedPseudonym
                according to Polymorphic Pseudonimization.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:restriction base="xsd:base64Binary" />
    </xsd:simpleType>
    <xsd:simpleType name="ReadableCardIDType">
        <xsd:restriction base="xsd:string">
            <xsd:maxLength value="40" />
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="RevocationURLType">
        <xsd:restriction base="xsd:anyURI">
            <xsd:maxLength value="1024" />
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="OINType">
        <xsd:annotation>
            <xsd:documentation>OIN type.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:restriction base="xsd:string">
            <xsd:length value="20" />
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:element name="RegisterStatusEIMResponse" type="bsnk:RegisterStatusEIMResponseType">
        <xsd:annotation>
            <xsd:documentation>
                Response to a RegisterStatusEIMRequest.
            </xsd:documentation>
        </xsd:annotation>
    </xsd:element>
    <xsd:complexType name="RegisterStatusEIMResponseType">
        <xsd:complexContent>
            <xsd:extension base="bsnk:BSNkProvideResponseBasetype">
                <xsd:sequence>
                    <xsd:element name="Status" type="bsnk:StatusType" />
                </xsd:sequence>
            </xsd:extension>
        </xsd:complexContent>
    </xsd:complexType>
    <xsd:complexType name="BSNkProvideResponseBasetype" abstract="true">
        <xsd:attribute name="DateTime" type="xsd:dateTime" use="required" />
        <xsd:attribute name="ResponseID" type="xsd:ID" use="required" />
        <xsd:attribute name="InResponseTo" type="xsd:NCName" use="required" />
    </xsd:complexType>
    <xsd:element name="RegisterStatusEIMFault" type="bsnk:RegisterStatusEIMFaultType">
        <xsd:annotation>
            <xsd:documentation>
                Fault response to a RegisterStatusEIMRequest.
            </xsd:documentation>
        </xsd:annotation>
    </xsd:element>
    <xsd:complexType name="RegisterStatusEIMFaultType">
        <xsd:sequence>
            <xsd:element name="FaultReason" type="bsnk:RegisterStatusEIMFaultReasonType" />
            <xsd:element name="FaultDescription" type="bsnk:FaultDescriptionType"
maxOccurs="unbounded" />
```

```
            </xsd:sequence>
        </xsd:complexType>
        <xsd:simpleType name="RegisterStatusEIMFaultReasonType">
            <xsd:union memberTypes="bsnk:FaultReasons bsnk:RegisterStatusEIMFaultReasons" />
        </xsd:simpleType>
        <xsd:simpleType name="FaultReasons">
            <xsd:restriction base="xsd:string">
                <xsd:enumeration value="NotFound">
                    <xsd:annotation>
                        <xsd:documentation>Provided information results in
                            zero matches.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="AuthorizationError">
                    <xsd:annotation>
                        <xsd:documentation>Authentication invalid or access denied.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="SyntaxError">
                    <xsd:annotation>
                        <xsd:documentation>Request invalid.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="TemporarilyUnavailable">
                    <xsd:annotation>
                        <xsd:documentation>Request could temporarily not be
                            processed. A new request for activation MAY be send
                            at a later moment by the requesting party.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="RegisterStatusEIMFaultReasons">
            <xsd:restriction base="xsd:string">
                <xsd:enumeration value="NotUnique">
                    <xsd:annotation>
                        <xsd:documentation>Provided information results in
                            more than one match.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="RegistrationRefused">
                    <xsd:annotation>
                        <xsd:documentation>Registration refused for other
                            (non-disclosed) reason.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:complexType name="FaultDescriptionType">
            <xsd:simpleContent>
                <xsd:extension base="xsd:string">
                    <xsd:attribute name="lang" type="xsd:language" />
                </xsd:extension>
            </xsd:simpleContent>
        </xsd:complexType>
    </xsd:schema>
</wsdl:types>

<wsdl:message name="BSNK_RegisterStatusEIMRequest">
    <wsdl:part name="in" element="bsnk:RegisterStatusEIMRequest" />
</wsdl:message>

<wsdl:message name="BSNK_RegisterStatusEIMResponse">
    <wsdl:part name="out" element="bsnk:RegisterStatusEIMResponse" />
</wsdl:message>

<wsdl:message name="BSNK_RegisterStatusEIMFault">
    <wsdl:part name="fault" element="bsnk:RegisterStatusEIMFault" />
</wsdl:message>

<wsdl:portType name="BSNK_RegisterStatusEIM_Port">
    <wsdl:operation name="BSNK_RegisterStatusEIM">
        <wsdl:input message="bsnk:BSNK_RegisterStatusEIMRequest"
wsam:Action="urn:nl-gdi-eid:1.0:webservices:RegisterStatusEIMRequest" />
        <wsdl:output message="bsnk:BSNK_RegisterStatusEIMResponse"
wsam:Action="urn:nl-gdi-eid:1.0:webservices:RegisterStatusEIMResponse" />
        <wsdl:fault message="bsnk:BSNK_RegisterStatusEIMFault"
name="BSNK_RegisterStatusEIM_Fault"/>
    </wsdl:operation>
</wsdl:portType>

<wsdl:binding name="BSNK_RegisterStatusEIM_SOAP" type="bsnk:BSNK_RegisterStatusEIM_Port">
    <soap:binding style="document"
        transport="http://schemas.xmlsoap.org/soap/http" />
    <wsdl:operation name="BSNK_RegisterStatusEIM">
        <soap:operation soapAction="urn:nl-gdi-eid:1.0:webservices:RegisterStatusEIMRequest" />
```

```
        <wsdl:input>
            <soap:body use="literal" />
        </wsdl:input>
        <wsdl:output>
            <soap:body use="literal" />
        </wsdl:output>
        <wsdl:fault name="BSNK_RegisterStatusEIM_Fault">
            <soap:fault name="BSNK_RegisterStatusEIM_Fault" use="literal" />
        </wsdl:fault>
    </wsdl:operation>
</wsdl:binding>

<wsdl:service name="BSNK_RegisterStatusEIM_Service">
    <wsdl:port binding="bsnk:BSNK_RegisterStatusEIM_SOAP" name="BSNK_RegisterStatusEIM">
        <soap:address location="https://.../TODO/RegisterStatusEIM" />
    </wsdl:port>
```

```
    </wsdl:service>
</wsdl:definitions>
```

Request

Consists of a registration request message <RegisterStatusEIMRequest> in the SOAP body of the request message. SOAP should be implemented accoording to the Web services requirements .

Element/@Attribute	0..n	Description
@DateTime	1	Time of issuing of the request.
@RequestID	1	Unique identifier for this request
<Requester>	1	EntityID (OIN) of the requesting Middelenuitgever.
<EncryptedPseudonym>	1	Encrypted Pseudonym of the user to be transformed to a pseudonym for the BSNk Inzageregister
<DeprecatedEP>	0..1	Optional previous Encrypted Pseudonym of the user to be transformed to a previous pseudonym of the BSNk Inzageregister, used for instance when Inzageregister changes from Beheerorganisatie BSNk to a other party.
<MeansType>	1	String max 25 chars. Value represents a readable version of the type of Electronic Identification Means; this can a generic description. e.g. 'All Means' or specify a specific Electronic Identification Mean ; For instance for government issued document possible values are "NL-Paspoort", "NL-Identiteitskaart" and "NL-Rijbewijs".
<LevelofAssurance>	1	choice http://eidas.europa.eu/LoA/substantial or http://eidas.europa.eu/LoA/high . Specifies the (highest) LoA of the Electronic Identitication Mean(s).
<SequenceNr>	1	Number or Date. SequenceNr identifies a specific Electronic Identification Means. For privacy reasons this SequenceNr MUST have a low entropy. preferably 01, 02 ...09. In case of a date, for example only use one weekday in a week for every means issued that week. In XML-schema a choice between 'number', 'date', 'gYear' or 'gYearMonth' format.
<Status>	1	MUST contain one of the specified statusses: Produced (not shown to the user), Issued (not shown to the user), Activated (as an electronic identification means in the government domain), Suspended (as an electronic identification means in the government domain), Expired (token by the issuer) or Revoked (token by the issuer). This element is required for every new registration and optional for any existing registration. Any new status will overwrite the old status, except when the old status is either revoked or expired. Then, this means cannot be reactivated. See Status (van het Authenticatiemiddel) for more information.

<IDP>	0..1	EntityID (OIN) of the Authenticatiedienst that will be using this specific Electronic Idendtfication Means. Only to be used when the Authenticatiedienst is not the Middelenuitgever as well. Eg RDW issues a means (drivers licence) and if the user activates this at DigiD, then RDW should register DigiD as <IDP> with status Activated (same thing when RDW registers a deactivation of DigiD.).
<StatusDateTime>	1	DateTime of status change, MUST not be after @DateTime of this request. MUST be present together with <Status>.
<ReadableCardID>	0..1	String max 40 chars. Readable CardID is text that has just enough information for a user to recognise the specific Electronic Authentication Means in the domain of the Middelenuitgever. Preferably this element is readable (recognizable but not identifying) for the user (eg validation date on a drivers licence or bankcard.). A Middelenuitgever has to take care of user language preferences. This element is required for every new registration and optional for any existing registration (any new will overwrite the old text).
<RevocationURL>	0..1	String max 1024 chars. RevocationURL is a valid URL which can be used by mijnoverheid (when providing the user an overview of electronic identification means) to redirect the user to the Middelenuitgever for a suspend or revoke process of this electronic identification means. For privacy reasons this RevocationURL MUST have a low entropy, preferably only elements in this request specification. This element is required for every new registration and optional for any existing registration (any new will overwrite the old text).

Processing rules for Status Registration Request

A requesting Middelenuitgever

- MUST await a successful response or retry to send the request. Requests MUST be buffered and retried during 7 days.
- MUST log and investigate failures.

Response

Consists of a response message <RegisterStatusEIMResponse> in the SOAP body of the request message. In case a response is received, the request resulted in new or a unique and valid match of an existing electronic identification means. In case an error occurs a SOAP fault will be used. The SOAP fault will contain error codes as <FaultReason> as described below, with one (or more) localized <FaultDescription>.

Element/@Attribute	0..n	Description
@DateTime	1	Time of issuing of the response.
@ResponseID	1	Unique identifier of the response
@InResponseTo	1	Unique identifier of the request this is a response to (@RequestID of request)
<Status>	1	The current status, after processing the optional status change in the request.

FaultReasons

The following response codes are used to indicate the status of a response.

ResponseCode	Description
NotUnique	Request rejected. Provided information results in more than one match.
NotFound	Request rejected. Provided information results in zero matches.
RegistrationRefused	Request rejected. Registration refused for other non-disclosed reason.
AuthorizationError	Request rejected. Authentication invalid or access denied. A HTTP 403 status response MAY be given instead of a SOAP-fault with this response.
SyntaxError	Request rejected. Request invalid.
TemporarilyUnavailable	Request could temporarily not be processed. A new request for registration MAY be sent at a later moment by the requesting party.

Interface Toegangsdienst - BSNk Sleutelbeheer: provideDVKeys

This interface between a Broker (Toegangsdienst) and BSNk Key Management (Sleutelbeheer) enables a Broker to request DV-keys that are required by every Service Provider (Dienstverlener) to get an identity (e.g. BSN) or persistent pseudonym as a result of an authentication request.

In order to decrypt an Encrypted Identity (e.g. social security number - Dutch: BSN) or Encrypted Pseudonym, a Dienstverlener (service provider) needs specific keys. A Service Provider can request these so called DV-keys via his Broker (Toegangsdienst). The BSNk provides a Key Management service to a Broker to request the DV-keys on behalf of his Service Provider-customers.

The interface described in this document is used to implement the use case AUC5 Verstrekken sleutelmateriaal Dienstverleners and MUST be implemented by every Broker that services the domain.

WSDL provideDVKeys

```
<wsdl:definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
                  xmlns:bsnk="urn:nl-gdi-eid:1.0:webservices"
                  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
                  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata"
                  name="BSNK_provideDVKeys"
                  targetNamespace="urn:nl-gdi-eid:1.0:webservices">

    <wsdl:types>
        <xsd:schema targetNamespace="urn:nl-gdi-eid:1.0:webservices"
                    attributeFormDefault="unqualified"
                    elementFormDefault="qualified">
```

```
            <xsd:element name="ProvideDVKeysRequest" type="bsnk:ProvideDVKeysRequestType">
                <xsd:annotation>
                    <xsd:documentation>Request message to provide DV keys.
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:complexType name="ProvideDVKeysRequestType">
                <xsd:complexContent>
                    <xsd:extension base="bsnk:BSNkProvideRequestBasetype">
                        <xsd:sequence>
                            <xsd:element name="RelyingParty" type="bsnk:OINType" />
                            <xsd:element name="RelyingPartyPKIoCertificate" type="bsnk:Certificate" />
                            <xsd:element name="SchemeKeySetVersion" type="bsnk:KeyVersionType"
minOccurs="0" />
                        </xsd:sequence>
                    </xsd:extension>
                </xsd:complexContent>
            </xsd:complexType>
            <xsd:complexType name="BSNkProvideRequestBasetype" abstract="true">
                <xsd:sequence>
                    <xsd:element name="Requester" type="bsnk:OINType" />
                </xsd:sequence>
                <xsd:attribute name="DateTime" type="xsd:dateTime" use="required" />
                <xsd:attribute name="RequestID" type="xsd:ID" use="required" />
            </xsd:complexType>
            <xsd:simpleType name="Certificate">
                <xsd:restriction base="xsd:string" />
            </xsd:simpleType>
            <xsd:simpleType name="KeyVersionType">
                <xsd:annotation>
                    <xsd:documentation>Key(set) version type.</xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:positiveInteger"/>
            </xsd:simpleType>
            <xsd:simpleType name="OINType">
                <xsd:annotation>
                    <xsd:documentation>OIN type.
                    </xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:string">
                    <xsd:length value="20" />
                </xsd:restriction>
            </xsd:simpleType>
            <xsd:element name="ProvideDVKeysResponse" type="bsnk:ProvideDVKeysResponseType">
                <xsd:annotation>
                    <xsd:documentation>
                        Response to a ProvideDVKeysRequest.
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:complexType name="ProvideDVKeysResponseType">
                <xsd:complexContent>
                    <xsd:extension base="bsnk:BSNkProvideResponseBasetype">
                        <xsd:sequence>
                            <xsd:element name="EncryptedDVKey" type="bsnk:EncryptedDVKeyType" />
                        </xsd:sequence>
                    </xsd:extension>
                </xsd:complexContent>
            </xsd:complexType>
            <xsd:complexType name="BSNkProvideResponseBasetype" abstract="true">
                <xsd:attribute name="DateTime" type="xsd:dateTime" use="required" />
                <xsd:attribute name="ResponseID" type="xsd:ID" use="required" />
                <xsd:attribute name="InResponseTo" type="xsd:NCName" use="required" />
            </xsd:complexType>
            <xsd:simpleType name="EncryptedDVKeyType">
                <xsd:annotation>
                    <xsd:documentation>Encrypted DV key.
                    </xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:base64Binary" />
            </xsd:simpleType>
            <xsd:element name="ProvideDVKeysFault" type="bsnk:ProvideDVKeysFaultType">
                <xsd:annotation>
                    <xsd:documentation>
                        Fault response to a ProvideDVKeysRequest.
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:complexType name="ProvideDVKeysFaultType">
                <xsd:sequence>
                    <xsd:element name="FaultReason" type="bsnk:ProvideDVKeysFaultReasonType" />
                    <xsd:element name="FaultDescription" type="bsnk:FaultDescriptionType"
maxOccurs="unbounded" />
                </xsd:sequence>
            </xsd:complexType>
            <xsd:simpleType name="ProvideDVKeysFaultReasonType">
                <xsd:union memberTypes="bsnk:FaultReasons bsnk:ProvideDVKeysFaultReasons" />
            </xsd:simpleType>
            <xsd:simpleType name="FaultReasons">
                <xsd:restriction base="xsd:string">
                    <xsd:enumeration value="NotFound">
                        <xsd:annotation>
```

```
                            <xsd:documentation>Provided information results in
                                zero matches.
                            </xsd:documentation>
                        </xsd:annotation>
                    </xsd:enumeration>
                    <xsd:enumeration value="AuthorizationError">
                        <xsd:annotation>
                            <xsd:documentation>Authentication invalid or access denied.
                            </xsd:documentation>
                        </xsd:annotation>
                    </xsd:enumeration>
                    <xsd:enumeration value="SyntaxError">
                        <xsd:annotation>
                            <xsd:documentation>Request invalid.
                            </xsd:documentation>
                        </xsd:annotation>
                    </xsd:enumeration>
                    <xsd:enumeration value="TemporarilyUnavailable">
                        <xsd:annotation>
                            <xsd:documentation>Request could temporarily not be
                                processed. A new request for activation MAY be send
                                at a later moment by the requesting party.
                            </xsd:documentation>
                        </xsd:annotation>
                    </xsd:enumeration>
                </xsd:restriction>
            </xsd:simpleType>
            <xsd:simpleType name="ProvideDVKeysFaultReasons">
                <xsd:restriction base="xsd:string">
                    <xsd:enumeration value="NotUnique">
                        <xsd:annotation>
                            <xsd:documentation>Provided information results in
                                more than one match.
                            </xsd:documentation>
                        </xsd:annotation>
                    </xsd:enumeration>
                    <xsd:enumeration value="InvalidRequest">
                        <xsd:annotation>
                            <xsd:documentation>Request contains invalid parameters.
                            </xsd:documentation>
                        </xsd:annotation>
                    </xsd:enumeration>
                    <xsd:enumeration value="ProvisioningRefused">
                        <xsd:annotation>
                            <xsd:documentation>Provisioning refused for other
                                (non-disclosed) reason.
                            </xsd:documentation>
                        </xsd:annotation>
                    </xsd:enumeration>
                </xsd:restriction>
            </xsd:simpleType>
            <xsd:complexType name="FaultDescriptionType">
                <xsd:simpleContent>
                    <xsd:extension base="xsd:string">
                        <xsd:attribute name="lang" type="xsd:language" />
                    </xsd:extension>
                </xsd:simpleContent>
            </xsd:complexType>
        </xsd:schema>
    </wsdl:types>

    <wsdl:message name="BSNK_ProvideDVKeysRequest">
        <wsdl:part name="in" element="bsnk:ProvideDVKeysRequest" />
    </wsdl:message>

    <wsdl:message name="BSNK_ProvideDVKeysResponse">
        <wsdl:part name="out" element="bsnk:ProvideDVKeysResponse" />
    </wsdl:message>

    <wsdl:message name="BSNK_ProvideDVKeysFault">
        <wsdl:part name="fault" element="bsnk:ProvideDVKeysFault" />
    </wsdl:message>

    <wsdl:portType name="BSNK_ProvideDVKeys_Port">
        <wsdl:operation name="BSNK_ProvideDVKeys">
            <wsdl:input message="bsnk:BSNK_ProvideDVKeysRequest"
wsam:Action="urn:nl-gdi-eid:1.0:webservices:ProvideDVKeysRequest" />
            <wsdl:output message="bsnk:BSNK_ProvideDVKeysResponse"
wsam:Action="urn:nl-gdi-eid:1.0:webservices:ProvideDVKeysResponse" />
            <wsdl:fault message="bsnk:BSNK_ProvideDVKeysFault" name="BSNK_ProvideDVKeys_Fault"/>
        </wsdl:operation>
    </wsdl:portType>

    <wsdl:binding name="BSNK_ProvideDVKeys_SOAP" type="bsnk:BSNK_ProvideDVKeys_Port">
        <soap:binding style="document"
            transport="http://schemas.xmlsoap.org/soap/http" />
        <wsdl:operation name="BSNK_ProvideDVKeys">
            <soap:operation soapAction="urn:nl-gdi-eid:1.0:webservices:ProvideDVKeysRequest" />
            <wsdl:input>
                <soap:body use="literal" />
            </wsdl:input>
            <wsdl:output>
```

