Bijlage 4: Privacy impact assessments (PIA) voor DigiD Hoog

Recentelijk heb ik de Nota naar aanleiding van het verslag (NnavV) over de wet digitale overheid (WDO) aan uw kamer gezonden, waarin ik de vragen van uw kamer ter voorbereiding van dit wetsvoorstel heb beantwoord.

De leden van de D66-fractie hebben mij in dat verband gevraagd of de uitgevoerde privacy impact assessments (PIA's) aan de kamer kunnen worden toegezonden. Ik heb daarop aangegeven daar graag gehoor aan te geven en deze bij gelegenheid van de komende eID-voortgangsrapportage aan u toe te zenden. Bijgaand treft u de PIA op DigiD hoog aan. Voor de volledigheid merk op dat eerdere PIA's op het eID-stelsel (brief van 6 juli 2017; Kamerstuk 26 643 nr. 481) en de PIA op DigiD substantieel (brief van 2 oktober 2017; Kamerstuk 26 643 nr. 491) reeds aan uw Kamer zijn gezonden.

De algemene conclusie van de PIA op DigiD hoog is dat de uitrol van DigiD hoog bijdraagt aan verbetering van privacybescherming. Zoals in de PIA aangegeven wordt daar thans in stappen naar toegewerkt.

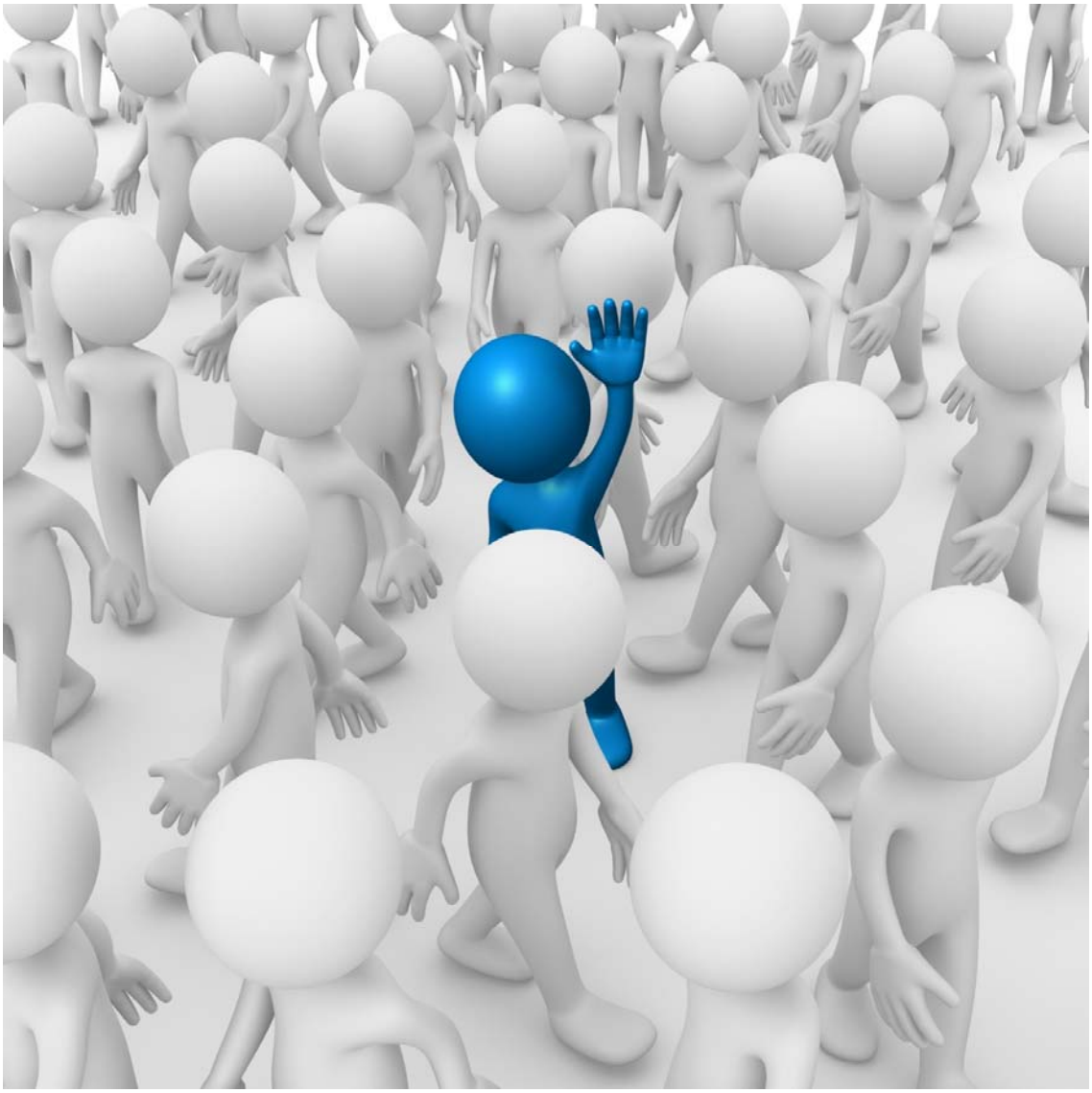
Ik merk op dat deze PIA – net als de andere genoemde PIA's - een momentopname van enige tijd geleden is. Inmiddels is en wordt daar opvolging aan gegeven. Zoals gebruikelijk bij de ontwikkeling van dergelijke systemen zal ik door de tijd PIA's blijven uitvoeren c.q. actualiseren om de ontwikkeling te kunnen sturen aan veranderende risico's. In die zin zijn het levende documenten.

