Gegevensbeschermingseffectbeoordeling (GEB) eID-stelsel

Versie 1.0

28 juni 2017

Inhoudsopgave

Managementsamenvatting

Programma eID heeft veel aandacht voor bescherming van privacy

Voor u ligt de rapportage van de gegevensbeschermingseffectbeoordeling (GEB). De insteek van deze GEB is om een doorkijk te bieden in de manier waarop bij de ontwikkeling van elektronische identificatie (eID) wordt nagedacht over, en invulling wordt gegeven aan de bescherming van persoonsgegevens.

Een belangrijke notie is dat deze GEB is gebaseerd op de in 2016 ontwikkelde multimiddelenstrategie. Deze is op basis van onderzoek en de reacties op de consultatie van de Wet GDI recentelijk – zie hierover de brief over de Voortgangsrapportage programma eID van 23 juni jl.- vereenvoudigd. Deze vereenvoudiging heeft mogelijk impact op de beoordeling van privacyrisico's. Dit houdt in dat bij een nadere uitwerking van de GEB hiermee rekening zal worden gehouden.

Privacybescherming blijft bij de vereenvoudiging onverminderd van belang. Bij de invulling daarvan zal gebruik worden gemaakt van de inzichten die deze GEB heeft opgeleverd.

De conclusie van deze GEB (voorheen genaamd PIA), is dat binnen het eID-stelsel veel aandacht is voor privacybescherming. Binnen het programma eID is nadrukkelijk oog en aandacht voor de privacyrisico's die aan het eID-stelsel zijn verbonden. Dat neemt niet weg dat deze GEB nog steeds aandachtspunten signaleert die moeten worden opgepakt.

Belangrijke risico's uit eerdere GEB zijn weggenomen of verkleind

Bij het ontwerp van het eID-stelsel worden privacybeschermende maatregelen getroffen (privacy by design), waarbij aan de meeste van de aanbevelingen uit de eerdere GEB invulling is gegeven. Er is belangrijke vooruitgang geboekt ten opzichte van het Introductieplateau eID.

De vorige GEB signaleerde een groot risico omdat wet- en regelgeving ontbrak om het BSN in het private domein te kunnen gebruiken. Verder werd het BSN-koppelregister aangemerkt als beschikbaarheids- en gegevensconcentratierisico (single point of failure en privacy hotspot). Ook mogelijke gegevensconcentraties bij partijen die meerdere rollen combineren in het stelsel werd als groot risico beoordeeld. Het advies is destijds geweest om het introductieplateau slechts heel beperkt uit te rollen en eerst maatregelen te nemen om de belangrijkste risico's op te lossen.

Inmiddels zijn in het eisenpakket (de Uniforme Set van Eisen, USvE) en de Wet EBV deze risico's ten aanzien van BSN-gebruik en grote gegevensconcentraties grotendeels weggenomen. De Wet EBV regelt een wettelijke grondslagvoor het verwerken van het BSN binnen het eID-stelsel en op dit moment de situatie dat de private partijen het BSN verwerken onder de verantwoordelijkheid van de minister van BZK. Een andere belangrijke maatregel is de polymorfe cryptografie en pseudonimisering. Dit zorgt voor compartimentering en privacy by design en minimalisering van verwerking van het BSN. Het BSN-koppelregister verwerkt in de nieuwe werking na het activatieproces geen BSN meer. Ook zijn er regels gesteld voor het scheiden van rollen in het stelsel.

De PIA op het introductieplateau signaleerde dat de maatregelen aangaande misbruikdetectie en interne controlemaatregelen niet waren gedefinieerd. Inmiddels zijn wel de contouren geschetst van misbruikbestrijding, maar de inrichting moet nog grotendeels plaatsvinden. Deze bevinding blijft daarmee onverkort staan.

Er is nog wel werk aan de winkel

In de GEB staat een aantal belangrijke aandachtspunten die moeten worden opgelost voordat de brede uitrol van eID-inlogmiddelen kan plaatsvinden. Dit zijn met name procedurele maatregelen, nadere afspraken en acties die ervoor moeten zorgen dat zaken en de keuzes die gemaakt worden op het gebied van privacy beter gedocumenteerd zijn en daardoor inzichtelijk worden gemaakt.

Het is belangrijk om als verantwoordelijke voor de verwerking van persoonsgegevens "aantoonbare controle" te hebben over de verwerkingen van persoonsgegevens. Dit is een belangrijk uitgangspunt van de Algemene Verordening Gegevensbescherming (AVG) die tijdens de looptijd van het voorlopertraject, op 25 mei 2018, van kracht zal worden.

De risico's die worden geconstateerd in de GEB zijn op dit moment nog niet manifest. De GEB heeft gekeken naar de ontwerpeisen voor eID. De verwachting is dat deze in 2018 geïmplementeerd worden. Zo biedt de GEB de mogelijkheid om de aanbevelingen door te voeren in het ontwerp en de uitvoering.

De GEB is een hulpmiddel

De GEB is een hulpmiddel voor planmatige inrichting van privacybescherming. Beoogd wordt om inzicht te geven in de gegevensverwerkingen die plaatsvinden, en daarmee bij te dragen aan de transparantie over de werking van eID. Er is voor gekozen om risico's en maatregelen op hoofdlijnen te benoemen, en bovenal om een bijdrage te leveren aan de verdere planmatige aanpak van bescherming van persoonsgegevens in de voorbereiding naar een grootschalige invoering van de nieuwe inlogmethoden. Waarbij op een samenhangende wijze, minder issue- en techniekgericht, de bescherming van persoonsgegevens wordt ingevuld.

Privacyrisico's

Uiteindelijk gaat het bij het voorkomen van privacyrisico's om het voorkomen van onwenselijke gevolgen ervan voor burgers. Bij onrechtmatige of onbedoelde verwerking van persoonsgegevens binnen het eID-stelsel kan gedacht worden en verlies (beschikbaarheid) van de toegang tot een groot aantal overheidsdienstverleners.

Verlies van eID-inlogmiddelen kan ongeoorloofde wijziging van gegevens bij dienstverleners (integriteit) betekenen, of ongeoorloofde afname van dienstverlening door derden. Dergelijke risico's kunnen binnen het eID-stelsel aan de orde zijn. Maar gelet op de schaalgrootte en context waarin het stelsel wordt gepositioneerd kunnen de negatieve gevolgen in potentie groot zijn, en doorwerken tot ver buiten het eID stelsel zelf. Verlies van controle over hun eID-middelen of een inbreuk op de goede werking kan voor gebruikers leiden tot (blootstelling aan) identiteitsdiefstal of –fraude en bijbehorende financiële verliezen. Omdat beoogd wordt dat ook zorgverleners gebruik kunnen maken van het stelsel zal ook verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens aan de orde kunnen zijn. Het eID-stelsel maakt voorts gebruik van pseudonimisering. Ongeoorloofde ongedaanmaking daarvan, d.w.z. het weer zichtbaar maken van het BSN, zou kunnen leiden tot ongeoorloofd en voor de gebruiker schadelijk inzicht in zijn gedrag in een bredere context.

Het is belangrijk te beseffen dat dergelijke risico's bij online dienstverlening en identiteitsvaststelling nu ook (al) spelen. En dat dergelijke risico's ook mede de aanleiding zijn geweest om het eID-stelsel als zodanig in het leven te roepen als opvolger van huidige authenticatiemogelijkheden. Het ontwerp is er nadrukkelijk op gericht om het hoofd te bieden aan dergelijke risico's voor de dienstverlening van een groot aantal overheidspartijen door een hogere betrouwbaarheid en continuïteit te bieden. Echter daarvoor is het dan wel essentieel dat het eID-stelsel zelf ook zodanig wordt ingericht dat de aan het stelsel inherente risico's zoveel mogelijk worden ondervangen. Immers voor de levering van eID-diensten worden noodzakelijkerwijs ook persoonsgegevens verwerkt. Daartoe wordt privacybescherming binnen het eID-stelsel ingericht.

Deze GEB beoogt daaraan een constructieve bijdrage te leveren door een aantal belangrijke risico's te signaleren, en deze direct aan voorgestelde acties te koppelen.

Van privacyrisico's naar planmatige bescherming van persoonsgegevens

Aan de hand van de belangrijkste beginselen uit de AVG is per beginsel een aantal risico's onderkend. De belangrijkste worden hieronder toegelicht, met daarbij voorgestelde maatregelen. Doelstelling daarvan is, door systematisch invulling te geven aan de privacybeginselen, de feitelijke privacyrisico's voor burgers te minimaliseren op een wijze waarop tevens naleving van de AVG wordt bereikt.

Rechtmatige grondslag: verwerkersovereenkomsten sluiten, verantwoordelijkheid MinBZK

De binnen het eID-stelsel voorgenomen verwerkingen van persoonsgegevens zijn rechtmatig. De Wet EBV en het Besluit GDI bieden een adequate grondslag voor de minister van BZK. Omdat de activiteiten door de andere partijen, zoals private authenticatiediensten in het eID-stelsel onder verantwoordelijkheid van de minister van BZK vallen, is het belangrijk verwerkersovereenkomsten op te stellen tussen/met private partijen om de gegevensverwerkingen rechtmatig te laten zijn.

Gelet op de verantwoordelijkheid van de minister van BZK wordt aanbevolen dat leveranciers van inlogmiddelen en publieke organisaties die betrokken zijn bij de bredere uitrol van eID zelf een GEB opstellen, om zicht te krijgen op de gegevens die zij -als verwerker van persoonsgegevens voor de minister van BZK- verwerken. Ook vanuit die invalshoek –naast de regeling van de verwerkingsgrondslag- moet inzicht gegeven kunnen worden in de voorgenomen/te treffen maatregelen. Aanbevolen wordt om dit onderdeel te laten uitmaken van de overeenkomsten die de minister van BZK met de partijen sluit. Dit is ook van belang om de minister van BZK zijn rol als verantwoordelijke te kunnen laten waarmaken.

Misbruikbestrijding inregelen

Een ander risico is dat misbruikbestrijding (fraude/incidentbestrijding) op stelselniveau nog niet is ingericht. Aanbevolen wordt om op zo kort mogelijke termijn invulling te geven aan de mogelijkheden om op stelselniveau misbruik te kunnen herkennen (detectie) en te herstellen als er misbruik van persoonsgegevens wordt geconstateerd. Het is belangrijk om een balans te vinden waarin pseudonimisering, om goede redenen bedoeld om herleidbaarheid tegen te gaan, zo kan worden ingezet dat bijvoorbeeld herstelprocessen en misbruikbestrijding op stelselniveau mogelijk blijven. Misbruikbestrijding en incidentbestrijding op stelselniveau en de gegevens die daarvoor kunnen worden gebruikt moeten nader uitgewerkt worden.

Afspraken maken om herleidbaarheid van logging te voorkomen

Binnen het eID-stelsel worden geen bijzondere of strafrechtelijke persoonsgegevens verwerkt. Wel kunnen patronen in andere persoonsgegevens die in het eID-stelsel worden verwerkt een indicatie of voorspeller zijn van bijzondere persoonsgegevens. Door noodzakelijke logging van de werking van het stelsel bestaat het risico dat daarin indicaties of voorspellers kunnen voorkomen van bijzondere persoonsgegevens, bijvoorbeeld als wordt ingelogd bij specifieke zorgverleners. Om herleidbaarheid tegen te gaan worden in het stelsel daarvoor reeds maatregelen getroffen. Onder meer door er met gebruikmaking van pseudonimisering voor te zorgen dat authenticatiediensten niet op "BSN-niveau" kunnen herleiden bij welke dienstverlener een gebruiker heeft ingelogd. De vormgeving met pseudoniemen vormt een belangrijk uitgangspunt voor de bescherming van persoonsgegevens binnen het eID stelsel. Beoogd wordt de gegevensverwerking zodanig in te richten dat geen enkele van de bij authenticatie betrokken partijen (inclusief publieke dienstverleners) kan zien welke andere websites door een gebruiker worden bezocht in het publieke domein. Dit is niet alleen een belangrijk punt voor de bescherming van persoonsgegevens als zodanig, maar doet tevens recht aan de wens en de verwachting dat de betrokken (private) partijen geen inzicht in of bemoeienis moeten kunnen hebben met zaken die gebruikers in het publieke domein afwikkelen.

Een andere maatregel die wordt getroffen is het werken met verschillende rollen, waardoor compartimentering van de persoonsgegevens binnen het stelsel ontstaat. Aanbevolen wordt om

expliciet nadere afspraken te maken dat deze logging niet voor andere doeleinden mag worden gebruikt dan de authenticatiedienstverlening. Hiervoor moet binnen het stelsel toezicht op naleving van deze afspraken georganiseerd worden.

Voorkom privacy *hotspots en single points of failure buiten het stelsel*

Met polymorfe pseudonimisering is binnen het stelsel dataminimalisatie en compartimentering ingeregeld, waardoor grote gegevensconcentraties worden vermeden. Dit is een belangrijke privacymaatregel. Belangrijk is dat ook buiten het eID-stelsel, aan de kant van de overheidsdienstverleners, deze compartimentering in stand blijft. Buiten het eID-stelsel zijn geen juridische of technische waarborgen die voorkomen dat een dienstverlener door compartimenten heen gegevens van gebruikers koppelt op het BSN. Het risico bestaat hierdoor dat compartimentering grotendeels teniet wordt gedaan doordat een aantal belangrijke leveranciers voor overheidspartijen in feite meerdere rollen invullen. Deze situatie wordt op dit moment binnen de Uniforme Set van Eisen niet geadresseerd. Aanbevolen wordt om eisen te stellen aan dienstverleners en leveranciers over combinaties van rollen en cumulatie van partijen binnen één leverancier. Minimaal zouden er garanties voor functiescheiding (Chinese muren) moeten komen.

Accountability (verantwoordingsplicht)

De conclusie op basis van de bovenstaande constateringen is dat op dit moment nog niet aan de verantwoordingsplicht zou worden voldaan. De verwerkingen van persoonsgegevens en informatie daarover zoals beschreven in de GEB zijn niet tot in detail uit de documentatie af te leiden, maar komen voor een belangrijk deel van de geraadpleegde deskundigen die bij de ontwikkeling van het eID-stelsel betrokken zijn. Op het moment dat eID-inlogmiddelen in gebruik genomen gaan worden door het hele Nederlandse publiek moet dat zijn opgelost. Aanbevolen wordt om er in de Uniforme Set van Eisen 1.1. voor te zorgen dat de verwerkingen van persoonsgegevens volledig en eenduidig worden beschreven. Advies is om deze GEB als hulpmiddel te gebruiken om daartoe te komen.

1. Inleiding

1.1 Aanleiding

Om de veiligheid van digitale identiteitsvaststelling te verbeteren en de afhankelijkheid van een enkel middel te verminderen, is het Elektronische Identiteit Stelsel (eID-stelsel) opgezet. Tijdens het Algemeen Overleg van 18 januari 2017 over de Digitale Infrastructuur / eID, heeft de minister van BZK toegezegd een zogeheten gegevensbeschermingseffectbeoordeling (GEB) uit te zullen voeren op het voorlopertraject van het eID-stelsel zoals dat begin 2018 wordt uitgerold, en deze op te leveren in het voorjaar van 2017.[1] De term GEB is afkomstig uit de Algemene Verordening Gegevensbescherming (AVG), de nieuwe Europese privacyverordening die in mei 2018 van kracht wordt. Een GEB was voorheen bekend onder de naam privacy impact assessment (PIA).

Naar aanleiding van de motie-Franken heeft het kabinet bepaald dat bij de ontwikkeling van beleid en wetgeving waaruit gegevensverwerkingen voortvloeien, bij de bouw van ICT-systemen en de aanleg van grote databestanden een GEB moet worden uitgevoerd.[2] Daarnaast verplicht de AVG[3] met ingang van mei 2018 tot het uitvoeren van een GEB voor gegevensverwerkingen met een hoog risico voor de rechten en vrijheden van natuurlijke personen. Bij een grootschalige ontwikkeling als het eID-stelsel is een GEB zonder meer aan de orde gezien een aantal indicaties van een hoog risico die de AVG geeft: er is sprake van grootschalige verwerking van persoonsgegevens. Er is sprake van technieken die voor het eerst in onderlinge samenhang en grootschalig worden ingezet. En de gewenste functionaliteit van het stelsel en de context, namelijk de identiteitsvaststelling voor een groot aantal (overheids)organisaties die daarvan afhankelijk zijn en er op moeten kunnen vertrouwen, stelt hoge eisen aan veiligheid, privacybescherming en misbruikbestrijding. Op grond van het kabinetsbeleid en de AVG is een GEB voor het eID-stelsel derhalve verplicht.

1.2 Doelstelling Gegevensbeschermingseffectbeoordeling

Een GEB heeft tot doel om van voorgenomen regelgeving of projecten waarbij persoonsgegevens worden verwerkt, de privacyrisico's op een gestructureerde en gestandaardiseerde wijze in kaart te brengen, om op basis hiervan maatregelen te treffen om deze risico's te voorkomen of verkleinen en transparante afwegingen mogelijk te maken tussen de privacyrisico's van verschillende alternatieven.[4] Daarmee draagt een GEB bij aan de nakoming van de verantwoordingsplicht tot naleving van de 'beginselen inzake verwerking van persoonsgegevens' zoals vastgelegd in de AVG. De GEB beoogt ook bij te dragen aan verdere verhoging van het privacybewustzijn bij de vele organisaties die het eID-stelsel mede ontwikkelen en implementeren.

Deze GEB wordt uitgevoerd voor de voorloperfase van het eID-stelsel. De beoogde en beschreven verwerkingen van persoonsgegevens vinden op dit moment nog niet plaats. Er wordt nog gewerkt aan de (detail)uitwerking van zowel functionaliteit van het eID-stelsel als de kaders daaromheen. Het eID-stelsel en de bescherming van persoonsgegevens zijn daardoor op dit moment dan ook nog niet "af". Het feit dat sprake is van een tussentijdse doorkijk betekent onvermijdelijk dat bepaalde zaken nog moeten worden uitgewerkt. Daar waar dit geconstateerd wordt zal dit als actiepunt aan het programma worden meegegeven.

Het betekent aan de ene kant dat de risico's/aandachtspunten op dit moment nog niet manifest zijn. Het betekent aan de andere kant ook dat de tijd tot de start van het voorlopertraject goed moet worden benut om de risico's tijdig te ondervangen.

---

[1] Verslag Algemeen Overleg 18 januari 2017, Kamerstuk nummer 26643 nr. 443; zie: https://zoek.officielebekendmakingen.nl/dossier/26643/kst-26643-443?resultIndex=1&sorttype=1&sortorder=4
[2] Motie-Franken c.s., Vergaderjaar 2010-2011, Kamerstuknummer 31 051.
[3] Art. 35 AVG.
[4] Motie-Franken c.s., Vergaderjaar 2010-2011, Kamerstuknummer 31 051.

De insteek van de GEB is daarom nadrukkelijk om een tussentijdse doorkijk te bieden in de wijze waarop bij de ontwikkeling van het eID-stelsel wordt nagedacht over en invulling wordt gegeven aan de bescherming van persoonsgegevens en bovenal ook om een bijdrage te leveren aan de verdere planmatige aanpak van bescherming van persoonsgegevens in de voorbereiding naar het voorlopertraject.

De aanpak van deze GEB wordt nader verantwoord in hoofdstuk 2.

1.3 Introductie op het eID-stelsel: betrouwbaarheid en continuïteit

Het kabinet acht de modernisering van elektronische identificatiemiddelen (eID-middelen) voor elektronische transacties in het BSN-domein van vitaal belang.[5] Dit is nodig om de veiligheid van, en het vertrouwen in digitale identiteitsvaststelling te waarborgen. Het kabinet wil daarnaast voor het publieke domein de continuïteit verhogen door de afhankelijkheid van DigiD als exclusief authenticatiemiddel te verminderen, door gebruikers op het moment dat een middel onverhoopt niet werkt in staat te stellen andere authenticatiemiddelen te gebruiken. Om dit mogelijk te maken, is ervoor gekozen om toegang tot digitale overheidsdienstverlening via meer dan één inlogmiddel te realiseren.

Om de doelen, hogere betrouwbaarheid en continuïteit te realiseren is het eID-stelsel opgezet. Het stelsel moet burgers en bedrijven in staat stellen op een veilige en betrouwbare manier digitaal zaken te doen met publieke én private aanbieders van online diensten. Binnen het publieke domein, ook wel het Burger Service Nummer domein (BSN-domein)[6] genoemd, omdat het overheidsorganisaties zijn die het BSN mogen en moeten gebruiken, kunnen zowel publieke als private leveranciers authenticatiemiddelen aanbieden. Om de betrouwbaarheid te kunnen garanderen, moeten deze leveranciers vooraf erkend worden. Om erkend te worden dienen zij aan eisen te voldoen om de veiligheid en betrouwbaarheid te waarborgen.

Met de komst van eID wil het kabinet de volgende maatschappelijke voordelen realiseren:

- De toegang tot de reeds bestaande dienstverlening voor de burger wordt betrouwbaarder. Dienstverleners kunnen met meer zekerheid vaststellen dat de identiteit van een persoon klopt. De digitale verbinding waarmee ze dit vaststellen, is veiliger omdat de kans op inbreuk (door bijvoorbeeld phishing) kleiner wordt.
- Door inloggen veiliger en betrouwbaarder te maken, zijn er meer vormen van digitale dienstverlening mogelijk, bijvoorbeeld inzage in zorgdossiers.
- Burgers kunnen vanaf 2018 op meerdere manieren inloggen. Ze kunnen straks bijvoorbeeld kiezen uit inloggen op een app op hun telefoon, met hun rijbewijs of identiteitskaart of via een privaat middel.
- Inloggen bij publieke en private dienstverleners wordt als makkelijker ervaren, omdat burgers een middel kunnen kiezen dat het beste bij hen past.
- De beschikbaarheid van digitale overheidsdienstverlening wordt minder kwetsbaar omdat de afhankelijkheid van één middel wordt opgelost. De burger kan naast DigiD ook met een ander erkend middel inloggen bij overheidsdienstverleners.

Het eID-stelsel stelt burgers in staat om ook grensoverschrijdend digitale diensten af te nemen in andere Europese lidstaten.

Beoogd wordt om in de USvE de overkoepelende minimale set van eisen voor veiligheid en betrouwbaarheid te stellen, waardoor een minimum betrouwbaarheidsniveau gegarandeerd wordt, en waar burgers en overheid vanuit kunnen gaan. Tegelijkertijd staat het de erkende partijen vrij

---

[5] Zie Tweede Kamerbrief van 21 december 2016, 2016-0000790934.
[6] BSN-domein of publiek domein: dienstverlening door overheden en andere instanties die gerechtigd zijn het Burgerservicenummer (BSN) te gebruiken.

om zelf deze eisen hoger te stellen of aan te vullen en daarmee te concurreren op hun dienstverlening. De kerngedachte is dat minimaal aan de USvE 1.0 wordt voldaan.