```
            <soap:body use="literal" />
        </wsdl:output>
        <wsdl:fault name="BSNK_ProvideDVKeys_Fault">
            <soap:fault name="BSNK_ProvideDVKeys_Fault" use="literal" />
        </wsdl:fault>
    </wsdl:operation>
</wsdl:binding>

<wsdl:service name="BSNK_ProvideDVKeys_Service">
    <wsdl:port binding="bsnk:BSNK_ProvideDVKeys_SOAP" name="BSNK_ProvideDVKeys">
        <soap:address location="https://.../TODO/ProvideDVKeys" />
    </wsdl:port>
</wsdl:service>
```

```
</wsdl:definitions>
```

Request

Consists of a DV-keys request message <ProvideDVRequest> in the SOAP body of the request message.

Element/@Attribute	0..n	Description
@DateTime	1	Time of issuing of the request.
@RequestID	1	Unique identifier for this Request
<Requester>	1	EntityID (OIN) of the requesting Toegangsdienst.
<RelyingParty>	1	EntityID (OIN) of the intended relying party.
<RelyingPartyPKIoCertificate>	1	PKIoverheid Certificate of the relying party for whom the key material is intended. The public key on this certificate will be used to encrypt the DV-keys. The PKIo-certificate MUST have a Subject.serialNumber containing the organizations OIN and MUST have a (extended) key usage that allows for keyEncipherment.
<SchemeKeySetVersion>	0..1	Optional scheme key set version to request keys for (default is most recent).

Rules for processing a Decryption Key Request

A requesting Toegangsdienst:

- MAY only request the decryption key(s) on behalf of contracted Dienstverleners.
- MUST verify the request originates from or is initiated on behalf of the Dienstverlener.
- MUST NOT request decryption key(s) for non-contracted Relying Parties .
- MUST check the if the PKIo certificate is valid before requesting decryption keys on behalf of the Dienstverlener.

Response

Consists of a response message <ProvideDKResponse> in the SOAP body of the response message, containing the Dienstverlener Encrypted DV-keys for requested Relying Party. In case an error occurs a SOAP fault will be used. The SOAP fault will contain error codes as <FaultReason> as described below, with one (or more) localized <FaultDescription>s.

Element/@Attribute	0..n	Description
@DateTime	1	Time of issuing of the response.
@ResponseID	1	Unique identifier of the Response

@InResponseTo	1	Unique identifier of the Request this is a response to (@RequestID of request).
<EncryptedDVKey>	1..n	One or more encrypted decryption keys, see DV-key format.

Rules for processing a Decryption Key Response

A receiving Toegangsdienst:

- MUST directly transfer the encrypted DV-keys to (systems under responsibility of) the Dienstverlener, using a secure transfer mechanism.
- MUST not store the requested keys anywhere else.

A receiving Dienstverlener:

- MUST verify the DV-keys before processing.
- MUST secure the DV-keys from disclosure or abuse.
- can decrypt the DV-keys using the private key corresponding to the PKIo-certificate used in the request.

FaultReasons

The following response codes are used to indicate the status of a response.

ResponseCode	Description
InvalidRequest	Request rejected. Request contains invalid parameter, e.g. invalid certificate or scheme key set version.
ProvisioningRefused	Request rejected. Creation of DV-keys refused for other non-disclosed reason.
AuthorizationError	Request rejected. Authentication invalid or access denied. A HTTP 403 status response MAY be given instead of a SOAP-fault with this response.
SyntaxError	Request rejected. Request invalid.
TemporarilyUnavailable	Request could temporarily not be processed. A new request for encription keys MAY be sent at a later moment by the requesting party.

DV-key format

This paragraph describes the technical format of key file provided to Dienstverleners (Service Providers).

Formats of cryptographic keys provided to Service Providers

Parties that are provided with either Encrypted Identities or Encrypted Pseudonyms are also provided cryptographic keys to decrypt them to respectively Identities or Pseudonyms. These cryptographic keys are provided as ECPrivateKey as specified in RFC5915, in three files formatted according to the PEM specifications (RFC1421). Two files corresponds the decryption of Encrypted Identities and Encrypted Pseudonyms respectively and one corresponds to a so-called Closing key that provides further protection of pseudonyms. We will refer to these files here by EI_Decryption.pem, EP_Decryption.pem and EP_Closing.pem respectively although these names are not mandatory.

NOTE: DV-keys will be provided in an encrypted form, using the relying parties PKIoverheid certificate for message encryption. The encryption algorithms and formats are to be determined.

As per RFC5915 (section 4), all three files contain a EC private key object, using the PEM-encoding of the DER-encoded ECPrivateKey structure. The actual key is preceded by the line

```
-----BEGIN EC PRIVATE KEY-----
```

and followed with the line

```
-----END EC PRIVATE KEY-----
```

All three files contain the following headers: SchemeVersion, SchemeKeyVersion, Type, Recipient, RecipientKeySetVersion. These headers use a 'key: value' notation, as specified in RFC1421. All headers except Type have the same meaning as specified in Polymorphic Pseudonymization Notation. The Type header is equal to the string “EI Decryption”, “EP Decryption” and “EP Closing” corresponding to the three files introduced above. Moreover, in scheme version 1, the RecipientKeySetVersion for a Service Provider corresponds with the issue date of the PKIoverheid certificate used to request their keys at the party generating the keys within the scheme. The RecipientKeySetVersion will therefore be an 8-digit decimal representation of a date in the YYYYMMDD format.

The key is a ECPrivateKey, defined by

```
ECPrivateKey ::= SEQUENCE {
    version        INTEGER { ecPrivkeyVer1(1) } (ecPrivkeyVer1),
    privateKey     OCTET STRING,
    parameters [0] ECParameters {{ NamedCurve }} OPTIONAL,
    publicKey  [1] BIT STRING OPTIONAL
}
```

thus consisting of 4 elements:

- a version (integer of value 1),
- an OCTET STRING corresponding to the actual private key (40 bytes)
- a tagged OBJECT IDENTIFIER of value 1.3.36.3.3.2.8.1.1.9 indicating the BrainpoolP320r1 curve.
- a tagged BIT STRING representing the corresponding public key (an EC point, uncompressed).

In line with RFC5915, both the curve name and the public key will be provided, even though these are indicated as optional.

We remark that the following OpenSSL (version 1.0.2) command will provide a PEM file corresponding to the above specification without the headers:

```
openssl ecparam -name brainpoolP320r1 -genkey -noout -out brainpoolP320r1key.pem
```

and key files can be read by the command

```
openssl ec -in /tmp/ec.pem -text
```

The confidentiality and authenticity of the key files in transport to the intended parties is required but not further specified. On receipt of a PEM file the intended party MUST validate that the PEM is correctly formed which also includes that the provided private key and public key match. That is, if x represents this private key and G the BrainpoolP320r1 generator, then the intended party needs to validate that x*G is equal to the public key in the key file. The recipient furthermore MUST ensure each key is adequately secured against disclosure or abuse.

Example EP decryption key file

```
-----BEGIN EC PRIVATE KEY-----
SchemeVersion: 1
SchemeKeyVersion: 1
Type: EP decryption
Recipient: 00000003123456780000
RecipientKeySetVersion: 20161201

MIGQAgEBBCikKZiJyHs5btM2JLTS3V7E7Kb3TarWX7yW8Scg1WbtdF+2b30UReEn
oAsGCSskAwMCCAEBCaFUA1IABLPWbbemrGwC5Cz02dq6XBRW8LQieNGRrgMDeLQv
or9OmLnEnPEJfiYELjxyYq1hFjrarWW2/t98sujlBImGMKifQvnT7mgp6jVDrPtF
Kt3J
-----END EC PRIVATE KEY-----
```

Note: OpenSSL PEM_read function (https://www.openssl.org/docs/man1.1.0/crypto/PEM_read.html) supports this format.

Polymorphic Pseudonymization Notation

This paragraph describes the technical format of polymorphic identities and pseudonyms and related key formats. Polymorphic identities and pseudonyms in the scheme are based on cryptographic properties of elliptic curves. For a more detailed description, see Polymorfe encryptie en pseudonimisering.

Usages of Polymorphic Pseudonymization

- Activation
  - Polymorphic Identity or Pseudonym
  - Encrypted Identity or Pseudonym
- Usage (transformation and decryption)
  - Encrypted Identity or Pseudonym
  - Identity or Pseudonym

Format for Polymorphic Identity or Pseudonym

A Polymorphic Identity or Pseudonym is a combination of points on an elliptic curve. In order for the Identity or Pseudonym to be properly usable in the scheme, some additional information is needed. This information is necessary for practical management and secure implementation of Identity or Pseudonym in the Scheme and consists of elements like versioning (for key management) and recipient. The syntax for expressing an Identity or Pseudonym with this information is listed below.

Values of the notations below SHALL be represented as (the base64 encoding of) the DER-encoded structure in ASN.1 notation.

Polymorphic Identity or Pseudonym

A Polymorphic Identity or Pseudonym consists of 3 points on an elliptic curve. Polymorphic Identity or Pseudonym are provided via the Interface spec BSNk: activate. They are used via the interface Interface spec BSNk: transform. The notation for a complete Polymorphic Identity or Pseudonym is as follows:

Polymorphic Identity or Pseudonym ASN.1 notation

```
PolymorphicIdentity ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-polymorphic-identity),
    schemeVersion INTEGER,
    schemeKeyVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    points SEQUENCE (SIZE (3)) OF ECPoint
}

PolymorphicPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-polymorphic-pseudonym),
    schemeVersion INTEGER,
    schemeKeyVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    type INTEGER,
    points SEQUENCE (SIZE (3)) OF ECPoint
}
```

Herein the schemeVersion indicates the version of the cryptographic scheme and this syntax and SHALL start at 1. The schemeKeyVersion is a version that SHALL start at 1 and represents the effective set of long term scheme master keys (PP-M, PD-M, etc...). The schemeKeyVersion defines the elliptic curve used in the scheme as well. The creator SHALL contain the entityID (OIN) of the creator, and the recipient SHALL contain the entityID (OIN) of the recipient. The recipientKeySetVersion holds the version number for the set of recipient's keys for Polymorphic Identities and Pseudonyms (PA-Di). Note: In schemeVersion 1 the recipientKeySetVersion for MUs and ADs is a sequence starting at 1. Type defines the identity type the Pseudonym is derived of, e.g. from a BSN or an eIDAS Uniqueness Identifier. This field is not necessary in identity based forms as here the identity type will become clear as part of decryption of the final structure, i.e. the Encrypted Identity. The values currently defined are the ASCII value of 'B' (0x42) for BSN based and 'E' (0x45) when based on a eIDAS uniqueness identifier. ECPoint is identical to ECPoint as defined in BSI TR 03111 and ANSI X9.62 (2005). Here two encodings are specified, compressed and compressed. Both encodings are allowed, with a preference for uncompressed encoding.

A Polymorphic Identity of Polymorphic Pseudonym can be signed for integrity protection:

```
SignedPolymorphicIdentity ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-polymorphic-identity-signed),
    signedPI SEQUENCE {
        polymorphicIdentity PolymorphicIdentity,
        auditElement OCTET STRING,
        signingKeyVersion INTEGER
    },
    signatureValue ECDSA-Signature
}

SignedPolymorphicPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-polymorphic-pseudonym-signed),
    signedPP SEQUENCE {
        polymorphicPseudonym PolymorphicPseudonym,
        auditElement OCTET STRING,
        signingKeyVersion INTEGER
    },
    signatureValue ECDSA-Signature
}
```

An auditElement holds an audit value consisting of an identifier for the creator, a timestamp and a sequence number from that creator. This auditElement is 16 bytes (32-bit creator, 32-bit timestamp and 64-bit sequence-number). The creator identifies the party providing the Polymorphic/Encrypted Identity or Pseudonym and the unique device used. The timestamp and sequence number can be used in case of a compromise or dispute, so that mitigating measure or resolution can be accomplished. Note: the timestamp is 32-bit in seconds since 1 jan 1970 UTC. The auditElement is encrypted under a key only retrievable by the supervisor of the scheme, which is provided to the supervisior by the keymanagement role.

The signatureValue can be used to assert the authenticity of the (polymorphic/encrypted) Identity or Pseudonym. The signature is applied to the byte sequence of the complete DER-encoded signed sequence (e.g. signedPP in a SignedPolymorphicPseudonym). The public key for verification can be retrieved using the creator from the structure covered under the signature and the signingKeyVersion.

```
-- ECPoint is described in ANSI X9.62 (2005), annex E.6.
-- In particular, encoding from point to octet string and
-- from octet string to a point is defined in annex A.5.7
-- and A.5.8 of ANSI X9.62.
ECPoint ::= OCTET STRING

ECDSA-Signature ::= SEQUENCE {
    signatureType      OBJECT IDENTIFIER (ecdsa-with-SHA384),
    signatureValue     EC-Sig-Value
}

-- EC-Sig-Value is identitical to BSI TR 03111 ECDSA-Sig-Value.
-- which is identical to ECDSA-Sig-Value defined in RFC5480 as well.
EC-Sig-Value ::= SEQUENCE {
    r  INTEGER,
    s  INTEGER
}

ecdsa-with-SHA384 OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4)
    ecdsa-with-SHA2(3) 3 }

id-BSNk-scheme-nl OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) nl(528)
nederlandse-organisatie(1) nederlandse-overheid(1003) ..... TODO }

id-BSNk-identifiers OBJECT IDENTIFIER ::= { id-BSNk-scheme-nl 1 }

id-BSNk-polymorphics OBJECT IDENTIFIER ::= { id-BSNk-identifiers 1 }

id-BSNk-polymorphic-identity OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 1 }

id-BSNk-polymorphic-pseudonym OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 2 }

id-BSNk-polymorphic-identity-signed OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 3 }

id-BSNk-polymorphic-pseudonym-signed OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 4 }
```

PIP – PPCA optimized

For privacy enhanced implementation, Polymorphic Identities and Pseudonyms can be implemented on a smartcard. This is called a PP-card application, or PPCA. A Polymorphic Identity and a Polymorphic Pseudonym can be combined to 5 points on an elliptic curve rather than six, for optimization in a smartcard implementation. The PPCA-optimized PIP version of Polymorphic Identities or Pseudonyms are provided in Interface spec BSNk: activate.

The combined notation for an Polymorphic Identity and Pseudonym is as follows:

Polymorphic Identity and Pseudonym (PIP) ASN.1 notation

```
PIP ::= SEQUENCE {
    notationIdentifier  OBJECT IDENTIFIER (id-BSNk-polymorphic-pip),
    schemeVersion INTEGER,
    schemeKeyVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    type INTEGER,
    points SEQUENCE (SIZE (5)) OF ECPoint
}
```

The first, second and fourth ECPoint in a PIP correspond to those of a PI. Similarly, the first, third and fifth correspond to those of a PP. In this fashion one can extract a PI and PP from a PIP.

There also exists a signed version of a PIP:

```
SignedPIP::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-polymorphic-pip-signed),
    signedPIP SEQUENCE {
        pip PIP,
        auditElement OCTET STRING,
        signingKeyVersion INTEGER
    }
    signatureValue ECDSA-Signature
}
```

Which follows the same concepts as described for a Polymorphic Identity or Polymorphic Pseudonym.

```
id-BSNk-polymorphic-pip OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 5 }

id-BSNk-polymorphic-pip-signed OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 6 }
```

Encrypted Identity or Pseudonym

An Encrypted Identity or Pseudonym consists of 3 points on an elliptic curve. The notation for a complete Encrypted Identity and an Encrypted Pseudonym is as follows:

Encrypted pseudoID ASN.1 notation

```
EncryptedIdentity ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-identity),
    schemeVersion INTEGER,
    schemeKeyVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    points SEQUENCE (SIZE (3)) OF ECPoint
}

EncryptedPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-pseudonym),
    schemeVersion INTEGER,
    schemeKeyVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    diversifier IA5String OPTIONAL,
    type INTEGER,
    points SEQUENCE (SIZE (3)) OF ECPoint
}

SignedEncryptedIdentity ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-identity-signed),
    signedEI SEQUENCE {
        encryptedIdentity EncryptedIdentity,
        auditElement OCTET STRING
    }
    signatureValue EC-Schnorr-Signature
}

SignedEncryptedPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-pseudonym-signed),
    signedEP SEQUENCE {
        encryptedPseudonym EncryptedPseudonym,
        auditElement OCTET STRING
    }
    signatureValue EC-Schnorr-Signature
}

DirectEncryptedPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-direct-pseudonym),
    schemeVersion INTEGER,
    schemeKeyVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    type INTEGER,
    points SEQUENCE (SIZE (3)) OF ECPoint
}

SignedDirectEncryptedPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-direct-pseudonym-signed),
    signedDEP SEQUENCE {
        directEncryptedPseudonym DirectEncryptedPseudonym,
        auditElement OCTET STRING
    }
    signatureValue EC-Schnorr-Signature
}
```

The fields correspond to the same fields in a Polymorphic Identity or Pseudonym. The recipientKeySetVersion holds the version number for the set of recipient's keys for Identities and Pseudonyms (PD-Di, PC-Di and PI-Di). Note: In schemeVersion 1 the recipientKeySetVersion for DVs is a value of 8 decimal digits corresponding with the issue date (notBefore) of the certificate, in the format YYYYMMDD, used to request the PEM file at the party generating the keys within the scheme.

A DirectEncryptedPseudonym is identitical to an EncryptedPseudonym, although an additonal processing step is needed before decryption. This form is only applicable for reporting from BSNk_registration to CIF.

```
EC-Schnorr-Signature ::= SEQUENCE {
        signatureType      OBJECT IDENTIFIER (ecschnorr-plain-SHA384),
        signatureValue     EC-Sig-Value
}

bsi-de OBJECT IDENTIFIER ::= {
    itu-t(0) identified-organization(4) etsi(0)
    reserved(127) etsi-identified-organization(0) 7
}

id-ecc OBJECT IDENTIFIER ::= { bsi-de algorithms(1) 1 }

ecschnorr-plain-signatures OBJECT IDENTIFIER ::= { id-ecc signatures(4) 3 }

ecschnorr-plain-SHA384 OBJECT IDENTIFIER ::= { ecschnorr-plain-signatures 3 }
```

The auditElement is similar to the auditElement of a Polymorphic Identity or Pseudonym. The signature is a Schnorr signature for efficiency.

```
id-BSNk-encrypted OBJECT IDENTIFIER ::= { id-BSNk-identifiers 2 }

id-BSNk-encrypted-identity OBJECT IDENTIFIER ::= { id-BSNk-encrypted 1 }

id-BSNk-encrypted-pseudonym OBJECT IDENTIFIER ::= { id-BSNk-encrypted 2 }

id-BSNk-encrypted-identity-signed OBJECT IDENTIFIER ::= { id-BSNk-encrypted 3 }

id-BSNk-encrypted-pseudonym-signed OBJECT IDENTIFIER ::= { id-BSNk-encrypted 4 }

id-BSNk-encrypted-direct-pseudonym OBJECT IDENTIFIER ::= { id-BSNk-encrypted 5 }

id-BSNk-encrypted-direct-pseudonym-signed OBJECT IDENTIFIER ::= { id-BSNk-encrypted 6 }
```

Identity or Pseudonym

Finally, an Encrypted Identity or Pseudonym can be decrypted into a Identity or Pseudonym respectively, consisting of (the X coordinate of) 1 point on an elliptic curve. The Identity or Pseudonym is not directly used in any of the interfaces, but is the RECOMMENDED representation of a Identity or Pseudonym for a relying party to use after decryption of a Encrypted Identity or Pseudonym.

Decrypted pseudoID ASN.1 notation

```
Identity ::= SEQUENCE {
    notationIdentifier     OBJECT IDENTIFIER (id-BSNk-decrypted-identifier),
    schemeVersion          INTEGER,
    schemeKeyVersion       INTEGER,
    recipient              IA5String,
    type                   INTEGER,
    identityValue          IA5String
}

Pseudonym ::= SEQUENCE {
    notationIdentifier     OBJECT IDENTIFIER (id-BSNk-decrypted-pseudonym),
    schemeVersion          INTEGER,
    schemeKeyVersion       INTEGER,
    recipient              IA5String,
    recipientKeySetVersion INTEGER,
    diversifier            IA5String,
    type                   INTEGER,
    pseudonymValue         IA5String
}
```

In case of an Identity, the identity can be extracted from the X coordinate of the EllipticCurvePoint of the Identity. In schemeVersion 1, the X coordinate, after conversion from a number to a bytearray, contains an encoded identity padded using OAEP as defined in Section 7.1 of RFC8017 (PKCS#1 v2.2). Here the following parameters are chosen:

- The place of n (RSA modulus) is taken by the order of curve q; length in bytes of q is denoted by k as in PKCS #1, i.e.

equal to 40 for the Brainpool320r1 curve used in version 1 of the scheme.
- Hash function is SHA384 truncated to first 10 bytes, i.e. hLen = 10.
- Message length mLen = to k – 2hLen – 2 (PKCS #1 only requires), i.e. equal to 18.
- MGF1 as defined in PKCS #1 is used as Mask Generation Function.
- Optional Label is empty string.

The decoded identity (18 bytes) consists of a prefix of three bytes and the identity (e.g. BSN). The prefix consists of a version, a type and a length of the identifier. All not used bytes are zero. That is, 15 bytes is the longest size supported for an identifier in version 1.

In case of a Pseudonym, the identifying, persistent pseudonym of a user is the EllipticCurvePoint of the Pseudonym. The RECOMMENDED representation of a Pseudonym used in a DV registration, consists of the recipientKeySetVersion (decimal string of length 8) of the closing key with the uncompressed EllipticCurvePoint appended. If two such representations are equal the pseudonyms correspond to the same person. However, we can only deduce that two pseudonyms do not correspond to the same person if the pseudonymValue differ while all other values are equal. We note that the recipientKeySetVersion of the closing key can be different from the recipientKeySetVersions of the EI and EP decryption key.

For each decrypted pseudonym the DV shall archive the additional fields decrypted from the Encrypted Pseudonym.