PRIVACY IMPACT ASSESSMENT

DigiD Hoog

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

21 december 2017



Versie 1.0

INHOUDSOPGAVE

1. Inleiding

1.1. Aanleiding en achtergrond PIA

DigiD wordt al geruime tijd gebruikt als middel door gebruikers om in te loggen op online systemen van publieke dienstverleners. Dienstverleners zijn bijvoorbeeld de Belastingdienst, DUO, UWV en Nederlandse gemeenten. DigiD wordt ook gebruikt om bij andere organisaties in het BSN-domein in te loggen, waaronder bij zorgverzekeraars. In totaal zijn er circa 600 dienstverleners die gebruikers laten inloggen met DigiD.

DigiD is een product van Logius, de Dienst Digitale Overheid. Logius is onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK). Over 2016 telt Logius 13,4 miljoen actieve DigiD accounts op haar systemen. In totaal zijn hiermee in één jaar 258 miljoen authenticaties gerealiseerd[1]. Het gebruik van DigiD blijft naar verwachting stijgen.

Het ministerie van BZK heeft aangekondigd de bestaande DigiD te willen versterken. De bestaande DigiD biedt de gebruiker de mogelijkheid om met een gebruikersnaam en wachtwoord in te loggen. Het is optioneel om naast een gebruikersnaam en wachtwoord een sms-functie te activeren, gekoppeld aan een telefoonnummer. Ook kan de gebruiker ervoor kiezen gebruik te maken van de DigiD app waarbij een (nog te bepalen) uniek gegeven wordt ingevuld, een QR-code wordt gescand indien de website wordt bezocht via een apparaat, en een pincode moet worden ingevuld [2]. Hoewel inloggen met sms en het gebruik van de DigiD app een betere bescherming bieden dan alleen een gebruikersnaam en een wachtwoord, voldoen deze wijzen van inloggen voor bepaalde dienstverlening niet aan de eisen die worden gesteld aan authenticatiediensten en gebruikte middelen.

In Europa zijn inmiddels criteria gedefinieerd waar een betrouwbare authenticatiedienst aan dient te voldoen en zijn betrouwbaarheidsniveaus van authenticatiediensten beschreven. Deze criteria staan bekend als de ‘eIDAS normen’.[3] [4] De eIDAS-verordening betreft de elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de Europese interne markt.

Het ministerie van BZK wil aan gebruikers en dienstverleners meerdere betrouwbaarheidsniveaus aanbieden voor authenticatie, door het aanbieden van DigiD met de betrouwbaarheidsniveaus eIDAS Substantieel[5] en eIDAS Hoog[6]. In 2017 zal door Logius DigiD Substantieel worden gerealiseerd en in 2018 zal de eerste release van DigiD Hoog worden geïmplementeerd. Met de introductie van DigiD Hoog wordt het authenticatieproces aanzienlijk versterkt door bij elke inlogtransactie de identiteit van de gebruiker online te verifiëren aan de hand van een Wettelijk Identiteitsdocument (hierna: WID) en externe gegevensbronnen. Hiermee biedt DigiD Hoog een extra waarborg ten opzichte van de overige DigiD betrouwbaarheidsniveau’s.

[1] Logius Jaarverslag 2016
[2] Nog niet bekend is of exact deze manier gehanteerd zal worden om de apparaten met elkaar te laten verbinden en of de gebruikersnaam gebruikt zal worden.
[3] Uitvoeringsverordening (EU) 2015/1502, 8 september 2015, tot vaststelling van de minimale specificaties voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening Nr 910/2014.
[4] Verordening (EU) Nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten en elektronische transacties in de interne markt.
[5] De toets of DigiD Substantieel voldoet aan eIDAS niveau Substantieel moet nog plaatsvinden.
[6] De toets of DigiD Hoog voldoet aan eIDAS niveau Hoog moet nog plaatsvinden.

DigiD Hoog impliceert het verwerken van persoonsgegevens. Het gebruik van persoonsgegevens, waaronder door de overheid, vormt in veel gevallen een inperking van het grondrecht van bescherming van de persoonlijke levenssfeer[7]. Onzorgvuldigheid, onbetrouwbaarheid van gegevens, verlies van gegevens (datalekken) en het gebruik van gegevens voor een ander doel dan waarvoor ze zijn verkregen kunnen een negatieve impact hebben op iemands sociaal en maatschappelijk welbevinden. Informatietechnologie en grootschalige digitale gegevensverwerkingen introduceren veelal additionele (privacy) risico's die inherent zijn aan de inzet van deze technologie (de IT-werkelijkheid), maar niet direct zichtbaar zijn op het niveau van eindgebruik voor de gebruiker. Omdat DigiD op grote schaal persoonsgegevens verwerkt is het van groot belang dat tijdens de ontwerpfase van DigiD Hoog wordt geïnventariseerd welke privacybedreigende risico's er zijn.

1.2. Aanpak en opbouw van de PIA

Deze PIA heeft betrekking op de Project Start Architectuur van DigiD Hoog van 26 juni 2017, versie 0.99 (hierna: PSA of PSA DigiD Hoog). De PIA is afgeleid van het PIA-toetsingsmodel dat specifiek op de Rijksdienst is gericht (Rijksoverheid, 2013). Daarbij is ook gebruik gemaakt van de handreiking en vragenlijst van de NOREA voor de uitvoering van een PIA[8]. Het toetsingsmodel is bedoeld voor toepassing op alle beleidsgebieden en binnen alle rechtsdomeinen.

De aanpak van Mazars gaat uit van de beschreven universele privacyprincipes door de OECD/OESO[9] (OECD, 2013). Mazars heeft in de loop der jaren een overzicht van universele privacyrisico's samengesteld. Deze risico's zijn te relateren aan de privacyprincipes en zijn per verwerking geanalyseerd en beschouwd. Per privacyprincipe zijn in deze PIA de bevindingen, risico's en aanbevelingen opgenomen. Voor de privacyprincipes en privacyrisico's die wij hebben onderkend verwijzen wij naar *Bijlage III* en *Bijlage IV*.