1.4 Juridisch en beleidsmatig kader

Deze paragraaf geeft een korte toelichting op het wettelijk kader dat ten grondslag ligt aan de ontwikkeling van het eID-stelsel en de belangrijkste uitgangspunten voor de inrichting ervan.

1.4.1 De eIDAS-verordening

De Europese eIDAS-verordening (910/2014) heeft tot doel om het vertrouwen in elektronische transacties binnen in de interne Europese markt te vergroten en te voorzien in een gemeenschappelijke grondslag voor veilige elektronische interactie tussen burgers, bedrijven en overheden. De verordening beoogt daarmee de doeltreffendheid van de elektronische handel binnen Europa te verhogen. De verordening beoogt een kader te scheppen voor wederzijdse (onderlinge) erkenning door nationale lidstaten van elektronische identificatiemiddelen, waardoor burgers hun authenticatiemiddel ook in andere lidstaten kunnen gebruiken. Áls middelen aan de gestelde eisen voldoen, kunnen zij genotificeerd worden en moeten zij in de EU geaccepteerd worden. Vanaf 18 september 2018 zijn lidstaten verplicht om genotificeerde inlogmiddelen uit andere lidstaten te accepteren voor de betrouwbaarheidsniveaus 'substantieel' en 'hoog' voor digitale diensten die dergelijke niveaus vereisen.

1.4.2 Wet EBV en het Besluit GDI

Om het eID-stelsel mogelijk te maken en de geschetste dienstverlening te leveren, zal het nodig zijn om persoonsgegevens te verwerken. Belangrijk is daarom dat de persoonsgegevens binnen de doelstelling van het eID-stelsel worden verwerkt, en dat de deelnemende partijen daartoe ook gerechtigd zijn. Een belangrijk punt is dat private partijen, ook de erkende partijen, in beginsel het Burger Servicenummer (BSN) niet mogen verwerken. Daar tegenover staat dat overheidspartijen het BSN juist moeten gebruiken ten behoeve van hun dienstverlening aan burgers.

Om ervoor te zorgen dat – in lijn met de strategie voor meer dan één middel – private dienstverleners toch authenticatiediensten in het publieke domein aan kunnen bieden is voorzien in een specifieke wettelijke grondslag in de Wet EBV, aangevuld met een verwerkersovereenkomst om eenmalig (voor het activatieproces) het BSN te verwerken en vervolgens op basis van pseudoniemen hun diensten te verlenen. Om dat mogelijk te maken is het BSNk ontworpen. Voor erkende partijen is het dan eenmalig mogelijk het BSN te ontvangen. Op basis daarvan wordt een pseudoniem verkregen aan de hand waarvan zij een gebruiker kunnen herkennen.[7]

Deze grondslag en vormgeving met pseudoniemen vormt een belangrijk uitgangspunt voor de bescherming van persoonsgegevens binnen het eID-stelsel. Beoogd wordt de gegevensverwerking zodanig in te richten dat geen enkele van de bij authenticatie betrokken partijen (inclusief publieke dienstverleners) kan zien welke andere websites door een gebruiker worden bezocht in het publieke domein. Dit is niet alleen een belangrijk punt voor de bescherming van persoonsgegevens als zodanig, maar doet tevens recht aan de wens en de verwachting dat de betrokken (private) partijen geen inzicht in of bemoeienis moeten kunnen hebben met zaken die gebruikers in het publieke domein afwikkelen.

Met de Wet generieke digitale infrastructuur (Wet GDI) beoogt het kabinet de wettelijke randvoorwaarden te creëren voor veilige en betrouwbare toegang tot alle digitale diensten van bestuursorganen. Een voorontwerp van het wetsvoorstel is op 21 december 2016 openbaar gemaakt en heeft in het eerste kwartaal van 2017 ter consultatie voorgelegen. Zolang de Wet GDI nog niet in werking is getreden, vormt de Wet elektronisch berichtenverkeer Belastingdienst (Wet EBV) het wettelijk kader voor elektronische authenticatie en de daartoe vereiste verwerking van

[7] Hoe het BSNk precies werkt inclusief de 6 verschillende functies van het BSNk wordt in hoofdstuk 3 nader toegelicht.

persoonsgegevens in het publieke domein. In artikel X, eerste lid van de Wet EBV is aan de minister van BZK de zorg c.q. de verantwoordelijkheid opgedragen voor de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van voorzieningen voor, onder meer, elektronische authenticatie. Artikel X, derde lid biedt een grondslag voor de verwerking van persoonsgegevens voor zover dat voor de vervulling van de taak noodzakelijk is. Het Besluit verwerking persoonsgegevens voorzieningen generieke digitale infrastructuur (hierna: Besluit GDI) kadert de verwerking van persoonsgegevens nader in, door te bepalen welke persoonsgegevens worden verwerkt, aan wie deze worden verstrekt en hoe lang deze worden bewaard. In de Regeling voorzieningen GDI worden regels gesteld met betrekking tot de werking, beveiliging en betrouwbaarheid van voorzieningen. Hoewel het besluit en de regeling hun grondslag hebben in de Wet EBV, is met de naamgeving en inhoud al geanticipeerd op de Wet GDI.[8]

Van belang is nog om op te merken dat de wettelijke grondslag in de EBV voor verwerking van persoonsgegevens de minister van BZK betreft. Hij kan als verantwoordelijke, private partijen inschakelen (als verwerkers, via een verwerkersovereenkomst) voor de aanlevering van het BSN t.b.v. het BSNk (zie verder). In de toekomstige situatie, onder de Wet GDI is op dit moment beoogd om een expliciete wettelijke grondslag voor private partijen op te nemen.

1.4.3 Uniforme Set van Eisen versie 1.0

In de Uniforme Set van Eisen (USvE) zijn de technische eisen voor de inrichting van het eID-stelsel uitgewerkt en de eisen voor erkenning van publieke en private authenticatiemiddelen op de betrouwbaarheidsniveaus Laag, Substantieel en Hoog. Op termijn kunnen burgers voor diensten in het publieke domein alleen terecht met authenticatiemiddelen op niveau Substantieel en Hoog. De eisen in het USvE hebben betrekking op veiligheid, privacy, betrouwbaarheid, interoperabiliteit en aansprakelijkheid. Partijen die met een authenticatiemiddel willen deelnemen binnen het eID-stelsel moeten minimaal aan de USvE voldoen.

De belangrijkste uitgangspunten van de USvE zijn:

1. ***Betrouwbaarheid:*** de authenticatiemiddelen en de onderliggende techniek moeten veilig zijn en de binding tussen het middel en de identiteit van de burger die eigenaar is van het middel moet voldoende sterk zijn. Identiteitsdiefstal en -verwisseling mogen niet mogelijk zijn.
2. ***Privacyvriendelijkheid:*** het eID-stelsel moet voldoen aan de privacyprincipes van de AVG. Zo mag het BSN alleen verwerkt worden als dat noodzakelijk is.
3. ***Gebruikersvriendelijkheid:*** authenticatiemiddelen moeten voor zowel burgers als dienstverleners eenvoudig te gebruiken zijn.
4. ***Privacy by Design:*** de privacy van gebruikers is al zoveel mogelijk gewaarborgd door de inrichting van het eID-stelsel, onder andere doordat iedere partij alleen data krijgt en opslaat die nodig is voor de rol van die partij, de impact van beveiligingsincidenten op voorhand te beperken, privacy hotspots te vermijden en privacy technisch af te dwingen.
5. ***Misbruikbestrijding:*** de USvE beschrijft maatregelen om misbruik van authenticatiemiddelen te signaleren en te voorkomen, omdat misbruik nooit geheel te voorkomen is.
6. ***Open standaarden:*** de eisen zijn technologieonafhankelijk en gebaseerd op open standaarden, zodat interoperabiliteit wordt geborgd.

De USvE versie 1.0 is op 21 december 2016 naar de Tweede Kamer verstuurd en heeft in het voorjaar van 2017 samen met het voorontwerp van het wetsvoorstel Wet GDI ter consultatie voorgelegen. De USvE is dynamisch: het document wordt stapsgewijs doorontwikkeld naar een

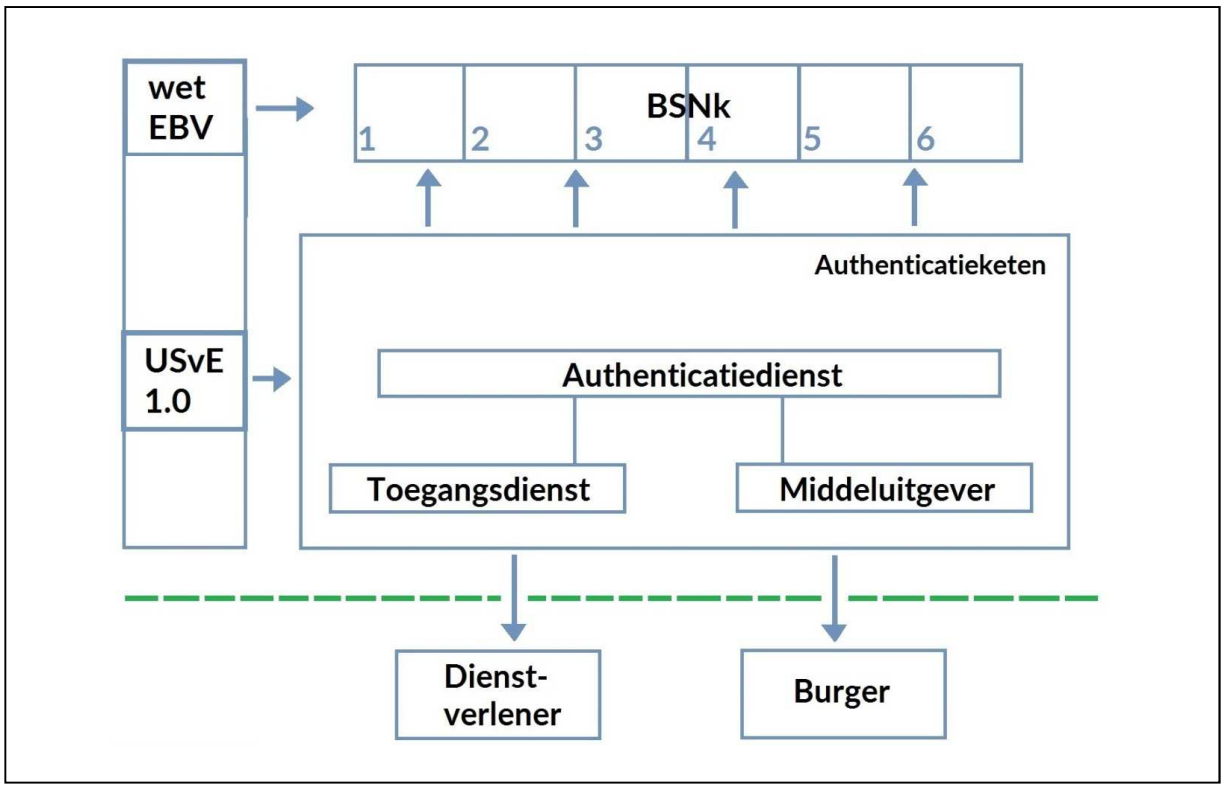
[8] Het Besluit GDI (artikel 5): https://zoek.officielebekendmakingen.nl/stb-2016-195.html. De Regeling voorzieningen GDI (artikel 4): http://wetten.overheid.nl/BWBR0037124/2015-11-01.

versie 2.0 waarop de inrichting en werking van het stelsel feitelijk gebaseerd zal zijn. Deze GEB gaat uit van de USvE versie 1.0.

1.5 De inrichting en werking van het eID-stelsel

Het eID-stelsel is zodanig ingericht dat de beoogde verhoging van de betrouwbaarheid en continuïteit wordt gerealiseerd en tegelijkertijd aan stringente eisen die de USvE stelt wordt voldaan. De inrichting van het stelsel is schematisch weergegeven in afbeelding 1.

Afbeelding 1: schematische weergave van het eID-stelsel.



In het stelsel zijn verschillende rollen, verantwoordelijkheden en processen uitgewerkt die een burger in staat stellen om veilig en betrouwbaar een authenticatiemiddel naar keuze aan te vragen en te activeren, het middel te gebruiken om in te loggen bij een overheidsorganisatie, de eigen authenticatiemiddelen te beheren en te beëindigen, en eigen persoonsgegevens in te zien. Ook zijn er processen voor misbruikbestrijding voorzien. De basale werking van het stelsel wordt hieronder geïntroduceerd. De afzonderlijke processen en de wijze waarop daarbinnen persoonsgegevens verwerkt, worden in hoofdstuk 3 uitvoerig omschreven.

Het BSNk als spil van het eID-stelsel

Het BSNk is een overheidsvoorziening om authenticatiemiddelen van zowel private als publieke partijen te koppelen aan het BSN van de houder van het authenticatiemiddel. Daarbij maakt het BSNk gebruik van zogenoemde ***polymorfe pseudoniemen***. Dat wil zeggen dat een burger die een authenticatiemiddel aanvraagt dat middel eenmalig activeert met behulp van het BSN. Het BSNk genereert vervolgens een pseudoniem van die burger, specifiek voor het betreffende middel. Het pseudoniem kan door een dienstverlener via het BSNk vervolgens weer worden omgezet in een leesbare identiteit: de dienstverlener weet dan dat de betreffende burger is wie hij/zij zegt te zijn. Voor overheidsdienstverleners wordt er een pseudoniem gemaakt waaruit het BSN door die dienstverlener te herleiden is, voor private dienstverleners wordt een pseudoniem gehanteerd dat niet naar een BSN te herleiden is. Dit maakt dat het BSN, waarmee de burger zich oorspronkelijk heeft geïdentificeerd, door partijen binnen het stelsel vervolgens niet meer te achterhalen is. Deze opzet is bewust gekozen als een invulling van privacy by design.

Het BSNk vervult binnen het stelsel de volgende functies:

- ***Activatiefunctie:*** eenmalige activatie van een authenticatiemiddel die een gebruiker heeft aangevraagd met behulp van het BSN, waarbij een identiteit van de gebruiker met een pseudoniem aan het authenticatiemiddel is gekoppeld.
- ***Transformatiefunctie:*** als de gebruiker met het authenticatiemiddel wil inloggen bij een dienstverlener wordt het pseudoniem dat gekoppeld is aan dat middel weer omgezet in een leesbare identiteit. Met deze functie stelt de dienstverlener vast dat de gebruiker is wie hij/zij zegt te zijn.
- ***Sleutelbeheerfunctie:*** het BSNk werkt met cryptografische versleuteling. Voor het functioneren van het BSNk zijn daarom cryptografische sleutels nodig. Met deze functie kunnen die sleutels veilig worden beheerd en verstrekt.
- ***Inzagefunctie:*** de gebruiker kan alle authenticatiemiddelen die hij/zij heeft geactiveerd (en gebruikt) inzien en desgewenst deactiveren of intrekken. Voor het daadwerkelijk tonen van de middelen is voorzien dat gebruik wordt gemaakt van MijnOverheid.
- ***Stelselbeheerfunctie:*** registratie van erkende partijen in het stelsel om ervoor te zorgen dat zij met hun rollen binnen het stelsel over en weer herkenbaar zijn.
- ***Misbruikdetectiefunctie:*** de registratie van 'opmerkelijke gebeurtenissen' bij een gebruiker in een misbruikbestrijdingsregister, zodat bij daadwerkelijk misbruik snel opgetreden kan worden en schade voor de gebruiker kan worden voorkomen.

Rollen en verantwoordelijkheden binnen het eID-stelsel

Afbeelding 1 laat zien dat er verschillende rollen worden onderscheiden binnen het eID-stelsel. Deze rollen en de daarbij omschreven verantwoordelijkheden zijn bepalend en kaderstellend voor de verwerkingen van persoonsgegevens binnen het eID-stelsel. Deze rollen worden hieronder toegelicht.

- De ***middelenuitgever (MU)*** stelt authenticatiemiddelen beschikbaar binnen het stelsel en geeft deze op verzoek uit aan de gebruiker. De MU is verantwoordelijk voor activering van een middel bij het BSNk en het actueel houden de status van een authenticatiemiddel.
- Een ***authenticatiedienst (AD)*** voert authenticatieprocedures wanneer een gebruiker een authenticatiemiddel inzet om in te loggen bij een bepaalde dienstverlener. De authenticatiedienst levert een authenticatieverklaring aan de toegangsdienst en legt daarnaast de authenticatiehistorie vast**.** De rollen van middelenuitgever en authenticatiedienst zijn conceptueel gescheiden, maar worden in de praktijk vaak door dezelfde partijen vervuld.
- Een ***toegangsdienst (TD)*** verstrekt verklaringen over de identiteit van een gebruiker aan de dienstverlener. De toegangsdienst biedt de gebruiker de mogelijkheid om een authenticatiedienst te kiezen en vervult in feite de rol van tussenpersoon. Een toegangsdienst is optioneel in het stelsel en vooral bedoeld om andere rollen in het stelsel te ontzorgen.

Buiten de authenticatieketen worden nog de rollen onderscheiden van de ***gebruiker*** van een authenticatiemiddel en van ***dienstverlener*** bij wie de gebruiker wil inloggen om een dienst af te nemen.

2 Aanpak Gegevensbeschermingseffectbeoordeling

2.1 Scope

Het eID-stelsel is nog volop in ontwikkeling. Dat vraagt om nauwgezette afbakening van de scope van deze GEB, om helder te maken welke delen van het stelsel aan de orde komen en welke (nog) niet. Voor die afbakening wordt een aantal uitgangspunten gehanteerd.

Allereerst heeft deze GEB in principe betrekking op ***het gehele eID-stelsel en de basale werking*** daarvan, zoals schematisch weergegeven in Afbeelding 1. In beginsel zijn alle verwerkingen van persoonsgegevens die plaatsvinden wanneer gebruikers digitale diensten afnemen bij een overheidsorganisatie onderwerp van deze GEB. Daartoe moeten alle informatiestromen tussen verschillende partijen (met het BSNk als spil) per deelproces worden geanalyseerd. Tegelijkertijd moet worden benadrukt dat de 'basale werking' de scope is en bepaalde gegevensverwerkingen niet in deze GEB aan bod komen. Dat wordt hieronder toegelicht.

Deze GEB kijkt vooruit naar het zogenoemde ***voorlopertraject***. Dit traject start in januari 2018 en eindigt wanneer de wet GDI in werking treedt. Deze inwerkingtreding is beoogd in januari 2019. De pilots die op dit moment al operationeel zijn mogen doorgang vinden tot aan 1 januari 2018; vanaf dat moment moeten partijen voldoen aan de vernieuwde eisen die – met inachtneming van de aanbevelingen uit deze GEB - gesteld worden, waarop deze GEB betrekking heeft. Tot aan dat moment zullen de huidige pilots doorlopen, maar gebonden zijn aan beperking in omvang ten aanzien van de uitrol, e weten een beperking van het aantal middelen dat mag worden uitgegeven tot maximaal 300.000.

Dat het eID-stelsel nog volop in ontwikkeling is, betekent dat deze GEB een ***momentopname*** is, met als doel privacyrisico's en mogelijke maatregelen te benoemen zoals die nu gezien worden en die in de verdere ontwikkeling kunnen worden geadresseerd. Deze GEB richt zich op de inrichting en werking van het eID-stelsel gedurende het voorlopertraject voor zover nu bekend. Dat betekent het volgende voor de scope:

- Artikel X van de ***Wet elektronisch berichtenverkeer Belastingdienst (Wet EBV)*** en de daarop gebaseerde uitvoeringsregeling vormen de wettelijke grondslag voor de verwerkingen van persoonsgegevens in het voorlopertraject. De rechtmatigheid van de gegevensverwerkingen wordt in deze GEB getoetst aan deze wet.
- Deze GEB gaat uit de ***Uniforme Set van Eisen versie 1.0*** die tot eind maart 2017 in consultatie is geweest. De vernieuwde versie (USvE 1.x) zal uiteindelijk de basis vormen voor het functioneren van eID-stelsel in het voorlopertraject.
- Gedurende het voorlopertraject zal ***BSNk versie 2.0*** operationeel zijn. Deze GEB gaat uit van het programma van eisen, de projectstartarchitectuur en de ontwerpdocumentatie van BSNk 2.0 die nu bekend zijn.

Buiten de scope

Deze GEB richt zich op de basale werking van het eID-stelsel. De volgende onderwerpen vallen buiten de scope van deze GEB:

- ***Publieke en private authenticatiemiddelen als zodanig:*** op grond van de AVG is een aparte GEB verplicht. Verplichting tot naleving privacywetgeving staat in USvE, een GEB zal daar onderdeel van zijn. Publieke authenticatiemiddelen zoals DigiD en private authenticatiemiddelen zoals Idensys en iDIN behoren niet tot de scope.
- ***Wet generieke digitale infrastructuur:*** omdat deze wet in 2019 in werking treedt, behoort deze wet niet tot de scope van deze GEB.
- ***Interne processen bij dienstverleners*** en de wijze waarop zij binnen de eigen organisatie gegevens opslaan en verwerken vallen buiten de scope van deze GEB. Voor de goede orde: de USvE 1.0 stelt geen eisen aan publieke dienstverleners.
- ***Burgers*** De genoemde documenten richten zich niet direct op burgers/gebruikers. In die zin vallen zij daarom buiten de scope van deze GEB. De privacybelangen van burgers spelen uiteraard wel een – juist fundamentele – rol in de GEB en zijn binnen scope.

Samenvattend: Deze GEB biedt inzicht in de verwerkingen van persoonsgegevens die nodig zijn voor de basale werking van het stelsel. Om een totaalbeeld te verkrijgen van de verwerking van persoonsgegevens in concrete situaties, zal het nodig zijn om ook de verwerkingen van

persoonsgegevens inzichtelijk te krijgen die plaatsvinden bij deelnemers binnen het stelsel die verschillende rollen invullen (zoals een middelenuitgever of authenticatiedienst). Deze verwerkingen tezamen maken het beeld compleet. Dat beeld kan, gezien de ruimte die de USvE bewust aan dienstverleners biedt, per situatie op onderdelen verschillen. Echter de verplichting om aan de AVG te voldoen zal onverkort gelden.

2.2 Opbouw

Op 25 mei 2018 worden de nieuwe Europese privacyverordening AVG en de Nederlandse Uitvoeringswet AVG van kracht. Deze GEB volgt de voorschriften die de AVG voor de uitvoering van GEB's stelt, niet in de laatste plaats omdat deze GEB zich richt op het eID-stelsel zoals dat gedurende het voorlopertraject vanaf 2018 gaat functioneren. Het Toetsmodel PIA Rijksdienst[9] dat voorheen voor het opstellen van een PIA werd gehanteerd, wordt op dit moment aangepast aan de voorschriften. Het conceptmodel GEB Rijksdienst is voor deze GEB gebruikt en tegelijkertijd getoetst.