```
id-BSNk-decrypted OBJECT IDENTIFIER ::= { id-BSNk-identifiers 3 }

id-BSNk-decrypted-identifier OBJECT IDENTIFIER ::= { id-BSNk-decrypted 1 }

id-BSNk-decrypted-pseudonym OBJECT IDENTIFIER ::= { id-BSNk-decrypted 2 }
```

Key formats

Polymorphic pseudonimization uses various keys. These keys have been versioned, see the syntax above.

Keys for relying parties are provided using the notation described in DV-key format.

Several of the scheme-wide keys are public, and can be used to use the polymorphism or verify signatures. These keys are defined in Metadata and under the role PPSteutelSet in RoleDescriptors non-Participants. For these public keys the brainpool P320r1 curve is used, which is a named curve defined as

```
-- Brainpool curves and the TeleTrust namespace are defined in BSI TR-03111
ecStdCurvesAndGeneration OBJECT IDENTIFIER ::= {
    iso(1) identified-organization(3) teletrust(36) algorithm(3)
    signature-algorithm(3) ecSign(2) ecStdCurvesAndGeneration(8)
}

ellipticCurve OBJECT IDENTIFIER ::= { ecStdCurvesAndGeneration 1 }

versionOne OBJECT IDENTIFIER ::= { ellipticCurve 1 }

brainpoolP320r1 OBJECT IDENTIFIER ::= { versionOne 9 }
```

Metadata specifications

The following metadata will be published by Beheerorganisatie BSNk:

- Metadata — Each Participant and non-Participant fulfilling a role in the Uniforme Set van Eisen MUST supply metadata to the Beheerorganisatie BSNk for every system that implements that role. The Beheerorganisatie BSNk will sign and publish the aggregated Metadata of all Participants and others (like BSNk) realizing specific roles.
- Autorisation List BSN format — The Beheerorganisatie BSNk provides the Autorisatielijst BSN containing the OIN's

of all organisations authorized to use BSN. Every OIN also accompanied by a name to improve problem solving activities. The Beheerorganisatie BSNk publishes the Autorisatielijst BSN in a fixed location. The file is available in XML format.

- Key provisioning list format — The Beheerorganisatie BSNk provides the Sleutelverstrekkingslijst containing the OIN's of all Service Providers (Dienstverlener) for whom DV-key material has been provided to their Broker (Toegangsdienst). The Sleutelverstrekkingslijst is mainly for transparency reasons (like Certificate Transparency, RFC6962 https://tools.ietf.org/html/rfc6962). The Beheerorganisatie BSNk publishes the Sleutelverstrekkingslijst in a fixed location. The file is available in XML format.

Metadata

Each Participant and non-Participant fulfilling a role in the Uniforme Set van Eisen MUST supply metadata to the Beheerorganisatie BSNk for every system that implements that role. The Beheerorganisatie BSNk will sign and publish the aggregated Metadata of all Participants and others (like BSNk) realizing specific roles.

A Participant that has several roles in the network MUST supply metadata for each role separately. Metadata documents SHOULD not have any other elements, attributes or extensions than those specified here.

EntitiesDescriptor per role

Each participant MUST publish one SAML2 metadata document per role containing one signed EntitiesDescriptor element, to the specifications defined below and specified in SAML2 for the namespace 'urn:oasis:names:tc:SAML:2.0:metadata'. Signing metadata MUST meet the requirements for XML Digital Signature. The metadata document MUST be downloadable as file by the Beheerorganisatie BSNk over a Secure connection (TLS) and MAY require TLS-mutual authentication.

The EntitiesDescriptor MAY contain an Extensions element that contains a PublicationInfo element with the URL and creation date of the metadata file, as per SAML2 Metadata RPI. An EntitiesDescriptor MAY contain other attributes, elements and extensions as specified in SAML2 Metadata specifications.

The EntitiesDescriptor element MUST contain one or more EntityDescriptor elements.

EntityDescriptor per system

Each EntityDescriptor element MUST contain the details (of a logical system operated under responsibility of the Participant) for that role by that Participant. A Participant MAY realize the same role using more than one logical system, one EntityDescriptor MUST be supplied for each of the systems.

Each EntityDescriptor MUST contain an entityID attribuut, referencing the OIN of the Participant/role. The format for the entityID is the prefix 'urn:nl-gdi-eid:entity:' with the 20-digit OIN concatenated. The entityID/OIN of each system MUST be identical for each system (EntityDescriptor) included for the Participant/role.

An EntityDescriptor MAY contain other attributes, elements and extensions as specified in SAML2 Metadata specifications.

Each EntityDescriptor MUST contain the (SAML2) RoleDescriptor(s) for that role, as specified under RoleDescriptors Participants and RoleDescriptors non-Participants. Furthermore, each EntityDescriptor, or the RoleDescriptor elements thereof, has to incorporate the following:

Organization

The EntityDescriptor element MUST contain information about one's own organization by including one element of the type Organization, which describes the official name (OrganizationName), the readable name for users (OrganizationDisplayName) and the website (OrganizationURL). The OrganizationName and OrganizationDisplayName

MUST match with a (trade) name as registered in the Business Register (Handelsregister).

ContactPerson

The EntityDescriptor MUST contain one or more elements of the type ContactPerson containing the name, email address and telephone number of the people that can be contacted by other Participants or the Beheerorganisatie BSNk in the event of an incident.

IDPSSODescriptors

Each IDPSSODescriptor element MUST contain one or more SingleSignOnService elements, with data of the endpoint(s) that can be used for authentication of users (unless other usage is specified for a particular role).

Each IDPSSODescriptor element MUST contain the WantAuthnRequestsSigned XML attribute with value "true".

An IDPSSODescriptor MAY contain one or more of the other elements specified in the SAML2 Metadata specification.

SPSSODescriptors

Each SPSSODescriptor element MUST contain one or more AssertionConsumerService elements, where other Participants can contact the Participant for the relevant role (unless other usage is specified for a particular role).

Each SPSSODescriptor element MUST contain the AuthnRequestsSigned XML attribute with value "true" and a WantAssertionsSigned XML attribute with value "true".

An SPSSODescriptor MAY contain one or more of the other elements specified in the SAML2 Metadata specification.

KeyDescriptor

Each IDPSSODescriptor or SPSSODescriptor element MUST contain one or more KeyDescriptor elements with the use XML attribute with value "signing". Alternatively, at least one KeyDescriptor without a use XML attribute MAY be included, indicating the default that the key is for both signing and encryption.

Each KeyDescriptor element marked for "signing" MUST contain a valid PKIoverheid certificate with which the participant's SAML messages and/or client-authentication for direct TLS connections can be authenticated. A certificate for server-authentication MAY be included as "signing" certificate, certificates for server-authentication SHOULD have a Subject.CommonName that matches the hostname fo the server's endpoint.

Additional KeyDescriptor elements for "encryption" MAY be included.

Additional KeyDescriptor elements without specificied "use" attribute MAY be included, to describe (derived) keys used in the Polymorphic Pseudonymzation algorithm. These KeyDescriptor MUST contain a KeyInfo element, with a KeyName element using 'urn:nl-gdi-eid:1.0:pp-key:<Environment>:<SchemeKeySetVersion>:<KeyName>:<KeyVersion>' to describe the key. In case of public keys, these MUST be included as KeyValue element using a ECKeyValue and a NamedCurve with PublicKey (NOTE: ECKeyValue is specified in XML-signature 1.1). In case of derived keys, other elements MUST NOT be included.

In case XML Digital Signature are created using a KeyName to reference the used certificate, the KeyName uniquely identifying the X509Certificate in the context of the EntityDescriptor MUST be included.

Example KeyDescriptors

```
...
<md:KeyDescriptor use="signing">
    <ds:KeyInfo>
        <ds:KeyName>2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12</ds:KeyName>
        <ds:X509Data>
            <ds:X509Certificate>
                ...
            </ds:X509Certificate>
        </ds:X509Data>
    </ds:KeyInfo>
</md:KeyDescriptor>
<md:KeyDescriptor use="encryption">
    <ds:KeyInfo>
        <ds:KeyName>xml-encryption-public-key-20161207</ds:KeyName>
        <ds:X509Data>
            <ds:X509Certificate>
                ...
            </ds:X509Certificate>
        </ds:X509Data>
    </ds:KeyInfo>
</md:KeyDescriptor>
<md:KeyDescriptor>
    <ds:KeyInfo>
        <ds:KeyName>urn:nl-gdi-eid:1.0:pp-key:test:1:AA_D999999990123456700000:1</ds:KeyName>
    </ds:KeyInfo>
</md:KeyDescriptor>
<md:KeyDescriptor>
    <ds:KeyInfo>
        <!-- PIP/PP/PI public signing key for BSNk-activate in test network -->
        <ds:KeyName>urn:nl-gdi-eid:1.0:pp-key:test:1:U:1</ds:KeyName>
            <ds:KeyValue>
            <ds11:ECKeyValue>
                <!-- brainpool P320r1 curve -->
                <ds11:NamedCurve URI="urn:oid:1.3.36.3.3.2.8.1.1.9"/>
                <ds11:PublicKey>
                   MQo=...
                </ds11:PublicKey>
            </ds11:ECKeyValue>
        </ds:KeyValue>
    </ds:KeyInfo>
</md:KeyDescriptor>
...
```

NameIDFormat

Each IDPSSODescriptor element MUST contain one or more NameIDFormat XML element(s), containing the identifier types the Participant is accredited for to support in this role.

Each SPSSODescriptor element MUST contain one or more NameIDFormat XML element(s), containing the identifier types the Participant can accept for this role.

The following NameIDFormats are defined:

name	ID type
urn:nl-gdi-eid:1.0:id:BSN	BSN, to be communicated as Encrypted Identity.
urn:nl-gdi-eid:1.0:id:Pseudonym	Pseudonym, to be communicated as Encrypted Pseudonym.

Example NameIDFormat

```
...
<md:IDPSSODescriptor>
    ...
 <md:NameIDFormat>urn:nl-gdi-eid:1.0:id:BSN</md:NameIDFormat>
    ...
</md:IDPSSODescriptor>
...
```

Level of assurance

An EntityDescriptor for a MU or AD MUST include the Level of Assurance at which recognition requests can be processed by the described entity, in the form of an extension in the EntityDescriptor element as described in the document SAML V2.0 Identity Assurance Profiles. In case the MU/AD is accredited for multiple LoAs, each LoA MUST be enumerated as an AttributeValue.

Example LoA

```
...
    <md:Extensions xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
        xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

        <mdattr:EntityAttributes>
            <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
Name="urn:oasis:names:tc:SAML:attribute:assurance-certification">
                <saml:AttributeValue>http://eidas.europa.eu/LoA/substantial</saml:AttributeValue>
                <saml:AttributeValue>http://eidas.europa.eu/LoA/high</saml:AttributeValue>
            </saml:Attribute>
        </mdattr:EntityAttributes>

    </md:Extensions>
...
```

Aggregated Metadata

One of the roles of the BSNk, is that of metadata aggregator. The metadata as supplied by each individual Participant, will be validated and aggregated. The aggregated metadata will be published as an authoritative list of accredited Participants. This aggregated metadata has the form of a SAML2 Metadata document, containing a signed EntitiesDescriptor.

The aggregated Metadata will have a @Name with the structure 'urn:nl-gdi-eid:1.0:metadata:<environment>:<sequence-number>'. This will identity the metadata for a specific environment (e.g. test) and a given sequence-number of publication for that environment. For example 'urn-nl-gdi-eid:1.0:metadata:test:76'.

For each role an EntitiesDescriptor will be included, the @Name containing the name of the role prefixed by 'urn:nl-gdi-eid:role:'.

The following roles are included:

- Middelenuitgever
- Authenticatiedienst
- Toegangsdienst

The EntitiesDescriptor for each role will contain one EntityDescriptor for each Participant under that role, which is a copy of the EntityDescriptor for that role supplied by the Participant.

Next to these roles, several public facilities are listed as well. These will all be grouped under an EntitiesDescriptor with the @Name 'urn:nl-gdi-eid:role:Basisvoorziening' and are:

- PPSleutelset
- Sleutelbeheer (Rol Sleutelbeheerder (SB)).
- Koppelregister (Rol Koppeldienst (KD)).
- Inzageregister (Rol Inzageregister (IR)).
- eIDAS-berichtenservice.

Other roles not listed above may be included; systems processing the Metadata SHOULD ignore unrecognized roles.

Processing rules for aggregated metadata

Each Participant:

- MUST validate the metadata and its signature before processing the metadata.
- MUST use actual metadata, using an update frequency as specified by the Beheerorganisatie BSNk.
- MUST use the metadata to verify peers in an authentication process are accredited for that role/LoA.
- MUST use the metadata to obtain endpoints for accredited peers.
- MUST NOT contact or accept endpoints / entities not listed in the metadata when handling requests for authentication for the public domain.
- MUST regularly verify the metadata contains their own metadata entries correctly.
- MUST use an automated process to process the metadata that finishes in 15 minutes and MUST be able to start this automated process (e.g., manually) between the predefined periods in agreement with the Beheerorganisatie BSNk to accommodate a rollback or other changes.
- SHOULD ignore EntitiesDescriptor/EntityDescriptors for unknown roles.

Example aggregated metadata

Example aggregated metadata

```
<md:EntitiesDescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"
    Name="urn-nl-gdi-eid:1.0:metadata:test:76"
    ID="sigref">

    <ds:Signature>...</ds:Signature>

    <md:Extensions>
        <mdrpi:PublicationInfo publisher="https://bsnk.example.nl/metadata/metadata.xml"
creationInstant="2016-12-14T11:25:07Z"/>
    </md:Extensions>

    <md:EntitiesDescriptor Name="urn:nl-gdi-eid:role:Middelenuitgever">
        <md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999012345670000">
            ...
        </md:EntityDescriptor>
        <md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999076543210000">
            ...
        </md:EntityDescriptor>
        ...
    </md:EntitiesDescriptor>

    <md:EntitiesDescriptor Name="urn:nl-gdi-eid:role:Authenticatiedienst">
        <md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999012345670000">
            ...
        </md:EntityDescriptor>
        <md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999888888880000">
            ...
        </md:EntityDescriptor>
        ...
    </md:EntitiesDescriptor>

    <md:EntitiesDescriptor Name="urn:nl-gdi-eid:role:Toegangsdienst">
        <md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999012435670000">
            ...
        </md:EntityDescriptor>
        <md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999012445670000">
            ...
        </md:EntityDescriptor>
        ...
    </md:EntitiesDescriptor>

    <md:EntitiesDescriptor Name="urn:nl-gdi-eid:role:Basisvoorziening">
        <md:EntitiesDescriptor Name="urn:nl-gdi-eid:role:BeheerderMetadata">
            <md:EntityDescriptor entityID="urn:nl-gdi-eid:entities:99999999012345670000">
                ...
            </md:EntityDescriptor>
            <md:EntityDescriptor entityID="urn:nl-gdi-eid:1.0:pp-keyset:test:1">
                ...
            </md:EntityDescriptor>
        </md:EntitiesDescriptor>
        <md:EntitiesDescriptor Name="urn:nl-gdi-eid:role:Sleutelbeheerder">
            <md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999012345670002">
                ...
            </md:EntityDescriptor>
        </md:EntitiesDescriptor>
        <md:EntitiesDescriptor Name="urn:nl-gdi-eid:role:Koppelregister">
            <md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999012345670003">
                ...
            </md:EntityDescriptor>
        </md:EntitiesDescriptor>
        <md:EntitiesDescriptor Name="urn:nl-gdi-eid:role:Inzageregister">
            <md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999012345670004">
                ...
            </md:EntityDescriptor>
        </md:EntitiesDescriptor>
        <md:EntitiesDescriptor Name="urn:nl-gdi-eid:role:eIDAS-berichtenservice">
            <md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999012345670005">
                ...
            </md:EntityDescriptor>
        </md:EntitiesDescriptor>

    </md:EntitiesDescriptor>

</md:EntitiesDescriptor>
```

(for examples of individual entities, see child pages)

RoleDescriptors Participants

A participant MUST supply metadata to the Beheerorganisatie BSNk for every system that implements the role of AD, MR, TD in the network.

A participant MUST NOT supply metadata for a role or functionality it has not been accredited for. This latter requirement is for metadata for the production network; for the test network this is allowed for roles for which the Participant is requesting accreditation.

The following role descriptors are defined for each of the various roles in the USvE. A Participant MUST supply metadata, as described under Metadata.

Rol Middelenuitgever (MU): IDPSSODescriptor

An EntityDescriptor for a MU MUST include one IDPSSODescriptor element.

Example MU metadata

```
<md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999012345670000"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

    <md:IDPSSODescriptor WantAuthnRequestsSigned="true"
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:Extensions>
            <mdattr:EntityAttributes>
                <saml:Attribute
                    Name="urn:oasis:names:tc:SAML:attribute:assurance-certification"
                    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                    <saml:AttributeValue>http://eidas.europa.eu/LoA/substantial
                    </saml:AttributeValue>
                    <saml:AttributeValue>http://eidas.europa.eu/LoA/high
                    </saml:AttributeValue>
                </saml:Attribute>
            </mdattr:EntityAttributes>
        </md:Extensions>
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>...</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:KeyDescriptor>
            <ds:KeyInfo>
                <ds:KeyName>urn:nl-gdi-eid:1.0:pp-key:1:AA_D99999999012345670000:1</ds:KeyName>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:NameIDFormat>urn:nl-gdi-eid:1.0:id:BSN</md:NameIDFormat>
        <md:NameIDFormat>urn:nl-gdi-eid:1.0:id:Pseudonym</md:NameIDFormat>
        <md:SingleSignOnService Location="https://mu.example.nl/subscribe"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" />
    </md:IDPSSODescriptor>
    <md:Organization>
        <md:OrganizationName xml:lang="nl">Voorbeeld MU B.V.</md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="nl">Voorbeeld MU</md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="nl">https://mu.example.nl/</md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson contactType="technical">
        <md:GivenName>John</md:GivenName>
        <md:SurName>Doe</md:SurName>
        <md:EmailAddress>john.doe@mu.example.nl</md:EmailAddress>
        <md:TelephoneNumber>+31-10-1234567</md:TelephoneNumber>
    </md:ContactPerson>