Privacyprincipes en -risico's staan onderling tot elkaar in relatie. Zij kunnen elkaar beïnvloeden, versterken, verzwakken en vertonen strijdigheden. De privacyprincipes doelbinding en dataminimalisatie versterken elkaar bijvoorbeeld door alleen de gegevens te verzamelen die nodig zijn om het doel te kunnen bereiken. Ter indicatie van deze afhankelijkheden is in *Bijlage I* een tabel opgenomen met de privacyprincipes en gerelateerde risico's. Per privacyprincipe zijn onderwerpen besproken en geanalyseerd met betrekking tot het ontwerp DigiD Hoog. De bevindingen met betrekking tot deze onderwerpen zijn gedetailleerd (per vraag) opgenomen in *Bijlage I*. Op deze wijze zijn de privacyrisico's geïdentificeerd en aanbevelingen gedaan voor de implementatie van mitigerende maatregelen.

1.3. Leeswijzer

In hoofdstuk 2 zijn de uitkomsten van de PIA samengevat in de meeste significante bevindingen en risico's van het ontwerp DigiD Hoog. Tevens worden in deze samenvatting enkele aanbevelingen gedaan voor mitigerende maatregelen.
Een beschrijving van de doelstellingen en een toelichting op de scope van de PIA op DigiD Hoog is gegeven in hoofdstuk 3. Dit hoofdstuk omvat ook een opsomming van de verwerkte persoonsgegevens.

[7] Zie artikel 10, leden 2 en 3 Grondwet, artikel 8 EVRM, artikel 8 EU-Grondrechtenhandvest
[8] NOREA: Privacy Impact Assessment, versie 1.2, November 2015
[9] OECD / OESO: Organization for Economic Co-operation and Development / Organisatie voor Economische Samenwerking en Ontwikkeling.

Hoofdstuk 4 geeft een beschrijving van DigiD Hoog, beginnend met de aanleiding en doelstelling van het ontwerp van DigiD Hoog. Vervolgens zijn de belanghebbenden van DigiD Hoog benoemd en is het wettelijk kader beschreven. In dit hoofdstuk is ook een beschrijving gemaakt van het aanvraag-, productie- en uitgifteproces van een DH-middel, het gebruik van een DH-middel, de rollen binnen DigiD Hoog en de verschillen tussen de eerste implementatie en de beoogde eindsituatie van DigiD Hoog. Tot slot zijn de componenten van DigiD Hoog beschreven en is een tabel opgenomen met de bewaartermijnen van de logging.
In hoofdstuk 5 zijn de conclusies van de PIA opgenomen. Hier is eerst de positionering van DigiD Hoog in de ontwikkelcyclus van DigiD beschreven, vervolgens de noodzakelijkheid van de verwerking van persoonsgegevens binnen DigiD Hoog en ten slotte de bevindingen en aanbevelingen met betrekking tot DigiD Hoog per privacyprincipe.

Onder het kopje "*Bronnen"* is de literatuurlijst opgenomen met bronnen die gebruikt zijn voor het uitvoeren van deze PIA en de totstandkoming van dit rapport. Ook is hierin een overzicht gegeven van de functionarissen die zijn geïnterviewd ten behoeve van de PIA.

Bijlage I bevat een matrix met de relatie tussen de universele privacyprincipes en de algemene privacyrisico's. Ook is in *Bijlage I* de PIA-vragenlijst met een gedetailleerd overzicht van alle vragen met betrekking tot de PIA, opgesplitst naar privacyprincipe, met de bevindingen, risico's en aanbevelingen per vraag opgenomen.
Bijlage II geeft een visuele weergave van het proces van het gebruik van het DigiD Hoog waarin ook de scope van de PIA is weergegeven.
Bijlage III geeft een overzicht en toelichting van de universele privacyprincipes die zijn gehanteerd in de PIA-vragenlijst.
De algemene privacyrisico's, vastgesteld op basis van literatuurstudie, zijn opgenomen in *Bijlage IV*.
Bijlage V geeft de betekenis van en een toelichting op de gebruikte afkortingen en begrippen in het rapport.
Bijlage VI geeft de privacyrisico's weer afkomstig uit de PIA op DigiD Substantieel. *Bijlage VII* geeft het onderscheid tussen de privacybevorderende maatregelen voor de bestaande DigiD, de eerste fase van DigiD Hoog en de laatste fase van DigiD Hoog weer.

Alvorens in te gaan op de privacyprincipes zal eerst worden vastgesteld of de met DigiD Hoog gepaard gaande verwerkingen van persoonsgegevens noodzakelijk zijn voor de te bereiken doelstellingen. Hierbij speelt zowel de vraag naar de proportionaliteit (kan met minder persoonsgegevens het doel worden bereikt) als de subsidiariteit (kan het doel op een andere wijze worden bereikt met minder persoonsgegevens) van DigiD Hoog. Deze Privacy Impact Assessment (hierna: PIA) is gebaseerd op de PSA DigiD Hoog, waarin een beschrijving is gegeven van de eindsituatie van DigiD Hoog. In 2018 wordt de eerste release van DigiD Hoog geïmplementeerd waarna in een aantal fasen de komende 2 à 3 jaar de volledige implementatie van DigiD Hoog wordt gerealiseerd. Deze gefaseerde realisatie impliceert dat in de eerste fase nog niet alle aan DigiD Hoog gerelateerde privacybevorderende maatregelen zijn gerealiseerd. Aanvullende privacybeschermende maatregelen worden geïmplementeerd naarmate het project vordert. Deze PIA richt zich op het gehele fasering van DigiD Hoog. In deze rapportage is waar relevant dit onderscheid in verwachte begin- en eindsituatie aangegeven.