Het conceptmodel GEB Rijksdienst bestaat uit vier onderdelen en omvat in totaal 16 toetspunten. Het volledige model en een korte samenvatting van deze GEB aan de hand van de 16 toetspunten is opgenomen als bijlage 1. De opbouw van deze GEB sluit aan bij de vier onderdelen. De beschrijving van algemene kenmerken van de gegevenswerking (onderdeel A) komt in hoofdstuk 3 aan de orde. De beschrijving van de rechtmatigheid van de gegevensverwerkingen, risico's voor de rechten en vrijheiden van betrokkene en voorgenomen maatregelen komen in hoofdstuk 4 aan bod.

2.3 Verantwoording

Deze GEB is in opdracht van de minister van Binnenlandse Zaken en Koninkrijksrelaties uitgevoerd in de periode februari – juni 2017, onder de verantwoordelijkheid van de programmaleider eID. Om kwaliteit van de GEB te waarborgen en periodiek te toetsen is een GEB begeleidingscommissie, bestaande uit de Functionaris voor de Gegevensbescherming van de ministeries van BZK en VenJ en vertegenwoordigers van de directie Constitutionele Zaken en Wetgeving (CZW) van het ministerie van BZK, CIO BZK, I-control BZK en Logius. De scope en aanpak van de GEB zijn in overleg met de begeleidingscommissie bepaald.

De GEB is gebaseerd op de volgende schriftelijke bronnen:

- De Wet EBV en onderliggende uitvoeringsregeling
- De USvE 1.0
- Ontwerpdocumenten BSNk 2.0 die door uitvoeringsorganisatie Logius beschikbaar zijn gesteld
- De eerder uitgevoerde PIA's ten aanzien van het ontwerp op hoofdlijnen eID-stelsel 1.0 van juli 2014[10] en het introductieplateau eID-stelsel 1.0 van juli 2015[11]

Daarnaast heeft er herhaaldelijk overleg plaatsgevonden met inhoudelijk deskundigen betrokken bij het ontwerp van het stelsel. Zo heeft Logius als ontwikkelorganisatie gezorgd voor de inbreng van technische en ontwerpkennis, om te zorgen voor een feitelijk juiste weergave van de verwerkingen van persoonsgegevens.

---

[9] De vragenlijst behorende bij het Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst van 24 juni 2013 (Bijlage bij TK, 26 643, nr. 282)

[10] Volg deze link voor de uitkomsten van de PIA op het ontwerp op hoofdlijnen eID-stelsel van juli 2014: https://www.idensys.nl/fileadmin/bestanden/idensys/documenten/basisdocumentatie/pia/Privacy_impactanalyse_eID_Stelsel.pdf

[11] Volg deze link voor de uitkomsten van de PIA op het introductieplateau Idensys: https://www.idensys.nl/actueel/item/artikel/privacy-impact-assessment-idensys-gereed-1/

2.4 Toetsingskader

Om de mate waarin privacybeginselen inzake de verwerking van persoonsgegevens worden nageleefd binnen het eID-stelsel en privacyrisico's te kunnen vaststellen, wordt in deze GEB getoetst in hoeverre de inrichting en de basale werking van het eID-stelsel voldoet aan de toetspunten van het model GEB Rijksdienst en de privacyprincipes van de AVG. Dit toetsingskader is weergegeven in afbeelding 2.

Afbeelding 2

Toetspunt	**Norm**
Grondslag	De persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. De gegevensverwerking is gebaseerd op tenminste één van de zes grondslagen genoemd in artikel 6, eerste lid, AVG.
Bijzondere en strafrechtelijke persoonsgegevens	Indien van toepassing: er geldt bij wet een uitzondering op het verbod tot verwerking van bijzondere persoonsgegevens (artikel 9, eerste lid, AVG). Verwerking van strafrechtelijke gegevens vindt plaats door of onder toezicht van de overheid, of is bij wet geregeld (artikel 10, AVG).
Doelbinding	Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld en worden niet verder verwerkt op een met die doeleinden onverenigbare wijze (artikel 5, eerste lid, onderdeel b, AVG).
Noodzaak en evenredigheid	Gegevensverwerking wordt beperkt tot wat noodzakelijk is voor de doeleinden waarvoor de gegevens worden verwerkt (artikel 6, AVG). De inbreuk op de persoonlijke levenssfeer van betrokkenen staat in evenredige verhouding tot de met de gegevensverwerkingen nagestreefde doelen (proportionaliteit). De verwerkingsdoeleinden kunnen niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt (subsidiariteit).
Dataminimalisatie	Persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (artikel 5, eerste lid, onderdeel c, AVG).
Opslagbeperking	Persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is (artikel 5, eerste lid, onderdeel e, AVG).
Juistheid	Alle redelijke maatregelen moeten worden genomen, die gelet op de doeleinden waarvoor persoonsgegevens worden verwerkt juist zijn, en als dat niet zo is, deze onverwijld te wissen of te rectificeren (artikel 5, eerste lid, onderdeel d, AVG).
Beveiliging	Er moeten passende technische of organisatorische maatregelen worden genomen, zodanig dat een passende beveiliging van de persoonsgegevens is gewaarborgd, zodat de persoonsgegevens ondermeer zijn beschermd tegen ongeoorloofde en onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (artikel 5, eerste lid, onderdeel f, AVG).
Accountability	De verwerkingsverantwoordelijke moet naleving van de privacyprincipes verantwoorden en aantonen (artikel 5, tweede lid, AVG). Er is een scherp en gedocumenteerd zicht op de gevoerde verwerking van persoonsgegevens, de redenen, grondslagen en verantwoordelijkheden.

3 Processen en stelselbrede verwerkingen van persoonsgegevens eID-stelsel

In dit hoofdstuk wordt zo volledig mogelijk beschreven welke verwerkingen van persoonsgegevens plaatsvinden. Daarbij wordt ook ingegaan op welke organisaties verantwoordelijk zijn voor welke gegevensverwerkingen en welke gegevens zij dan verwerken. Dat is uit de USvE niet volledig af te leiden.

Dit is ook niet de primaire doelstelling van de USvE. De documenten zijn juridisch en technisch/functioneel van aard. Ten behoeve van de GEB is een vertaalslag nodig geweest om de werking van het eID-stelsel en de wijze waarop persoonsgegevens worden verwerkt inzichtelijk te maken.

De USvE benoemt dat er participanten kunnen zijn, organisaties die verschillende rollen kunnen hebben: authenticatiedienst, middeluitgever en toegangsdienst. Daarnaast zijn er dienstverleners en burgers en is er het BSNk, waar zoals eerder gezegd in de USvE zelf geen eisen aan worden gesteld. Bij de verschillende rollen beschrijft de USvE welke verantwoordelijkheden de participant die de rol uitvoert in ieder geval heeft. Daarmee geeft de USvE een aanduiding van de processen waarin de gegevens verwerkt worden. Er wordt niet exact aangegeven welke gegevens verwerkt worden. Voor de beschrijvingen in dit hoofdstuk is daarom naast de informatie uit de genoemde documenten dan ook voor een belangrijk deel geput uit onderliggende ontwerpdocumenten en de informatie zoals die in diverse gesprekken en overleggen met bij de ontwikkeling van het stelsel betrokken deskundigen is verkregen.

De werking van het eID-stelsel wordt beschreven aan de hand van hoofdprocessen waarbinnen persoonsgegevens worden verwerkt. Deze hoofdprocessen sluiten aan bij de “life cycle” (activering, authenticatie en statusbeheer & deactivering) van eID middelen in het publieke domein. Daarnaast worden processen ten behoeve van de inzage voor burgers in hun gegevens (inzage) en het voorkomen van misbruik van middelen (misbruikbestrijding) beschreven.

Dit leidt tot de volgende procesbeschrijvingen en verwerkingen van persoonsgegevens:

1. Activering van een authenticatiemiddel bij het eID-stelsel (aanmelding)
2. Authenticatie met een middel binnen het eID-stelsel (het gebruik)
3. Statusbeheer van een authenticatiemiddel (beheer)
4. Proces van inzage in persoonsgegevens
5. Misbruikbestrijding

Om deze processen heen bestaan nog functionaliteiten die deze hoofdprocessen faciliteren. De belangrijkste daarvan betreffen de functionaliteiten van het BSNk. Deze functionaliteiten zijn opgenomen in de procesbeschrijvingen van de hoofdprocessen. De functionaliteiten van het BSNk zullen daarnaast nog apart worden uitgewerkt bij de functionele bespreking van het BSNk.

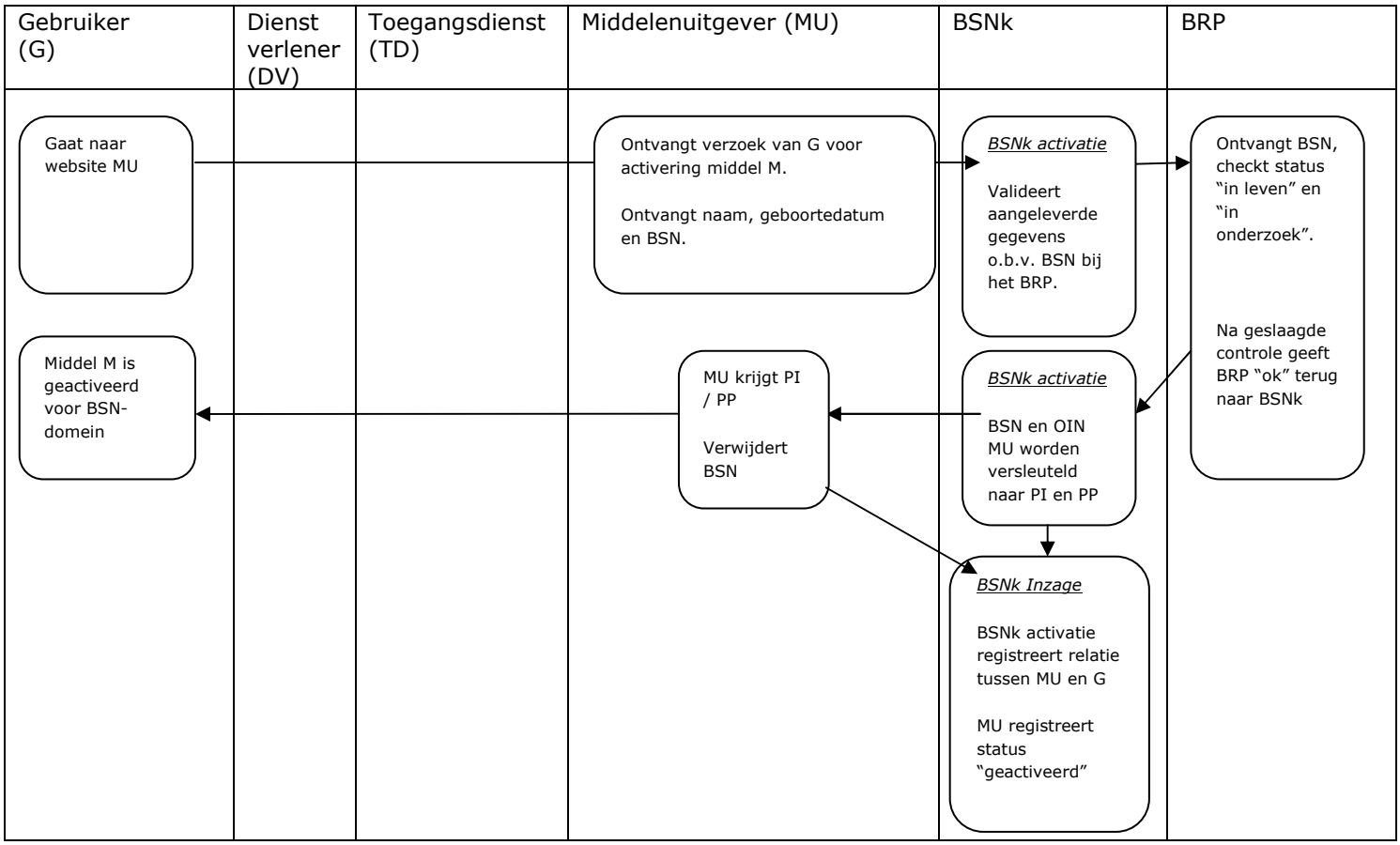
3.1 Activeringsproces (aanmelding)

3.1.1 Doel van het proces

Het doel van dit proces is om ervoor te zorgen dat een gebruiker éénmalig, op basis van zijn BSN, op een betrouwbare wijze in het stelsel geregistreerd wordt, zodat in het vervolg – als de gebruiker het middel gebruikt voor authenticatie bij een dienstverlener – op deze registratie kan worden vertrouwd en met pseudoniemen gewerkt kan worden.

3.1.2 Schematische weergave

Afbeelding 3: Activeren van een middel voor het publieke domein



3.1.3 Procesbeschrijving

In afbeelding 3 zijn de stappen weergegeven die worden doorlopen bij de activering van een authenticatiemiddel voor het publieke domein. Voor de goede orde wordt opgemerkt dat de aanvraag van een middel buiten scope is van dit proces. Dit is een proces voorafgaand aan de activering en hangt af van de manier waarop een middelenuitgever dit proces binnen de eIDAS eisen heeft ingericht. Het activatieproces start op het moment dat een gebruiker een middel wil activeren voor gebruik in het publieke domein. De start van dit proces vereist een actieve handeling (instemming) van de gebruiker.

De gebruiker gaat daarvoor naar (de website van) de middelenuitgever en geeft aan het middel te willen activeren. Om de middelenuitgever voldoende zekerheid te bieden dat de gebruiker daadwerkelijk is wie hij/zij aangeeft te zijn, zal de gebruiker ook WID-gegevens[12] dienen aan te leveren, indien dat nog niet eerder is gebeurd. Dit betreft naam, geboortedatum en BSN.

De middelenuitgever verzendt deze gegevens van de gebruiker, tezamen met zijn eigen overheidsidentificatienummer (OIN) via een beveiligde verbinding naar de zogeheten activatiefunctie van het BSNk (hierna: BSNk-activatie). Deze functie zorgt voor de creatie van polymorfe identiteiten. Voordat de pseudonieme identiteiten worden gecreëerd, verifieert BSNk-activatie de gebruikersgegevens (naam, geboortedatum) bij de BRP. Tevens wordt gecontroleerd of de persoon als "in leven" staat geregistreerd en of de gegevens niet "in onderzoek"[13] zijn.

De controle op deze gegevens is primair bedoeld om (invoer)fouten te voorkomen, maar werkt daarnaast als extra veiligheidsmaatregel om zeker te stellen dat de door de gebruiker

[12] Gegevens op wettelijke identiteitsdocumenten (WID).
[13] Dat houdt in of er geen gerede twijfel bestaat ten aanzien van de juistheid van bepaalde gegevens in de BRP.

aangeleverde set gegevens overeenkomt met de registratie in de BRP en dat niet ten onrechte een pseudoniem voor een andere persoon wordt gecreëerd. De controle draagt daarmee tevens bij aan de juistheid van de verwerkte gegevens binnen het stelsel.

Als deze controle is geslaagd wordt over het aangeleverde BSN tezamen met het OIN van de aanvragende middelenuitgever door BSNk-activatie een versleuteling uitgevoerd. Het resultaat daarvan is een polymorf versleutelde identiteit. Die identiteit is specifiek gekoppeld aan een gebruiker én de middeluitgever, doordat het BSN van een gebruiker en het OIN van een middelenuitgever als input dienen.

BSNk-activatie verstrekt deze polymorf versleutelde (pseudo)identiteit aan de middelenuitgever. BSNk-activatie registreert vervolgens de relatie tussen de middelenuitgever en de gebruiker bij het BSNk-inzageregister, zodat de gebruiker het inzageregister kan raadplegen (zie hiervoor het proces "Inzage"). Ook de middelenuitgever legt ten slotte de polymorf versleutelde (pseudo)identiteit vast en registreert de geactiveerde status van het authenticatiemiddel bij het BSNk-inzageregister. Voor de werking van deze registratie, zie het proces "Statusbeheer en deactivering van een authenticatiemiddel".

Na het doorlopen van deze stappen kan een gebruiker het authentatiemiddel gebruiken in het publieke domein. En indien de gebruiker dat wenst kan hij op elk gewenst moment het BSNk-inzageregister raadplegen om een overzicht van zijn registreerde middelen en status ervan in te zien. Daarmee is het activatieproces voltooid.

3.1.4 Verwerking van persoonsgegevens per rol/verantwoordelijkheid

Rol/verantwoordelijkheid middelenuitgever

Na activering bij het BSNk worden de bijbehorende PP / PI opgeslagen[14][15]. Het BSN wordt door de middelenuitgever, na de activatie, voor dit proces niet meer bewaard. De geboortedatum en naam van de gebruiker blijven wel bewaard als de MU daar een noodzaak voor heeft, bijvoorbeeld als 'accountgegeven' om de dienstverlening te kunnen uitvoeren. Deze gegevens zijn nodig om de gebruiker de dienst te kunnen verlenen en worden, zo blijkt uit de USvE 1.0, bewaard gedurende de dienstverlening en voor een periode van 18 maanden daarna, om een gebruiker de mogelijkheid te bieden om ook een periode na beëindiging van de dienstverlening inzicht te kunnen bieden. Daarnaast blijven gegevens bewaard ten behoeve van foutopsporing en verantwoording (voor de borging dat het proces juist is doorlopen).

Rol/verantwoordelijkheid BSNk

Het BSN, geboortedatum en naam van de gebruiker worden verwerkt. Na validatie bij de BRP wordt het BSN verwijderd uit het BSNk. Daarnaast worden logistieke bericht- en verwerkings-gegevens ten behoeve van foutopsporing en verantwoording (de borging dat het proces juist is doorlopen) bewaard. Daarbij gaat het om het loggen van het resultaat van elke verwerkingsstap, zodat inzichtelijk blijft hoe het proces is verlopen.

Rol/verantwoordelijkheid BRP

Het BSN, geboortedatum en naam van de gebruiker worden verwerkt. De BRP krijgt het BSN aangeleverd van het BSNk voor de validatie, en geeft daarop als resultaat aan het BSNk de bijbehorende naam en geboortedatum, ten behoeve van de validatie, terug aan het BSNk.

3.1.5 Toelichting op het proces vanuit oogpunt van bescherming van persoonsgegevens

Gebruik van Polymorfe Identiteiten

[14] En eventueel doorgeleverd aan gelieerde authenticatiediensten.
[15] Een toelichting op polymorfe pseudoniemen (PP) en polymorfe identiteiten (PI) worden nader uitgelegd in paragraaf 3.1.5

Ten behoeve van privacy, dat wil zeggen minimalisering van het gebruik van het BSN, worden er als resultaat van het proces feitelijk twee typen polymorfe identiteiten tegelijk verstrekt:

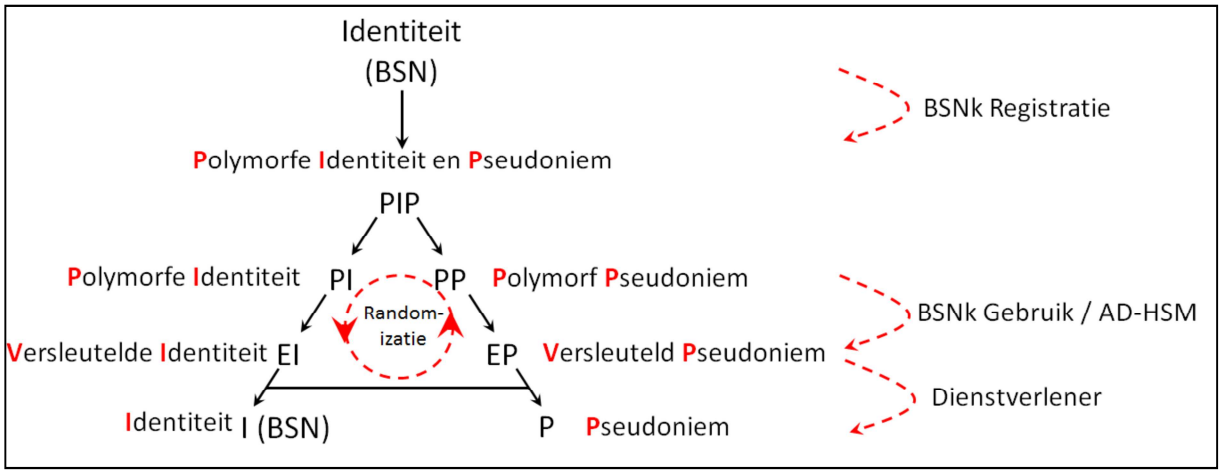
1. Een identiteit gebaseerd op versleuteling van het BSN van een gebruiker met een OIN van de middelenuitgever. Dit is een zogeheten polymorfe identiteit (PI), waaruit het BSN is te ontcijferen. Deze is bedoeld voor gebruik in het publieke (BSN) domein.
2. Een identiteit gebaseerd op een vooraf onomkeerbaar versleuteld BSN en het OIN van de middelenuitgever. Dit is een zogeheten polymorf pseudoniem (PP). Het BSN kan hieruit niet worden herleid. Dit is bedoeld voor gebruik in het private domein of voor gebruik in het publieke domein waarvoor geen BSN mag worden gebruikt.

Het PI en PP worden gegenereerd als het BSN voor activatie wordt aangeleverd. Deze stellen gebruikers in staat om met een eID-middel zowel in te loggen in het publieke domein (op basis van de PI) als in het private domein (op basis van het PP). Door de activatie is de identiteit van de gebruiker gecontroleerd en verzekerd. Ook zijn de identiteiten van de gebruiker aan elkaar én aan een middelenuitgever verzekerd en gekoppeld.

Op het moment dat de koppeling tussen PP en PI en het authenticatiemiddel is gelegd, schrijft de USvE voor dat de middelenuitgever het BSN verwijdert. Wel blijven bij de middelenuitgever accountgegevens bewaard om de dienstverlening te kunnen leveren. Daarnaast blijven enkel gegevens ten behoeve van foutopsporing en verantwoording (de borging dat het proces juist is doorlopen) bewaard.

Door deze combinatie van processtappen zijn de oorspronkelijk identificerende gegevens (BSN) binnen het eID-stelsel zelf niet meer te achterhalen en voor vervolggebruik binnen het stelsel ook niet meer nodig. Alleen de BSN-gerechtigde dienstverlener kan het BSN nog herleiden. Authenticatie vindt vervolgens plaats op basis van polymorf versleutelde identiteiten die specifiek zijn voor de betreffende middelenuitgever. De authenticatie bouwt daarmee voort op de betrouwbare activatie. Dit vormt de kern van de privacy-ontwerpmaatregel van het stelsel (dataminimalisatie). In onderstaand schema (afbeelding 4) is dit schematisch weergegeven.