</md:EntityDescriptor>
```

MU - AD affiliation

In case means for authentication issued by an MU are used by another entity in the role of AD – that is, if the entityID/OIN of

MU and AD are not equal – then the MU MUST publish an additional EntityDescriptor defining this affiliation, in the form of an AffiliationDescriptor.

The AffiliationDescriptor MUST reference the MU as affiliationOwnerID. The AffiliationDescriptor MUST reference each AD that is contracted to use the means issued by the MU as AffiliateMember. The MU itself MUST be included as AffiliateMember.

Example MU-AD AffiliationDescriptor

```
<md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999012345670000"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">

    <md:AffiliationDescriptor affiliationOwnerID="urn:nl-gdi-eid:entity:99999999012345670000">
        <md:AffiliateMember>urn:nl-gdi-eid:entity:99999999012345670000</md:AffiliateMember>
        <md:AffiliateMember>urn:nl-gdi-eid:entity:99999999876543210000</md:AffiliateMember>
    </md:AffiliationDescriptor>

</md:EntityDescriptor>
```

Rol Authenticatiedienst (AD): IDPSSODescriptor

An EntityDescriptor for an AD MUST include one IDPSSODescriptor element.

Example AD EntityDescriptor

```
<md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999012345670000"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

    <md:IDPSSODescriptor WantAuthnRequestsSigned="true"
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:Extensions>
            <mdattr:EntityAttributes>
                <saml:Attribute
                    Name="urn:oasis:names:tc:SAML:attribute:assurance-certification"
                    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                    <saml:AttributeValue>http://eidas.europa.eu/LoA/substantial</saml:AttributeValue>
                </saml:Attribute>
            </mdattr:EntityAttributes>
        </md:Extensions>
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>...</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:KeyDescriptor>
            <ds:KeyInfo>
                <ds:KeyName>urn:nl-gdi-eid:1.0:pp-key:1:AA_D99999999012345670000:1</ds:KeyName>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:NameIDFormat>urn:nl-gdi-eid:1.0:id:BSN</md:NameIDFormat>
        <md:NameIDFormat>urn:nl-gdi-eid:1.0:id:Pseudonym</md:NameIDFormat>
        <md:SingleSignOnService Location="https://ad.example.nl/signon"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" />
    </md:IDPSSODescriptor>
    <md:Organization>
        <md:OrganizationName xml:lang="nl">Voorbeeld AD B.V.</md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="nl">Voorbeeld AD</md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="nl">https://ad.example.nl/</md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson contactType="technical">
        <md:GivenName>John</md:GivenName>
        <md:SurName>Doe</md:SurName>
        <md:EmailAddress>john.doe@ad.example.nl</md:EmailAddress>
        <md:TelephoneNumber>+31-10-1234567</md:TelephoneNumber>
    </md:ContactPerson>

</md:EntityDescriptor>
```

Rol Toegangsdienst (TD): IDPSSODescriptor and SPSSODescriptor

An EntityDescriptor for a TD MUST include one IDPSSODescriptor and one SPSSODescriptor.

The IDPSSODescriptor MUST contain the technical details where DVs (SPs) can request authentication for a User.

The SPSSODescrioptor MUST contain the technical details for other roles (i.e. AD).

Example HM descriptor

```
<md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:9999999912345670000"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">

    <md:IDPSSODescriptor WantAuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>...</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:NameIDFormat>urn:nl-gdi-eid:1.0:id:BSN</md:NameIDFormat>
        <md:NameIDFormat>urn:nl-gdi-eid:1.0:id:Pseudonym</md:NameIDFormat>
        <md:SingleSignOnService Location="https://td.example.nl/signon"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" />
    </md:IDPSSODescriptor>
    <md:SPSSODescriptor WantAssertionsSigned="true" AuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>...</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:NameIDFormat>urn:nl-gdi-eid:1.0:id:BSN</md:NameIDFormat>
        <md:NameIDFormat>urn:nl-gdi-eid:1.0:id:Pseudonym</md:NameIDFormat>
        <md:AssertionConsumerService Location="https://td.examnple.nl/acs" index="1"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" />
    </md:SPSSODescriptor>
    <md:Organization>
        <md:OrganizationName xml:lang="nl">Voorbeeld TD B.V.</md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="nl">Voorbeeld TD</md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="nl">https://td.example.nl/</md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson contactType="technical">
        <md:GivenName>John</md:GivenName>
        <md:SurName>Doe</md:SurName>
        <md:EmailAddress>john.doe@td.example.nl</md:EmailAddress>
        <md:TelephoneNumber>+31-10-1234567</md:TelephoneNumber>
    </md:ContactPerson>

</md:EntityDescriptor>
```

RoleDescriptors non-Participants

The Beheerorganisatie BSNk will sign and publish the aggregated Metadata of all BSNk roles and all Participants. The roles for BSNk and other non-Participants are described below.

Various roles in the Uniforme Set van Eisen are described, that are part of a central facility. These include the roles fulfilled by for instance the BSNk.

These roles will have their details described in Metadata as well. The description follows per role:

Rol Beheerder Metadata (BM)

Metadata of all Participants is aggregated by the Beheerder Metadata. The metadata is signed by the actor fulfilling this role, its publication location is included using a SAML2 Metadata RPI extension (see Metadata).

For the Rol Beheerder Metadata (BM) an EntityDescriptor is included. This EntityDescriptor will hold and AffiliationDescriptor, listing the entities with a role

The metadata itself is published by this role, as is the Autorisatielijst BSN and Sleutelverstrekkingslijst. Both lists are included as AdditionalMetadataLocation elements under the EntityDescriptor for the Rol Beheerder Metadata (BM). Both lists will be signed using a key listed for use 'signing' in the AffiliationDescriptor.

Example RoleDescriptor beheerder metadata

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntitiesDescriptor Name="urn:nl-gdi-eid:roles:BeheerderMetadata"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">

    <md:EntityDescriptor entityID="urn:nl-gdi-eid:entities:99999999012345670000">
        <md:AffiliationDescriptor affiliationOwnerID="urn:nl-gdi-eid:entities:99999999012345670000">
            <md:AffiliateMember>urn:nl-gdi-eid:entity:99999999012345670000</md:AffiliateMember>
            <md:AffiliateMember>urn:nl-gdi-eid:entity:99999999012345670001</md:AffiliateMember>
            <md:KeyDescriptor use="signing">
                <ds:KeyInfo>
                    <ds:X509Data>
                        <ds:X509Certificate>...</ds:X509Certificate>
                    </ds:X509Data>
                </ds:KeyInfo>
            </md:KeyDescriptor>
        </md:AffiliationDescriptor>
        <md:AdditionalMetadataLocation namespace="urn:nl-gdi-eid:1.0:autorisatielijst-bsn">
            https://bsnk.example.nl/metadata/bsn-autorisatielijst.xml
        </md:AdditionalMetadataLocation>
        <md:AdditionalMetadataLocation namespace="urn:nl-gdi-eid:1.0:sleutelverstrekkingslijst">
            https://bsnk.example.nl/metadata/sleutelverstrekkingslijst.xml
        </md:AdditionalMetadataLocation>
    </md:EntityDescriptor>

    <md:EntityDescriptor entityID="urn:nl-gdi-eid:1.0:pp-keyset:test:1">
        ...
    </md:EntityDescriptor>

</md:EntitiesDescriptor>
```

For Polymorfe encryptie en pseudonimisering, scheme wide keys are in use. To facilitate key management procedures, all scheme-wide keys are versioned using schemeKeySetVersion (see Polymorphic Pseudonymization Notation).

Public scheme-wide keys are published as additional EntityDescriptor element with an entityID of 'urn:nl-gdi-eid:1.0:pp-keyset:<Environment>:<SchemeKeySetVersion>', where SchemeKeySetVersion is the version number of the scheme-wide key set for the network environment (eg 'test' or 'production'). One or more of these set may be included in the EntitiesDescriptor for the Rol Beheerder Metadata (BM). The actual keys are listed as an AffiliationDescriptor under this EntityDescriptor.

Example PPKeySet EntityDescriptor

```
<md:EntityDescriptor entityID="urn:nl-gdi-eid:1.0:pp-keyset:test:1"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:ds11="http://www.w3.org/2009/xmldsig11#"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">

    <md:AffiliationDescriptor affiliationOwnerID="urn:nl-gdi-eid:1.0:pp-keyset:test:1">
        <md:AffiliateMember>urn:nl-gdi-eid:pp-key:test:1:Y:1</md:AffiliateMember>
        <md:AffiliateMember>urn:nl-gdi-eid:pp-key:test:1:Z:1</md:AffiliateMember>
        <md:KeyDescriptor>
            <ds:KeyInfo>
                <!--  public key Y for PI/EI in test network -->
                <ds:KeyName>urn:nl-gdi-eid:pp-key:test:1:Y:1</ds:KeyName>
                <ds:KeyValue>
                    <ds11:ECKeyValue>
                        <!-- brainpool P320r1 curve -->
                        <ds11:NamedCurve URI="urn:oid:1.3.36.3.3.2.8.1.1.9"/>
                        <ds11:PublicKey>
                           MQo=...
                        </ds11:PublicKey>
                    </ds11:ECKeyValue>
                </ds:KeyValue>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:KeyDescriptor>
            <ds:KeyInfo>
                <!--  public key Z for PP/EP in test network -->
                <ds:KeyName>urn:nl-gdi-eid:pp-key:test:1:Z:1</ds:KeyName>
                <ds:KeyValue>
                    <ds11:ECKeyValue>
                        <ds11:NamedCurve URI="urn:oid:1.3.36.3.3.2.8.1.1.9"/>
                        <ds11:PublicKey>
                           Mgo=...
                        </ds11:PublicKey>
                    </ds11:ECKeyValue>
                </ds:KeyValue>
            </ds:KeyInfo>
        </md:KeyDescriptor>
    </md:AffiliationDescriptor>

</md:EntityDescriptor>
```

Rol Sleutelbeheerder (SB)

The Sleutelbeheer MUST publish its details as an SPSSODescriptor. The AssertionConsumerEndpoint element MUST contain the endpoint for obtaining Dienstverlener keys (AUC5 Verstrekken sleutelmateriaal Dienstverleners).

The EntityDescriptor of the Sleutelbeheerder MUST contain an AdditionalMetadataLocation element, containing the location where the Autorisatielijst BSN can be obtained (see also Autorisation List BSN format).

Example SleutelBeheer EntityDescriptor

```
<md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999012345670000"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">

    <md:SPSSODescriptor WantAssertionsSigned="true" AuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>...</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:NameIDFormat>urn:nl-gdi-eid:1.0:id:Pseudonym</md:NameIDFormat>
        <md:AssertionConsumerService Location="https://bsnk.example.nl/keymgmt/dv/key-request"
index="1" isDefault="true" Binding="http://schemas.xmlsoap.org/soap/http" />
    </md:SPSSODescriptor>
    <md:Organization>
        <md:OrganizationName xml:lang="nl">Voorbeeld BSNk</md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="nl">Voorbeeld BSNk</md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="nl">https://bsnk.example.nl/</md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson contactType="technical">
        <md:SurName>BSNk sleutelbeheer</md:SurName>
        <md:EmailAddress>sleutelbeheer@bsnk.example.nl</md:EmailAddress>
        <md:TelephoneNumber>+31-10-1234567</md:TelephoneNumber>
    </md:ContactPerson>

</md:EntityDescriptor>
```

Rol Koppeldienst (KD)

The koppelregister MUST publish its details as an IDPSSODescriptor. This IDPSSODescriptor MUST contain the endpoint(s) for activation (AUC1 Activeren BSN) as SingleSignOnService element and the endpoint(s) for transformation (AUC2 Transformeren) as NameIDMapping element.

Example KR EntityDescriptor

```
  <md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999012345670000"
     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
     xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
     xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">

     <md:IDPSSODescriptor WantAuthnRequestsSigned="true"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
         <md:KeyDescriptor use="signing">
             <ds:KeyInfo>
                 <ds:X509Data>
                     <ds:X509Certificate>...</ds:X509Certificate>
                 </ds:X509Data>
             </ds:KeyInfo>
         </md:KeyDescriptor>
         <md:KeyDescriptor use="encryption">
             <ds:KeyInfo>
                 <ds:X509Data>
                     <ds:X509Certificate>...</ds:X509Certificate>
                 </ds:X509Data>
             </ds:KeyInfo>
         </md:KeyDescriptor>
         <md:KeyDescriptor>
             <ds:KeyInfo>
                 <!--  PIP/PP/PI public signing key U for BSNk-activate in test network -->
                 <ds:KeyName>urn:nl-gdi-eid:pp-key:test:1:U:1</ds:KeyName>
                 <ds:KeyValue>
                     <ds11:ECKeyValue>
                         <ds11:NamedCurve URI="urn:oid:1.3.36.3.3.2.8.1.1.9"/>
                         <ds11:PublicKey>
                            Mwo=...
                         </ds11:PublicKey>
                     </ds11:ECKeyValue>
                 </ds:KeyValue>
             </ds:KeyInfo>
         </md:KeyDescriptor>
         <md:NameIDFormat>urn:nl-gdi-eid:1.0:id:Pseudonym</md:NameIDFormat>
         <md:NameIDFormat>urn:nl-gdi-eid:1.0:id:BSN</md:NameIDFormat>
         <md:SingleSignOnService Location="https://bsnk.exmaple.nl/kr/activate"
 Binding="http://schemas.xmlsoap.org/soap/http" />
         <md:NameIDMappingService Location="https://bsnk.exmaple.nl/kr/tranform"
 Binding="http://schemas.xmlsoap.org/soap/http" />
     </md:IDPSSODescriptor>
     <md:Organization>
         <md:OrganizationName xml:lang="nl">Voorbeeld BSNk</md:OrganizationName>
         <md:OrganizationDisplayName xml:lang="nl">Voorbeeld BSNk</md:OrganizationDisplayName>
         <md:OrganizationURL xml:lang="nl">https://bsnk.example.nl/</md:OrganizationURL>
     </md:Organization>
     <md:ContactPerson contactType="technical">
         <md:SurName>BSNk koppelregister</md:SurName>
         <md:EmailAddress>koppelregister@bsnk.example.nl</md:EmailAddress>
         <md:TelephoneNumber>+31-10-1234567</md:TelephoneNumber>
     </md:ContactPerson>

 </md:EntityDescriptor>
```

Rol Inzageregister (IR)

The inzageregister MUST publish its details as an SPSSODescriptor. The AssertionConsumerEndpoint element MUST contain the endpoint for providing status updates (AUC3 Aanpassen status relatie en/of authenticatiemiddel).

Example IR EntityDescriptor

```
<md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999012345670000"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">

    <md:SPSSODescriptor WantAssertionsSigned="true" AuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>...</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:NameIDFormat>urn:nl-gdi-eid:1.0:id:Pseudonym</md:NameIDFormat>
        <md:AssertionConsumerService Location="https://bsnk.example.nl/ir/update" index="1"
isDefault="true" Binding="http://schemas.xmlsoap.org/soap/http" />
    </md:SPSSODescriptor>
    <md:Organization>
        <md:OrganizationName xml:lang="nl">Voorbeeld BSNk</md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="nl">Voorbeeld BSNk</md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="nl">https://bsnk.example.nl/</md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson contactType="technical">
        <md:SurName>BSNk inzageregister</md:SurName>
        <md:EmailAddress>inzageregister@bsnk.example.nl</md:EmailAddress>
        <md:TelephoneNumber>+31-10-1234567</md:TelephoneNumber>
    </md:ContactPerson>

</md:EntityDescriptor>
```

Role eIDAS berichtenservice

The eIDAS-berichtenservice MUST publish its details in the same way as a MU and AD for its role as identity provider. The eIDAS-berichtenservice MUST publish its details as an SPSSODescriptor for its role as Dienstverlener.

The 'eIDAS-berichtenservice' is the Dutch implementation of an eIDAS node. It is listed in the metadata to allow Dienstverleners and Participants to verify its messages. Any (public) DV should consider the eIDAS-berichtenservice as an Authenticatiedienst, per eIDAS regulation (EU 910/2014).

Autorisation List BSN format

The Beheerorganisatie BSNk provides the Autorisatielijst BSN containing the OIN's of all organisations authorized to use BSN. Every OIN also accompanied by a name to improve problem solving activities. The Beheerorganisatie BSNk publishes the Autorisatielijst BSN in a fixed location. The file is available in XML format.

XML

The XML-file consists of a signed XML document, according to the schema defined below. This document has an AuthorizationListBSN as root element with the following definition for its contents:

element	0..n	Description
@ID	1	An identifier unique to this document, for usage in the Signature
@publicationEnvironment	1	the environment for this list (e.g. 'production', 'acceptance' or 'test')

@publicationVersion	1	a sequence number that distinguishes the different published versions of the Autorisatielijst BSN.
@publicationInstance	1	Timestamp of publication of this list.
@cacheDuration	1	Duration this list may be cached.
Signature	1	XML-Signature by the publisher (BSNk).
AuthorizedOrganization	1..n	one entry per authorized organization
OIN	1	OIN of the authorized organisation
authorizationDate	1	Date of first authorization.
formalName	1	formal registered name of the organisation; for easier usage of the list
alias	0..n	alias, e.g. registered trade names; for easier usage of the list
policyReason	0..1	Optional reference to a policy reason why the organization is authorized.

Processing rules for AuthorizationListBSN

An Authenticatiedienst or Toegangsdienst:

- MUST validate Signature of the published Autorisatielijst BSN before processing it.
- MUST check that the published XML file is signed with a valid digital signature.
- MUST NOT process the message if it contains parts that are not signed with a valid digital signature.
- MUST process the Autorisatielijst BSN periodically at a time that is predefined by the Beheerorganisatie BSNk.
- MUST use an automated process to process the Autorisatielijst BSN that finishes in 15 minutes.
- MUST be able to start this automated process (e.g., manually) between the predefined periods in agreement with the Beheerorganisatie BSNk to accommodate a rollback or other changes.
- MUST verify a Service Provider is listed as authorized before processing a request for a Encrypted Identifier (containing a BSN) or providing a Encrypted Identifier (containing a BSN) to a Service Provider.