Op DigiD Substantieel is door Mazars reeds een PIA uitgevoerd[10]. Een deel van de bevindingen en aanbevelingen van de PIA DigiD Substantieel zijn ook van toepassing op de beginsituatie van DigiD Hoog. Risico's vanuit de PIA DigiD Substantieel, met name welke te maken hebben met het BSN-gebruik en de koppeling van accountgegevens en transactiegegevens, worden met de realisatie van DigiD Hoog gemitigeerd naarmate het project vordert. Het is de bedoeling van Logius om de cryptografische en andere aanvullende maatregelen die in de doorontwikkeling van DigiD Hoog worden gerealiseerd ook in te voeren voor DigiD Substantieel en de bestaande DigiD. Hierdoor worden bestaande privacyrisico's van DigiD Substantieel, zoals opgenomen in *Bijlage VI,* en de bestaande DigiD gereduceerd en ook beter beheersbaar. Ook deze impact van de realisatie van DigiD Hoog op andere voorzieningen van DigiD is in deze rapportage beschouwd.

[10] Gepubliceerd: https://www.rijksoverheid.nl/documenten/rapporten/2017/09/06/privacy-impact-assessment-pia-digid-substantieel

2. Managementsamenvatting

De hoofdconclusie van deze PIA is dat het ontwerp van DigiD Hoog aanzienlijk bijdraagt aan een betere bescherming van persoonsgegevens van betrokkenen ten opzichte van de al bestaande DigiD-voorzieningen. Het ontwerp van DigiD Hoog omvat een mix van organisatorische en technische privacybevorderende maatregelen. Deze privacybevorderende maatregelen zijn echter pas effectief als het ontwerp ook volledig wordt gerealiseerd én de concepten van DigiD Hoog ook worden toegepast op de systeemcomponenten van de bestaande DigiD en DigiD Substantieel. Bovendien kunnen belangrijke privacyrisico's die zijn onderkend voor bestaand DigiD en DigiD Substantieel met de concepten van DigiD Hoog aanzienlijk beter worden beheerst.

Kenmerken DigiD Hoog
Met de introductie van DigiD Hoog verwacht Logius een versterking van DigiD te realiseren naar het hoogste betrouwbaarheidsniveau op basis van de uitgangspunten zoals gedefinieerd in de Europese eIDAS-verordening. Of DigiD Hoog voldoet aan de Europese eisen van de eIDAS niveau 'Hoog' kan pas op een later moment (na notificatie) worden vastgesteld. Met DigiD Hoog wordt een variant toegevoegd aan de bestaande voorzieningen van DigiD.

Een maatregel om een hoger betrouwbaarheidsniveau te bereiken is dat de chip van het WID uitgerust wordt met een gepersonaliseerde applet en de gebruiker iedere keer bij het inloggen met DigiD Hoog het WID scant waarbij de identiteit van de gebruiker wordt geverifieerd. De verificatie bestaat uit het toetsen van identiteitsgegevens en de geldigheid van het WID bij een externe gezaghebbende bron. Het aanvraag-, productie- en uitgifteproces van het WID met de personaliseerde applet, ofwel het DH-middel, wordt uitgevoerd door de middelenuitgevers en de producenten, zoals de RvIG en de RDW. Deze technische en organisatorische ontvlechting impliceert een reductie van de verwerking van persoonsgegevens op het niveau van DigiD Hoog bij de authenticatiedienst van Logius ten opzichte van de bestaande DigiD-voorzieningen. Bij het aanvraag- en uitgifteproces van het DH-middel wordt minimaal één keer een 'face-to-face' controle uitgevoerd.

Een andere belangrijke verandering in het ontwerp van DigiD Hoog dat uiteindelijk het gehele DigiD-landschap raakt, is het gebruik van polymorfe identiteiten en pseudoniemen. Het effect van de invoering van deze technologie is dat de authenticatiedienst geen BSN meer ontvangt als gevolg van het inloggen van een gebruiker bij een dienstverlener, maar een polymorfe identiteit en pseudoniem. Deze maatregel heeft als positief effect dat, ook al zou er sprake zijn van een onrechtmatige toegang tot de inloghistorie, het vervaardigen van profielen op basis van BSN of pseudoniemen niet mogelijk is zonder in het bezit te zijn van de encryptiesleutel. Bescherming tegen onrechtmatig gebruik van de inloghistorie wordt hiermee op het niveau van DigiD Hoog aanzienlijk verbeterd.

De voorgaande beschrijving geeft de belangrijkste eigenschappen weer waarmee het ontwerp van DigiD Hoog zich onderscheidt van de bestaande DigiD-voorzieningen.

Gefaseerde realisatie en invoering van DigiD Hoog
DigiD Hoog wordt in fasen geïmplementeerd. Vanaf de eerste release van DigiD Hoog kunnen gebruikers bij dienstverleners inloggen met een hoog betrouwbaarheidsniveau. Bij deze eerste release van DigiD Hoog zijn nog niet alle beoogde privacybevorderende maatregelen geëffectueerd. De verdere realisatie van het DigiD Hoog concept binnen het gehele DigiD-landschap zal volgens planning 2 à 3 jaar in beslag nemen. Het toenemend gebruik van het DigiD Hoog authenticatiemiddel loopt parallel met de vernieuwing van het WID dat voorzien moet zijn van een nieuwe gepersonaliseerde chip. De vervangingscyclus van een WID omvat een periode van tien jaar.

De uitkomsten van de PIA op de PSA van DigiD Hoog geven aan dat met de volledige invoering van DigiD Hoog niet alleen een authenticatievoorziening van een hoger betrouwbaarheidsniveau wordt gerealiseerd, maar dat de daarbij gekozen architectuur en technologische uitrusting ook sterke privacybevorderende maatregelen bevatten. Vanwege de gefaseerde invoering zullen deze maatregelen in de eerste fase nog niet volledig zijn gerealiseerd. Privacyrisico's die voortvloeien uit de bestaande DigiD en privacyrisico's die gerelateerd zijn aan DigiD Substantieel blijven dan voorlopig nog bestaan. Deze risico's zijn opgenomen in *Bijlage VI* van dit rapport. Pas als het ontwerp van DigiD Hoog volledig is gerealiseerd, worden alle beoogde privacybevorderende maatregelen effectief.