Afbeelding 4



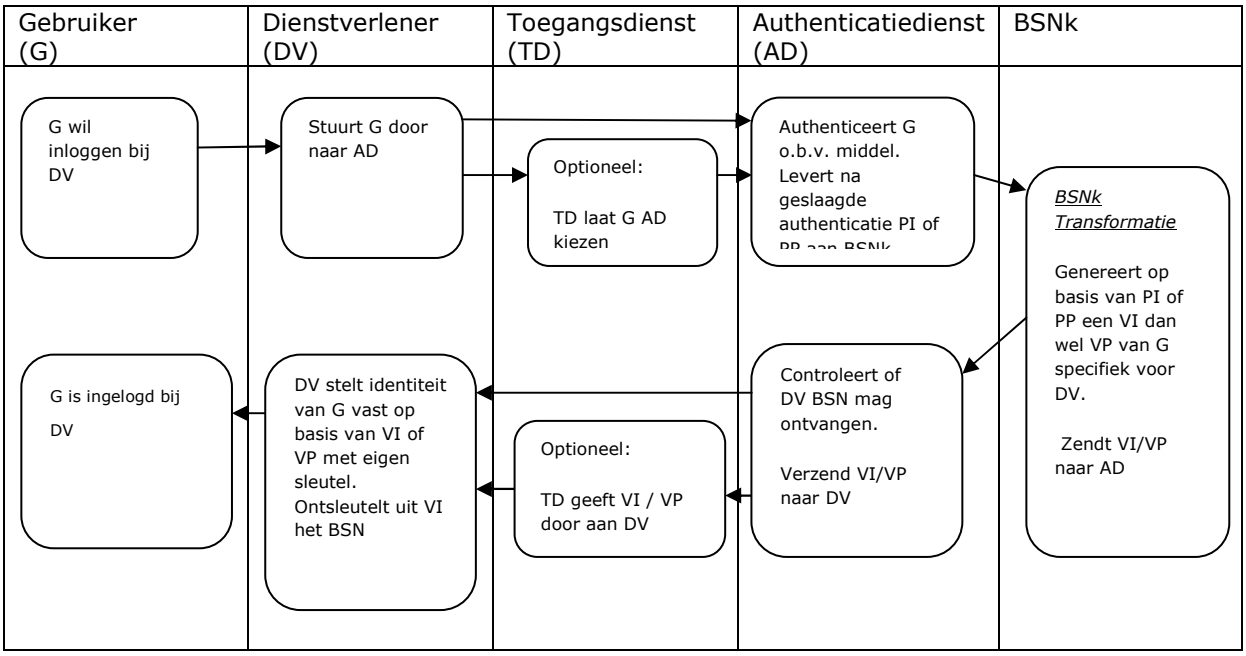
3.2 Authenticatie met een middel binnen het eID-stelsel

3.2.1 Doel van het proces

Het doel van dit proces is om de gewenste zekerheid te verkrijgen over de identiteit van een gebruiker en deze op basis van een pseudoniem toegang te verlenen tot de (overheids)dienstverlener.

3.2.2 Schematische weergave

Afbeelding 5: authenticatieproces



3.2.3 Procesbeschrijving

Het proces start op het moment dat een gebruiker bij een overheidsdienstverlener met zijn geactiveerde middel wil inloggen om zaken te regelen. De gebruiker gaat dan naar de website van een dienstverlener om zich te authenticeren.

Omdat gebruikers binnen het eID-stelsel, gelet op de multimiddelenstrategie, meerdere geregistreerde authenticatiemiddelen kunnen hebben en van meerdere authenticatiediensten

gebruik kunnen maken, kan de gebruiker eerst doorgeleid worden naar een zogeheten toegangsdienst. Deze toegangsdienst helpt gebruikers om hun gewenste middel voor de betreffende authenticatie te kiezen. Daar maakt de gebruiker de keuze voor een authenticatiedienst. De inzet van een toegangdienst is overigens optioneel. Het is ook mogelijk dat een gebruiker direct vanaf een overheidsdienstverlener naar de authenticatiedienst wordt doorgeleid.

Een gebruiker wordt – al dan niet door tussenkomst van een toegangsdienst – doorgeleid naar de gekozen authenticatiedienst. De authenticatiedienst informeert de gebruiker over de dienstverlener waarvoor hij gaat authenticeren en authenticeert vervolgens de gebruiker met behulp van diens eerder geregistreerde authenticatiemiddel. De authenticatiedienst heeft op dat moment zekerheid over de identiteit van de gebruiker.

Nadat authenticatie heeft plaatsgevonden, dient de authenticatiedienst de identiteit van de gebruiker terug te koppelen aan de dienstverlener. Deze terugkoppeling vindt in versleutelde vorm plaats. De authenticatiedienst gebruikt hiervoor de PP of PI van de gebruiker die hij van BSNk-activatie heeft gekregen. Om dat mogelijk te maken wordt gebruik gemaakt van de zogeheten transformatiefunctie van het BSNk (hierna: BSNk-transformatie). De BSNk-transformatie zet een polymorfe identiteit of een polymorf pseudoniem om in een versleutelde identiteit (VI, als het publieke dienstverlener is) respectievelijk versleuteld pseudoniem (VP, als het een private dienstverlener is). De versleuteling is zodanig dat alleen de beoogde dienstverlener de daadwerkelijke identiteit van de gebruiker kan herleiden. Om herkenning van de identiteit verder tegen te gaan zorgt de transformatie er ook nog voor dat de VP en VI er telkens ander uit zien (dit heet "randomisatie").

De BSNk-transformatie kan centraal bij het BSNk uitgevoerd worden maar ook bij de authenticatiedienst zelf. De BSNk beheerorganisatie verstrekt voor dit doel via een speciale veilige manier (key ceremony[16]) sleutelmateriaal, ten behoeve van een BSNk transformatiemodule voor een zogeheten beveiligde omgeving (Hardware Security Module ofwel HSM) bij de authenticatiedienst. Uitgangspunt is dat authenticatiediensten dit zelf doen omdat daarmee het authenticatieproces geen afhankelijkheid meer heeft met het BSNk en de gegevensconcentratie bij het BSNk vermindert. Het BSNk is daarmee geen privacy hotspot en ook geen single point of failure meer. Na de transformatie beschikt de authenticatiedienst op basis van de PI of het PP van de gebruiker over een specifieke voor de dienstverlener VI of VP.
Voordat een authenticatiedienst een VI terugzendt naar een overheidsdienstverlener, controleert hij of de betreffende dienstverlener is opgenomen in de zogeheten autorisatielijst BSN (ALB). Hierop staan de dienstverleners die gerechtigd zijn het BSN te gebruiken. Deze ALB wordt door de BSNk beheerorganisatie gepubliceerd. Als een dienstverlener niet is opgenomen in deze ALB mag de authenticatiedienst geen VI terugzenden. Dat zou overigens ook geen zin hebben omdat een dienstverlener die niet op de ALB staat ook geen sleutelmateriaal bij het BSNk kan krijgen om een BSN uit een VI te ontsleutelen. Deze twee maatregelen zorgen voor een dubbele controle een organisatie alleen een BSN ontvangt als die daartoe gerechtigd is.

Op het moment dat een overheidsdienst is opgenomen op de ALB stuurt de authenticatiedienst de VI (nogmaals versleuteld via een beveiligde verbinding) terug naar de dienstverlener, indien van toepassing via de toegangsdienst. De dienstverlener kan vervolgens met zijn eigen sleutelmateriaal de VI ontsleutelen naar een BSN. Ook dit sleutelmateriaal wordt verstrekt door de beheerorganisatie van het BSNk via de zogeheten BSNk sleutelbeheerfunctie. De dienstverlener beschikt op dat moment over het BSN van de gebruiker die zich heeft geauthenticeerd en kan de dienstverlening aan de gebruiker starten.

[16] https://en.wikipedia.org/wiki/Key_ceremony

3.2.4 Verwerking van persoonsgegevens per rol/verantwoordelijkheid

Rol/verantwoordelijkheid toegangsdienst (optioneel)

De toegangsdienst ontvangt het authenticatieverzoek van de gebruiker van de overheidsdienstverlener. Daarbij wordt het benodigde betrouwbaarheidsniveau vermeld, evenals het benodigde identificatietype (PI of PP). De toegangsdienst presenteert de gebruiker een overzicht van de voor de gebruiker beschikbare (geactiveerde) authenticatiemiddelen en authenticatiediensten. Nadat de gebruiker zijn keuze heeft gemaakt wordt de gebruiker doorgezonden naar de authenticatiedienst. Nadat deze stap is uitgevoerd blijven gegevens bewaard ten behoeve van foutopsporing en verantwoording (de borging dat het proces juist is doorlopen).

Rol/verantwoordelijkheid authenticatiedienst

De authenticatiedienst ontvangt het authenticatieverzoek van de gebruiker van de overheidsdienstverlener, met benodigde betrouwbaarheidsniveau en authenticatietype (de manier waarop geauthenticeerd wordt). Na authenticatie verwerkt de authenticatiedienst de bij de gebruiker behorende PI of PP. Indien de authenticatiedienst zelf beschikt over een HSM zet de authenticatiedienst de PI of PP zelf om naar een VI respectievelijk VP. Nadat deze omzetting heeft plaatsgevonden verzendt de authenticatiedienst de VI of VP, na controle op de ALB, naar de overheidsdienstverlener. Nadat deze stap is uitgevoerd slaat de authenticatiedienst gegevens op ten behoeve van gebruikshistorie en misbruikbestrijding. Daarnaast blijven ook gegevens bewaard ten behoeve van foutopsporing en verantwoording (de borging dat het proces juist is doorlopen).

Rol/verantwoordelijkheid BSNk

Indien een authenticatiedienst niet zelf beschikt over een HSM ontvangt het BSNk (BSNk-transformatiefunctie) van een authenticatiedienst een PI of PP, met het verzoek om deze om te zetten naar een VI respectievelijk VP. De PI of PP moeten door de authenticatiedienst elke keer opnieuw 'gerandomiseerd' worden zodat de BSNk transformatie de PI of PP niet kan herkennen. Nadat deze omzetting is gebeurd, stuurt BSNk-transformatie de verkregen VI of VP terug naar de authenticatiedienst. Nadat deze stap is uitgevoerd blijven enkel logistieke gegevens bewaard ten behoeve van foutopsporing en verantwoording (de borging dat het proces juist is doorlopen)

3.2.5 Toelichting op het proces vanuit oogpunt van bescherming van persoonsgegevens

Rollenscheiding en compartimentering van functies

Bij de beschrijving van het authenticatieproces (en overigens ook bij het activatieproces) komt naar voren dat een proces over meerdere schijven (rollen) verloopt. De keus om de processtappen onder te verdelen is er een die expliciet binnen de USvE is gemaakt en die een belangrijke privacy-ontwerpmaatregel vormt (privacy by design).

De rollen toegangsdienst, authenticatiedienst en middelenuitgever zorgen samen voor de authenticatie van een gebruiker. De rolverdeling moet onder andere zorgen voor compartimentering van persoonsgegevens. Die kunnen namelijk per rol beperkt worden tot die gegevens die nodig zijn voor het uitvoeren van die rol. Elke rol kan door een aparte partij uitgevoerd worden maar partijen kunnen ook meerdere rollen invullen. Dit USvE verbiedt deze "rolvermenging" niet. Maar de USvE schrijft wel voor dat áls dit het geval is, compartimentering aangebracht moet worden tussen deze drie rollen. Met name de compartimentering tussen de rol van middelenuitgever (gebruikersgegevens) en authenticatiedienst (gebruiksgegevens) is van belang om te voorkomen dat concentraties van opgeslagen persoonsgegevens (privacy hotspots) ontstaan.

Naast deze rollenscheiding zorgt de polymorfe cryptografie voor compartimentering tussen deelnemers onderling. Authenticatie vindt immers plaats op basis van polymorf versleutelde identiteiten (PI/PP) die specifiek zijn voor de betreffende middelenuitgever. Deze polymorf versleutelde identiteiten kunnen daardoor alleen door de betreffende middelenuitgever gebruikt

worden of door een authenticatiedienst die 'geaffilieerd' (door samenwerking verbonden) is met deze middelenuitgever. Andere partijen binnen het stelsel kunnen hieruit geen persoonsgegevens afleiden.

Ook de pseudoniemen die een dienstverlener krijgt voor een dienst waarbij geen BSN nodig is (of waarbij een BSN niet gebruikt mag worden) zijn specifiek voor die dienstverlener. Dienstverleners worden daarmee onderling gecompartimenteerd omdat hun pseudoniemen onderling niet relateerbaar zijn. Deze eigenschap wordt door het BSNk ook gebruikt.

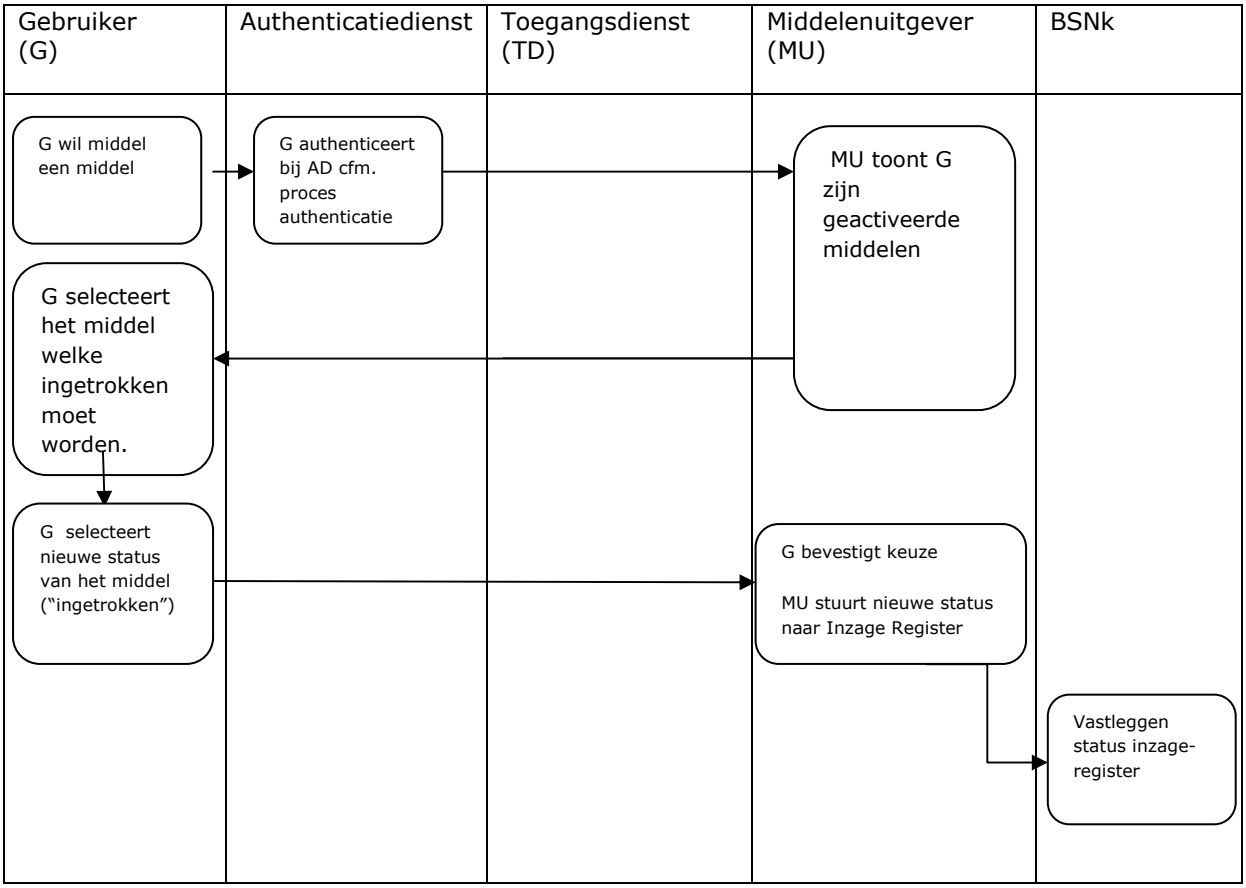
3.3 Statusbeheer van een middel

3.3.1 Doel van het proces

Het doel van het proces is om statusregistratie van een middel voor een gebruiker actueel te houden, zodat de gebruiker desgewenst inzage kan worden geboden in de status(historie) van zijn geactiveerde middelen.

3.3.2 Schematische weergave

Afbeelding 6: intrekken van een middel door de gebruiker.



In deze paragraaf wordt het proces beschreven waarmee de middelenuitgever de nieuwe of gewijzigde status van een authenticatiemiddel bij het BSNk-inzageregister kan registreren. Deze status kan door verschillende oorzaken (moeten) wijzigen, bijvoorbeeld doordat de geldigheid van een middel verloopt, een gebruiker een middel verliest of de gebruiker zijn middel beëindigt. Een middel kan in het BSNk-inzageregister de volgende statussen hebben:

- ***Geactiveerd:*** het middel kan gebruikt worden in het publieke domein.
- ***Gedeactiveerd (suspended):*** het middel kan niet meer worden gebruikt in het publieke domein. Een middel kan gedeactiveerd worden door een gebruiker zelf als deze zijn middel

(eigen keuze) niet meer in het publieke domein wil gebruiken of door een middelenuitgever indien een indicatie voor misbruik bestaat. Een middel kan na deactivatie weer geactiveerd worden.

- ***Ingetrokken (revoked):*** een middel kan worden ingetrokken bijvoorbeeld als een gebruiker zijn middel kwijt is of als het gestolen is, of door een middelenuitgever als de gebruiker geen klant meer is. Een eenmaal ingetrokken middel kan niet meer geactiveerd worden.
- ***Verlopen (expired):*** een middel kent een maximale geldigheidsduur. Als deze termijn verstreken is, verloopt het authenticatiemiddel. Een verlopen authenticatiemiddel kan niet meer geactiveerd worden.

Bij het activeringsproces wordt als laatste stap (zie paragraaf 3.1) door de middelenuitgever de geactiveerde status van het authenticatiemiddel bij het BSNk-inzageregister geregistreerd. Deze registratie is identiek voor de registratie van elke statuswijziging (deactivering, intrekking, verlopen) van een authenticatiemiddel.

Het proces tot aanpassing van de status start bij een middelenuitgever. Een middelenuitgever is verplicht om de status actueel te houden in de registratie bij het BSNk. Bijvoorbeeld het scenario waarin een gebruiker zijn middel wil intrekken. Aan de hand van dit intrekscenario (revocatie) wordt in deze paragraaf het proces van de statuswijziging beschreven.

3.3.3 Procesbeschrijving

Statuswijziging (revocatie) van een middel op initiatief van de gebruiker

Indien een gebruiker dat wenst, kan hij zelf zijn middel intrekken en het gebruik van zijn middel in het publieke domein beëindigen. De gebruiker gaat daarvoor naar de website van zijn middelenuitgever. De middelenuitgever laat de gebruiker bij de authenticatiedienst (meestal dezelfde partij) het authenticatieproces – op tenminste hetzelfde betrouwbaarheidsniveau als het middel zelf - doorlopen om de identiteit van de gebruiker vast te stellen.

Na authenticatie toont de middelenuitgever de gebruiker diens actieve middelen. De gebruiker selecteert het middel dat ingetrokken moet worden, aan de hand van een herkenbaar volgnummer en/of einddatum. De gebruiker geeft daarna expliciet aan dat de geldigheid van een middel moet worden ingetrokken en bevestigt deze keuze nogmaals. De middelenuitgever moet vervolgens de gewijzigde status bij het BSNk-inzageregister registreren. Hiervoor heeft de middelenuitgever het VP van deze gebruiker bij het BSNk-inzageregister nodig. De middelenuitgever kan (evt. met behulp van de BSNk-transformatiefunctie) de PP van de gebruiker transformeren naar een VP specifiek voor het BSNk-inzageregister[17].

Omdat een gebruiker meerdere middelen kan hebben (gehad), dient de middelenuitgever bij een registratie het betreffende middel te identificeren met behulp van een middeltype (de manier waarop geauthenticeerd wordt), en een volgnummer. Om het de gebruiker wat makkelijker te maken om het middel te herkennen, kan de middelenuitgever ook een middelbeschrijving meeleveren. De middelenuitgever kan met deze gegevens de nieuwe status van het authenticatiemiddel bij het inzageregister registeren. Na ontvangst van een verzoek tot statuswijziging controleert het BSNk-inzageregister of de aanleverende partij een erkende middelenuitgever is. Tevens wordt gecontroleerd of de aanvraag voor statuswijziging daadwerkelijk en ongewijzigd van deze middelenuitgever afkomstig is.

Vervolgens ontsleutelt het BSNk-inzageregister uit het aangeleverde Versleutelde Pseudoniem het specifieke pseudoniem van de Gebruiker bij het BSNk-inzageregister. Dan wordt nieuwe status van het authenticatiemiddel samen met de meegeleverde gegevens geregistreerd.

---

[17] De middelenuitgever hoeft dit overigens maar een keer te doen en kan het VP dan opslaan bij de gebruikersgegevens voor toekomstig herhaalt gebruik.

3.3.4 Verwerking van persoonsgegevens per rol/verantwoordelijkheid

Rol/verantwoordelijkheid middelenuitgever

De middelenuitgever verwerkt bij dit proces de accountgegevens van de gebruiker (relatiegegevens, statusgegevens). Om de gewijzigde status van een middel door te geven verwerkt de middelenuitgever het VP van de gebruiker voor het BSNk-inzageregister. De middelenuitgever is verantwoordelijk om er voor te zorgen dat in de statuswijzigingsgegevens (met name het volgnummer en middelbeschrijving) de gebruiker niet uniek kunnen identificeren.[18] Nadat deze stap is uitgevoerd worden de registratiegegevens bewaard ten behoeve van foutopsporing en verantwoording. Uiteraard registreert de middelenuitgever intern ook de status(-historie) van de authenticatiemiddelen.

Rol/verantwoordelijkheid authenticatiedienst

De rol van de Authenticatiedienst in dit proces is identiek aan diens rol in het authenticatieproces.

Rol/verantwoordelijkheid BSNk

Het BSNk-inzageregister verwerkt voor elke activatie het OIN van de middelenuitgever, het pseudoniem van de gebruiker en de het tijdstip ("timestamp") van de activering. Voor een middelstatus verwerkt het BSNk-inzageregister ook nog een identificatie en een beschrijving van het middel dat de gebruiker kan herkennen en optioneel een link waarmee een gebruiker direct doorgeleid kan worden naar een middelbeheer functie van de middelenuitgever.

Het BSNk-inzageregister ontvangt voor een statuswijziging het VP van de gebruiker voor het BSNk-inzageregister, met daarbij het identificatienummer en einddatum van het middel. Na ontvangst van een verzoek tot statuswijziging controleert het BSNk-inzageregister de identiteit van de middelenuitgever en tevens of de middelenuitgever gerechtigd is om een authenticatiemiddel van een gebruiker te activeren voor het publieke domein. Ook wordt gecontroleerd of de aanvraag voor statuswijziging daadwerkelijk en ongewijzigd van de middelenuitgever afkomstig is. Indien deze controles slagen, ontsleutelt het BSNk-inzageregister uit de VP het specifieke pseudoniem van de gebruiker bij het BSNk-inzageregister. De nieuwe status van het authenticatiemiddel wordt vervolgens geregistreerd tezamen met de authenticatiedienst en het volgnummer of einddatum van het authenticatiemiddel.