XML-schema AuthorizationListBSN

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
             xmlns="urn:nl-gdi-eid:1.0:schema"
             xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
             targetNamespace="urn:nl-gdi-eid:1.0:schema"
             elementFormDefault="qualified">

    <xs:import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLocation="xmldsig-core-schema.xsd"
/>

    <xs:element name="AuthorizationListBSN" type="AuthorizationListBSNType" />

    <xs:complexType name="AuthorizationListBSNType">
        <xs:sequence>
            <xs:element ref="ds:Signature" />
            <xs:sequence minOccurs="0" maxOccurs="unbounded">
                <xs:element name="AuthorizedOrganization" type="AuthorizedOrganizationType" />
            </xs:sequence>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID" use="required" />
        <xs:attribute name="publicationEnvironment" type="xs:string" use="required" />
        <xs:attribute name="publicationVersion" type="xs:nonNegativeInteger" use="required" />
        <xs:attribute name="publicationInstance" type="xs:dateTime" use="required" />
        <xs:attribute name="cacheDuration" type="xs:duration" use="optional" />
    </xs:complexType>

    <xs:complexType name="AuthorizedOrganizationType">
        <xs:sequence>
            <xs:element name="OIN" type="OINType" />
            <xs:element name="authorizationDate" type="xs:date" />
            <xs:element name="formalName" type="xs:string" />
            <xs:sequence minOccurs="0" maxOccurs="100">
                <xs:element name="alias" type="xs:string" />
            </xs:sequence>
            <xs:element name="policyReason" type="xs:anyURI" minOccurs="0" />
        </xs:sequence>
    </xs:complexType>

    <xs:simpleType name="OINType">
        <xs:annotation>
            <xs:documentation>OIN type.</xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:length value="20" />
        </xs:restriction>
    </xs:simpleType>

</xs:schema>
```

XML example AuthorizationListBSN

```
<AuthorizationListBSN
    ID="_whitelist"
    publicationEnvironment="test"
    publicationInstance="2016-11-30T16:00:00Z"
    publicationVersion="16"
    xmlns="urn:nl-gdi-eid:1.0:schema"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:nl-gdi-eid:1.0:schema Whitelist.xsd">

    <ds:Signature>...</ds:Signature>

    <AuthorizedOrganization>
        <OIN>99999999012345670000</OIN>
        <authorizationDate>2016-02-28</authorizationDate>
        <formalName>Gemeente Voorbeeld</formalName>
        <alias>voorbeeld</alias>
        <policyReason>http://www.bsnk.nl/gdi/besluit-gemeenten</policyReason>
    </AuthorizedOrganization>

    <AuthorizedOrganization>
        <OIN>99999999876556780000</OIN>
        <authorizationDate>2016-12-08</authorizationDate>
        <formalName>Huisartsenpraktijk Voorbeeld</formalName>
        <policyReason>http://www.bsnk.nl/gdi/besluit-zorg</policyReason>
    </AuthorizedOrganization>

</AuthorizationListBSN>
```

Key provisioning list format

The Beheerorganisatie BSNk provides the Sleutelverstrekkingslijst containing the OIN's of all Service Providers (Dienstverlener) for whom DV-key material has been provided to their Broker (Toegangsdienst). The Sleutelverstrekkingslijst is mainly for transparency reasons (like Certificate Transparency, RFC6962). The Beheerorganisatie BSNk publishes the Sleutelverstrekkingslijst in a fixed location. The file is available in XML format.

XML

The XML-file consists of a signed XML document, according to the schema defined below. This document has a KeyProvisioningList as root element with the following definition for its contents:

element	0..n	Description
@ID	1	An identifier unique to this document, for usage in the Signature
@publicationEnvironment	1	the environment for this list (e.g. 'production', 'acceptance' or 'test')
@publicationVersion	1	a sequence number that distinguishes the different published versions of the Autorisatielijst BSN.
@publicationInstance	1	Timestamp of publication of this list.
@cacheDuration	1	Duration this list may be cached.
Signature	1	XML-Signature by the publisher (BSNk).
KeyProvisioning	1..n	one entry per organization provided with keys
OIN	1	OIN of the authorized organization
formalName	0..1	optional formal registered name of the organization; for easier usage of the list
KeyProvisioningInstance	1..n	One or more (active) key set versions provided.
schemeKeySetVersion	1	Version (integer) of the scheme key set version of the key set provided.
keySetVersion	1	Version (integer) of the key set provided.
provisioningInstance	1	Timestamp of providing the key set.

Processing rules for KeyProvisioningList

The Sleutelverstrekkingslijst is for information only. When processing the list, an Authenticatiedienst or Toegangsdienst:

- SHOULD validate Signature of the published Sleutelverstrekkingslijst before processing it.
- SHOULD check that the published XML file is signed with a valid digital signature.
- SHOULD NOT process the message if it contains parts that are not signed with a valid digital signature.
- SHOULD process the Sleutelverstrekkingslijst periodically at a time that is predefined by the Beheerorganisatie BSNk.
- MAY verify the KeySetVersion for a Service Provider is listed before processing a request for a Encrypted Identifier / Encrypted Pseudonym or providing a Encrypted Identifier / Encrypted Pseudonym to a Service Provider.

XML-schema KeyProvisioningList

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
             xmlns="urn:nl-gdi-eid:1.0:schema"
             xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
             targetNamespace="urn:nl-gdi-eid:1.0:schema"
             elementFormDefault="qualified">

    <xs:import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLocation="xmldsig-core-schema.xsd"
/>

    <xs:element name="KeyProvisioningList" type="KeyProvisioningListType" />

    <xs:complexType name="KeyProvisioningListType">
        <xs:sequence>
            <xs:element ref="ds:Signature" />
            <xs:sequence minOccurs="0" maxOccurs="unbounded">
                <xs:element name="KeyProvisioning" type="KeyProvisioningType" />
            </xs:sequence>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID" use="required" />
        <xs:attribute name="publicationEnvironment" type="xs:string" use="required" />
        <xs:attribute name="publicationVersion" type="xs:nonNegativeInteger" use="required" />
        <xs:attribute name="publicationInstance" type="xs:dateTime" use="required" />
        <xs:attribute name="cacheDuration" type="xs:duration" use="optional" />
    </xs:complexType>

    <xs:complexType name="KeyProvisioningType">
        <xs:sequence>
            <xs:element name="OIN" type="OINType" />
            <xs:element name="formalName" type="xs:string" minOccurs="0"/>
            <xs:sequence minOccurs="1" maxOccurs="100">
                <xs:element name="KeyProvisioningInstance" type="KeyProvisioningInstanceType" />
            </xs:sequence>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="KeyProvisioningInstanceType">
        <xs:sequence>
            <xs:element name="schemeKeySetVersion" type="xs:integer" />
            <xs:element name="keySetVersion" type="xs:integer" />
            <xs:element name="provisioningInstance" type="xs:dateTime" />
        </xs:sequence>
    </xs:complexType>

    <xs:simpleType name="OINType">
        <xs:annotation>
            <xs:documentation>OIN type.</xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:length value="20" />
        </xs:restriction>
    </xs:simpleType>

</xs:schema>
```

XML example KeyProvisioningList

```
<KeyProvisioningList
    ID="_sp_keys"
    publicationEnvironment="test"
    publicationInstance="2016-11-30T16:00:00Z"
    publicationVersion="16"
    xmlns="urn:nl-gdi-eid:1.0:schema"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

    <ds:Signature>...</ds:Signature>

    <KeyProvisioning>
        <OIN>99999999012345670000</OIN>
        <KeyProvisioningInstance>
            <schemeKeySetVersion>1</schemeKeySetVersion>
            <keySetVersion>20161009</keySetVersion>
            <provisioningInstance>2016-12-01T14:11:36Z</provisioningInstance>
        </KeyProvisioningInstance>
        <KeyProvisioningInstance>
            <schemeKeySetVersion>1</schemeKeySetVersion>
            <keySetVersion>20160101</keySetVersion>
            <provisioningInstance>2016-07-01T07:21:45Z</provisioningInstance>
        </KeyProvisioningInstance>
    </KeyProvisioning>

    <KeyProvisioning>
        <OIN>99999999012345680000</OIN>
        <formalName>Voorbeeld instantie</formalName>
        <KeyProvisioningInstance>
            <schemeKeySetVersion>1</schemeKeySetVersion>
            <keySetVersion>20161124</keySetVersion>
            <provisioningInstance>2016-12-01T14:16:13Z</provisioningInstance>
        </KeyProvisioningInstance>
    </KeyProvisioning>

</KeyProvisioningList>
```

Processing rules

The Sleutelverstrekkingslijst is for information only, but when processed:

- validate Signature of the published Sleutelverstrekkingslijst before processing it.
- check that the published XML file is signed with a valid digital signature.
- NOT process the message if it contains parts that are not signed with a valid digital signature.
- process the Autorisatielijst BSN at any time

Privacy en Informatiebeveiliging

Dit hoofdstuk bevat in een viertal paragrafen een belangrijke kern van vereisten.

De volgende zaken worden beschreven:

- Betrouwbaarheidsniveaus — Deze paragraaf definieert de betrouwbaarheidsniveaus van Authenticatiemiddelen, de eisen betreffen de fasen van de levenscyclus van Authenticatiemiddelen.
- Privacy — Deze paragraaf bevat specifieke waarborgen voor de privacy van Gebruikers en de naleving van privacyregelgeving.
- Informatiebeveiliging — Deze paragraaf bevat de eisen aan de organisatorische, procedurele en meer technische informatiebeveiliging van de participanten. De paragraaf benoemt eisen aan het beheer van informatiebeveiliging en de focus van de te nemen beveiligingsmaatregelen. Daarnaast wordt vereist dat doeltreffende faciliteiten worden ingericht voor de detectie, melding en afhandeling van beveiligingsinbreuken en vermoedens van misbruik.
- Pseudonimisering — Deze paragraaf beschrijft de manier waarop met het toepassen van pseudonimisering de privacy van Gebruikers wordt beschermd.

Betrouwbaarheidsniveaus

Deze paragraaf definieert de betrouwbaarheidsniveaus van Authenticatiemiddelen, de eisen betreffen de fasen van de levenscyclus van Authenticatiemiddelen.

De aanvraag en uitreiking van een Authenticatiemiddel vereisen zorgvuldige procedures waaronder de controle van de identiteit van de aanvrager en de verificatie van zijn Persoonsidentificatiegegevens. Zeker gesteld moet worden dat identiteit die aan het Authenticatiemiddel wordt gekoppeld ook daadwerkelijk behoort bij de persoon aan wie het Authenticatiemiddel is uitgereikt.

De mogelijkheid moet bestaan dat Authenticatiemiddelen worden geschorst, ingetrokken en vernieuwd. Dit op wens van de gebruiker of naar aanleiding van geconstateerd misbruik of identiteitsdiefstal. Zeker gesteld moet worden dat schorsing, intrekking, reactivering en vernieuwing met de juiste mate van zorgvuldigheid is omgeven en op de juiste gronden plaatsvindt. Dit om ongewenste discontinuïteit van het middel maar ook identiteitsdiefstal te voorkomen.

Daarnaast zijn er in deze paragraaf vereisten opgenomen om de technische kwaliteit van Authenticatiemiddelen en het gebruik van het Authenticatiemiddel op het juiste niveau te waarborgen. Technologische ontwikkelingen scheppen nieuwe mogelijkheden voor bescherming van de Gebruiker maar ook voor cybercriminelen, daarom zijn er periodieke tests vereist van het Authenticatiemiddel en authenticatiemechanisme.

De eisen betreffen hier de Authenticatiemiddelen die aan natuurlijke personen worden verstrekt. De vereisten voor uitgifte van Authenticatiemiddelen aan natuurlijke personen die rechtspersonen vertegenwoordigen worden in de volgende fase ingevuld.

Deze paragraaf bevat eisen en interpretaties ter invulling en verduidelijking van de eIDAS uitvoeringsverordening EU 2015 / 1502 voor de organisaties die diensten leveren in de authenticatieketen. De tekst in de eIDAS kolommen is overgenomen uit de formele Nederlandstalige versie van de uitvoeringsverordening.

Leeswijzer

- 2.1.1 Aanvraag en Registratie (natuurlijke persoon) — Betreft de vereisten voor registratie van de natuurlijke persoon die voor zichzelf een authenticatiemiddel aanvraagt en gebruiksvoorwaarden.
- 2.1.2 Bewijs en verificatie identiteit (natuurlijk persoon) — Betreft de vereisten voor de verificatie van aangeleverde identiteitsinformatie.
- 2.2.1 Kenmerken en ontwerp van elektronische Identificatiemiddelen — De eisen in deze paragraaf betreffen specificaties voor het ontwerp van middelen in relatie tot het gebruik op elk Betrouwbaarheidsniveau.
- 2.2.2 Uitgifte, uitreiking en activering — Betreft de vereisen voor de manier waarop de Gebruiker zijn Authenticatiemiddel in bezit krijgt.
- 2.2.3 Schorsing, Herroeping en Reactivering — Betreft de vereisten voor het schorsen, verzoeken voor intrekking en reactivering van authenticatiemiddelen.
- 2.2.4 Verlenging en vervanging — Betreft de vereisten voor de levensduur van authenticatiemiddelen, de levensduur van de identificatie en vervanging/verlenging van authenticatiemiddelen
- 2.3.1 Authenticatiemechanisme — Deze paragraaf bevat de vereisten voor de betrouwbaarheid van alle handelingen die de gebruiker moet verrichten met zijn Authenticatiemiddel om in te kunnen loggen bij een Dienstverlener en de betrouwbaarheid van de elektronische communicatie tussen het Authenticatiemiddel en de Authenticatiedienst.

2.1.1 Aanvraag en Registratie (natuurlijke persoon)

Betreft de vereisten voor registratie van de natuurlijke persoon die voor zichzelf een authenticatiemiddel aanvraagt en gebruiksvoorwaarden.

Niveau betrouwbaarheid	eIDAS tekst uitvoeringsverordening	Nadere invulling en specificatie Uniforme Set van Eisen
Laag	1. De aanvrager moet bekend zijn met de voorwaarden die aan het gebruik van het elektronische identificatiemiddel zijn verbonden. 2. De aanvrager moet bekend zijn met de aanbevolen veiligheidsvoorzorgen die aan het gebruik van het elektronische identificatiemiddel zijn verbonden. 3. De relevante identiteitsgegevens die voor het bewijs en de verificatie van de identiteit vereist zijn, moeten zijn verzameld.	Geen nadere invulling of specificatie voor niveau laag.
Substantieel	Hetzelfde als niveau laag.	Ad 1 t/m 3 bij Laag en van toepassing op niveau Substantieel en Hoog. 1. Ad 1: De Middelenuitgever MOET de Gebruiker aantoonbaar bekend maken met de voorwaarden voor het gebruik van het Authenticatiemiddel. De voorwaarden MOETEN in elk geval betreffen: 1. geldigheidsduur van het middel, indien van toepassing. 2. de kosten van het middel. 3. procedures voor het schorsen, her-activeren, intrekken en vernieuwen van het middel. 2. Ad 2: De Middelenuitgever MOET de Gebruiker aantoonbaar bekend maken zijn met de veiligheidsvoorschriften voor het gebruik van het Authenticatiemiddel. De veiligheidsvoorschriften MOETEN in elk geval betreffen: 1. De verplichting voor gebruikers om vermoedens van misbruik of inbreuken op de veiligheid van het middel te melden aan de Middelenuitgever, opdat middelen tijdig geschorst of ingetrokken kunnen worden. 2. De verplichting voor gebruikers om hun middel niet door anderen te laten gebruiken en daarmee het geheimhouden van wachtwoorden, activeringscodes, pincodes en dergelijke. 3. Ad 3: De Middelenuitgever MOET Persoonsidentificatiegegevens verifiëren door registratie van het Authenticatiemiddel in het BSNk. De verificatie MOET plaats vinden met het BSN en een door het BSNk verplicht gestelde set van Persoonsidentificatiegegevens van de aanvrager. 4. De Middelenuitgever MOET het BSN en de overige te registreren zichtbare Persoonsidentificatiegegevens overnemen uit het WID van de aanvrager. 1. In elk geval MOET worden geregistreerd: 1. Voornamen 2. Achternaam 3. Geboortedatum 4. Geboorteplaats (optioneel) 2. De Middelenuitgever MAG het BSN na aanmelding bij het BSNk NIET archiveren. 5. Ad 3: De Middelenuitgever MOET gegevens registreren om in contact te kunnen treden met de juiste gebruiker van het middel. Toelichting bij 4: Nederlandse geldige identiteitsbewijzen die voorzien zijn van een BSN worden beschouwd als een betrouwbare afgeleide van de Basisregistratie Personen en daarmee een 'gezaghebbende bron' voor verificatie van Persoonsidentificatiegegevens. De over te nemen gegevens uit een WID betreffen de gegevens die zichtbaar zijn op het WID. Als een Authenticatiemiddel bruikbaar moet zijn in een andere EU lidstaat zullen de volledige voornamen geregistreerd moeten worden conform de eIDAS vereisten (EU 2015/1501). Deze verordening schrijft voor dat bij grensoverschrijdend gebruik ook de volledige voornamen als attribuut mee MOETEN worden geleverd. Opgemerkt wordt dat op het WID Rijbewijs slechts de eerste voornaam en eventuele verdere initialen zichtbaar zijn. Eisen 1 t/m 5 zijn van toepassing de Middelenuitgever.
Hoog	Hetzelfde als niveau laag.	Zelfde als niveau Substantieel

2.1.2 Bewijs en verificatie identiteit (natuurlijk persoon)

Betreft de vereisten voor de verificatie van aangeleverde identiteitsinformatie.

Niveau betrouwbaarheid	eIDAS tekst uitvoeringsverordening	Nadere invulling en specificatie Uniforme Set van Eisen
Laag	1. De persoon kan worden verondersteld in het bezit te zijn van bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt. 2. Het bewijs kan worden verondersteld echt te zijn, dan wel volgens een gezaghebbende bron te bestaan, en het bewijs lijkt geldig te zijn. 3. Een gezaghebbende bron weet dat de opgegeven identiteit bestaat en er kan worden ver-ondersteld dat de persoon die de identiteit opgeeft, dezelfde persoon is.	Geen nadere invulling of specificatie.

Substantieel	Niveau laag plus één van de onder de punten 1 tot en met 4 vermelde alternatieven.
	
	1. Er is geverifieerd dat de persoon in het bezit is van bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt;
	
	en
	
	het bewijs is gecontroleerd op de echtheid ervan; of het bestaan ervan is volgens een gezaghebbende bron bekend en het heeft betrekking op een werkelijk bestaande persoon;
	
	en
	
	er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat het bewijsstuk verloren, gestolen, geschorst, ingetrokken of verlopen is.
	
	of
	
	2. Er is een identiteitsdocument overgelegd tijdens een registratieproces in de lidstaat waar het document is afgegeven, en het document lijkt betrekking te hebben op de persoon die het heeft overgelegd;
	
	en
	
	er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat documenten verloren, gestolen, geschorst, ingetrokken of verlopen zijn.
	
	of
	
	3. Indien procedures die eerder door een publieke of private entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria die gelijkwaardig zijn aan die van punt 2.1.2 voor het betrouwbaarheidsniveau substantieel, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad (1) of een daaraan gelijkwaardige instantie.
	
	of
	
	4. Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau substantieel of hoog, is het, rekening houdend met het risico van een wijziging van de persoonsidentificatiegegevens, niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau substantieel of hoog worden bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie.
		1. Ad 1 en 2 De Middelenuitgever MOET een Gebruiker (het BSN van) activeren bij het BSNk zoals beschreven in AUC1 Activeren BSN.
		    1. De Middelenuitgever MOET het Polymorfe Pseudoniem dat hij bij activering van de Gebruiker terug krijgt veilig opslaan op een eigen beveiligde systeem of op een beveiligd authenticatiemiddel (secure device) van de Gebruiker.
		2. Ad 1 en 2 De Middelenuitgever MOET de status van de abonnee-relatie registreren bij het BSNk met behulp van AUC2 Registreren status authenticatiemiddel.
		3. Ad 1 en 2 De Middelenuitgever MOET het risico mitigeren dat een Authenticatiemiddel wordt uitgegeven op basis van een vervalst, ongeldig wettelijk identiteitsdocument (WID) of aan een persoon die niet behoort bij het identiteitsdocument. Dit betekent dat:
		    1. De Middelenuitgever personele en technische faciliteiten in MOET richten om de echtheid en geldigheid van identiteitsbewijzen adequaat te controleren en om personen te identificeren aan de hand van een WID.
		    2. De door de Middeluitgever gebruikte identificatiemethoden moeten gelijkwaardig zijn aan een fysieke identiteitscontrole tegen een WID document.
		4. Ad 3 en 4. De bedoelde conformiteitsbeoordelingsinstanties MOETEN zijn geaccrediteerd voor de toetsing van de Uniforme Set van Eisen.
		5. Ad 3 en 4 De Middelenuitgever MOET bij de uitgifte van een Authenticatiemiddel op basis van een bestaand Authenticatiemiddel de Persoonsidentificatiegegevens die in paragraaf 2.1.1 zijn opgenomen registreren. Dit geldt eveneens voor de registratie van het middel bij het BSNk koppelregister. Dit betekent:
		    1. De Middelenuitgever MOET voor de uitgifte van middelen op basis van bestaande middelen beschikken over de gevalideerde Persoonsidentificatiegegevens die nodig zijn voor de uitgifte van een Authenticatiemiddel .
		    2. De Middelenuitgever MOET de actuele juistheid verifiëren van de verstrekte attributen van de gebruiker.
		    3. De Middelenuitgever MOET zich ervan vergewissen dat de persoon die behoort bij de gevalideerde attributen daadwerkelijk over het middel beschikt dat wordt gebruikt om een nieuw middel aan te vragen.
		