Doordat DigiD Hoog ook gebruik maakt van componenten van de bestaande DigiD en DigiD Substantieel, is het van belang dat de gegevensverzamelingen die verwerkt worden met deze componenten van dezelfde privacybevorderende maatregelen worden voorzien als bij DigiD Hoog. Bestaand DigiD, DigiD Substantieel en DigiD Hoog maken bijvoorbeeld gebruik van dezelfde databases met inloghistorie. Indien bij DigiD Hoog wordt gerealiseerd dat het BSN is ontkoppeld van het IP-adres en dit bij bestaand DigiD of DigiD Substantieel niet wordt gerealiseerd, dan gaan de voordelen van DigiD Hoog op dit onderdeel min of meer teniet. Het is de bedoeling van Logius om de architectuur van DigiD Hoog ook te gaan hanteren voor de componenten in gebruik voor de bestaande DigiD en DigiD Substantieel. Het is bijzonder belangrijk dat dit voornemen ook daadwerkelijk wordt gerealiseerd.

Status privacybevorderende maatregelen en resterende privacyrisico's eerste fase
De belangrijkste privacybevorderende maatregelen van DigiD Hoog in de eerste fase zijn:

<u>Betrouwbare authenticatie</u>
- Een hoger betrouwbaarheidsniveau van authenticatie per inlogtransactie;
- Personaliseren van de chip bij nieuw uitgegeven WID met cryptografische bescherming;

Verregaande dataminimalisatie en functiescheidingen

- Organisatorische en technische ontvlechting van het aanvraag-, productie- en uitgifte proces uit de authenticatiedienst;
- Minimalisering van de gegevensuitwisseling tussen middelenuitgevers en de authenticatiedienst, onder andere door de inzet van de Status Controller. De Status Controller is een register dat wordt gevoed vanuit de RvIG en RDW en alleen de informatie aan de authenticatiedienst verstrekt die benodigd is voor de verificatie van het DH-middel;
- Realisatie van compartimentering binnen de authenticatiedienst met als gevolg een verdergaande scheiding in verantwoordelijkheden tussen verschillende rollen binnen de authenticatiedienst van Logius. Het datagebruik per rol wordt hiermee geminimaliseerd;

Beveiliging en privacy by design

- Beveiliging van de middleware (eID server en de eID client) volgens industriestandaarden;
- Hanteren van polymorfe identiteiten en pseudoniemen in de keten van eindgebruiker tot de centrale authenticatiedienst. Hiermee wordt bereikt dat in dit deel van de keten geen BSN meer verwerkt wordt. Het risico van ongewenste herleiding van transacties naar individuen en profiling is binnen dit deel van keten hiermee ook gemitigeerd;
- BSNk functioneert buiten de authenticatiedienst als beheerder van de encryptiesleutels (ketensleutels) benodigd voor het ontsleutelen van de verschillende polymorfe identiteiten en pseudoniemen die zijn gebruikt binnen de componenten van de authenticatiedienst.

Met de eerste release van DigiD Hoog blijven de privacyrisico's van de bestaande DigiD en DigiD Substantieel vooralsnog ongewijzigd.
In *tabel 1* zijn op hoofdlijnen de effecten van de privacybevorderende maatregelen van DigiD Hoog afgezet tegen bestaand DigiD en DigiD Substantieel, zowel in de eerste fase van realisatie van DigiD Hoog, als in de laatste fase van realisatie van DigiD Hoog.

Tabel 1: Overzicht effecten van de privacybevorderende maatregelen van DigiD Hoog afgezet tegen bestaand DigiD en DigiD Substantieel, zowel in de eerste fase van realisatie van DigiD Hoog, als in de laatste fase van realisatie van DigiD Hoog.

Onderwerp	Bestaand DigiD & DigiD Substan-tieel	DigiD Hoog eerste fase	DigiD Hoog laatste fase	Toelichting
Betrouwbaarheid authenticatie				Met DigiD Hoog wordt een hoger betrouwbaarheidsniveau van authenticatie bereikt.
Functiescheiding uitgifte en gebruik authenticatiemiddel				De middelenuitgever is verantwoordelijk voor de uitgifte van een DH-middel en het authenticatieproces is de verantwoordelijkheid van Logius. De authenticatiedienst van Logius krijgt alleen die gegevens die strikt noodzakelijk zijn.
Randomisering				Randomisering van de PI en het PP heeft als positief effect dat iedere keer een ander PI/PP wordt gegenereerd waardoor onrechtmatig gebruik van de data voor profiling bemoeilijkt wordt. De risico's van een onverhoopt datalek wordt geminimaliseerd.
Beheersing systemen				Door de afbouw en/of compartimentering van bestaande systemen en de implementatie van nieuwe compartimenten wordt de privacybescherming in de eindsituatie beter beheersbaar.
Fraudeonderzoek				Een separate voorziening voor fraudeonderzoek wordt ontwikkeld waardoor de toegang tot de specifiek daarvoor benodigde informatie beter beheersbaar wordt.
Dataminimalisatie				DigiD Hoog verzamelt en gebruikt minder gegevens door onder andere het gebruik van pseudoniemen en het scheiden van het uitgifteproces met het authenticatieproces.
Compartimentering				Compartimentering wordt gerealiseerd door technische scheiding van systemen. In de beginsituatie zal dit nog niet volledig gerealiseerd zijn.
BSN-gebruik vs. Pseudonimisering				Het BSN-gebruik neemt af door het gebruik van polymorfe identiteiten en pseudoniemen. De authenticatiedienst zet in de eerste fase het pseudoniem vroegtijdig om naar het BSN. In de eindsituatie wordt dit pas laat in het proces, door de dienstverlener, gedaan. Het BSN wordt dan niet meer binnen de authenticatiedienst van Logius verwerkt.
Cumulatie persoonsgegevens				Door compartimentering neemt de cumulatie van inloghistorie, waaruit is te herleiden welke persoon bij welke dienstverlener heeft ingelogd, af. Risico's van onrechtmatige profiling worden hiermee gemitigeerd.
Impact datalek				In de eindsituatie van DigiD Hoog is een encryptiesleutel van het BSNk benodigd om uit de inloghistorie te kunnen herleiden welke gebruiker bij welke dienstverlener heeft ingelogd. De impact van een datalek neemt af indien deze gegevens niet herleid kunnen worden zonder sleutel.
IP-adressen				Op dit moment is nog in onderzoek of het IP-adres in de eindsituatie van DigiD Hoog in de transactielog moet worden opgenomen. Indien het IP-adres wordt opgenomen is de verwachting dat dit in versleutelde vorm zal gebeuren.