De gegevens ten aanzien van de relatie tussen de middelenuitgever en de gebruiker en statushistorie worden bewaard zolang de relatie en het betreffende middel actief is en nog een aantal jaren daarna, om de gebruiker te kunnen informeren over zijn middelenhistorie. Het BSNk bewaart gegevens over inactieve relaties en middelen tot maximaal vijf jaar. Als daar gegevens ten onrechte verdwijnen uit het BSNk-inzageregister is het van groot belang dat die gegevens weer teruggehaald kunnen worden. Het kan voorkomen dat fouten pas na langere tijd worden opgemerkt, mogelijk pas als gebruikers het zelf opmerken. Om de kans op gegevensverlies te minimaliseren wordt een backup-periode van één jaar aangehouden voor het BSNk-inzageregister.

Nadat een processtap (zoals activatie of statuswijziging) in het BSNk is uitgevoerd, blijven ten aanzien van die processtap enkel gegevens bewaard ten behoeve van foutopsporing en verantwoording (de borging dat het proces juist is doorlopen). Gegevens ten behoeve van foutopsporing en verantwoording worden maximaal drie maanden respectievelijk 18 maanden bewaard. Back-ups van deze gegevens worden alleen bewaard voor een termijn van maximaal één maand ten behoeve van foutherstel naar aanleiding van een incident.

3.3.5 Toelichting op het proces vanuit oogpunt van bescherming van persoonsgegevens

De USvE gaat uit van een multimiddelenaanpak. Dat heeft tot gevolg dat burgers authenticatiemiddelen kunnen hebben van meerdere middelenuitgevers, ook uit andere EU-landen.

[18] Bijvoorbeeld bij het rijbewijs moet niet het document-ID geregistreerd worden want die is uniek herleidbaar tot betreffende persoon.

Deze multimiddelenaanpak heeft veel voordelen, maar het kan voor de gebruiker lastig zijn om overzicht te houden over zijn authenticatiemiddelen. De USvE schrijft daarom voor dat de gebruiker laagdrempelig, op één plaats via MijnOverheid, een (historisch) overzicht moet kunnen krijgen van al zijn authenticatiemiddelen die gebruikt kunnen (of konden) worden in het publieke domein. Bij twijfel kan een gebruiker direct contact opnemen met de middelen beheerfunctie van de betreffende middelenuitgever.

Het overzicht van middelen wordt verstrekt door het BSNk-inzageregister dat op zijn beurt deze gegevens aangereikt krijgt door de middelenuitgevers. De middelenuitgevers zijn verplicht deze gegevens te verstrekken. Om de volledigheid van het overzicht nog beter te kunnen garanderen, zal BSNk-activeren elke activatie proactief registreren bij het BSNk-inzageregister. Dit is feitelijk een vangnet voor het geval dat een middelenuitgever een middel ten onrechte niet registreert, bijvoorbeeld als gevolg van een fout of manipulatie (inbraak).

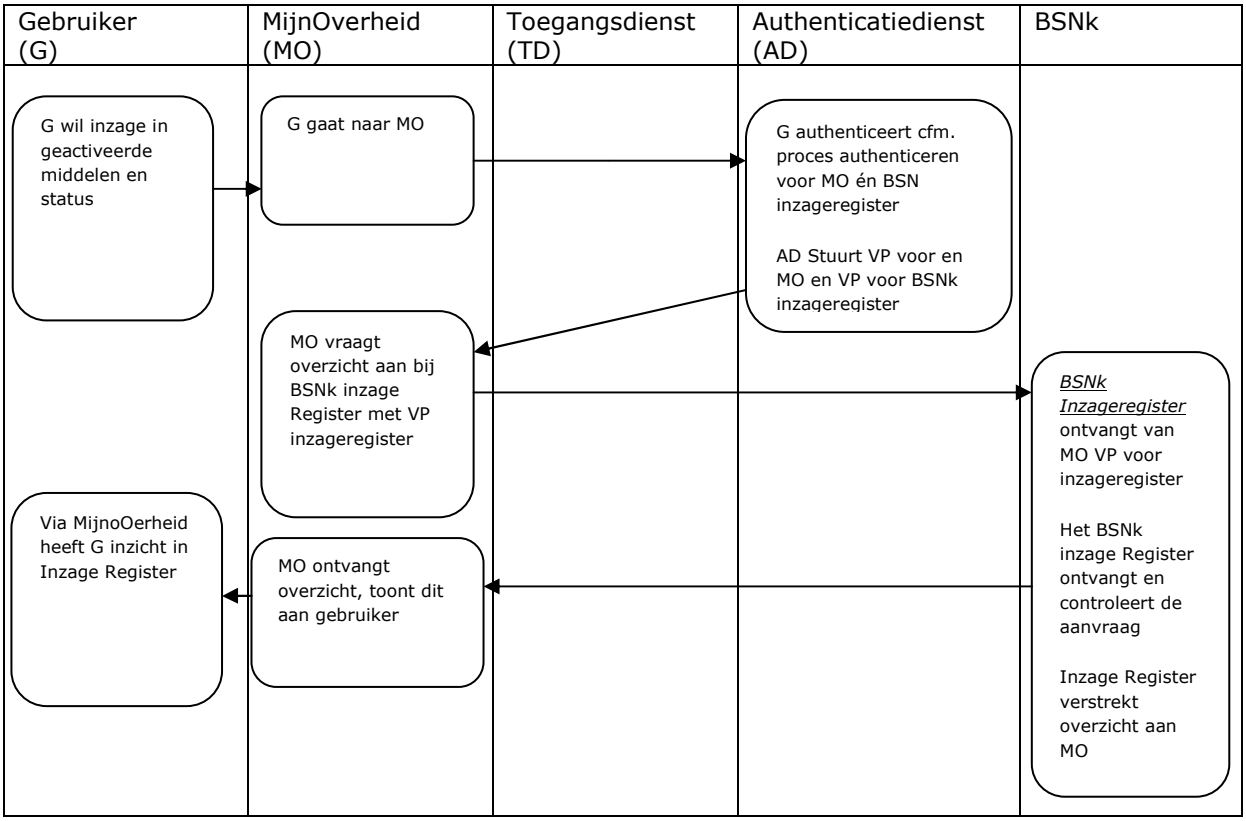
3.4 Inzageproces

3.4.1 Doel van het proces

Het doel van het proces is om de gebruiker inzage te bieden in de status(historie) van zijn geactiveerde middelen, door op diens verzoek deze inzage via mijn overheid.nl aan te bieden. Het betreft hier inzage in de gegevens die op stelselniveau beschikbaar zijn. Voor de inzage in de persoonsgegevens die bijvoorbeeld bij de middelenuitgever beschikbaar zijn, dient de gebruiker zich tot de betreffende middelenuitgever te richten.

3.4.2 Schematische weergave

Afbeelding 7: proces inzage in geactiveerde authenticatiemiddelen



De gebruiker zal de mogelijkheid geboden worden om via MijnOverheid een overzicht te krijgen met de (historische) status van alle authenticatiemiddelen die op zijn naam geregistreerd staan en actief zijn in het publiek domein, zoals ze geregistreerd zijn door de middelenuitgevers bij het

BSNk-inzageregister. Het overzicht biedt gegevens waaraan de gebruiker de middelen en hun status kan herkennen. Indien een gebruiker een status niet herkent, kan de gebruiker doorklikken naar de beheerfunctie van de betreffende middelenuitgever. Daar kan de gebruiker het gebruik van zijn middel meer in detail bekijken en eventueel actie ondernemen indien er zaken niet kloppen.

De gegevens worden geregistreerd bij het BSNk-inzageregister. De inzagefunctie zelf wordt gefaciliteerd door MijnOverheid[19], waar de mogelijkheid wordt geboden om op verzoek van de gebruiker bij het BSNk-inzageregister een overzicht op te halen van de op naam van de gebruiker geregistreerde middelen, de statushistorie daarvan en dit vervolgens in een overzicht van de authenticatiemiddelen te tonen.

3.4.3 Procesbeschrijving

Een gebruiker die inzage wenst in zijn middelen, gaat naar de website van MijnOverheid, met het verzoek om inzage in zijn geactiveerde authenticatiemiddelen. Naar aanleiding van dit verzoek vraagt MijnOverheid de gebruiker om zich voor MijnOverheid zelf, en voor het BSNk-inzageregister te authenticeren.

De authenticatiedienst levert na een geslaagde authenticatie aan MijnOverheid een versleutelde identiteit voor MijnOverheid zelf én een versleutelde pseudoniem voor het inzage register. MijnOverheid kan met het VP voor het BSNk-inzageregister vragen om de bijbehorende middelenhistorie. Het BSNk-inzageregister zoekt de middelen en de statushistorie bij het meegeleverd (BSNk-inzageregister specifieke) pseudoniem van de Gebruiker en verstrekt deze historie aan MijnOverheid.

MijnOverheid toont de gebruiker het verkregen overzicht van geactiveerde middelen en statushistorie op de website van MijnOverheid. Hierdoor heeft de gebruiker uiteindelijk via MijnOverheid inzicht in de status van zijn geactiveerde authenticatiemiddelen. Daarmee is inzage voor de gebruiker gerealiseerd en is dit proces voltooid.

3.4.4 Verwerking van persoonsgegevens per rol/verantwoordelijkheid

Rol/verantwoordelijkheid MijnOverheid

Naar aanleiding van een inzageverzoek vraagt MijnOverheid de gebruiker om zich voor MijnOverheid zelf en voor het BSNk-inzageregister te authenticeren. MijnOverheid ontvangt na authenticatie een VI voor MijnOverheid zelf én een VP voor het inzageregister. Mijn overheid vraagt met het VP voor het BSNk-inzageregister om de bijbehorende middelenhistorie. MijnOverheid toont de gebruiker het verkregen overzicht van geactiveerde middelen en statushistorie op de website van MijnOverheid. Nadat deze stap is uitgevoerd blijven enkel gegevens bewaard ten behoeve van foutopsporing en verantwoording (de borging dat het proces juist is doorlopen).

Rol/verantwoordelijkheid Authenticatiedienst

De authenticatiedienst levert na ontvangst van een authenticatieverzoek en een geslaagde authenticatie aan MijnOverheid een VI voor MijnOverheid zelf én een VP voor het BSNk-inzageregister. Nadat deze stap is uitgevoerd blijven enkel gegevens bewaard ten behoeve van foutopsporing en verantwoording (de borging dat het proces juist is doorlopen).

Rol/verantwoordelijkheid BSNk

Het BSNk-inzageregister ontvangt van MijnOverheid het VP van de gebruiker voor het BSNk-inzageregister met het verzoek om de bijbehorende middelenhistorie. Het BSNk-inzageregister zoekt de middelen en de statushistorie bij het meegeleverd (BSNk-inzageregister specifieke) pseudoniem van de gebruiker en verstrekt deze historie aan MijnOverheid. Nadat deze stap is uitgevoerd blijven enkel gegevens bewaard ten behoeve van foutopsporing en verantwoording (de borging dat het proces juist is doorlopen).

[19] Het is nog niet besloten dat de inzage functionaliteit via mijnoverheid.nl te raadplegen is.

3.5 Misbruikbestrijding

Misbruikbestrijding op centraal niveau is in de USvE 1.0 genoemd, maar nog niet specifiek uitgewerkt. Wel wordt in de USvE aangegeven dat misbruikbestrijding zal moeten worden ingeregeld. De USvE 1.0 voorziet daartoe in een functie om een zogeheten opmerkelijke gebeurtenis te registreren door een middelenuitgever en een authenticatiedienst (op decentraal niveau).

Dit loopt als volgt. De authenticatiedienst registreert een opmerkelijke gebeurtenis.[20] De authenticatiedienst classificeert de opmerkelijke gebeurtenis en identificeert de gebruiker die daarbij betrokken is aan de hand van zijn VP die bekend is bij de authenticatiedienst. Optioneel wordt ook het authenticatiemiddel geïdentificeerd dat daarbij betrokken is. De authenticatiedienst (of middelenuitgever) meldt de opmerkelijke gebeurtenis bij het in te richten BSNk-misbruikbestrijdingsregister met het VP van de gebruiker bij het misbruikbestrijdingsregister en indien van toepassing de identiteit van het authenticatiemiddel (meestal volgnummer en/of einddatum).

Het BSNk-misbruikbestrijdingsregister controleert of de authenticatiedienst gemachtigd is om een opmerkelijke gebeurtenis te registreren en of de aanvraag daadwerkelijk en ongewijzigd van de authenticatiedienst afkomstig is. Het BSNk-misbruikbestrijdingsregister legt de opmerkelijke gebeurtenis vast met behulp van de combinatie van authenticatiedienst, pseudoniem van de gebruiker en de identiteit van het authenticatiemiddel (meestal het volgnummer en/of einddatum). Het BSNk-misbruikbestrijdingsregister heeft dan vervolgens een opmerkelijke gebeurtenis vastgelegd.

Het pseudoniem van het BSNk-misbruikbestrijdingsregister is een ander pseudoniem dan het BSNk-inzageregister ontvangt. Deze twee pseudoniemen zijn onderling niet te relateren.

3.6 De ondersteunende functionaliteiten van het BSNk

De functionaliteiten van het BSNk zijn bij de beschrijving van de hoofdprocessen binnen het eID-stelsel al deels aan bod geweest. Voor de volledigheid worden de functionaliteiten van het BSNk in deze paragraaf nog eens beschreven.

De inrichting van het BSNk is zodanig dat bij de koppeling tussen het private en het publieke domein geen koppeling gemaakt kan worden tussen pseudoniem en BSN en er geen onwenselijke concentratie van persoonsgegevens ontstaat (privacy hotspot). De voorziening binnen eID die het werken met pseudoniemen mogelijk maakt en die de processen zoals hierboven beschreven laat functioneren, is het BSNk. Deze voorziening voorziet daartoe – voor de werking binnen de USvE 1.0 - in de volgende functionaliteiten:[21]

Voor de volledigheid wordt op deze plaats opgemerkt dat voor de onderstaande beschrijvingen wordt uitgegaan van de functionele beschrijvingen van het BSNk zoals deze op dit moment beschikbaar zijn. Dit betekent dat de technische detailuitwerking in de GEB – bewust - niet is beschreven (en niet beoordeeld), maar de beschrijving functioneel gehouden is.

Aan het BSNk wordt op dit moment volop ontwikkeld. Gelet op de zogeheten "Agile/SCRUM" werkwijze die bij de technische ontwikkeling wordt gehanteerd, waarbij een systeem – en derhalve ook de beschrijving ervan - werkenderwijs in detail wordt vormgegeven zal een gedegen technische check pas op een later moment goed mogelijk zijn. Een marginale check wijst dat op dit moment overigens ook uit.

---

[20] Wat verstaan wordt onder een opmerkelijke gebeurtenis moet nog nader worden uitgewerkt.
[21] Zoals beschreven in de Projectstartarchitectuur BSNk (conceptversie 16-2-2017) voor de uniforme set van Eisen 1.0.

Op een later moment dient daarom gecontroleerd te worden of technische implementatie zodanig is (of wordt) uitgevoerd dat de beschreven functionaliteit daadwerkelijk adequaat wordt ingevuld.

Deze check valt buiten de reikwijdte van deze GEB. Deze technische check is overigens geen GEB zoals de AVG die beoogt, maar een controle die (functionele test) doorgaans wordt uitgevoerd bij implementatie van ICT-systemen. Als daaruit zou blijkt dat de techniek de beoogde functionaliteit niet ondersteunt of technische systeembeveiliging niet op orde is, zou dat – gezien de aard van het ondersteunde proces – wel privacyrisico's kunnen opleveren. Om die op te lossen dient dan de techniek zodanig aangepast zodat het werkt zoals het functioneel moet.

3.6.1 Activatiefunctie (verplicht)

Deze functie zorgt ervoor dat op basis van een aangeleverd BSN of een zogeheten eIDAS Uniqueness ID (indien het een burger uit een andere EU-lidstaat zonder BSN betreft) gepseudonimiseerde identiteiten voor gebruikers worden gecreëerd. Vervolgens wordt ervoor gezorgd dat deze worden toegekend en uitgegeven aan toegelaten middelenuitgevers. De activatiefunctie wordt ingezet in het activatieproces zoals dat is beschreven in de USvE 1.0.

Voordat de pseudonieme identiteiten worden gecreëerd verifieert de activatiefunctie eerst de verplicht door de gebruiker en middelenuitgever aan te leveren set controlegegevens (naam geboortedatum en BSN) bij de BRP. Dit is bedoeld als veiligheidsmaatregel om zeker te stellen dat de aangeleverde set gegevens daarmee overeenkomt en niet dat ten onrechte een pseudoniem wordt gecreëerd.

Als deze controlegegevens overeenkomen, en de verificatie is geslaagd, wordt over het aangeleverde BSN of eIDAS Uniqueness ID tezamen met het OIN van de aanvragende middelenuitgever een versleuteling uitgevoerd. Het resultaat daarvan is een aantal gekoppelde versleutelde (polymorfe) identiteiten. Doordat het BSN van een gebruiker en het OIN van een middelenuitgever als input dienen zijn deze identiteiten specifiek gekoppeld aan een gebruiker én een middelenuitgever.

Er kunnen – afhankelijk van de gegevens die als input voor de versleuteling zijn gebruikt - drie typen polymorfe identiteiten worden uitgegeven:

1. Een identiteit gebaseerd op versleuteling van het BSN van een gebruiker met een OIN van de middelenuitgever. Dit is de Polymorfe Identiteit (PI), waaruit het BSN is te ontcijferen. Deze is bedoeld voor gebruik in het publieke (BSN) domein.
2. Een identiteit gebaseerd op een vooraf onomkeerbaar versleuteld BSN en het OIN van de middelenuitgever. Dit is de Polymorfe Pseudoniem (PP). Dit is bedoeld voor gebruik in het private domein of voor gebruik in het publieke domein waarvoor geen BSN mag worden gebruikt. Het BSN kan hieruit niet worden herleid.
3. Een EU-identiteit gebaseerd op het eIDAS Uniqueness ID. Dit is een zogeheten polymorf pseudoniem EU (PP EU). Dit is bedoeld voor gebruik in het publieke domein voor gebruikers zonder BSN.

De PI en PP worden gegenereerd als het BSN wordt aangeleverd. Deze stellen gebruikers met een BSN in staat om in te loggen in het publieke domein (op basis van de PI) of in het private domein (op basis van het PP). Door de activatie is de identiteit van de gebruiker gecontroleerd en verzekerd. Ook zijn de identiteiten van de gebruiker aan elkaar én aan een middelenuitgever verzekerd en gekoppeld. En tevens zijn de oorspronkelijk identificerende gegevens (BSN) binnen het eID-stelsel zelf niet meer te achterhalen en voor vervolggebruik binnen het stelsel ook niet meer nodig. Dit vormt de kern van de privacy-ontwerpmaatregel van het stelsel.

Om de inzagefunctie van het BSNk mogelijk te maken wordt de registratie van de polymorfe identiteit (PI en PP) tenslotte geregistreerd bij het BSNk-inzageregister. Dit maakt het voor de gebruiker mogelijk om een overzicht van al zijn geregistreerde inlogmiddelen en de status daarvan in te zien.

3.6.2 Transformatiefunctie (optioneel)

De (centrale) transformatiefunctie wordt ingezet bij het authenticatieproces in het publieke domein. Transformatie betekent dat een polymorfe identiteit of een polymorf pseudoniem die door de authenticatiedienst wordt aangeleverd als een gebruiker zich wil authenticeren bij een dienstverlener, door een versleuteling wordt omgezet in een voor een dienstverlener leesbare VI (bij een publieke dienstverlener) of een VP (in het geval van een private dienstverlener). De versleuteling vindt zodanig plaats dat alleen de dienstverlener die daartoe gerechtigd is de daadwerkelijke identiteit van de gebruiker kan herleiden. Om te zorgen dat de identiteiten tijdens de verzending van de authenticatiedienst naar de dienstverlener vanaf de buitenkant niet herkenbaar zijn worden deze als veiligheidsmaatregel voorafgaand aan de verzending nogmaals willekeurig versleuteld (dit heet "randomisatie").

De centrale transformatiefunctie van het BSNk is optioneel en vindt alleen plaats als een authenticatiedienst zelf geen HSM heeft om de vertaalslag van een PI naar een VI te maken. Uitgangspunt is dat authenticatiediensten dit zelf doen, omdat daarmee de afhankelijkheid van het BSNk als single point of failure wordt verminderd.

3.6.3 Sleutelbeheerfunctie

De activatie- en de transformatiefunctie werken op basis van cryptografische versleuteling. Dat betekent dat voor deze functies cryptografische distributie- en transformatiesleutels nodig zijn. Voor de veiligheid en betrouwbaarheid van de functies en daarmee van het eID-stelsel worden deze sleutels veilig beheerd en verstrekt. Om de versleuteling veilig te kunnen uitvoeren, dienen de cryptografische sleutels daarom in een veilige omgeving te worden beheerd. De sleutelbeheerfunctie van het BSNk zorgt daarvoor. Het betreft hier het beheer van de cryptografische sleutels die partijen in het stelsel nodig hebben om identiteiten en pseudoniemen te kunnen verwerken, om uit een VI het BSN te kunnen ontsleutelen. Het betreft hier niet de sleutels voor de beveiliging/versleuteling van de onderliggende technische verbindingen. Daarvoor wordt aangesloten bij regulier beschikbare PKI-dienstverlening (zoals PKI Overheid).

De sleutelbeheerfunctie faciliteert tevens een proces waarmee dienstverleners cryptografische sleutels op een veilige manier kunnen aanvragen en verkrijgen. Daarbij wordt gecontroleerd of de dienstverlener is opgenomen in de autorisatielijst BSN (ALB), waarbij controle plaatsvindt of een dienstverlener daarin is opgenomen. Dit wordt beheerd door het stelselbeheer eID. Als een dienstverlener niet is opgenomen in de ALB wordt geen sleutel verstrekt waarmee het BSN kan worden herleid. Deze stap vormt daarom een belangrijke waarborg in het authenticatieproces om te voorkomen dat het BSN wordt verstrekt aan organisaties die daarvan geen gebruik mogen maken. Onderdeel van de sleutelbeheerfunctie vormt daarnaast een publiek toegankelijke sleutelverstrekkingslijst, met daarop dienstverleners aan wie een sleutel is uitgereikt. Ten slotte is een proces ingericht om cryptografische sleutels gecontroleerd te vervangen.