		Toelichting bij eisen 1 t/m 5: De Basisregistratie Personen is in Nederland de gezaghebbende bron waartegen Persoonsidentificatiegegevens geverifieerd mogen worden. De verificatie moet in elk geval worden uitgevoerd door registratie van een elektronische identificatiemiddel bij het BSNk. Nederlandse geldige identiteitsbewijzen die voorzien zijn van een BSN worden beschouwd als een betrouwbare afgeleide van de Basisregistratie Personen en daarmee een ‘gezaghebbende bron’ voor verificatie van de Persoonsidentificatiegegevens.
		
		Eisen 1, 2, 3 en 5 zijn van van toepassing op de Middelenuitgever
		
		Eis 4 is van toepassing op de Middelenuitgever en Authenticatiedienst

Hoog	Er moet zijn voldaan aan de vereisten van punt 1 of punt 2. 1. Niveau substantieel plus een van de onder a) tot en met c) vermelde alternatieven. 1. Indien is geverifieerd dat de persoon in het bezit is van een bewijs dat voorzien is van een foto of biometrische gegevens, dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt, wordt het bewijs gecontroleerd op geldigheid aan de hand van een gezaghebbende bron; en de door de aanvrager opgegeven identiteit wordt geverifieerd door vergelijking van één of meer fysieke kenmerken van de persoon met een gezaghebbende bron. of b. Indien procedures die eerder door een publieke of private entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria die gelijkwaardig zijn aan die van punt 2.1.2 voor het betrouwbaarheidsniveau hoog, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie; en er zijn maatregelen getroffen om aan te tonen dat de resultaten van de eerdere procedures nog steeds geldig zijn. of c. Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau hoog, is het, rekening houdend met het risico van een wijziging van de persoonsidentificatiegegevens, niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau hoog worden bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie; en er zijn maatregelen getroffen om aan te tonen dat de resultaten van deze eerdere uitgifteprocedure van een aangemeld elektronisch identificatiemiddel nog steeds geldig zijn. OF 2. Indien de aanvrager geen erkend identiteitsdocument met een foto of biometrische kenmerken overlegt, worden dezelfde procedures toegepast die op nationaal niveau van toepassing zijn in de lidstaat van de verantwoordelijke instantie voor de verkrijging van een dergelijk bewijsstuk met foto of biometrische kenmerken.	Niveau substantieel, plus 1. De Middelenuitgever MOET bij uitgifte van een middel op basis van een bestaand middel naast de eisen voor niveau Substantieel in punt 5 ook de volgende eis toepassen: 1. De validatie van het bezit van het middel en actuele juistheid van de attributen MOET onder de supervisie van een medewerker van de uitgever van het middel staan en het resultaat MOET door een medewerker worden bevestigd. 2. Ad 2 De verstrekking van een WID is voorbehouden aan de daartoe wettelijke aangewezen bestuursorganen. De Middelenuitgever MOET de identiteit van aanvragers van authenticatiemiddelen verifiëren aan de hand van identiteitsbewijzen die door de Nederlandse Staat zijn erkend. Toelichting bij 1: Het uitgeven van een middel op basis van een bestaand middel mag niet een volledig geautomatiseerd proces zijn. Eisen 1 en 2 zijn van toepassing op de Middelenuitgever.

Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 (PB L 218 van 13.8.2008, blz. 30).

2.2.1 Kenmerken en ontwerp van elektronische Identificatiemiddelen

De eisen in deze paragraaf betreffen specificaties voor het ontwerp van middelen in relatie tot het gebruik op elk Betrouwbaarheidsniveau.

Niveau betrouwbaarheid	eIDAS tekst uitvoeringsverordening	Nadere invulling en specificatie Uniforme Set van Eisen
Laag	1. Het elektronische identificatiemiddel maakt gebruik van ten minste één authenticatiefactor. 2. Het elektronische identificatiemiddel is zodanig ontworpen dat de uitgever ervan redelijke stappen onderneemt om te verifiëren dat het slechts wordt gebruikt door of onder controle van de persoon aan wie het toebehoort.	Geen nadere invulling of specificatie.
Substantieel	1. Het elektronische identificatiemiddel maakt gebruik van ten minste twee authenticatiefactoren die tot verschillende categorieën behoren. 2. Het elektronische identificatiemiddel is zodanig ontworpen dat het kan worden verondersteld slechts te worden gebruikt door of onder controle van de persoon aan wie het toebehoort.	1. Ad2 Een eenmaal uitgegeven Authenticatiemiddel MAG NIET aan een andere identiteit worden gekoppeld. Naleving van deze eis MOET worden aangetoond door gedocumenteerde procedures voor het gecontroleerd uitgeven van authenticatiefactoren, wijzigen van Persoonsidentificatiegegevens en het vastleggen van uitgiftes en wijzigingen (AO/IC) Eis 1 is van toepassing op de Middelenuitgever
Hoog	Niveau substantieel, plus: 1. Het elektronische identificatiemiddel biedt bescherming tegen kopiëring en vervalsing en tegen aanvallers met een hoog aanvalspotentieel. 2. Het elektronische identificatiemiddel is zodanig ontworpen dat het door de persoon aan wie het toebehoort op betrouwbare wijze kan worden beschermd tegen gebruik door anderen.	Zelfde als niveau substantieel, plus: 1. Het correct functioneren van het Authenticatiemiddel MOET weerstand bieden tegen fysieke en logische manipulatie door een aanvaller met een 'hoog aanvalspotentieel' (high attacker potential) in de zin van de Common Criteria (ISO 15408-3) en de bijbehorende evaluatienorm (ISO/IEC 18045 Annex B). 1. De validatie van de weerstand MOET worden bevestigd door een ter zake deskundige en onafhankelijke beoordelende instantie. 2. De Middelenuitgever MOET de beoordelende instantie bedoeld in 1a minimaal 1 maal per 3 jaar en bij wijzigingen aan het Authenticatiemiddel of de werking daarvan, de weerstand van het middel tegen een 'hoog aanvalspotentieel' laten valideren. 3. De eisen aan de beoordelende instantie zoals is bedoeld in 1a en 1b zijn opgenomen in de paragraaf Compliance en audit. Toelichting: De validatie van de weerstand tegen een hoog aanvalspotentieel kan worden uitbesteed aan een andere organisatie dan de geaccrediteerde certificerende instelling voor de Uniforme Set van Eisen. In dat geval bepaalt de geaccrediteerde certificerende instelling voor de Uniforme Set van Eisen of het bewijs van de validatie kan worden geaccepteerd en onderdeel kan worden van het conformiteitsrapport. Eis 1 is van toepassing op de Middelenuitgever.

2.2.2 Uitgifte, uitreiking en activering

Betreft de vereisen voor de manier waarop de Gebruiker zijn Authenticatiemiddel in bezit krijgt.

Niveau betrouwbaarheid	eIDAS tekst uitvoeringsverordening	Nadere invulling en specificatie Uniforme Set van Eisen

Laag	Na de uitgifte wordt het elektronische identificatiemiddel uitgereikt via een mechanisme waarmee het kan worden verondersteld alleen de beoogde persoon te bereiken.	Geen nadere invulling of specificatie
Substantieel	Na de uitgifte wordt het elektronische identificatiemiddel uitgereikt via een mechanisme waarmee kan worden verondersteld dat alleen de persoon aan wie het toebehoort in het bezit ervan wordt gesteld.	1. De Middelenuitgever en Authenticatiedienst MOETEN de Gebruiker bekend maken met het proces voor uitgifte, uitreiking en activering. De Gebruiker MOET met deze kennis in staat gesteld te worden afwijkingen te ontdekken in het proces. 1. Gebruiker MOET geïnformeerd worden over het moment van verstrekking van één of meerdere authenticatiefactoren via door gebruiker opgegeven of door de gebruiker beheerde contactgegevens. 2. Gebruiker MOET in staat worden gesteld om met een vermoeden van afwijking in het proces van uitgifte, uitreiking en activering in contact te treden met de Middelenuitgever respectievelijk de Authenticatiedienst. 3. Voor uitgifte van authenticatiefactoren MOETEN persoonlijke contactgegevens worden gebruikt, het gebruikt van postbusnummers of algemene bedrijfsadressen MOET worden uitgesloten. 2. De authenticatiefactoren MOETEN afzonderlijk worden verstrekt via gescheiden kanalen of gescheiden in tijd. 3. Als een activatiecode wordt verstrekt MOET de bruikbaarheid daarvan beperkt zijn tijd. 4. De activatie van het middel bij de Authenticatiedienst MOET het nodig maken dat het middel door de Gebruiker wordt gebruikt. Toelichting bij 3 en 4: In het geval de rollen van Middelenuitgever en Authenticatiedienst door afzonderlijke Participanten worden vervuld kan het proces van uitgifte van het middel gescheiden zijn van het proces activatie bij de Authenticatiedienst. Daarnaast kan een middel bij meerdere authenticatiediensten gebruikt worden. De waarborg MOET daarom zijn dat de activatie van een middel bij een Authenticatiedienst altijd een wilsuiting van de Gebruiker MOET bevatten. Een Middelenuitgever ZOU MOETEN waarborgen dat een vorm van zijn toestemming nodig is om een Authenticatiemiddel bij een Authenticatiedienst te activeren. Eis 1 t/m 4 zijn van toepassing op de Middelenuitgever en de Authenticatiedienst.
Hoog	Bij het activeringsproces wordt geverifieerd dat slechts de persoon aan wie het elektronische identificatiemiddel toebehoort ervan in het bezit wordt gesteld.	Zelfde als bij niveau Substantieel m.u.v. punt 2 1. De Middelenuitgever MOET de authenticatiefactoren afzonderlijk verstrekken via gescheiden kanalen of gescheiden in tijd. De verstrekking aan de Gebruiker MOET plaatsvinden met eenzelfde betrouwbaarheid als het identificatieproces voor Betrouwbaarheidsniveau Hoog. Eis 1 is van toepassing op de Middelenuitgever.

2.2.3 Schorsing, Herroeping en Reactivering

Betreft de vereisten voor het schorsen, verzoeken voor intrekking en reactivering van authenticatiemiddelen.

Niveau betrouwbaarheid	eIDAS tekst uitvoeringsverordening	Nadere invulling en specificatie Uniforme Set van Eisen
Laag	1. Het is mogelijk het elektronische identificatiemiddel snel en doeltreffend te schorsen en/ of te herroepen. 2. Er bestaan maatregelen om ongeoorloofde schorsing, herroeping en reactivering te voorkomen. 3. Een elektronisch identificatiemiddel mag slechts worden gereactiveerd indien nog steeds wordt voldaan aan dezelfde betrouwbaarheidsvereisten als die welke voorafgaand aan de schorsing of herroeping van kracht waren.	Geen nadere invulling of specificatie.

Substantieel	Zelfde als niveau laag.	Addenda bij Laag van toepassing op niveau Substantieel
		
		1. Ad 1 De Middelenuitgever respectievelijk de Authenticatiedienst MOET bij gerede vermoedens van misbruik, fraude of vermissing een Authenticatiemiddel of de authenticatiefunctie op het middel intrekken of schorsen.
		2. Ad 1 De Middelenuitgever en MOET de procedure voor schorsing, intrekking en reactivering publiceren. De procedure MOET in elk geval bevatten:
		    1. Wie gerechtigd is om het verzoek te doen, dit zijn in elk geval:
		        1. de gebruiker zelf en;
		        2. de bevoegde vertegenwoordiger van de gebruiker en;
		        3. de bevoegde medewerker van de Middelenuitgever of de Authenticatiedienst.
		    2. De weg waarlangs het verzoek gedaan moet worden;
		    3. De urgentie van verzoeken faciliteren;
		    4. De verplichting voor de gebruiker om de reden voor het verzoek in het verzoek op te nemen.
		3. De Middelenuitgever en de Authenticatiedienst MOETEN binnen 24 uur na een verzoek is gedaan volgens de gepubliceerde procedure, betrouwbaar vaststellen dat het verzoek afkomstig is van de juist persoon zoals bedoeld in 2a.
		4. De Middelenuitgever en Authenticatiedienst MOETEN binnen 60 minuten nadat is geconcludeerd dat het verzoek door de juist persoon is gedaan het verzoek tot schorsing, intrekking of reactivering uitgevoerd hebben.
		5. Ad 3 De Middelenuitgever en Authenticatiedienst MOETEN in geval van schorsingen kiezen voor één van de volgende procedures van her-activatie waarbij:
		    1. het identificatieproces wordt gevolgd dat is gebruikt voor de uitgifte van het Authenticatiemiddel of;
		    2. wordt vastgesteld dat de gebruiker nog in bezit is van een authenticatiefactor van het Authenticatiemiddel en waarbij een back-up authenticatiefactor wordt ingevoerd door de gebruiker. De back-up authenticatiefactor MOET met dezelfde betrouwbaarheid als de primaire factor zijn uitgereikt. Of;
		    3. een tweede Authenticatiemiddel van de gebruiker wiens eerste middel is geschorst wordt ingezet.
		6. Ad 3 Een middel dat na onderzoek blijkt ten onrechte op initiatief van de Middelenuitgever respectievelijk de Authenticatiedienst te zijn geschorst MAG door de Middelenuitgever respectievelijk de Authenticatiedienst worden gereactiveerd.
		7. Ad 2 en 3 De Middelenuitgever en Authenticatiedienst MOETEN verzoeken tot- en de uitvoering van schorsingen, intrekkingen en reactiveringen loggen met het oog op onderzoek van misbruik en geschillen. De logging MOET actief worden geanalyseerd.
		
		Toelichtend: punten 2, 3 en 4 zijn deels ontleent aan de norm ETSI EN 319411-1 voor gekwalificeerde certificaten, par 6.2.4 Identification en authentication for revocation request.
		
		Eisen in punten 1 t/m 7 zijn van toepassing op Middelenuitgever en Authenticatiedienst

Hoog	Zelfde als niveau laag.	Zelfde als niveau Substantieel.

2.2.4 Verlenging en vervanging

Betreft de vereisten voor de levensduur van authenticatiemiddelen, de levensduur van de identificatie en vervanging/verlenging van authenticatiemiddelen

Niveau betrouwbaarheid	eIDAS tekst uitvoeringsverordening	Nadere invulling en specificatie USvE

Laag	Rekening houdend met het risico dat de persoonsidentificatiegegevens zijn gewijzigd, moet voor verlenging of vervanging aan dezelfde betrouwbaarheidsvereisten zijn voldaan als voor het initiële proces van bewijs en verificatie van de identiteit, of moet worden uitgegaan van een geldig elektronisch identificatiemiddel met hetzelfde of een hoger betrouwbaarheidsniveau.	Geen nadere invulling of specificatie
Substantieel	Zelfde als niveau laag.	1. De Middelenuitgever MOET minimaal 1 maal per 5 jaar de juistheid verifiëren van de geregistreerde Persoonsidentificatiegegevens van de gebruiker. 2. De Middelenuitgever MOET de gebruiker verplichten tot het actueel houden van zijn contactgegevens. 3. Indien de Middelenuitgever één enkele authenticatiefactor vervangt, MOET de uitgifte daarvan met dezelfde betrouwbaarheid plaatsvinden als de initiële uitgifte van die authenticatiefactor. Toelichting bij 1: De verificatie vindt initieel plaats door verificatie van het pseudoniem bij het BSNk waarbij het BSNk de actualiteit van het BSN verifieert. In latere fase ontwikkelt het BSNk ook de mogelijkheid om andere attributen zoals voornamen en achternaam op actualiteit worden gecontroleerd. Eisen 1 t/m 3 zijn van toepassing op de Middelenuitgever.
Hoog	Niveau laag, plus: Als voor verlenging of vervanging wordt uitgegaan van een geldig elektronisch identificatiemiddel, worden de identiteitsgegevens geverifieerd aan de hand van een gezaghebbende bron.	Zelfde als niveau substantieel.

2.3.1 Authenticatiemechanisme

Deze paragraaf bevat de vereisten voor de betrouwbaarheid van alle handelingen die de gebruiker moet verrichten met zijn Authenticatiemiddel om in te kunnen loggen bij een Dienstverlener en de betrouwbaarheid van de elektronische communicatie tussen het Authenticatiemiddel en de Authenticatiedienst.

Niveau betrouwbaarheid	eIDAS tekst uitvoeringsverordening	Nadere invulling en specificatie Uniforme Set van Eisen
Laag	1. Alvorens persoonsidentificatiegegevens worden vrijgegeven, worden het elektronische identificatiemiddel en de geldigheid ervan op betrouwbare wijze geverifieerd. 2. Indien als onderdeel van het authenticatiemechanisme persoonsidentificatiegegevens worden opgeslagen, wordt die informatie beveiligd ter bescherming tegen verlies en schending, met inbegrip van offline analyse. 3. Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, her-afspelen of manipuleren van communicatie door een aanvaller met een laag aanvalspotentieel.	
Substantieel	Niveau laag, plus:	Addenda bij Laag en van toepassing op niveau Substantieel en Hoog

1. Alvorens persoonsidentificatiegegevens worden vrijgegeven, worden het elektronische identificatiemiddel en de geldigheid ervan op betrouwbare wijze geverifieerd door middel van dynamische authenticatie.
2. Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, her-afspelen of manipuleren van communicatie door een aanvaller met een gematigd aanvalspotentieel.

1. Ad 2 De Participant MOET waarborgen dat persoonsidentificatiegegevens wordt beschermd conform het bepaalde in de paragraaf Privacy.
2. Ad 2 Een Toegangsdienst MAG de individuele gegevens van Gebruikers over verschillende Dienstverleners heen NIET met elkaar correleren.

Eis 1 is van toepassing op alle Participanten

Eis 2 is van toepassing op Participant: Toegangsdienst

Addenda bij Substantieel en ook van toepassing op niveau Hoog

1. Ad 1 Elke Participant MOET waarborgen dat de afhandeling van een Authenticatieverzoek minimaal voldoet aan de eisen voor het Betrouwbaarheidsniveau van het betreffende authenticatieverzoek.
2. Ad 1 De Middelenuitgever MOET de Authenticatiedienst de relevante informatie verstrekken om authenticaties van het juiste betrouwbaarheidsniveau te kunnen realiseren.
3. Ad1 De Authenticatiedienst MOET waarborgen dat:
    1. zowel de identificatie (i.c. het gebruikte Authenticatiemiddel) als het proces van de authenticatie minimaal het door de Dienstverlenergew enste Betrouwbaarheidsniveau heeft.
    2. dat het Authenticatiemiddel geldig is op het moment van authenticatie met een geldigheidscontrole bij de Middelenuitgever.
4. Ad 1 De Authenticatiedienst MAG NIET andere dan de door de Minister erkende Betrouwbaarheidsniveaus toepassen in het publieke domein.
5. Ad 2 De Authenticatiedienst MOET de Gebruiker bij gebruik van zijn middel notificeren (berichten) dat hij op het punt staat in te loggen op een specifieke Dienstverlener en, indien van toepassing, een specifieke door de Dienstverlener geregistreerde Dienst.
    1. De Gebruiker MOET in staat gesteld worden om met deze informatie het inloggen af te breken.
    2. Het authenticatiemechanisme MOET de Gebruiker betrouwbaar notificeren dat er sprake is van een Uniforme Set van Eisen -authenticatie.
    3. De notificatie MOET ook betrouwbaar zijn als applicatie waarvoor de authenticatie bestemd is of het platform waarop deze applicatie actief is, gecorrumpeerd is.
    4. De Toegangsdienst MOET waarborgen dat de Dienstverlener de naam van zijn organisatie en zijn dienst bij aansluiting op de Toegangsdienst zodanig registreert dat deze herkenbaar voor de Gebruiker getoond kan worden.
6. Ad 2 De Authenticatiedienst MOET de Gebruiker in staat stellen met adequate informatie over uitgevoerde informatietransacties in contact te treden met een Dienstverlener over afwijkende transacties of mogelijke geschillen ten aanzien van transacties:
    1. In paragraaf 'Informatie voor gebruikers' zijn de verplichtingen opgenomen voor de Authenticatiedienst om gebruikers inzage te bieden in transacties die hij heeft uitgevoerd met zijn middel om daarmee afwijkend gebruik van zijn middel te ontdekken;
    2. De Authenticatiedienst MOET met de Gebruiker in contact treden zodra de Authenticatiedienst gerede vermoedens heeft van misbruik van het middel van de Gebruiker. De Authenticatiedienst ZOU ten behoeve van zelfcontrole een Gebruiker tijdens het authenticatieproces MOETEN informeren over een Opmerkelijke gebeurtenis;
    3. Het contact met de Gebruiker MOET plaatsvinden via een ander kanaal dan het middel van de Gebruiker.
7. Ad 2 De Authenticatiedienst MOET waarborgen hij een reeds uitgevoerde authenticatie niet opnieuw gebruikt voor een her-authenticatie bij zelfde dienstverlener of aanloggen bij een andere dienstverlener.
8. Ad 2 Het correct functioneren van het authenticatiemechanisme MOET weerstand bieden tegen fysieke en logische manipulatie door een aanvaller met een 'gematigd aanvalspotentieel' (moderate attacker potential) in de zin van de Common Criteria (ISO 15408-3) en de bijbehorende evaluatienorm (ISO/IEC 18045 Annex B).
    1. De weerstand tegen het aanvalspotentieel MOET worden bevestigd door ter deskundige en onafhankelijke beoordelende instantie. De eisen aan deze beoordelende instantie zijn opgenomen in de paragraaf Compliance en audit.
    2. De Authenticatiedienst respectievelijk de Middelenuitgever MOET de weerstand tegen het aanvalspotentieel minimaal 1 maal per 3 jaar en bij wijzigingen aan het authenticatiemechanisme, de werking daarvan en publicatie van relevante technische kwetsbaarheden laten valideren.
9. Ad2 De Toegangsdienst MOET de Dienstverlener de verklaringen aanleveren conform de in de Uniforme Set van Eisen vastgelegde Interface specifications.
10. Ad2 De Toegangsdienst MOET een veilig, betrouwbaar, laagdrempelig proces inrichten voor Dienstverleners om een fouten en misbruik te melden, te onderzoeken en te herstellen.