Tabel 1: privacybevorderende maatregelen per fase
Legenda

	Privacybevorderende maatregel op laag niveau
	Privacybevorderende maatregel deels geïmplementeerd
	Privacybevorderende maatregel op hoog niveau

Aanbevelingen DigiD Hoog voor eerste fase

Het ontwerp van DigiD Hoog beschikt over sterke privacy bevorderende maatregelen. Uit deze PIA zijn de volgende aanbevelingen naar voren gekomen welke voor de eerste fase van implementatie relevant zijn. Het betreft vooral aanvullingen op de bestaande ontwerpbeschrijvingen. De aanbevelingen zijn geordend naar privacyprincipe.

Verantwoordingsprincipe en procedurele aspecten

- Bij de verdere detaillering van het ontwerp is een nadere uitwerking van de organisatorische inrichting van de verschillende functies en verantwoordelijkheden binnen Logius nog nodig. De huidige voorgestelde systeemopzet met verregaande compartimentering biedt hier uitstekende mogelijkheden toe.
- Stel een nadere uitwerking op van de wijze waarop informatie wordt verzameld en verstrekt binnen DigiD Hoog. Het is aan te bevelen procedurebeschrijvingen te maken voor de verschillende gegevensverwerkende activiteiten ten behoeve van de implementatie van DigiD Hoog.
- Ga na of de nieuw beoogde werking van de keten met RvIG en RDW via de Status Controller gevolgen heeft voor de te maken afspraken met deze partijen. Met bestaande (sub)verwerkers moeten overeenkomsten mogelijk aangepast worden en voor eventuele nieuwe verwerkers moeten verwerkersovereenkomsten afgesloten worden.

Transparantie principe

- De huidige doelstellingen van DigiD Hoog zijn op functioneel gebruiksniveau eenduidig en gelimiteerd beschreven. Het verdient aanbeveling om een meer integrale beschrijving te maken van het volledige DigiD- landschap en -infrastructuur, zodat de verwerkingen van DigiD Basis, Midden, Substantieel en Hoog in samenhang kunnen worden geëvalueerd op privacy- en beveiligingsrisico's. Daarbij is een eenduidige beschrijving van het doel van de verwerking van gegevens per component noodzakelijk vanuit privacyoptiek. Besteed in het bijzonder aandacht aan de verwerkingen van persoonsgegevens op technisch niveau, waaronder netwerkcomponenten. Beschrijvingen van deze verwerkingen kunnen worden meegenomen als aanvulling op het register van verwerkingen dat reeds aanwezig is.
- Stel gebruikers van DigiD Hoog bij het activeren en het gebruik van een DH-middel op de hoogte van de verwerking en het doel van de gegevensverwerking door een verwijzing op te nemen naar de privacyverklaring. De privacyverklaring dient uitgebreid te worden met de gegevens die additioneel verwerkt of uitgewisseld worden voor DigiD Hoog. Hierbij is het vooral relevant om aan te geven dat een gebruiker, voordat hij zijn WID scant, op de hoogte wordt gesteld wat er gebeurt bij het scannen van het WID. Aanbevolen wordt transparant te maken dat controle plaatsvindt met statusinformatie uit de BRP of het CRB, welke gegevens worden verwerkt (ook dat dit gepseudonimiseerd gebeurt) en wat het doel van deze verwerking is[11].
- Het verdient aanbeveling om voor DigiD Hoog gedetailleerd te beschrijven hoe invulling wordt gegeven aan het inzagerecht dat gebruikers hebben tot hun eigen gegevens en hoe de identiteit van de gebruiker in een pseudoniem-gebaseerde omgeving wordt vastgesteld.

[11] In de toekomst wordt controle uitgevoerd via CORI (Centraal Register Opslag Reis- en Identiteitskaarten)

Datakwaliteit

- Beschrijf maatregelen om de actualiteit van accountgegevens te waarborgen. Hierbij kan gedacht worden aan het periodiek versturen van een e-mail waarin de gebruiker wordt herinnerd aan het, indien van toepassing, actualiseren van de gegevens.
- Ontwerp interne controlemaatregelen gericht op datakwaliteit en de rapportages daarover. Ten behoeve van bewijslast achteraf en om verantwoording af te kunnen leggen over datakwaliteit en de integere werking van systemen zijn naast preventieve controles ook repressieve controles relevant. Te denken valt aan het gebruik van hashing op bepaalde gegevensverzamelingen of het gebruik van de bestaande database replica om de integriteit van (historische) data te kunnen valideren. De hier bedoelde interne controlemaatregelen zijn andere maatregelen dan de bestaande maatregelen om indicaties van misbruik te onderzoeken. De component die voor DigiD Hoog wordt ontworpen ten behoeve van fraudeonderzoek lijkt ook mogelijkheden te bieden voor de bedoelde interne controlemaatregelen gericht op datakwaliteit.

Beveiliging gegevens

- Geef bij het verdere ontwerp van DigiD Hoog specifiek aandacht aan de interne afscherming van IP-adressen. Ga na in welke (ook al bestaande) componenten IP-adressen worden opgeslagen en onderbouw wat de noodzakelijkheid is om deze gegevens te bewaren.
- Beschrijf de maatregelen die de werkelijke toegang tot systemen en gegevens waarborgen én controleerbaar maken zodat periodieke of wellicht permanente monitoring én rapportage over de beveiligingsaspecten plaatsvindt. Dit betreft zowel beveiliging van externe toegang als intern gebruik van systemen.