3.6.4 Stelselbeheer

Registratie erkende partijen

Deze functie zorgt ervoor dat erkende partijen in het stelsel gebruik kunnen maken van het BSNk, onderling kunnen samenwerken doordat zij voor elkaar herkenbaar zijn aldus hun rol in het stelsel kunnen invullen. Als erkende partijen willen aansluiten op het BSNk dienen deze partijen gegevens aan te leveren waaraan zij herkenbaar zijn (zogeheten metagegevens) zodat zij in het stelsel en voor het BSNk te herkennen zijn, zoals het OIN.

Beheer Autorisatielijst BSN

Stelselbeheer controleert deze (meta)gegevens en beheert en publiceert deze, zodat deze te allen tijde voor alle erkende partijen herkenbaar en controleerbaar zijn. Daarnaast beheert het stelselbeheer eID de lijst met dienstverleners die gerechtigd zijn het BSN te verwerken, de autorisatielijst BSN (ALB).

3.6.5 BSNk-inzageregister

Het BSN-inzageregister houdt voor elke gebruiker een registratie bij van authenticatiemiddelen die op naam van die gebruiker zijn geactiveerd, en de status daarvan. Nadat een authenticatiemiddel is geactiveerd ontvangt het inzageregister daarvan een melding. Daarbij wordt aangegeven welke PI, PP of PP EU voor een gebruiker aan welke middelenuitgever is uitgegeven en welke authenticatiedienst gebruik maakt van het middel. De betreffende authenticatiedienst dient statuswijzigingen (uitgegeven, geactiveerd, gedeactiveerd, ingetrokken) bij te werken. Daartoe biedt het inzageregister de technische mogelijkheden (koppelvlak).

Het inzageregister verzorgt de genoemde registratie van de middelen, maar biedt zelf geen functionaliteit om de gegevens in te zien. Voorzien is dat daarvoor portalen (bijvoorbeeld MijnOverheid) geautoriseerd worden om de gegevens voor een gebruiker – op diens verzoek - op te halen en via het portaal aan de gebruiker te tonen. De achtergrond hiervan is dat op basis van de gegevens in het inzage register zelf geen persoonlijke gegevens te herleiden zijn, omdat het inzage register zelf alleen pseudoniemen heeft en geen sleutels om de identiteit te herleiden. Op het moment van een inzageverzoek door een gebruiker haalt het portaal de pseudoniemen op uit het inzage register, ontsleutelt deze met zijn eigen sleutels naar de identiteit van de gebruiker en toont deze in het portaal aan de gebruiker.

3.6.6 BSNk-misbruikbestrijdingsregister

Deze functionaliteit is op termijn voorzien, maar valt voor het voorlopertraject buiten de scope van het BSNk.

3.6.7 Verwerking van (persoons)gegevens door functionaliteiten

Nadat een processtap door een functie van het BSNk is uitgevoerd blijven ten aanzien van die processtap enkel gegevens bewaard ten behoeve van foutopsporing en verantwoording (de borging dat het proces juist is doorlopen). Het betreft hier het BerichtID (authenticatieverzoek), AanleverendePartij (wie heeft het bericht geleverd), BerichtSignature (ondertekening om integriteit te controleren), BerichtTimestamp (tijdstempel). Verder worden er logistieke gegevens vastgelegd die het mogelijk maken om het resultaat van het bericht (resp. PI/PP, VI/VP, MiddelStatus, Sleutelmateriaal) te herleiden naar dit bericht. Verder worden ook ‘logistieke resultaten’ van het betreffende verwerkingsprocesstappen vastgelegd zodat verantwoord kan worden waarom een bericht juist wel of juist niet succesvol afgehandeld kon worden.

Gegevens t.b.v. foutopsporing en verantwoording worden maximaal drie maanden respectievelijk 18 maanden bewaard. Back-ups van deze gegevens worden alleen bewaard voor een termijn van maximaal één maand ten behoeve van foutherstel naar aanleiding van een incident.

3.6.8 Scheiding van functies binnen het BSNk

De verschillende functies van het BSNk zoals hierboven besproken zijn technisch en organisatorisch van elkaar gescheiden (Chinese muren).

4 Beoordeling, risico's en maatregelen

Het eID-stelsel levert gebruikers en overheden veel voordelen op, in termen van gebruikersgemak, snelheid, betrouwbaarheid en continuïteit van dienstverlening en ook kostenbesparing. Dit zijn belangrijke, doorslaggevende redenen om het stelsel in het leven te roepen. Onvermijdelijk kleven er aan deze ontwikkeling tevens risico's. Ook privacyrisico's voor burgers. Deze risico's zullen geïnventariseerd moeten worden, en vervolgens tot een minimum worden beperkt, door maatregelen te treffen.

De beoordeling in deze GEB start met de signalering van de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van betrokken burgers die gebruik maken van het eID-stelsel. Daarbij wordt in ogenschouw genomen welke negatieve gevolgen de gegevensverwerkingen binnen eID op zichzelf kunnen hebben voor de rechten en vrijheden van betrokkene, wat de oorsprong ervan is en hoe groot de kans is dat deze gevolgen zullen intreden en wat de impact van als er zich problemen of incidenten voordoen bij de gegevens verwerkingen.

De eerste stap is om potentiële privacyrisico's vast te stellen. Een privacyrisico is een (hypothetische) situatie waarin persoonsgegevens (onrechtmatig of op een onjuiste wijze) verwerkt worden met gevolgen voor de rechten en vrijheden van de betrokkene. Gelet op de aard, het toepassingsgebied, de context en de doeleinden van de gegevensverwerkingen binnen het eID-stelsel is er een aantal belangrijke risico's te onderkennen. Bij (onrechtmatige) verwerking van persoonsgegevens binnen het eID-stelsel kan gedacht worden aan al dan niet opzettelijke vernietiging en verlies (beschikbaarheid) van de toegang tot een groot aantal overheidsdienstverleners, wijziging (integriteit), ongeoorloofde toegang tot dienstverlening met eID middelen en verstrekking (vertrouwelijkheid) van persoonsgegevens, waaronder eID-middelen.

Dergelijke risico's kunnen binnen het eID-stelsel aan de orde zijn, gelet op de schaalgrootte en context waarin het stelsel wordt gepositioneerd kunnen de negatieve gevolgen in potentie groot zijn, en doorwerken tot ver buiten het eID-stelsel zelf, waaronder bij overheidsinstanties. Verlies van controle over hun eID-middelen zou voor gebruikers kunnen leiden tot (blootstelling aan) identiteitsdiefstal of –fraude en bijbehorende financiële verliezen waarvan zij het slachtoffer worden. Misbruik van gegevens door partijen binnen het stelsel zouden kunnen leiden discriminatie, stigmatisering en (daardoor) uitsluiting van bepaalde rechten. Omdat beoogd wordt dat ook zorgverleners gebruik kunnen maken, zal ongeoorloofd gebruik van de gegevens in potentie ook kunnen leiden tot gezondheidsschade omdat bijvoorbeeld medicatie kan worden gewijzigd of verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens. Het eID-stelsel maakt gebruik van pseudonimisering. Ongeoorloofde ongedaanmaking daarvan zou kunnen leiden tot ongeoorloofd en voor de gebruiker schadelijk inzicht in zijn gedrag in een bredere context.

Het is belangrijk deze risico's te onderkennen, en daarop maatregelen te treffen. Bij de onderstaande beoordeling aan de hand van de aspecten wordt ten aanzien van een aantal toetspunten uit de AVG een conclusie getrokken, en worden (normatieve) risico's benoemd en maatregelen voorgesteld om bovenstaande materiële risico's te helpen verkleinen. De beoordeling vindt plaats in paragrafen 4.2 t/m 4.5. Het toetspunt dat aan de orde is, is bij het begin van iedere paragraaf in een grijskader weergegeven. Op deze manier wordt beoogd enerzijds te komen tot het verkleinen en zoveel als mogelijk opheffen van de normatieve risico's, waardoor aan de AVG kan worden voldaan, met uiteindelijk als doel om de bovenbeschreven materiële risico's voor gebruikers te minimaliseren.

Voordat wordt overgegaan tot bespreking van de beoordeling van de conclusies, risico's en maatregelen in deze GEB, wordt teruggeblikt op de risico's en maatregelen zoals die zijn geconstateerd in de PIA op het Introductieplateau, en hoe deze maatregelen zijn opgepakt binnen de ontwikkeling van het eID-stelsel.

4.1 Beoordeling opvolging aanbevelingen GEB op Introductieplateau

Een aantal risico's is op dit moment niet aan de orde, omdat bepaalde functionaliteit buiten de scope van de USvE 1.0 is geplaatst (dit geldt bijvoorbeeld voor machtigingen en attributen). Dit risico zal voor latere ontwikkeling vermoedelijk weer in scope vallen.

Destijds is als risico op het Introductieplateau eID-stelsel benoemd dat het gebruik van het BSN in het private domein wet- en regelgeving benodigd was, omdat anders het BSN niet rechtmatig kan worden verwerkt door deze partijen. Inmiddels is de Wet EBV tot stand gekomen, die het gebruik van het BSN binnen het eID-stelsel regelt. Daarbij is op dit moment de situatie dat de private partijen het BSN verwerken onder de verantwoordelijkheid van de minister van BZK. Zie hierover nader paragraaf 4.2.

De PIA op het Introductieplateau eID-stelsel signaleerde daarnaast het risico dat gegevensconcentraties ontstaan binnen het stelsel (privacy hotspots), onder meer door samenloop van rollen die privacyrisico's inhouden op het moment dat deze gegevens onrechtmatig worden verwerkt. Binnen het stelsel is mede om deze reden gekozen voor de werking met polymorfe pseudonimisering. Deze privacy-by-design maatregel zorgt voor compartimentering binnen het stelsel (omdat iedere dienstverlener zijn specifieke eigen sleutel nodig heeft) en minimalisering van verwerking van het BSN. Dit gaat herleidbaarheid tegen. Daarmee is tevens het gesignaleerde risico dat het BSNk een privacy hotspot was, weggenomen. Het BSNk verwerkt in de nieuwe werking na de activatie geen BSN meer. Tevens is ervoor gekozen om te werken met verschillende rollen, en aan de samenloop van rollen nadere regels te stellen (Chinese muren) waardoor gegevensconcentraties worden verminderd. Met deze maatregelen is het gesignaleerde risico aanzienlijk verminderd, maar overigens nog niet weggenomen. Zie daarover ook paragraaf 4.4 en 4.5.

Om gegevensconcentraties verder terug te dringen is in de PIA op het Introductieplateau aanbevolen om niet alle persoonsgegevens voor dezelfde periode te bewaren, maar de bewaarperiode te differentiëren en waar mogelijk te bekorten. Deze aanbeveling is opgevolgd. Op grond van de Wet EBV, in hoofdstuk 4 van het onderliggende besluit verwerking persoonsgegevens GDI en in de USvE worden bewaartermijnen gedifferentieerd en waar mogelijk bekort.

In de PIA op het Introductieplateau eID is voorts als risico onderkend dat het gevaar bestaat van function creep en het risico dat het introductieplateau sluipenderwijs gebruik gaat worden voor een breder doel/dienstenpakket dan op dat moment beoogd. Binnen het programma heeft dit risico de aandacht. Deze aandacht zal overigens nodig blijven. Zie daarover nader in paragraaf 4.3 en 4.4.

De PIA op het introductieplateau signaleerde dat de maatregelen aangaande fraudedetectie en interne controlemaatregelen niet waren gedefinieerd. Inmiddels zijn wel de contouren geschetst van misbruikbestrijding, maar de inrichting moet nog grotendeels plaatsvinden. Deze bevinding blijft onverkort staan. Zie daarover paragrafen 4.2 en 4.5. Overigens wordt in de PIA op het Introductieplateau eID nog aangestipt dat opsporing door OM en politie nog niet zijn gereguleerd. Het voornemen is om dat overigens ook niet te doen. Misbruikbestrijding zal binnen het stelsel worden ingevuld als operationele verantwoordelijkheid van de partijen, waarbij, op het moment dat mogelijk strafbare feiten – zoals fraudezaken - worden geconstateerd, opsporingsinstanties kunnen en zullen worden betrokken. Deze instanties kunnen dan handelen op grond en met de waarborgen van hun strafvorderlijk instrumentarium.

Als laatste aandachtpunt uit de PIA op het Introductieplateau is het belang naar voren gekomen dat gebruikers tijdens het Introductieplateau goed worden geïnformeerd over de risico's van het gebruik. Dit is destijds meegenomen in de communicatie rond het Introductieplateau. Echter het belang van communicatie rondom het voorlopertraject geldt – ook gezien het belang dat de aankomende privacywetgeving hecht aan transparantie voor gebruikers – onverkort.

4.2 Grondslag

De persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. De gegevensverwerking is gebaseerd op tenminste één van de zes volgende grondslagen genoemd in artikel 6, eerste lid, AVG.

Conclusie: de binnen het eID-stelsel voorgenomen verwerkingen van persoonsgegevens zijn rechtmatig. De Wet EBV en het Besluit GDI bieden een adequate grondslag.

Artikel X, eerste lid, Wet EBV kent de minister van BZK de zorgplicht toe voor de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van voorzieningen voor (onder meer) elektronische authenticatie. Het derde lid bepaalt dat de minister daartoe persoonsgegevens verwerkt, waaronder het BSN, voor zover dat noodzakelijk is voor de vervulling van de taak. In het Besluit GDI wordt dit nader gespecificeerd voor – voor zover in dit kader van belang – het BSNk en daaruit direct volgende verwerkingen van persoonsgegevens die nodig zijn voor de basale werking van het eID-stelsel.

Uit de USvE komen de in hoofdstuk 3 beschreven verwerkingen van persoonsgegevens en bijbehorende doelstellingen naar voren. Deze doelstellingen en verwerkingen lijken te passen binnen de in de wet omschreven grondslagen. Hoewel in detail de verwerkingen – gezien de doorontwikkeling van de USvE met polymorfe pseudonimisering – op punten afwijken van de omschrijving zoals deze in het Besluit GDI ten aanzien van het BSNk is vastgelegd, is dit voor de grondslag niet problematisch, aangezien de verwerking juist een inperking van het gebruik van het BSN beoogt. Binnen de grondslag wordt de verwerking beperkt.

Risico: verwerkersovereenkomsten gegevensverwerking andere rollen ontbreken

De keuze van de verwerkingsgrondslag betekent in de eerste plaats dat de basale verwerkingen van persoonsgegevens voor toegang tot het publieke domein onder de verantwoordelijkheid van de minister van BZK plaatsvinden. De minister van BZK is verwerkingsverantwoordelijke. Voor de overige private rollen (middelenuitgever, authenticatiedienst en toegangsdienst) is geen eigenstandige wettelijke grondslag gecreëerd. Dit betekent dat zij voor de verwerkingen die zij uitvoeren ten behoeve van de werking van het stelsel als verwerker voor de minister van BZK dienen te handelen. Het is daarom van belang dat afspraken (verwerkersovereenkomsten) worden gemaakt tussen de minister van BZK en de organisaties die de andere rollen binnen het stelsel vervullen. Als deze verwerkersovereenkomsten niet gesloten worden, is er voor de overige rollen geen grondslag om de verwerkingen van persoonsgegevens ten behoeve van de werking van het eID-stelsel uit te voeren, wat overtreding van de AVG inhoudt.

Maatregel: opstellen verwerkersovereenkomsten

Een maatregel om het genoemde risico weg te nemen is het opstellen van verwerkers-overeenkomsten tussen de minister van BZK en de erkende partijen die de overige private rollen binnen het stelsel uitvoeren. Voor zover bekend is deze actie reeds opgepakt.

In het verlengde hiervan – om de verwerkersovereenkomsten te kunnen sluiten – moet in de USvE duidelijk zijn welke organisatie/rol welke persoonsgegevens verwerkt. De weergave van de verwerkingen in deze GEB in hoofdstuk 3 beoogt daaraan een bijdrage te leveren, maar er bestaat in de USvE (nog) onduidelijkheid over welke persoonsgegevens exact verwerkt worden, vooral als de scheiding van de rollen niet duidelijk is. Overigens zullen de exacte persoonsgegevens die worden verwerkt afhankelijk zijn van de wijze waarop partijen hun dienstverlening inrichten. De USvE laat bewust die vrijheid. In het kader van transparantie moet uiteindelijk duidelijk zijn wie, wat, waar, wanneer en waarom welke persoonsgegevens verwerkt.[22] Dat is nu nog niet het geval. Het is van belang daar in de komende periode invulling aan te geven. Dat zal deels ook moeten gebeuren in de verwerkersovereenkomsten die worden gesloten.

[22] Artikel 15 AVG.

Gezien bovenstaande wordt tevens aanbevolen dat partijen die deel uit maken van het voorlopertraject zelf een GEB opstellen, teneinde zicht te krijgen op de specifieke risico's (en maatregelen ter beperking daarvan) voor de verwerking persoonsgegevens die volgen uit de eigen inrichtingskeuzes, die zij voeren als verwerker van persoonsgegevens voor de minister van BZK. Ook vanuit die invalshoek moet inzicht gegeven kunnen worden in voorgenomen/te treffen maatregelen. Aanbevolen wordt om dit onderdeel te laten uitmaken van de overeenkomsten die de minister van BZK met de voorloperpartijen sluit. Dit is ook van belang om de minister van BZK zijn rol als verantwoordelijke te kunnen laten waarmaken.

Risico: misbruikbestrijding (fraude/incidentbestrijding) op stelselniveau niet ingericht

Het Besluit GDI biedt, voortvloeiend uit de verantwoordelijkheid van de minister van BZK om voor veilige en betrouwbare voorzieningen te zorgen, de grondslag om persoonsgegevens te verwerken om misbruik (waaronder fraude) te bestrijden. Deze verantwoordelijkheid – als onderdeel van de bescherming van persoonsgegevens c.q. belangen van gebruikers (die als gevolg van onverhoopt misbruik geschaad kunnen worden), wordt in de USvE op stelselniveau nog niet nader ingevuld. Weliswaar worden contouren voor een oplossingsrichting geschetst (zoals een misbruikregister en het melden van opmerkelijke gebeurtenissen), maar daarmee is misbruikbestrijding op stelselniveau nog niet ingevuld.

Het feit dat misbruikbestrijding op stelselniveau niet is ingevuld, is een risico. Niet in de zin dat buiten de grondslag persoonsgegevens zouden worden verwerkt, maar juist dat een noodzakelijke gegevensverwerking niet plaats vindt en geen invulling wordt gegeven aan een toegekende verantwoordelijkheid ter bescherming van gebruikers tegen onverhoopte inbreuk op hun (privacy)belangen.

Maatregel: zo snel mogelijk invulling geven aan misbruikbestrijding op stelselniveau

Een maatregel die wordt aanbevolen is om op zo kort mogelijke termijn invulling te geven aan de mogelijkheden om op stelselniveau misbruik te kunnen herkennen (detectie) en te herstellen indien misbruik wordt geconstateerd. Daarbij wordt opgemerkt dat misbruikbestrijding op zichzelf een verwerking van persoonsgegevens is, die onverkort langs de beginselen van de AVG moet worden ingericht.

4.3 Bijzondere en strafrechtelijke persoonsgegevens

Indien van toepassing: er geldt bij wet een uitzondering op het verbod tot verwerking van bijzondere persoonsgegevens (artikel 9, eerste lid, AVG). Verwerking van strafrechtelijke gegevens vindt plaats door of onder toezicht van de overheid, of is bij wet geregeld (artikel 10, AVG).

Conclusie: er worden geen bijzondere of strafrechtelijke persoonsgegevens verwerkt binnen het eID-stelsel. Wel kunnen patronen in andere persoonsgegevens die in het eID-stelsel worden verwerkt een indicatie of voorspeller zijn van bijzondere persoonsgegevens.

Hoewel het strikt genomen geen bijzonder persoonsgegeven is (maar een nummer dat ter identificatie van een persoon bij wet is voorgeschreven) wordt hier toch aangestipt dat het BSN wordt verwerkt, en dat in de Wet EBV is voorzien in een wettelijke grondslag daarvoor.

Bijzondere en strafrechtelijke persoonsgegevens worden in het eID-stelsel niet verwerkt. Dit neemt echter niet weg dat – afhankelijk van de dienstverleners die gebruik maken van het stelsel – het gebruik van het stelsel inzicht kan bieden of een indicatie kan vormen in bijzondere persoonsgegevens van een gebruiker. Zo kan het inloggedrag – en de voor de werking van het stelsel vastgelegde logging - van een gebruiker bij een gespecialiseerde zorgverlener een indicatie vormen voor de gezondheidsgegevens van de betreffende gebruiker. En inloggen bij een reclasseringsdienstverlener kan een indicatie vormen voor een strafrechtelijk verleden van de gebruiker.

Risico: er kunnen indicaties of voorspellers van bijzondere persoonsgegevens ontstaan

Hoewel primair geen bijzondere of strafrechtelijke persoonsgegevens worden verwerkt binnen het stelsel zelf is het belangrijk om ervoor te zorgen dat gegevens die ontstaan en die een indicatie kunnen vormen voor een bijzonder persoonsgegeven tot een minimum worden beperkt. Onbevoegd of onbedoeld gebruik of misbruik van deze gegevens kan voor gebruikers aanzienlijke (negatieve) gevolgen hebben.

Maatregel: toezicht op naleving van afspraken over compartimentering

Verwerking van persoonsgegevens en logging van de (goede) werking is noodzakelijk en inherent aan de authenticatiedienstverlening. Echter gezien het geconstateerde risico is het van belang om ervoor te zorgen dat gegevens die mogelijk inzicht kunnen geven in het inloggedrag – overigens ook als het geen bijzondere persoonsgegevens betreft - van een gebruiker, tot een minimum worden beperkt en dat maatregelen worden getroffen om onbevoegd/onbedoeld gebruik en misbruik tegen te gaan.

In het stelsel worden daarvoor, als opvolging van een bevinding uit de PIA op het Introductieplateau, reeds maatregelen getroffen, onder meer door er met gebruikmaking van pseudonimisering voor te zorgen dat authenticatiediensten niet op BSN-niveau kunnen herleiden bij welke dienstverlener een gebruiker heeft ingelogd. Een andere getroffen maatregel is het werken met verschillende rollen, waardoor compartimentering van de persoonsgegevens binnen het stelsel ontstaat. Doordat een proces over meerdere schijven (rollen) verloopt, worden gegevensconcentraties voorkomen. Dit vormt een privacy-ontwerpmaatregel (privacy-by-design).