		Toelichting bij punt 5: Een Dienstverlener kan besluiten om al zijn diensten via een portaal te ontsluiten of als afzonderlijke Dienst. De eis om zowel de Dienst als de Dienstverlener aan de Gebruiker te tonen heeft tot doel om de Gebruiker optimaal te informeren over authenticaties die al dan niet mogelijke rechtsgevolgen kunnen hebben. Daarnaast beoogt deze een Dienstverlener te ontzorgen bij vertegenwoordiging van de Gebruiker voor specifieke handelingen bij de Dienstverlener. Het tweede deel van de eis betreft eisen aan de betrouwbaarheid van het bericht aan de Gebruiker. Eis 1 is van toepassing op alle participanten Eis 2 is van toepassing op de Middelenuitgever Eisen 3 t/m 7 zijn van toepassing op de Authenticatiedienst Eis 8 is van toepassing op de Authenticatiedienst en de Middelenuitgever Eisen 5d, 9 en 10 zijn van toepassing op de Toegangsdienst
Hoog	Niveau substantieel, plus: Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, her afspelen of manipuleren van communicatie door een aanvaller met een hoog aanvalspotentieel.	Niveau substantieel met uitzondering van punt 8, plus; 1. Het correct functioneren van het authenticatiemechanisme MOET weerstand bieden tegen fysieke en logische manipulatie door een aanvaller met een 'hoog aanvalspotentieel' (high attacker potential) in de zin van de Common Criteria (ISO 15408-3) en de bijbehorende evaluatienorm (ISO/IEC 18045 Annex B). 1. Het authenticatiemechanisme MOET een betrouwbaar kanaal bevatten voor notificatie van de inlogpoging van de gebruiker en de bevestiging van het authenticatieverzoek door de Gebruiker. Deze notificatie geeft de Gebruiker aan dat deze op het punt staat in te loggen op een een specifieke Dienstverlener en, indien van toepassing, een specifieke door de Dienstverlener geregistreerde Dienst. De Gebruiker MOET in staat gesteld worden om met deze informatie het inloggen af te breken. Het kanaal MOET ook betrouwbaar zijn als applicatie waarvoor de authenticatie bestemd is of het platform waarop deze applicatie actief is, gecorrumpeerd is. 2. De weerstand tegen het aanvalspotentieel MOET worden bevestigd door ter zake deskundige en onafhankelijke beoordelende instantie. De eisen aan deze beoordelende instantie zijn opgenomen in de paragraaf Compliance en audit. 3. De Authenticatiedienst respectievelijk de Middelenuitgever MOET de weerstand tegen het aanvalspotentieel minimaal 1 maal per 3 jaar de werking daarvan en publicatie van relevante technische kwetsbaarheden laten valideren. Toelichting bij punt 1a: Een Dienstverlener kan besluiten om al zijn diensten via een portaal te ontsluiten of als afzonderlijke Dienst . De eis om zowel de Dienst als de Dienstverlener aan de Gebruiker te tonen heeft tot doel om de Gebruiker optimaal te informeren over authenticaties die al dan niet mogelijke rechtsgevolgen kunnen hebben. Daarnaast beoogt deze een Dienstverlener te ontzorgen bij vertegenwoordiging van de Gebruiker voor specifieke handelingen bij de Dienstverlener. Het tweede deel van de eis betreft eisen aan de betrouwbaarheid van het bericht aan de Gebruiker. Eisen in punt 1 zijn van toepassing op Authenticatiedienst en Middelenuitgever.

De validatie van de weerstand tegen een hoog aanvalspotentieel kan worden uitbesteed aan een andere organisatie dan de geaccrediteerde certificerende instelling voor de Uniforme Set van Eisen. In dat geval bepaalt de geaccrediteerde certificerende instelling voor de Uniforme Set van Eisen of het bewijs voor de validatie kan worden geaccepteerd en opgenomen wordt in zijn rapport over de naleving van Uniforme Set van Eisen door de Participant of kandidaat participant.

Privacy

Deze paragraaf bevat specifieke waarborgen voor de privacy van Gebruikers en de naleving van privacyregelgeving.

Belangrijke context voor de opname van een deel van de maatregelen is dat dit hoewel ze zijn afgeleid van wettelijke vereisten, toch nodig is als handvat voor pro-actieve controle door de Toezichthouder op de naleving van de Uniforme Set van Eisen.

De eisen volgen het uitgangspunt 'Privacy by design' en omvatten onderwerpen als dataminimalisatie, vermijden van privacy-hotspots, de toepassing van PSA: Privacy Enhancing Technology en het beperken van de privacy-impact van incidenten.

Eisen aan alle participanten

1. De Participant MOET verantwoordelijkheid nemen voor het daadwerkelijk voldoen aan de bepalingen in de Wbp/Europese verordening 2016/679 ongeacht hetgeen hieronder is aangegeven.
2. De Participant MOET, in relatie tot de diensten die hij levert in de Authenticatieketen, processen ingericht hebben waarmee hij in continuïteit de naleving waarborgt van de bepalingen van de Wbp/Europese verordening. De processen hebben minimaal betrekking op:
    1. De inventarisatie en vastlegging van de verwerking van persoonsgegevens. De vastlegging bevat per gegeven de doelbinding, de rechtmatigheidsgrondslag en de noodzaak voor de verwerking gezien het doel. De volgende doelen MOETEN worden onderscheiden:
        1. Identificatie en authenticatie: dit betreft gegevens die noodzakelijk zijn om authenticatiemiddelen uit te geven en gebruikers in staat te stellen zicht zich te laten authenticeren bij dienstverleners;
        2. Verantwoording: dit betreft gegevens die noodzakelijk zijn om de naleving van de Wet GDI en Uniforme Set van Eisen aan te tonen;
        3. Geschilbeslechting: dit betreft gegevens die noodzakelijk zijn om om geschillen tussen een Gebruiker en een Dienstverlener over juistheid of rechtmatigheid van een informatietransactie te kunnen beslechten;
        4. Foutopsporing en correctie; dit betreft gegevens die noodzakelijk zijn om technische foutieve bewerkingen van systemen te kunnen opsporen en te herstellen;
        5. Misbruikbestrijding; dit betreft gegevens die noodzakelijk zijn om misbruik van een authenticatiemiddel door een onbevoegde derde, misbruik met een authenticatiemiddel door de Gebruiker en de onbevoegde manipulatie van systemen en data van de Participant te detecteren en te onderzoeken.
    2. Het uitvoeren van Privacy Impact Analyse (PIA) voorafgaande aan de introductie van een nieuwe dienst of bij wijzigingen aan een bestaande dienst.
    3. Het waarborgen van de opvolging van aanbevelingen die uit een uitgevoerde PIA volgen.
    4. Het waarborgen dat de verplichting tot het melden van datalekken in relatie is gebracht met het proces van incidentmanagement.
    5. Het waarborgen van de bepalingen uit de Wbp/Europese verordening 2016/679 zoals de informatieplicht en informatieverstrekking aan derden, rechten van betrokkenen en bewaartermijnen.
    6. Het waarborgen van de beveiliging van de verwerking en opslag van persoonsgegevens door:
        1. Het beheersen van privacy-risico's onderdeel te maken van het beheerssysteem voor de informatiebeveiliging zoals bedoeld in de eisen voor Informatiebeveiliging;
        2. Beperken van de toegang tot persoonsgegevens, in elk geval de Persoonsidentificatiegegevens en de informatietransacties (inlog-historie), van gebruikers tot personeel dat contact met de gebruiker MOETEN onderhouden en personeel dat de specifieke bevoegdheid heeft gekregen om vermoedens van misbruik te onderzoeken;
        3. Het vastleggen van de toegang tot- en verwerking van- de bedoelde persoonsgegevens door het personeel zoals bedoeld in punt ii en de actieve periodieke controle van de rechtmatigheid van de gezochte toegang en verwerking door het betrokken personeel zoals bedoeld in punt ii;
        4. het implementeren van doeltreffende technische maatregelen voor de beveiliging van persoonsgegevens.

7. Het waarborgen van de juistheid van verwerkte persoonsgegevens.
8. Het waarborgen dat het gebruik van de gearchiveerde gegevens beperkt blijft tot de gedefinieerde doelen in 2a.

3. De Participant MOET Persoonsidentificatiegegevens van de Gebruiker en de gegevens over het gebruik van het Authenticatiemiddel door de gebruiker gescheiden opslaan. De relatie tussen de gegevens in beide bestanden van elke Gebruiker MOET zijn beveiligd. Het doorbreken van deze beveiliging MOET een gespecificeerde handeling van bevoegd personeel vergen. De bevoegdheid van de uitvoering van deze handeling MOET doeltreffend worden gecontroleerd.
4. De Participant MOET een verantwoordelijke aanwijzen die belast is met de actieve monitoring van de naleving van de bovenstaande punten.
5. De Middelenuitgever MOET zijn privacyverklaring tonen aan de Gebruiker voorafgaand zijn wilsuiting om het Authenticatiemiddel af te nemen en online en openbaar publiceren.
6. De Authenticatiedienst MOET zijn privacyverklaring tonen aan de Gebruiker van een Authenticatiemiddel voorafgaande aan zijn wilsuiting om zijn Authenticatiemiddel bij de Authenticatiedienst te activeren en online en openbaar publiceren.
7. De Toegangsdienst MOET zijn privacyverklaring online en openbaar publiceren.
8. De Participant MOET een verantwoordelijke aanwijzen de namens organisatie verantwoording aflegt aan de Toezichthouder over de naleving van bovenstaande punten.

Toelichting bij punt 3: Participanten hebben tijd nodig om om aan deze eis voor scheiding van gebruiks- en Persoonsidentificatiegegevens van de Gebruiker te voldoen. Hiermee moet rekening gehouden worden wanneer de Uniforme Set van Eisen onderdeel wordt van de aansluitvoorwaarden van het BSNk.

Good Practice: Gebruiksgegevens (inlog-historie) wordt en opgeslagen met een Participant-specifiek-pseudoniem dat na gebruik (bijv. inzage in gebruikshistorie) meteen weer weggegooid wordt. Elke gegeven wordt ook nog versleuteld m.b.v. een sleutel die is afgeleid van het Participant-specifiek-pseudoniem (incl. het pseudoniem zelf).

Informatiebeveiliging

Deze paragraaf bevat de eisen aan de organisatorische, procedurele en meer technische informatiebeveiliging van de participanten. De paragraaf benoemt eisen aan het beheer van informatiebeveiliging en de focus van de te nemen beveiligingsmaatregelen. Daarnaast wordt vereist dat doeltreffende faciliteiten worden ingericht voor de detectie, melding en afhandeling van beveiligingsinbreuken en vermoedens van misbruik.

Leeswijzer

De paragraafstructuur volgt de eIDAS uitvoeringsverordening EU 2015 / 1502. De tekst in de eIDAS-kolommen is overgenomen uit de formele Nederlandstalige versie van de uitvoeringsverordening.

- 2.4.3 Beheer voor informatiebeveiliging — Deze paragraaf betreft de eisen aan het management van informatiebeveiliging voor alle organisaties die diensten leveren in de authenticatieketen.
- 2.4.6 Technische controles — Dit betreft specifieke technische beveiligingsmaatregelen

2.4.3 Beheer voor informatiebeveiliging

Deze paragraaf betreft de eisen aan het management van informatiebeveiliging voor alle organisaties die diensten leveren in de authenticatieketen.

Niveau betrouwbaarheid	eIDAS tekst uitvoeringsverordening	Nadere invulling en specificatie Uniforme Set van Eisen
Laag	Er bestaat een doeltreffend beheerssysteem voor informatiebeveiliging dat zorg draagt voor het beheer en de beheersing van informatiebeveiligingsrisico's.	Geen nadere invulling of specificatie
Substantieel	Niveau laag, plus: Het beheerssysteem voor informatiebeveiliging voldoet aan beproefde normen en beginselen voor het beheer en de beheersing van informatiebeveiligingsrisico's.	

1. De Participant MOET een werkend beheerssysteem voor informatiebeveiliging ingericht hebben. Dit beheerssysteem MOET in elk geval omvatten:
    1. Een managementcyclus (PDCA);
    2. De diensten die in de authenticatieketen wordt geleverd inclusief de daaraan ondersteunende processen en systemen;
    3. Een analyse van de beveiligingsrisico's behorende bij de diensten die worden geleverd inclusief de ondersteunende processen en systemen;
    4. Een vastlegging van de beheersmaatregelen die op basis van de risicoanalyse zijn genomen inclusief vastlegging van de relatie tussen risico's en beheersmaatregelen;
    5. Een periodieke evaluaties of audits van de werking van beheersmaatregelen en een vastlegging van opvolging van verbeterpunten. Hieronder wordt ook verstaan het periodiek testen van ondersteunende systemen op kwetsbaarheden. De periodiciteit MOET worden bepaald aan de hand van een vastgelegde risico afweging;
    6. Een management review van het beheerssysteem.
2. De Participant MOET de toegang tot gegevensverzamelingen met betrekking tot de dienstverlening en ondersteunende systemen beveiligingen tegen toegang door onbevoegden. Dit betreft zowel de logische toegang als de fysieke toegang.
3. De Participant MOET doeltreffende faciliteiten inrichten ten behoeve van het detecteren, onderzoeken en afhandelen van identiteitsdiefstal, fraude en misbruik met het Authenticatiemiddel.
4. De Participant MOET doeltreffende faciliteiten inrichten ten behoeve van het detecteren, onderzoeken en corrigeren van kwetsbaarheden en daadwerkelijk optredende beveiligingsinbreuken.
5. De Participant MOET doeltreffende faciliteiten inrichten voor het tijdig melden van incidenten over inbreuken op de beveiliging, datalekken, fraude en misbruik.
6. De Authenticatiedienst ZOU een Opmerkelijke gebeurtenis met betrekking tot het middelengebruik MOETEN registreren bij het BSNk met behulp van AUC4 Registreren Opmerkelijke Gebeurtenis.
7. De Participant MOET inbreuken op de betrouwbaarheid van de geleverde diensten onverwijld te melden aan de Toezichthouder.
8. De Participant MOET een verzoek om verstrekken van informatie controleren op rechtmatigheid voordat hij gegevens verstrekt.
    1. De Participant MOET de door hem uitgevoerde controle bij elk gehonoreerd verzoek aan kunnen tonen.
    2. De Participant MAG NIET meer gegevens verstrekken dan waarom is verzocht.
    3. De Participant MOET de vertrouwelijkheid van de informatie bij overdracht waarborgen.
    4. De Participant MOET een 'bevestiging van overdracht' ontvangen en archiveren.
9. De Participant MOET bij uitbesteding van activiteiten zijn onderaannemers de relevante verplichtingen opleggen en waarborgen dat deze onderaannemers de opgelegde verplichtingen nakomen.

Toelichtende tekst bij punt 1: De standaard ISO/IEC 27001 en een zogeheten Three Lines of Defence model voor Risicomanagement worden in dit kader beschouwd als referenties voor het inrichten van het beheersysteem voor in formatiebeveiliging. Voor het vaststellen van maatregelen kunnen meerdere bronnen worden gebruikt zoals de standaarden Cobit, ISO 27002 of Baseline Informatiebeveliging Rijk.

Toelichtende tekst bij punt 3: De hier opgenomen verplichting waarborgt dat Participanten over afdoende informatie beschikken over door hem gedetecteerd misbruik. Nader bepaald moet worden welke andere faciliteiten en procedures voor melding, onderzoek en afhandeling nodig en wenselijk zijn om Participant-overstijgend misbruik te bestrijden.

Toelichtende tekst bij punt 4: De Participanten worden met deze vereiste veronderstelt hun systemen en applicaties in continuïteit veilig te houden door bijvoorbeeld het meerde malen per jaar uitvoeren van beveiligingstests gericht op detectie em correctie van kwetsbaarheden zoals aangeven door de OWASP en de NCSC handreiking voor beveiliging van webapplicaties. Daarnaast moeten participanten in staat worden geacht om een daadwerkelijke doorbreking van de beveiliging op te merken en af te handelen.

Toelichtende tekst bij punt 5, 6 en 8: De hier opgenomen vereiste waarborgt dat de Participanten incidenten die zij detecteren melden. Nader moet worden bepaald wat de definities zijn van 'opmerkelijke gebeurtenissen', 'meldenswaardige incidenten', het meldpunt of meldpunten en procedures voor onderzoek en afhandeling en terugkoppeling. Voor wat betreft de rol van de Toezichthouder en definitie van meldenswaardige incidenten is het het voornemen om aan te sluiten bij de rol die de Toezichthouder heeft bij zijn toezicht op Trust Service Providers zoals dat in de eIDAS verordening 910/2014 is opgenomen in artikel 19 lid 2. In dat kader wordt in Europees verband door de nationale toezichthouders van de lidstaten onder leiding van ENISA een uitwerking gemaakt die leidend wordt voor de uitwerking in de Uniforme Set van Eisen.

Toelichtende tekst bij punt 7: De verplichting om misbruik van een authenticatiemiddel te melden aan de Gebruiker is opgenomen in paragraaf 2.3.1 Authenticatiemechanisme punt 6.

Toelichtende tekst bij punt 9: Indien de uitbesteding van activiteiten de verwerking van persoonsgegevens omvat moeten de opgelegde verplichtingen tevens een bewerkersovereenkomst bevatten conform de vereisten uit de Wbp.

Toelichtende tekst bij punt 1,2,3,4 en 9:

Noot bij 1: Referentie ISO/IEC 27001:2013, ISO/IEC 27002:2013 paragraaf 4 en 5

Noot bij 2: Referentie ISO/IEC 27002:2013 paragraaf 9, 10, 11

Noot bij 3,4,5: Referentie ISO/IEC 27002:2013 paragraaf 12, 16

Eisen 1 t/m 9 met uitzondering van punt 6 zijn van toepassing op alle participanten,

		Eis 6 is alleen van toepassing op de Authenticatiedienst.
Hoog	Zelfde als niveau substantieel.	