Aanbevelingen DigiD Hoog na eerste fase

Belangrijke privacy bevorderende maatregelen van DigiD Hoog worden pas gerealiseerd als de concepten van DigiD hoog ook over DigiD Basis, Midden en Substantieel worden uitgerold. Hierbij bestaan de volgende aanbevelingen.

Mitigeren van privacyrisico's gekoppeld aan DigiD Basis, Midden en Substantieel

- Het is belangrijk dat de doorontwikkeling naar de eindsituatie van DigiD Hoog zoals is voorgenomen wordt afgerond en de concepten van DigiD Hoog ook worden gerealiseerd voor de bestaande DigiD-voorzieningen. Dit impliceert ook conversie van de inloghistorie naar de gespeudonimiseerde gegevens zoals gebruikt binnen DigiD Hoog.
- Een high level ontwerp van de gefaseerde implementatie van DigiD Hoog is aanwezig. Aanbevolen wordt een meer concrete uitwerking op te stellen van hoe en met welke fasering de invoering van de concepten van DigiD Hoog worden gerealiseerd voor de bestaande DigiD-voorzieningen. Denk hierbij ook aan de conversie van transactiehistorie.
- Onderzoek bij de verdere realisatie van de eindsituatie van DigiD Hoog wat de consequenties zijn van het gebruik van de verschillende loggings gegeven de inzet van een diversiteit aan componenten. Analyseer de risico's en tref zo nodig additionele privacybeschermende maatregelen of minimaliseer de vastlegging van van loggegevens. In elk geval is meer duidelijkheid wenselijk over de wijze waarop de loggings in samenhang van de verschillende DigiD-voorzieningen en componenten functioneren en welke privacyrisico's dit met zich meebrengt.

Reductie van risico's als gevolg van een grotere historische dataset van inloggegevens

- Logius is voornemens om de concepten van DigiD Hoog ook toe te gaan passen op DigiD Basis, Midden en Substantieel. Zolang dit niet gerealiseerd is, verdient het aanbeveling om na te gaan of de getroffen beveiligingsmaatregelen in de tussenliggende periode van DigiD Basis, Midden en Substantieel voldoende recht doen aan de gevoeligheid van de omvangrijke verzameling van inlogacties door gebruikers. Doordat DigiD Hoog gebruik maakt van dezelfde componenten als van DigiD Basis, Midden en Substantieel ondermijnen de daaraan gekoppelde gegevensverzamelingen de effectiviteit van een deel van de maatregelen van DigiD Hoog. Als alternatieve benadering kan worden nagegaan of de DigiD Hoog concepten versneld, of wellicht in delen versneld, kunnen worden uitgerold over de bestaande DigiD-voorzieningen.
- De wettelijke bewaartermijnen zijn in het Besluit GDI vastgesteld op vijf jaar voor de inloghistorie van gebruikers. Bij het vaststellen van deze termijn is rekeninggehouden met het belang van betrokkenen om inzage te kunnen hebben in historische gegevens en het belang om de datakwaliteit te kunnen controleren. De cumulatie van inloghistorie neemt door de verruiming van de bewaartermijn toe. In de inloghistorie is vastgelegd bij welke dienst de gebruiker heeft ingelogd waardoor een privacygevoelige dataset ontstaat. Het verdient aanbeveling om na te gaan of de getroffen beveiligingsmaatregelen gedurende de overgangsperiode, totdat DigiD Hoog volledig is uitgerold over de andere DigiD voorzieningen, in lijn zijn met de risico's die deze bewaartermijnen met zich meebrengen. Voor het ontwerp van DigiD Hoog geldt dat deze risico's in belangrijke mate worden gemitigeerd als het concept van DigiD Hoog volledig is geïmplementeerd, ook voor de bestaande DigiD-voorzieningen. Additionele maatregelen gedurende de overgangsperiode kunnen zijn: encryptie of hashing van gevoelige data zoals IP-adressen en monitoring en periodieke rapportage over de toegang tot gegevens. Onderzoek hierbij ook de risico's van netwerkcomponenten over de hele technologische keten die eveneens metadata genereren die mogelijk informatie kunnen onthullen over gebruikers.
- Tijdens ons onderzoek bleek dat er nog niet eerder een integrale PIA was uitgevoerd op de bestaande DigiD. In de ontwikkelcycli van de bestaande DigiD zijn per fase de eisen van de Wbp meegenomen. Een hanteerbaar integraal overzicht van alle verwerkingen van persoonsgegevens op zowel functioneel als technisch niveau, inclusief de verwerkingen van persoonsgegevens gekoppeld aan technische systemen en een beschrijving van de bijbehorende doelstellingen, is nog niet volledig voorhanden. Het verdient aanbeveling om bij de doorontwikkeling van DigiD een dergelijk overzicht op te stellen en de privacyrisico's hiervan integraal te analyseren.

3. Doelstelling en scope van de PIA

3.1. Doelstellingen van de PIA

Een PIA is een hulpmiddel bij ontwikkeling van beleid en de daarmee gepaard gaande wetgeving of bij de bouw van ICT-systemen en aanleg van databestanden. Hiermee kunnen privacyrisico's op een gestructureerde en heldere wijze in kaart worden gebracht. Een PIA is gedurende een ontwikkelproces iteratief en dynamisch van karakter. Het blijft per fase maatwerk. Belangrijk is te benoemen dat deze PIA uitgaat van de situatie van DigiD Hoog zoals deze op het moment van uitvoering van de PIA, namelijk in het derde kwartaal van 2017, is geschetst en bekend is bij Logius. Wettelijke aanpassingen, zoals wijzigingen in de Wet GDI, of wijzigingen in het ontwerp of de implementatie van DigiD Hoog kunnen invloed hebben op de privacyrisico's. Door een PIA gedurende het ontwerpproces regelmatig uit te voeren, kunnen (nieuwe) risico's vroegtijdig worden ontdekt en kan de bewustwording van risico's worden vergroot. Het doel van deze PIA is het in kaart brengen van de relevante privacyrisico's en de maatregelen die zijn genomen om de risico's te mitigeren. Zo nodig worden richtinggevende aanbevelingen gedaan om privacyrisico's te elimineren of te mitigeren. Een PIA is met deze doelstellingen geen formele audit.