Hoewel door bovengenoemde maatregelen het risico aanzienlijk wordt verkleind, lijkt het nog steeds niet uitgesloten dat een organisatie, zeker als de rollen van authenticatiedienst en middelenuitgever daarin verenigd worden – aan de hand van ontvangen en doorgeleide authenticatieverzoeken naar dienstverleners – uit de logging kan herleiden welke dienstverlening door de gebruiker is afgenomen. Afspraken ten aanzien van compartimentering zijn er wel, maar in de praktijk is hier nog weinig ervaring mee opgedaan. Aanbevolen wordt om hier nog expliciet nadere afspraken te maken dat deze logging niet voor andere doeleinden mag worden gebruikt dan de authenticatiedienstverlening en binnen het stelsel toezicht op naleving van deze afspraken te organiseren. Privacywetgeving biedt hier overigens handvatten, maar gezien het feitelijke belang en risico wordt geadviseerd nadrukkelijk te adresseren.

4.4 Doelbinding

Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld en worden niet verder verwerkt op een met die doeleinden onverenigbare wijze (artikel 5, eerste lid, onderdeel b, AVG).

Conclusie: gelet op de beoogde verwerkingsdoelen uit de Wet EBV, is de conclusie dat de nu voorziene verwerkingen van persoonsgegevens in de USvE 1.0 in opzet aan het principe van doelbinding voldoen.

De doelen van het BSNk zijn vastgelegd en omschreven in de Wet EBV en het Besluit GDI. De doelbinding van de authenticatieketen is daarmee getrapt omschreven (via wet, besluit en USvE). Uit de toelichting van het Besluit GDI volgt dat met de verwerkingsdoelen wordt beoogd om gegevensverwerking mogelijk te maken voor een aantal processen, die ten aanzien van het BSNk te onderscheiden zijn en voor de goede werking noodzakelijk zijn. Daarbij gaat het om het proces van aanvraag en/of activering via het BSNk, het daadwerkelijke gebruik van het BSNk (waaronder het authenticeren en doorleveren van BSN c.q. pseudoniem), het verwerken van gegevens in verband met het borgen van de beveiliging en betrouwbaarheid van de voorzieningen (incident- en misbruikbestrijding) en het afhandelen van vragen en klachten van gebruikers.

Op grond van de documentatie USvE 1.0 en ontwerpdocumentatie BSNk zijn de volgende verwerkingen van persoonsgegevens (hoofdprocessen) te onderkennen: activatie van een middel voor het publieke domein (aanmelding), authenticatie (gebruik) inzage en misbruikbestrijding. Deze processen vallen binnen de doelstelling van het eID-stelsel, zoals in de Wet EBV en het Besluit GDI zijn bepaald.

Risico: mogelijkheid voor deelnemers om gegevens uit verschillende rollen te koppelen (function creep)

Als gevolg van het bovenstaande is de conclusie dat in opzet de verwerkingen van persoonsgegevens zoals die zijn voorzien binnen de in de wet vastgelegde doelstellingen passen. Een ander punt is of de genoemde gegevensverwerkingen in de praktijk ook daadwerkelijk binnen de doelbinding zullen plaatsvinden. Aan de erkende partijen worden in de USvE normatieve eisen gesteld door deze op te leggen aan de verschillende rollen die worden onderkend binnen het stelsel (middelenuitgever, authenticatiedienst, toegangsdienst). Onder meer is als eis opgenomen dat privacywetgeving dient te worden nageleefd. Omdat partijen die uit hoofde van hun rol doorgaans ook beschikken over andere gegevens (voor legitieme doeleinden, in het kader van hun dienstverleningsrelatie met klanten), bestaat het risico dat gegevens kunnen worden gebruikt voor andere doeleinden dan waarvoor een grondslag bestaat, zeker op het moment dat er sprake is van concentratie van meerdere rollen binnen een organisatie. Dit verschijnsel staat bekend als function creep.

Hiermee samenhangend kan vanuit de dienstverleners de vraag ontstaan aan deelnemers om meer gegevens (“attributen”) te leveren dan op voorhand is afgesproken. Ook hierop is nauwgezette controle nodig. Om deze druk tegen te gaan wordt geadviseerd om de verstrekking van attributen, met de waarborgen voor gebruikers die daarbij horen, (weer) in het stelsel adequaat te regelen.

Maatregel: verbod op ander gebruik van persoonsgegevens expliciet opnemen in bestaande voorwaarden en toezicht op naleving organiseren

Door met pseudonimisering te werken wordt de mogelijkheid om persoonsgegevens te combineren voor andere doeleinden al sterk teruggedrongen. Zo beschikken deelnemende partijen niet over het BSN om voor andere doeleinden te gebruiken. Dit is een belangrijke technische maatregel die bijdraagt om function creep te voorkomen. Echter met de beschikbare gegevens is nog steeds niet uitgesloten dat de gegevens die wel beschikbaar zijn (denk aan loggingregistraties die inzicht bieden in gebruiksgegevens) voor andere doeleinden gebruikt kunnen worden. Aanbevolen wordt om een dergelijk verbod om ander gebruik van persoonsgegevens – hoewel strikt genomen al verboden op grond van privacywetgeving – expliciet op te nemen in de bestaande voorwaarden en daarop te controleren (toezicht) zodat snel en adequaat maatregelen kunnen worden genomen als function creep wordt geconstateerd. Op het moment dat dit optreedt, kan dit niet alleen concrete gevolgen voor privacy hebben, maar ook direct raken aan het bredere vertrouwen in het stelsel.

4.5 Noodzaak en evenredigheid

Gegevensverwerking wordt beperkt tot wat noodzakelijk is voor de doeleinden waarvoor de gegevens worden verwerkt (artikel 6, AVG). De inbreuk op de persoonlijke levenssfeer van betrokkenen staat in evenredige verhouding tot de met de gegevensverwerkingen nagestreefde doelen (proportionaliteit). De verwerkingsdoeleinden kunnen niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt (subsidiariteit).

De beoordeling van de noodzaak en evenredigheid van de gegevensverwerking bestrijkt in feite vrijwel alle beginselen die de AVG kent. Omwille van de overzichtelijkheid wordt hieronder op een aantal beginselen een conclusie getrokken, risico(‘s) benoemd en (voorgestelde) maatregelen beschreven.

4.5.1 Dataminimalisatie

Persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (artikel 5, eerste lid, onderdeel c, AVG).

Conclusie: minimale gegevensverwerking is een expliciete ontwerpdoelstelling binnen het eID-stelsel. Met polymorfe pseudonimisering wordt het gebruik van het BSN tot een minimum beperkt.

In de USvE zijn de technische eisen opgenomen waaraan partijen moeten voldoen om diensten in het BSN-domein aan te bieden. Binnen de USvE is het voldoen aan de norm van minimale gegevensverwerking (dataminimalisatie) als expliciete ontwerpdoelstelling opgenomen. Dit uit zich in het gebruik van (polymorfe) pseudonimisering om het gebruik van het BSN bij de activering tot een minimum terug te dringen en bij authenticatie helemaal uit te sluiten, door bij de authenticatie voort te bouwen op een eenmalige check op het BSN die bij de activatie van het eID-middel heeft plaatsgevonden. Dit vormt de kerngedachte van de inrichting van het eID-stelsel in de USvE en daarmee lijkt het gebruik van het BSN – technisch – tot een absoluut minimum te worden beperkt. Een eenmalige check lijkt niet anders te kunnen worden uitgevoerd dan door het eenmalig gebruik van het BSN. Deze check verhoudt zich bovendien tot het nagestreefde doel, te weten zekerheid omtrent de identiteit van de gebruiker.

Daarnaast wordt voor het BSNk voorgeschreven welke logging dient te worden bewaard. Uit onder meer de gesprekken met inhoudelijk deskundigen bij de ontwikkeling van het stelsel komt naar voren dat enkel gegevens bewaard blijven ten behoeve van foutopsporing en verantwoording (de borging dat het proces juist is doorlopen). Overigens blijkt deze eis niet overal eenduidig in de USvE. Het verdient aanbeveling dit consistent en expliciet op te nemen. Voor de andere rollen in het stelsel wordt bepaald dat het BSN niet mag worden vastgelegd nadat een middel is geactiveerd. Logging waarover dienstverleners? zelf kunnen beschikken is afhankelijk van de inrichting van de dienstverlening aan hun klanten, die afhankelijk van de dienstverlening kan (en op grond van de USvE mag) verschillen. Het is van belang dat de wijze waarop dit gebeurt, voldoet aan de normen die de AVG op dit punt stelt en dat een dienstverlener dit – ook op grond van de AVG – kan aantonen.

Risico: misbruikbestrijding op stelselniveau wordt bemoeilijkt

Met de getroffen maatregelen lijkt dataminimalisatie in absolute zin te worden nagestreefd, in die zin dat wordt voorgeschreven dat gegevens zoveel mogelijk worden gepseudonimiseerd en dat per rol alleen gegevens voor (technisch) foutopsporing dienen te worden bewaard. Hoewel dit uit oogpunt van dataminimalisatie een goed uitgangspunt is, brengt het het risico met zich mee dat incident- en misbruikbestrijding worden bemoeilijkt omdat (tijdige) detectiemogelijkheden en monitoring daarmee worden ingeperkt. De zorg over adequate detectie en incidentbestrijdings-mogelijkheden is ook eerder door het AP bij de minister van BZK onder de aandacht gebracht.

Maatregel: evenwicht tussen dataminimalisatie en adequate misbruikbestrijding

Hoewel dataminimalisatie een belangrijk privacyuitgangspunt is, is het ook belangrijk dat bij misbruik of (beveiligings)incidenten snel te kunnen optreden en gebruikers die daarvan het slachtoffer zijn in hun (privacy)belang te kunnen ondersteunen. Aanbevolen wordt om voor de daarvoor benodigde gegevens een evenwicht te zoeken tussen het streven naar dataminimalisatie en de noodzakelijke gegevens, zodat tevens kan worden opgetreden tegen onverhoopte verstoringen en deze te kunnen herstellen. Dit is een – uit hoofde van de wet EBV gelegitimeerd – doel. Dataminimalisatie is in die zin niet absoluut en zou ook een ondergrens moeten kennen.

4.5.2 Opslagbeperking

Persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is (artikel 5, eerste lid, onderdeel e, AVG).

Conclusie: in de USvE zijn bewaartermijnen voor verschillende typen gegevens vastgelegd, onder verwijzing naar *best practices*. De inhoudelijke onderbouwing waarom betreffende bewaartermijnen noodzakelijk zijn, ontbreekt echter.

Het privacybeginsel van opslagbeperking houdt in dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen moet nemen om de rechten en vrijheden van betrokkenen te beschermen. Persoonsgegevens mogen dan ook niet langer worden bewaard dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is. Daartoe moeten bewaartermijnen voor gegevens worden bepaald en vastgesteld. In het Besluit GDI worden eisen aan de opslagtermijn van persoonsgegevens gesteld. Voor het BSNk worden de bewaartermijnen, per persoonsgegeven, in het besluit concreet beschreven.

In de USvE 1.0 wordt – in opzet – nadere invulling gegeven aan de opslag van persoonsgegevens. Zo moeten organisaties verschillende bewaartermijnen in acht nemen. Deze bewaartermijnen in de USvE zijn gebaseerd op *best practices,* dat wil zeggen de in de praktijk veel gebruikte en bewezen termijnen. De argumentatie c.q. normatieve onderbouwing *waarom* de genoemde periodes zijn opgenomen, zijn voor zover de opstellers van de GEB hebben kunnen nagaan, niet vastgelegd.

Risico: bewaartermijnen in regelgeving en de USvE komen niet overeen

In ieder geval wordt vastgesteld dat de bewaartermijnen in de wet en de USvE 1.0 niet met elkaar overeenkomen. Deels zou dit te verklaren kunnen zijn omdat het BSNk sinds de vaststelling van het Besluit GDI is doorontwikkeld, waarbij grosso modo is gestreefd naar kortere bewaartermijnen. Het is echter van belang om over een normatieve onderbouwing van de bewaartermijnen te beschikken, omdat anders niet onomstotelijk kan worden vastgesteld dat de bewaartermijnen aan de geldende privacywet- en regelgeving voldoen.

Maatregel: bewaartermijnen expliciet vaststellen en onderbouwen

Vanwege de lopende doorontwikkeling van met name het BSNk kan op dit moment niet met zekerheid gezegd worden wat de opslagperioden van persoonsgegevens zijn. In de USvE wordt opgemerkt dat de genoemde bewaartermijnen nog kunnen wijzigen als gevolg van nadere besluiten over de invulling van de bestrijding van misbruik en fraude.

Aanbevolen wordt om bij de verdere ontwikkeling expliciet aandacht te besteden aan de vaststelling van de bewaartermijnen van verschillende persoonsgegevens, en bij deze vaststelling de normatieve onderbouwing (het "waarom") expliciet vast te leggen. Deze onderbouwde bewaartermijnen dienen de basis te vormen voor de (eventuele) aanpassing van zowel het besluit GDI als de USvE op dit punt. Het is essentieel dat deze documenten met elkaar in lijn worden gebracht. Overigens behoeft de onderbouwing niet in de USvE zelf te worden opgenomen. Belangrijk is dat de gemaakte keuzes inzichtelijk zijn. Dat kan ook in onderliggende documentatie.

4.5.3 Juistheid

Alle redelijke maatregelen moeten worden genomen, die gelet op de doeleinden waarvoor zij worden verwerkt juist zijn, en als dat niet zo is, deze onverwijld te wissen of te rectificeren (artikel 5, eerste lid, onderdeel d, AVG).

Conclusie: er zijn binnen het eID-stelsel reeds waarborgen voor de juistheid van gegevens getroffen en voorzien, doordat gebruikers hun authenticatiemiddelen kunnen inzien en gegevens kunnen wijzigen indien nodig. Het is belangrijk dat deze waarborgen niet alleen zijn ontwikkeld, maar onder de aandacht blijven en daadwerkelijk worden ingevuld.

In de diverse documenten binnen de scope van deze GEB wordt het belang van juistheid van gegevens onderkend en worden er op diverse plaatsen normen en eisen gesteld en maatregelen voorgesteld. Echter ook op dit punt geldt sterk dat het een traject in ontwikkeling is en dat nadere uitwerking nodig zal zijn om tot een samenhangend geheel aan maatregelen te komen dat afdoende invulling geeft aan het privacyprincipe van juistheid.

Organisaties moeten borgen dat persoonsgegevens feitelijk juist en nauwkeurig zijn, gelet op de doeleinden waarvoor ze worden verwerkt. Verantwoordelijken moeten ervoor zorgen dat persoonsgegevens juist zijn en zo nodig worden geactualiseerd. De AVG stelt dat alle redelijke maatregelen moeten worden genomen die zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist zijn en als dat niet zo is, deze onverwijld gewist of gerectificeerd worden. Gezien de context is het belang van juiste gegevens binnen het eID-stelsel groot, omdat onjuistheid van authenticaties niet alleen gevolgen heeft binnen het eID zelf, maar voor burgers/gebruikers grote gevolgen kan hebben voor transacties die op basis van deze gegevens bij dienstverleners plaatsvinden. Onjuistheid van gegevens kan verregaand negatief doorwerken tot ver buiten het eID-stelsel.

De Wet EVB, het Besluit GDI en de regeling GDI stellen regels ten aanzien van de werking, betrouwbaarheid en goede werking van onder meer voor voorzieningen voor elektronische authenticatie. Uit de USvE 1.0 komt naar voren dat aandacht is besteed aan kwaliteitsborging van de gegevens die worden verwerkt binnen het stelsel. Op diverse plaatsen komen eisen naar voren, bijvoorbeeld de beveiligingseisen of de beoogde inzagemogelijkheid voor burgers, welke zullen bijdragen aan de kwaliteit en juistheid van gegevens. Een belangrijk uitgangspunt waarop de USvE 1.0 is gebaseerd is betrouwbaarheid. In de USvE worden de eisen uit de eIDAS-verordening, die de betrouwbaarheid en kwaliteit beogen te beschermen, onverkort gesteld en op onderdelen ook verder aangescherpt. Procedures zijn erop gericht om maximale zekerheid te verkrijgen over identiteitsvaststelling en derhalve de juistheid van gegevens.

Uit de USvE blijkt tevens dat wordt beoogd de gebruiker door middel van inzicht in zijn middelen de status van zijn middelen te laten bekijken. Daarmee kunnen ook mogelijke fouten in de verwerking van de gebruikersgegevens worden opgemerkt. Ook in de ontwerpdocumentatie van het BSNk komt naar voren dat op diverse plaatsen controles zijn ingebouwd om de juistheid van gegevens te verzekeren.[23]

Risico: (beheer)processen/waarborgen voor borging juistheid niet (volledig) ingevuld

Procedures en (beheer)processen worden beschreven, maar belangrijk is dat zij feitelijk niet ook daadwerkelijk worden ingericht. Een risico is dat de procedures die zijn beschreven niet of onvoldoende worden geoperationaliseerd, waardoor essentiële controles kunnen ontbreken. Concreet is in dit verband geconstateerd (op grond van de documentatie en gesprekken met deskundigen), dat de functionaliteit die de autorisatielijst BSN faciliteert wel wordt ontwikkeld, maar dat afspraken over het adequate beheer en dus juistheid van de lijst nog niet zijn ingericht. Dit is belangrijk omdat de veronderstelde controle op deze lijst als doel heeft om te voorkomen dat (private) partijen die geen recht hebben op het BSN dit ook niet krijgen. Als het beheer van deze lijst niet goed is ingericht, kan het voorkomen dat BSN's onbedoeld aan private partijen worden geleverd. Dit wordt ingeschaald als een serieus risico, omdat juist en minimaal gebruik van het BSN één van de kerndoelstellingen is die ten grondslag ligt aan de inrichting van het eID-stelsel.

Maatregelen: beheerprocessen feitelijk inrichten

Naast de inrichting van de functionaliteit/techniek van het stelsel dient expliciet aandacht te zijn voor de (beheer)processen daaromheen, die zorgen voor een juiste werking van het stelsel en de ingebouwde controle daarop. Het adequate beheer van de autorisatielijst BSN is in die context een essentiële maatregel en dient te zijn ingericht voordat gestart wordt met de ingebruikname van het BSNk in de voorloperfase.

Aanbevolen wordt om meer in het algemeen de inrichting van beheerprocessen die zorgen voor transparantie en bijdragen aan de juistheid van gegevens expliciet te beleggen en ook feitelijk in te richten.

[23] N.a.v. de technische check op het BSNk zal dit element nog verder worden uitgewerkt.

4.5.4 Beveiliging

Er moeten passende technische of organisatorische maatregelen moeten worden genomen, zodanig dat een passende beveiliging van de persoonsgegevens is gewaarborgd, zodat de persoonsgegevens ondermeer zijn beschermd tegen ongeoorloofde en onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (artikel 5, eerste lid, onderdeel f, AVG).

Conclusie: er is binnen het eID-stelsel een breed scala aan maatregelen getroffen om de beveiliging van persoonsgegevens te waarborgen. Dit zijn maatregelen die op een goede manier bijdragen aan de beveiliging van persoonsgegevens. Omdat het stelsel nog volop wordt doorontwikkeld, kan op dit moment echter nog niet worden vastgesteld of de beveiliging ook adequaat is.

De USvE adresseert expliciet informatiebeveiliging en privacy en schrijft participanten toegangsdiensten, middelenuitgevers en authenticatiediensten organisatorische, procedurele en meer technische beveiligingsmaatregelen voor.

Ten aanzien van de aanvraag en registratie van authenticatiemiddelen worden nadere eisen gesteld om betrouwbare uitgifte van middelen te verzekeren, waarbij wordt aangesloten bij de eIDAS-normen. Ondermeer wordt verlangd dat een middelenuitgever voorziet in procedures rond schorsing, intrekking en reactivering van middelen. Tevens wordt in de privacyparagraaf van de USvE aan participanten de verplichting opgelegd om misbruikbestrijding in te regelen. Er dienen processen voorhanden te zijn om onbevoegde handelingen te detecteren en te onderzoeken. Bij vermissing, misbruik of fraude dienen maatregelen te worden genomen. Verder moeten participanten gebruikers wijzen op de veiligheidsvoorschriften die gelden voor het gebruiken van authenticatiemiddelen.

Binnen het ontwerp van het stelsel biedt polymorfe pseudonimisering een belangrijke beveiligingsmaatregel. Het voorkomt dat een grote concentratie van gegevens op één plek ontstaat en zorgt voor compartimentering binnen het stelsel. Polymorfe pseudonimisering wordt daarom gezien als een belangrijke security (en derhalve ook privacy) by design maatregel.

Strikt genomen zijn er qua architectuur en techniek meerdere invullingen van de beveiliging van persoonsgegevens mogelijk. Een aantal van deze invullingen zou kunnen worden overwogen, waarna de verantwoordelijke moet afwegen met welke invulling security by design (zoals vereist vanuit de AVG) het best wordt ingevuld.

Polymorfe pseudonimisering kan als zodanig geen eis/norm zijn (want het is een mogelijke PET-maatregel[24] die een eis dan wel norm invult). Echter het kan gezien de combinatie van de norm (dataminimalisatie van BSN gebruik) en compartimentering in de context (multimiddelenstrategie waarbij het juridisch niet toegestaan en maatschappelijk ongewenst is dat private authenticatiediensten activiteiten van burgers bij de overheid op BSN-niveau kunnen herkennen) wel als de facto eis voortvloeien. Gelet op de invulling die polymorfe pseudonimisering biedt aan zowel dataminimalisatie als beveiliging wordt aanbevolen om vanuit privacyoogpunt PP als eis te hanteren.

Risico: incident- en misbruikbestrijding is uitdaging door polymorfe pseudonimisering

Een adequate beveiliging en bescherming van persoonsgegevens wordt echter niet alleen bereikt door – op zichzelf goede – technische privacymaatregelen vooraf (zoals pseudonimisering), waardoor wordt getracht inbreuken op de beveiliging c.q. misbruik van persoonsgegevens te voorkomen. Adequate bescherming van persoonsgegevens vloeit voort uit een goede samenhang tussen en samenspel van verschillende maatregelen, ook maatregelen die inbreuken of misbruik van persoonsgegevens kunnen herkennen en herstellen als het onverhoopt toch gebeurt. In dat

[24] PET staat voor "Privacy Enhancing Technology", oftewel een technische maatregel ter bescherming van privacy.

verband dient nog bekeken te worden hoe PP als invulling van het AVG-beginsel dataminimalisatie (d.w.z. minimalisatie van verwerking van het BSN) zich verhoudt tot andere – even belangrijke – privacybeginselen als garanderen van juistheid, beveiliging (waaronder incident- en misbruikbestrijding).

Maatregel: misbruik- en incidentbestrijding op stelselniveau uitwerken

Het is belangrijk om een balans te vinden waarin PP zo kan worden ingezet dat bijvoorbeeld herstelprocessen en misbruikbestrijding op stelselniveau mogelijk blijven. Misbruikbestrijding en incidentbestrijding op stelselniveau, en de gegevens die daarvoor kunnen worden gebruikt zijn in de USvE nog niet uitgewerkt. Dit moet voor een evenwichtige bescherming van persoonsgegevens echter nog wel gebeuren.