2.4.6 Technische controles

Dit betreft specifieke technische beveiligingsmaatregelen

Niveau betrouwbaarheid	eIDAS tekst uitvoeringsverordening	Nadere invulling en specificatie Uniforme Set van Eisen
Laag	1. Er is voorzien in proportionele controles ter beheersing van de risico's voor de veiligheid van de diensten, waarbij de vertrouwelijkheid, integriteit en beschikbaarheid van de ver-werkte informatie worden beschermd. 2. De elektronische communicatiekanalen die voor de uitwisseling van persoonsgegevens en gevoelige gegevens worden gebruikt, worden beschermd tegen afluisteren, manipuleren en her-afspelen. 3. De toegang tot gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, is beperkt tot de uitoefening van taken en toepassingen waarvoor de toegang strikt noodzakelijk is. Er wordt op toegezien dat dergelijk materiaal niet permanent in onversleutelde staat wordt opgeslagen. 4. Er zijn procedures die waarborgen dat de veiligheid duurzaam wordt gehandhaafd en dat een respons mogelijk is op wijzigingen van het risiconiveau, incidenten en veiligheidsinbreuken. 5. Alle media die persoonsgegevens, cryptografische informatie of andere gevoelige informatie bevatten, worden veilig opgeslagen, vervoerd en verwijderd.	Geen nadere invulling of specificatie
Substantieel	Zelfde als niveau laag, plus: Gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, wordt beschermd tegen ongeoorloofde manipulatie.	Addenda bij laag en van toepassing op substantieel en hoog

1. Ad1 De Participant MOET technische beheersmaatregelen nemen. In elk geval MOETEN deze technische beheersmaatregelen betreffen:
    1. De doeltreffende beheersing van de fysieke en logische toegang tot relevante gegevensverwerkende systemen.
    2. De doeltreffende controleerbaarheid van uitgevoerde handelingen op de relevante gegevensverwerkende systemen
    3. De doeltreffende controleerbaarheid van de gegevensverwerking.
    4. Doeltreffende faciliteiten voor de bescherming tegen aanvallen op de beschikbaarheid van de dienstverlening.
    5. Doeltreffende faciliteiten om de inbreuken op de relevante informatieverwerkende systemen te detecteren en de integere werking van die systemen te waarborgen.
    6. Risico-beperkende maatregelen voor de dreiging dat een medewerker met valse voorwendselen een elektronisch identificatiemiddel creëert voor een fictieve identiteit, of op een bestaande identiteit zonder dat de eigenaar van de identiteit zelf dit heeft gevraagd.
2. Ad1 De Participant MOET de beschikbaarheid van de dienstverlening waarborgen. De vereisten zijn van toepassing voor de dienstverlening van alle Participanten en zijn daarnaast van toepassing op de klantportalen van de Authenticatiedienst en de Middelenuitgever:
    1. 07:00 uur tot 00:00 uur 99,5%
    2. 00:00 uur tot 07:00 uur 93,5%
    3. Gemiddelde afhandeling van authenticaties: 95% binnen 4 seconden
3. Ad1 De vereisten voor de samenstelling van koppelvlakken, berichten en berichten uitwisseling zijn opgenomen in Functionaliteit en Techiek .
4. Ad2 Participanten MOETEN berichten en verbindingen betreffende de dienstverlening ondertekenen en versleutelen conform marktstandaarden. De betreffende specificaties zijn op genomen in Functionaliteit en Techniek.
5. Ad2 De Authenticatiedienst en de ontsluitende Toegangsdienst MOETEN realiseren dat de authenticatie-resultaten correct worden verwerkt in de authenticatie-antwoorden die de toegangsdiensten afleveren aan Dienstverlener.

Toelichting punt 1: Het aantonen van de doeltreffendheid van maatregelen die de doelstellingen genoemd bij 1a t/m f invullen veronderstelt het inrichten van monitoringsystemen, processen voor alarmering en opvolging, het periodiek testen van de relevante systemen op kwetsbaarheden en het aanleggen en veiligstellen van relevante loggings (zie hiervoor ook paragraaf 2.4.4 Bijhouden van de administratie).

Toelichting punt 2: Reden voor opnemen is het duidelijkheid verschaffen aan Gebruikers en Dienstverleners ten aanzien van het onderhoudsvenster en het creëren van een meetlat voor de Toezichthouder om Participanten aan te kunnen spreken. De opgenomen beschikbaarheidspercentages doen recht aan reeds bestaande afspraken van Participanten met Dienstverleners. Daarnaast is het uitgangspunt dat het BSNk een Authenticatie afhandelt in 1 seconde en beschikt over een gemiddelde uptime van 99,3.%, dat is inclusief onderhoud.

Toelichting bij punt 3: Verwijzing naar Functionaliteit en Techniek betreffende de paragrafen over Interface specifications

Toelichting bij punt 4: Verwijzing naar Techniek en Functionaliteit betreffen de paragrafen over (SAML) Encryption, XML Digital Signature en Secure connection (TLS).

Noot bij 1a: Referentie ISO/IEC 27002:2013 paragraaf 9,11, 12.4

Noot bij 1b: Referentie ISO/IEC 27002:2013 paragraaf 9, 12.4

Noot bij 1d: Referentie ISO/IEC 27002:2013 paragraaf 12,6, 14.1.2

Noot bij 1e: Referentie ISO/IEC 27002:2013 paragraaf 18.2.3

Noot bij 1f: Referentie ISO/IEC 27002:2013 paragraaf 6.1.2

Noot bij 3, 4: Referentie ISO/IEC 27002:2013 paragraaf 13.2.3

Eisen 1 t/m 4 zijn van toepassing op alle participanten.

Hoog	Zelfde als niveau substantieel.	

Pseudonimisering

Deze paragraaf beschrijft de manier waarop met het toepassen van pseudonimisering de privacy van Gebruikers wordt beschermd.De Uniforme Set van Eisen beschrijft hoe een Dienstverlener met een wettelijke taak binnen het Publieke Domein een BSN als identiteit van een Gebruiker op een betrouwbare, veilige en privacy-vriendelijke manier aangeleverd krijgt. De toepassing van Privacy-Enhancing-Technology in de vorm van polymorfe pseudonimiserig speelt hierin een belangrijke rol. Deze technologie maakt daarbij onder meer mogelijk dat er in het authenticatieproces geen noodzaak is voor centrale componenten.

Deze technologie biedt ook ondersteuning voor Diensten in het Publieke Domein die geen noodzaak hebben voor een BSN of waar het BSN zelfs ongewenst is, bijvoorbeeld voor referenda, enquetes of activiteiten ten bate van fraudebestrijding. Ook buiten het Publieke Domein, waar het BSN niet gebruikt mag worden om Gebruikers te identificeren, kan deze technologie worden gebruikt. Het ontwerp voorziet voor deze scenario's in het gebruik van pseudoniemen als identificerend alternatief voor het BSN.

De pseudoniemen zijn cryptogrammen die afhankelijk zijn van zowel de identiteit van de persoon (BSN) als de Dienstverlener identiteit. Bij verschillende Dienstverleners, krijgt een persoon een voor hem uniek, doch persistent, pseudoniem. Compatibiliteit is een belangrijke functionele eis vanuit gebruikersgemak: als een persoon vanuit verschillende authenticatiediensten aanlogt bij dezelfde Dienstverlener dan moet dit leiden tot dezelfde persistente en unieke pseudoniem. Pseudoniemen zijn dus Authenticatiedienst-onafhankelijk.

Voor een authenticatie van een Gebruiker bij een Dienstverlener, stuurt de Dienstverlener een authenticatieverzoek naar de Authenticatiedienst. De Authenticatiedienst stelt conform de eisen die hieraan gesteld zijn betrouwbaar de identiteit vast. Het authenticatieresultaat wordt in een bericht naar de Dienstverlener gestuurd. Dit bericht bevat een versleuteld pseudoniem van de gebruiker specifiek (alleen bruikbaar) voor de Dienstverlener. Na ontsleuteling verkrijgt de Dienstverlener hieruit het Pseudoniem (of, afhankelijk van de use case, het BSN).

Er zijn dus drie verschillende statussen waarin een pseudoniem zich kan bevinden:

1. De stamvorm; het polymorfe pseudoniem
2. De eindvorm; het pseudoniem (of BSN) van de Gebruiker bij de Dienstverlener
3. Een tussenvorm tussen deze twee; het versleuteld pseudoniem welke een Authenticatiedienst op basis van het polymorfe pseudoniem maakt voor een specifieke Dienstverlener.

Voor de transformatie van de stamvorm naar de eindvorm beschikken partijen in de authenticatieketen over cryptografisch Sleutelmateriaal dat wordt verstrekt en beheerd door een centrale partij (Sleutelbeheer).

Cryptografische bescherming

Bij de berichtencommunicatie tussen de partijen moet de verzendende partij het bericht digitaal ondertekenen en is de verzendende partij ook in staat (delen van) het bericht te versleutelen voor de beoogde ontvangende partij. Dit betekent dat in beginsel iedereen kan vaststellen dat een bericht afkomstig is van de verzendende partij (bescherming authenticiteit en integriteit), maar ook dat alleen de ontvangende partij inzage kan krijgen in het bericht zelf (bescherming, vertrouwelijkheid). De sleutelinfrastructuur is gebaseerd op een publieke sleutelinfrastructuur conform de eisen van PKIoverheid.

Op Identiteit niveau wordt door de toepassing van de polymorfe pseudonimisering hierbij additionele authenticiteit en privacy zekerheden toegevoegd. De technologie garandeert dat een identiteit niet alleen leesbaar, maar zelfs alleen bekend is bij de beoogd ontvanger. Ook zijn er waarborgen voor integriteit in de pseudoniem/BSN ontsleuteling opgenomen: de ontvangende partij kan losstaand van de berichten communicatie vaststellen dat het pseudoniem/BSN van de Authenticatiedienst afkomstig is en integer is. De pseudonimiseringsinfrastructuur is gebaseerd op de sleutelinfrastructuur welke wordt verzorgd door het BSNk.

Compliance en audit

Deze paragraaf bevat eisen voor de manier waarop conformiteit met de Uniforme Set van Eisen moet worden aangetoond. Het eerste deel van de eisen betreffen de generieke vereisten ten behoeve van het proces van 'erkenning' door de Minister en het onderhouden van de 'erkenning'. Het tweede deel beschrijft de wijze hoe moet worden aangetoond dat aan de specifieke eIDAS vereisten voor de kwaliteit van het Authenticatiemiddel en het bijbehorende 2.3.1 Authenticatiemechanisme wordt voldaan. Die specifieke vereisten zijn opgenomen in de paragrafen 2.2.1 Kenmerken en ontwerp van elektronische Identificatiemiddelen en 2.3.1 Authenticatiemechanisme.

De eisen in deze paragraaf zijn een invulling en verduidelijking van de eIDAS uitvoeringsverordening EU 2015 / 1502. De tekst in de eIDAS-kolom is overgenomen uit de formele Nederlandstalige versie van de uitvoeringsverordening.

2.4.7 Compliance en audit

Niveau betrouwbaarheid	eIDAS tekst uitvoeringsverordening	Nadere invulling en specificatie Uniforme Set van Eisen
Laag	Er vinden periodieke interne audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn om de naleving van het desbetreffende beleid te waarborgen.	Geen nadere invulling of specificatie
Substantieel	Er vinden periodieke onafhankelijke interne of externe audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn teneinde de naleving van het desbetreffende beleid te waarborgen.	1. Een kandidaat Participant MOET een rapport over de conformiteit met de Uniforme Set van Eisen van een geaccrediteerde certificerende instelling instantie voegen bij de aanvraag voor erkenning. In dit rapport is een zogenaamde conformiteitsverklaring opgenomen. 2. Een Participant MOET eens per 2 (twee) jaar een conformiteitsbeoordeling over de volledige voor hen van toepassing zijnde vereisten laten uitvoeren door een geaccrediteerde certificerende instelling. 3. Een Participant MOET 1 (één) maal per jaar een zogenaamde onderhoudsbeoordeling laten uitvoeren door een geaccrediteerde certificerende instelling. 4. Een Participant MOET de conformiteitsverklaring en -rapport en de correctieve actieplannen naar aanleiding van de beoordelingen, zoals bedoelt in punt 2 en 3, na acceptatie van de correctieve actieplannen door de certificerende instelling onverwijld aan de Toezichthouder ter beschikking stellen. 5. Een Participant MOET alle wijzigen die hij aanbrengt aan de erkende diensten administreren. 6. Een Participant MOET bij essentiële wijzigingen van de erkende diensten de betreffende wijziging laten beoordelen door een geaccrediteerde certificerende instelling. De vaststelling van mate waarin een wijziging essentieel MOET worden geacht is in eerste instantie aan de geaccrediteerde certificerende instelling. Het resultaat van de beoordeling en nog aan te brengen correcties MOET na acceptatie van de correctieve actieplannen onverwijld aan de Toezichthouder ter beschikking worden gesteld. Toelichtende tekst: De Wet GDI stelt als voorwaarde voor 'erkenning' door de Minister Binnenlandse Zaken dat de kandidaat participant zijn diensten laten beoordelen door een geaccrediteerde certificerende instelling. Een geaccrediteerde certificerende instelling is in dit kader een partij die door de Raad van Accreditatie (RvA) is geaccrediteerd om de conformiteit met de Uniforme Set van Eisen te beoordelen. Deze certificerende instelling voert de conformiteitsbeoordeling uit op basis van de Uniforme Set van Eisen en geeft daarover een conformiteitsverklaring af. In het proces van erkenning heeft de Toezichthouder een rol als adviseur van de Minister. Na erkenning door de Minister heeft de betreffende kandidaat de status van Participant. Wanneer een dienst van een Participant eenmaal is erkend houdt Toezichthouder toezicht op het onderhoud van de conformiteit met de vereisten. Het wettelijke context van het Toezicht bestaat uit de Wet GDI en de Awb. Conform deze wettelijke context is een eindoordeel over de conformiteit met de vereisten aan de Toezichthouder en heeft hij de bevoegdheid op eigen initiatief inspecties bij Participanten uit te voeren. De vereisten betreffende de kern van de verplichtingen van Participanten inzake het aantonen van de naleving van de Uniforme Set van Eisen. De operationele procedures voor erkenning en toezicht krijgen een nadere invulling. Toelichting punt 1 t/m 6: Daar waar organisaties meerdere rollen vervullen, bijvoorbeeld een combinatie van de rol van Middelenuitgever en Authenticatiedienst mag de organisatie de conformiteitsbeoordeling en rapportage over de conformiteit samen brengen in één beoordeling en één rapportage.

Toelichting bij punt 6: Het betreft hier essentiële wijzigingen die de Participant aanbrengt ongeacht de oorzaak van de wijziging. Bijvoorbeeld de betreffende wijziging kan op initiatief van de Participant worden aangebracht ter verbetering van de dienst maar ook aangebracht zijn om te voldoen aan een aanpassing van de Uniforme Set van Eisen.

Eisen 1 is van toepassing op kandidaat participanten

Eisen 2 t/m 6 zijn van toepassing op alle participanten.

De beoordeling van de weerstand tegen een 'gemiddeld' (moderate) respectievelijk hoog (high) aanvalspotentieel van een Authenticatiemiddel met bij behorend authenticatiemechanisme zoals bedoeld in paragrafen 2.2.1 Kenmerken en ontwerp van elektronische Identificatiemiddelen en 2.2.3 Schorsing, Herroeping en Reactivering MOET in elk geval voldoen aan de volgende vereisten:

1. De Middelenuitgever en Authenticatiedienst MOET ten behoeve van de conformiteitsbeoordeling een actueel overzicht kunnen opleveren van de aan het Authenticatiemiddel en authenticatiemechanisme, uitgevoerde wijzigingen, met daarbij een beschrijving van de impact op de conformiteit aan de gestelde eisen.
2. Bij de conformiteitsbeoordeling MOET onderscheid gemaakt worden tussen verschillende typen onderzoek, te weten: een initieel onderzoek, een herhalingsonderzoek en een heronderzoek.
    1. Een initieel onderzoek is een eerste beoordeling over de volledige scope van het object van onderzoek op basis van de gestelde eisen;
    2. Een herhalingsonderzoek vindt uitsluitend plaats bij uitgevoerde wijzigingen aan het object van onderzoek die van invloed (kunnen) zijn op de conformiteit aan de gestelde eisen. De scope is beperkt tot de wijzigingen aan het object van onderzoek;
    3. Een heronderzoek vindt minimaal binnen drie jaar na uitgifte van de rapportage initieel onderzoek plaats over de volledige scope van het object van onderzoek.
3. De conformiteitsbeoordelaar die de conformiteitsbeoordeling uitvoert MOET:
    1. Aantoonbaar ruime ervaring hebben met het uitvoeren van technische beoordelingsopdrachten van authenticatiemiddelen of vergelijkbare objecten van onderzoek;
    2. Voor de opdracht personeel inzetten met ruime ervaring en de voor de beoordeling benodigde competenties;
    3. Bij het uitvoeren van de beoordeling en in haar oordeelsvorming geheel onafhankelijk zijn van haar opdrachtgever en de Middelenuitgever en Authenticatiedienst;
    4. Een intern kwaliteitssysteem en/of vaktechnische richtlijnen en procedures hebben voor het uitvoeren van beoordelingsopdrachten, met inbegrip van registratie van ondersteunend bewijs, rapportering aan opdrachtgever en aan derden en – waar nodig - interne (peer) review;
    5. Toestemming verstrekken dat toezichthouder op elk moment, binnen 7 jaar na het uitbrengen van de rapportage van conformiteitsbeoordelaar inzage kan vorderen in de rapportage en in het bijbehorende dossier waarin het ondersteunend bewijs is vastgelegd;
    6. Voorafgaand aan de opdrachtverstrekking aan de opdrachtgever of de MU/AD een formele verklaring opleveren waarin conformiteit aan sub a tot en met sub e op het moment van opdrachtverstrekking en gedurende de conformiteitsbeoordeling verklaard en onderbouwd wordt;
    7. Beschikken over een bedrijfs- of beroepsaansprakelijkheidsverzekering.
4. Een testlaboratorium ingevolge ISO 17025 voor de scope "testing of information technology products" wordt vermoed aan sub 3b tot en met sub 3d te voldoen;
5. Een onderzoek van de conformiteitsbeoordelaar MOET zodanig worden gepland en uitgevoerd dat een zogeheten 'redelijke mate van zekerheid' kan worden verkregen dat het object van onderzoek op het in de rapportage aangegeven moment aan de gestelde eisen voldoet.
6. De rapportage van de conformiteitsbeoordelaar MOET minimaal bevatten:
    1. De doelstelling van de opdracht, een beschrijving van het object van onderzoek (uniek identificerend, met datum en versienummer), de eisen op basis waarvan het object van onderzoek is beoordeeld en het plan van aanpak met de gevolgde stappen en de gehanteerde onderzoeksmethoden en aanvalstechnieken;
    2. Het eindoordeel over de mate waarin het object op het aangegeven moment aan de gestelde eisen voldoet, met onderbouwing;
    3. Belangrijkste bevindingen en aanbevelingen;
    4. Detailbevindingen, met vermelding van referenties naar het geregistreerde bewijs over de conformiteit aan de betreffende eis.

		Toelichtende tekst: Het beoordelen van de weerstand tegen bedoelde niveaus aanvalspotentieel is zeer technisch en specialistisch. Doorgaans zal de bedoelde geaccrediteerde certificerende instelling die een (kandidaat) participant beoordeeld steunen op rapportages van technische tests die door gekwalificeerde specialisten in opdracht van de (kandidaat) participant zijn uitgevoerd. De geaccrediteerde certificerende instelling is wel verantwoordelijk voor de beoordeling of de rapporten van technische tests geaccepteerd kunnen worden. De bovengenoemde eisen zijn opgenomen ten behoeve van het creëren van een solide basis voor dat oordeel. Eisen 1 t/m 5 zijn van toepassing op de Middelenuitgever en de Authenticatiedienst.
Hoog	1. Er vinden periodieke onafhankelijke externe audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn, teneinde de naleving van het desbetreffende beleid te waarborgen. 2. Indien een stelsel wordt beheerd door een overheidsinstantie, vinden audits plaats overeenkomstig het nationaal recht.	Zelfde als niveau Substantieel.