Risico: ontstaan privacy hotspots en single points of failure buiten het stelsel

Door middel van polymorfe pseudonimisering is binnen het stelsel dataminimalisatie en compartimentering ingeregeld, waardoor grote gegevensconcentraties worden vermeden. Het is belangrijk dat deze compartimentering ook aan de zijde van overheidsdienstverleners, ook buiten het eID-stelsel, in stand blijft. Binnen het eID-stelsel zijn geen juridische of technische waarborgen die voorkomen dat een dienstverlener door compartimenten heen gegevens van gebruikers koppelt op het BSN.

Bij het vaststellen van de identiteit van de gebruiker kan de dienstverlener ontzorgd worden door meerdere koppelvlakken naast elkaar toe te laten staan. Zo hoeft de dienstverlener niet zelf te zorgen voor aansluiting. ICT-leveranciers in de markt zouden de ontzorging van dienstverleners op zich kunnen nemen. Dit is op zichzelf een begrijpelijke en, zeker voor kleinere overheidsdienst-verleners verstandige ontwikkeling, omdat de inrichting dan door een gespecialiseerde deskundige partij wordt ingericht. Echter als een dergelijke leverancier meerdere dienstverleners gaat ontzorgen, bestaat er een kans op een nieuwe privacy hotspot of een single point of failure, omdat de leverancier de gegevens van veel overheidsdienstverleners tezamen onder zijn verantwoordelijkheid krijgt. Het risico bestaat dat compartimentering grotendeels teniet wordt gedaan doordat een aantal belangrijke leveranciers voor overheidspartijen in feite meerdere rollen invullen. Dat risico wordt op dit moment binnen de USvE niet geadresseerd.

Maatregel: eisen stellen aan dienstverleners en leveranciers bij cumulatie van rollen

Voorgesteld wordt om gezien het beschreven risico, eisen te stellen aan dienstverleners en leveranciers, ten aanzien van combinaties van rollen en cumulatie van partijen binnen één leverancier. Minimaal zouden er garanties voor functiescheiding (Chinese muren) moeten komen.

Maatregel: nogmaals risicoanalyse uitvoeren op nieuwe versie USvE

Uit de AVG volgt dat "passende technische of organisatorische maatregelen moeten worden genomen, zodanig dat een passende beveiliging van de persoonsgegevens is gewaarborgd, zodat de persoonsgegevens ondermeer zijn beschermd tegen ongeoorloofde en onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging". Bij het treffen van maatregelen dient rekening gehouden te worden met de stand van techniek, kosten, de context van de verwerking van persoonsgegevens en de risico's die worden gelopen. Beoogd wordt om een op het risico afgestemd beveiligingsniveau te waarborgen. Dit laatste veronderstelt dat de verantwoordelijke een risicoanalyse uitvoert. Aanbevolen wordt om deze risicoanalyse – nogmaals uit te voeren, toegespitst om de situatie zoals die na oplevering van de nieuwe versie van de USvE bestaat. Op deze wijze kunnen eventueel nog aanvullende maatregelen op maar worden getroffen.

4.5.5 Accountability

De verwerkingsverantwoordelijke moet naleving van de privacyprincipes verantwoorden en kunnen aantonen(artikel 5 lid 2, AVG). Er is een scherp en gedocumenteerd zicht op de gevoerde verwerking van persoonsgegevens, de redenen, grondslagen en verantwoordelijkheden.

Conclusie: op dit moment is nog onvoldoende voldaan aan het privacybeginsel accountability. De verwerkingen en informatie zoals beschreven in de GEB zijn niet tot in detail uit de documentatie af te leiden, maar komen voor een belangrijk deel ook van de geraadpleegde deskundigen die bij de ontwikkeling van het eID-stelsel betrokken zijn.

Om 'accountable' te zijn zou beschreven moeten worden welke organisatie verantwoordelijk is voor welke gegevensverwerkingen, waarbij ook duidelijk moet zijn waar precies de grenzen liggen en welke gegevens worden verwerkt. Dat is uit de USvE nu nog niet volledig af te leiden. De USvE benoemt dat er participanten kunnen zijn, organisaties die verschillende rollen kunnen hebben: authenticatiedienst, middeluitgever en toegangsdienst. Daarnaast zijn er dienstverleners, gebruikers en het BSNk, waar zoals eerder gezegd in de USvE geen nadere eisen aan gesteld worden. Bij de verschillende rollen beschrijft de USvE welke verantwoordelijkheden de organisatie die de rol uitvoert in ieder geval heeft. Daarmee geeft de USvE een aanduiding van de processen waarin de gegevens verwerkt worden. Er wordt in de documentatie niet aangegeven welke gegevens verwerkt worden. Soms is uit de eisen die gesteld worden in het normenkader iets af te leiden over de gegevens, maar zeker niet volledig en eenduidig.

Risico: niet voldaan aan verantwoordingsplicht AVG

Op basis van de constateringen is dat op dit moment nog niet zou worden voldaan aan het privacybeginsel van accountability, en daarmee op dit punt niet aan de AVG. Op dit moment is dat overigens begrijpelijk, omdat de documentatie een tussenresultaat is van het traject waarnaar wordt toegewerkt. Echter op het moment dat gestart wordt met de verwerkingen van persoonsgegevens in het voorlopertraject, in januari 2018, is het noodzakelijk om de accountability op orde te hebben. Op het moment dat dit niet het geval, is ontstaat onder de AVG een formeel-juridisch risico dat de verplichting niet wordt nageleefd. Echter belangrijker is dat dan een situatie zou ontstaan waarin de verwerkingen van persoonsgegevens binnen het eID-stelsel niet 'in control' zijn, waardoor de kwaliteit en betrouwbaarheid van de gegevens niet (aantoonbaar) kan worden gegarandeerd.

Maatregel: verwerkingen van persoonsgegevens volledig en eenduidig beschrijven

Aanbevolen wordt om er in de aankomende periode naar januari 2018 voor te zorgen dat de beschrijvingen van verwerkingen van persoonsgegevens in de USvE (of onderliggende ontwerpdocumentatie) volledig en eenduidig worden beschreven. Advies is om deze GEB – als momentopname met een aanzet tot deze beschrijving – als hulpmiddel/startpunt te gebruiken om daartoe te komen.

Bijlagen

1 Concept Model Gegevensbeschermingseffectbeoordeling Rijksdienst

De opbouw van deze GEB volgt grotendeels het concept Model GEB Rijksdienst gebruikt. Dit model bestaat vier onderdelen en omvat in totaal 16 toetspunten. Het model is in deze bijlage volledig opgenomen. Deze GEB wordt hier kort samengevat aan de hand van de 16 toetspunten uit het model. Bij onderdeel B, de beoordeling van de rechtmatigheid van de gegevensverwerkingen, zijn de normen waaraan is getoetst in grijze kaders weergegeven, volgens dezelfde systematiek als in hoofdstuk 4 is gevolgd.

A. Beschrijving algemene kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

1. Voorstel

Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet op hoofdlijnen.

Om de veiligheid van digitale identiteitsvaststelling te verbeteren en de afhankelijkheid van een enkel middel te verminderen, is het Elektronische Identiteit Stelsel (eID-stelsel) opgezet. Het stelsel moet burgers en bedrijven in staat stellen op een veilige en betrouwbare manier digitaal zaken te doen met publieke én private aanbieders van online diensten. In het stelsel zijn verschillende rollen, verantwoordelijkheden en processen uitgewerkt die een burger in staat stellen om veilig en betrouwbaar een authenticatiemiddel te gebruiken om in te loggen bij een overheidsorganisatie, de eigen authenticatiemiddelen te beheren en te beëindigen, en eigen persoonsgegevens in te zien. Deze GEB heeft betrekking op ***het gehele eID-stelsel en de basale werking*** daarvan en kijkt vooruit naar het zogenoemde ***voorlopertraject*** dat in januari 2018 start en eindigt wanneer de Wet GDI in werking treedt. Dat het eID-stelsel nog volop in ontwikkeling is, betekent dat deze GEB een ***momentopname*** is, met als doel privacyrisico's en mogelijke maatregelen te benoemen zoals die nu gezien worden en die in de verdere ontwikkeling kunnen worden geadresseerd. Zie verder de paragrafen 1.3, 1.4 en 1.5 en hoofdstuk 3.

2. Persoonsgegevens

Som alle categorieën persoonsgegevens op die worden verwerkt. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder of strafrechtelijk. Geef per persoonsgegeven tevens aan op wie die betrekking hebben.

Het eID-stelsel bestaat uit verschillende processen: activering, authenticatie, statusbeheer, inzage en misbruikbestrijding. Binnen al die processen worden gewone persoonsgegevens verwerkt. De wijze waarop wordt uitgebreid per proces toegelicht in hoofdstuk 3, in de paragrafen 3.1.4, 3.2.4, 3.3.4, 3.4.4 en 3.6.7. Er worden binnen het eID-stelsel geen bijzondere of strafrechtelijke persoonsgegevens verwerkt.

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

Op welke wijze gegevens worden verwerkt binnen de onder 2 genoemde processen wordt uitgebreid per proces toegelicht in hoofdstuk 3, in de paragrafen 3.1.3, 3.2.3, 3.3.3, 3.4.3, 3.5 en 3.6.

4. Verwerkingsdoeleinden

Beschrijf de hoofd- en nevendoeleinden van de voorgenomen gegevensverwerkingen.

De verwerkingsdoeleinden worden per proces toegelicht in hoofdstuk 3, in de paragrafen 3.1.1, 3.2.1, 3.3.1, 3.4.1 en 3.5

5. Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker of ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Binnen het eID-stelsel worden vijf verschillende rollen onderscheiden:

- De ***gebruiker*** van een authenticatiemiddel.
- Een ***dienstverlener*** bij wie de gebruiker wil inloggen om een dienst af te nemen.
- De ***middelenuitgever (MU)*** stelt authenticatiemiddelen beschikbaar binnen het stelsel en geeft deze op verzoek uit aan de gebruiker. De MU is verantwoordelijk voor activering van een middel bij het BSNk en het actueel houden de status van een authenticatiemiddel. Bestaande middelenuitgevers zijn uitgevers van Idensys eID-middelen en bijvoorbeeld DigiD.
- Een ***authenticatiedienst (AD)*** voert authenticatieprocedures wanneer een gebruiker een authenticatiemiddel inzet om in te loggen bij een bepaalde dienstverlener. De authenticatiedienst levert een authenticatieverklaring aan de toegangsdienst en legt daarnaast de authenticatiehistorie vast. De rollen van middelenuitgever en authenticatiemiddelen zijn conceptueel gescheiden, maar worden in de praktijk vaak door dezelfde partijen vervuld: zo zorgt DigiD als authenticatiedienst voor authenticatie van de gebruiker als deze met DigiD wil inloggen bij een overheidsdienstverlener.
- Een ***toegangsdienst (TD)*** verstrekt verklaringen over de identiteit van een gebruiker aan de dienstverlener. De toegangsdienst biedt de gebruiker de mogelijkheid om een authenticatiedienst te kiezen en vervult in feite de rol van tussenpersoon. Een toegangsdienst is optioneel in het stelsel en vooral bedoeld om andere rollen in het stelsel te ontzorgen.

Deze rollen kunnen door dezelfde partijen worden vervuld. Op grond van artikel X, eerste lid, Wet EBV is de minister van BZK de verwerkingsverantwoordelijke binnen het eID-stelsel. De gebruiker is verstrekker van informatie. Alle overige rollen zijn zowel verwerker, verstrekker en ontvanger van informatie. Zie verder de schema's en procesbeschrijvingen in hoofdstuk 3. Welke functionarissen binnen de betreffende organisaties toegang hebben tot persoonsgegevens valt buiten de scope van deze GEB, omdat die toeziet op de basale werking van het eID-stelsel als geheel. De GEB ziet op de conceptuele vormgeving van het eID-stelsel, niet op de functionele detailinvulling ervan.

6. Belangen bij de gegevensverwerking

Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

De verwerkingsverantwoordelijke (de minister van BZK) heeft als belang dat de doelen die het kabinet heeft met het eID-stelsel worden gerealiseerd, namelijk om (1) burgers en bedrijven in staat te stellen op een veilige en betrouwbare manier digitaal zaken te doen met publieke en private aanbieders van online diensten en (2) de continuïteit te verhogen door de afhankelijkheid van DigiD als exclusief authenticatiemiddel te verminderen. Daarmee zijn ook direct de belangen van de gebruiker en de dienstverlener verwoord. Daarnaast spelen commerciële belangen van private partijen die binnen het stelsel diensten bieden en uiteraard het privacybelang van de gebruiker.

7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

De GEB ziet op de conceptuele vormgeving van het eID-stelsel, niet op de functionele detailinvulling ervan. Daarom valt op basis van de huidige documentatie hierover geen oordeel te

geven. Dit vindt plaats door partijen zelf. Zij dienen hiermee rekening te houden en indien nodig maatregelen te treffen als verwerkingen buiten de EU plaatsvinden.

8. Techniek van gegevensverwerking: geautomatiseerde besluitvorming, profilering en big data

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen de persoonsgegevens worden verwerkt. Benoem of sprake is van geautomatiseerde besluitvorming, profilering of big data en, zo ja, beschrijf waaruit een en ander bestaat.

Het BSNk vormt de spil van het eID-stelsel. Het BSNk vervult binnen het stelsel verschillende functies die veilig gebruik van een authenticatiemiddel door de gebruiker waarborgen. De techniek die daarbij wordt toegepast is ***polymorfe pseudonimisering.*** Dat wil zeggen dat een burger die een authenticatiemiddel aanvraagt dat middel eenmalig activeert met behulp van het BSN. Het BSNk genereert vervolgens een pseudoniem van die burger, specifiek voor het betreffende middel. Het pseudoniem kan door een dienstverlener via het BSNk vervolgens weer worden omgezet in een leesbare identiteit: de dienstverlener weet dan dat de betreffende burger is wie hij/zij zegt te zijn. Dit maakt dat het BSN, waarmee de burger zich oorspronkelijk heeft geïdentificeerd, door partijen binnen het stelsel vervolgens niet meer te achterhalen is. Met deze opzet is bewust gekozen als een invulling van privacy by design. Zie ook paragraaf 1.5, de procesbeschrijvingen in paragrafen 3.1 t/m 3.4 en paragraaf 3.6.

9. Juridisch en beleidsmatig kader

Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerkingen.

Het juridische en beleidsmatig kader wordt gevormd door de Europese eIDAS-verordening, de Wet EBV, het Besluit GDI, de Regeling voorzieningen GDI en het Uniforme Set van Eisen versie 1.0. De kaders worden toegelicht in paragraaf 1.4.

10. Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

De bewaartermijnen zijn – voor zover in deze fase van de ontwikkeling van het eID-stelsel bekend – per proces beschreven in hoofdstuk 3.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel de grondslag, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen.

11. Grondslag

Bepaal op welke grondslagen de gegevensverwerkingen worden gebaseerd.

De persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. De gegevensverwerking is gebaseerd op tenminste één van de zes volgende grondslagen genoemd in artikel 6, eerste lid, AVG.

De binnen het eID-stelsel voorgenomen verwerkingen van persoonsgegevens zijn rechtmatig. De Wet EBV en het Besluit GDI bieden een adequate grondslag. Zie verder paragraaf 4.2.

12. Bijzondere en strafrechtelijke persoonsgegevens

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, bepaal of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is op de voorgenomen gegevensverwerkingen.

Indien van toepassing: er geldt bij wet een uitzondering op het verbod tot verwerking van bijzondere persoonsgegevens (artikel 9, eerste lid, AVG). Verwerking van strafrechtelijke gegevens vindt plaats door of onder toezicht van de overheid, of is bij wet geregeld (artikel 10, AVG).

Er worden geen bijzondere of strafrechtelijke persoonsgegevens verwerkt binnen het eID-stelsel. Wel kunnen patronen in andere persoonsgegevens die in het eID-stelsel worden verwerkt een indicatie of voorspeller zijn van bijzondere persoonsgegevens. Zie verder paragraaf 4.3.

13. Doelbinding

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld en worden niet verder verwerkt op een met die doeleinden onverenigbare wijze (artikel 5, eerste lid, onderdeel b, AVG).

Gelet op de beoogde verwerkingsdoelen uit de wet EBV, is de conclusie dat de nu voorziene verwerkingen van persoonsgegevens in de USvE 1.0 in opzet aan het principe van doelbinding voldoen. Zie verder paragraaf 4.4.

14. Noodzaak en evenredigheid

Beoordeeld of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de nagestreefde doeleinden. Ga hierbij in ieder geval in op:

a) Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer van betrokkenen in evenredige verhouding tot de met de gegevensverwerkingen nagestreefde doelen?
b) Subsidiariteit: kunnen de verwerkingsdoeleinden niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?

Gegevensverwerking wordt beperkt tot wat noodzakelijk is voor de doeleinden waarvoor de gegevens worden verwerkt (artikel 6, AVG). De inbreuk op de persoonlijke levenssfeer van betrokkenen staat in evenredige verhouding tot de met de gegevensverwerkingen nagestreefde doelen (proportionaliteit). De verwerkingsdoeleinden kunnen niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt (subsidiariteit).

De beoordeling van de noodzaak en evenredigheid van de gegevensverwerking bestrijkt in feite vrijwel alle beginselen die de AVG kent. Omwille van de overzichtelijkheid wordt hieronder op een aantal beginselen een conclusie getrokken, risico('s) benoemd en (voorgestelde) maatregelen beschreven.

Dataminimalisatie: persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (artikel 5, eerste lid, onderdeel c, AVG).

Minimale gegevensverwerking is een expliciete ontwerpdoelstelling binnen het eID-stelsel. Met polymorfe pseudonimisering wordt het gebruik van het BSN tot een minimum beperkt. Zie verder paragraaf 4.5.1.

Opslagbeperking: persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is (artikel 5, eerste lid, onderdeel e, AVG).

In de USvE zijn bewaartermijnen voor verschillende typen gegevens vastgelegd, onder verwijzing naar *best practices*. De onderbouwing waarom betreffende bewaartermijnen noodzakelijk zijn, ontbreekt echter. Zie verder paragraaf 4.5.2.

Juistheid: alle redelijke maatregelen moeten worden genomen, die gelet op de doeleinden waarvoor zij worden verwerkt juist zijn, en als dat niet zo is, deze onverwijld te wissen of te rectificeren (artikel 5, eerste lid, onderdeel d, AVG).

Er zijn binnen het eID-stelsel reeds waarborgen voor de juistheid van gegevens getroffen en voorzien, doordat gebruikers hun authenticatiemiddelen kunnen inzien en gegevens kunnen wijzigen indien nodig. Belangrijk is dat deze waarborgen – naast de ontwikkeling van de functionaliteit – onder de aandacht blijven en daadwerkelijk worden ingevuld. Zie verder paragraaf 4.5.3.

Beveiliging: er moeten passende technische of organisatorische maatregelen worden genomen, zodanig dat een passende beveiliging van de persoonsgegevens is gewaarborgd, zodat de persoonsgegevens ondermeer zijn beschermd tegen ongeoorloofde en onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (artikel 5, eerste lid, onderdeel f, AVG).

Er is binnen het eID-stelsel een breed scala aan maatregelen getroffen om de beveiliging van persoonsgegevens te waarborgen. Dit zijn maatregelen die op een goede manier bijdragen aan de beveiliging van persoonsgegevens. Of er sprake is van een passende beveiliging kan op dit moment echter nog niet worden vastgesteld, gelet op het feit op dit moment nog wordt gewerkt aan de doorontwikkeling. In lijn met de risicogerichte benadering voor de bescherming van persoonsgegevens, wordt geadviseerd om op het moment dat de ontwikkeling nagenoeg is afgerond een risicoanalyse uit te voeren en daarop de concrete – aanvullende beveiligingsmaatregelen te treffen. Zie verder paragraaf 4.5.4.

Accountability: de verwerkingsverantwoordelijke moet naleving van de privacyprincipes verantwoorden en kunnen aantonen(artikel 5 lid 2, AVG). Er is een scherp en gedocumenteerd zicht op de gevoerde verwerking van persoonsgegevens, de redenen, grondslagen en verantwoordelijkheden.

De conclusie op basis van de constateringen is dat op dit moment nog niet zou worden voldaan aan het privacybeginsel van accountability. De verwerkingen en informatie zoals beschreven in de GEB zijn niet tot in detail uit de documentatie af te leiden, maar komen voor een belangrijk deel ook van de geraadpleegde deskundigen die bij de ontwikkeling van het eID-stelsel betrokken zijn. Zie verder paragraaf 4.5.5.

C. Beschrijving en beoordeling risico's voor de rechten en vrijheden betrokkene

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van betrokkene. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking.

15. Risico's

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van betrokkene. Ga in ieder geval in op:

a) welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van betrokkene;
b) de oorsprong van deze gevolgen;
c) de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
d) de ernst (impact) van deze gevolgen voor de betrokkene wanneer deze intreden.

Houd bij elk aspect rekening met de aard, omvang, context en doelen van de gegevensverwerking.

In hoofdstuk 4 zijn geordend naar de verschillende toetspunten de risico's beschreven.

D. Beschrijving voorgenomen maatregelen

Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de voorgenomen gegevensverwerkingen voor de vrijheden en rechten van betrokkene aan te pakken.

16. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven privacyrisico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

In hoofdstuk 4 zijn per geconstateerd risico maatregelen voorgesteld.

2 Lijst van Afkortingen en Begrippen

Afkortingen

AVG = Algemene Verordening Gegevensbescherming
BRP = Basisregistratie Personen
BSN = Burgerservicenummer
BSNk = Burgerservicenummer Koppelregister
BZK = Binnenlandse Zaken en Koninkrijksrelaties
EBV = Elektronisch Berichtenverkeer
FG = Functionaris voor de Gegevensbescherming
GDI = Generieke Digitale Infrastructuur
OIN = Overheidsidentificatienummer
PIA = Privacy Impact Assessment
USvE = Uniforme Set van Eisen
Wbp = Wet Bescherming Persoonsgegevens
WID = Wettelijke Identiteitsdocument

Begrippen

Authenticatiedienst	= Voert authenticatieprocedures uit waarmee gebruikers worden geauthenticeerd.
Authenticatiemiddel	= Inlogmiddel op grond waarvan authenticatie van een gebruiker kan plaatsvinden.
BSNk	= Voorziening die het mogelijk maakt om publieke en private authenticatiemiddelen te gebruiken in het publieke domein
Dienstverlener	= Biedt elektronische diensten aan gebruikers aan. Een voorbeeld van een dienstverlener is de Belastingdienst.
Inzageregister	= Register waarbij de status van authenticatiemiddelen wordt geregistreerd en gebruikers deze status kunnen inzien.
Middelenuitgever	= Partij die een authenticatiemiddel verstrekt aan de gebruiker.
Toegangsdienst	= 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 deze dienst.

Uniforme Set van Eisen	= Bevat de eisen voor erkenning van zowel publieke als private authenticatiemiddelen voor het publieke domein.