De PIA kan worden gebruikt om transparantie en draagvlak voor het project DigiD Hoog bij de diverse stakeholders te creëren, zoals bij verantwoordelijke overheden, gebruikers, betrokken derden en belangenorganisaties. De PIA-rapportage is in die zin een communicatiemiddel. De uitkomsten van de PIA kunnen hergebruikt worden in geval van ontwerp- en systeemaanpassingen en doorontwikkeling. Hierbij dient uiteraard kritisch beoordeeld te worden wat de impact is van deze wijzigingen op de verschillende onderwerpen die zijn behandeld in deze PIA.

3.2. Scope van de PIA

DigiD Hoog wordt in fasen geïmplementeerd. Vanaf de eerste release van DigiD Hoog kunnen gebruikers inloggen met een hoog betrouwbaarheidsniveau bij dienstverleners die DigiD Hoog faciliteren. Bij deze eerste release van DigiD Hoog zijn nog niet alle beoogde privacybevorderende maatregelen geëffectueerd. Het DigiD Hoog concept wordt uiteindelijk binnen het gehele DigiD-landschap toegepast, waarbij de bestaande DigiD voorzieningen van dezelfde privacybevorderende maatregelen worden voorzien.

Deze PIA richt zich in beginsel op de laatste fase van DigiD Hoog. Omdat de privacybevorderende maatregelen in de verwachte eerste fase van DigiD Hoog nog beperkt zijn geëffectueerd, wordt ook aandacht besteed aan de privacyrisico's die op dat moment van toepassing zijn.

De scope van de PIA op DigiD Hoog bestaat uit het gebruik van een DigiD Hoog-middel (hierna te noemen: DH-middel) bij het inloggen bij dienstverleners in het BSN-domein, voor zover dit de onderdelen van de architectuur betreffen die binnen het verantwoordelijkheidsgebied van Logius vallen.

De verantwoordelijkheid van het aanvraag-, productie- en uitgifteproces van het DH-middel is belegd bij de middelenuitgever (hierna te noemen: MU) en vormt geen onderdeel van deze PIA. De MU beheert de gehele logistieke keten van het WID en voert een sluitende administratie over de betreffende documenten naast de daadwerkelijke productie en personalisatie van het document. Richting DigiD fungeert de MU als enig aanspreekpunt voor de documentketen in kwestie. De MU van de NIK is de Rijksdienst voor Identiteitsgegevens

(hierna te noemen: RvIG) en de MU van het rijbewijs is de Dienst Wegverkeer (hierna te noemen: RDW). Hiermee wijkt DigiD Hoog af van de eerdere voorzieningen van DigiD, waarbij het uitgifteproces van het authenticatiemiddel binnen het verantwoordelijkheidsdomein van Logius valt.

Voor een visuele weergave van het proces van het gebruik van DigiD Hoog verwijzen wij naar *Bijlage II*. In het processchema is te zien welke componenten in scope zijn van de PIA en welke geen deel uitmaken van de scope van deze PIA. Indien gebleken is dat de invoering van DigiD Hoog privacyeffecten heeft gerelateerd aan bestaande DigiD componenten, die strikt genomen buiten de scope van deze PIA vallen, maar wel reële privacyrisco's impliceren voor DigiD Hoog, is naar vermogen daar wel aandacht aan besteed. Voor een beter begrip van de werking van de gehele authenticatieketen en het proces daarvan is in paragraaf 4.5 een beschrijving opgenomen van het gehele proces met alle onderdelen van de keten.

3.3. Overzicht verwerking persoonsgegevens DigiD Hoog

Eén van de doelen van DigiD Hoog is dat de privacy van de gebruiker verbeterd wordt ten opzichte van de huidige DigiD door het inzetten van Privacy Enhancing Technologies. Hiermee wordt onder meer bereikt dat het BSN-gebruik bij het inlog- en activatieproces wordt geminimaliseerd. In de laatste fase van DigiD Hoog wordt het BSN in de gehele keten van de DH Authenticatiedienst vervangen door een pseudoniem. Deze werkwijze heeft positieve effecten op de privacybescherming en maakt ook de beheersing van privacyrisico's beter.

DigiD Hoog bouwt voort op het ontwerp en de bestaande componenten van DigiD. DigiD Hoog introduceert binnen het DigiD systeemdomein, waar Logius verantwoordelijk voor is, additionele persoonsgegevens ten opzichte van DigiD Substantieel, waaronder gerandomiseerde polymorfe identiteiten (hierna: PI) en polymorfe pseudoniemen (hierna: PP) en enkele noodzakelijke gegevens benodigd voor statusbeheer en beheer van operationele en technische processen rond het DH-middel.

Hieronder is een opsomming weergegeven van de gegevens die in de eerste fase verwerkt worden bij het gebruik van DigiD Hoog. De gegevens die in de laatste fase van DigiD Hoog niet meer verwerkt worden zijn in het groen aangegeven. De gegevens die additioneel worden verwerkt ten opzichte van de huidige DigiD zijn in het blauw aangegeven.

- Over bezoekers van DigiD:
  - Gegevens over herkomst en kenmerken van het netwerkverkeer;
  - Kenmerken van de gebruikte software en hardware van de bezoeker.
- Over bezoekers van www.digid.nl die een aanvraagprocedure hebben gestart maar niet voltooid, in aanvulling op bovenstaande gegevens:
  - BSN;
  - Datum en tijd aanvraag en reden niet voltooid.
- Over gebruikers van DigiD, in het bijzonder DigiD Hoog:
  - Middelengegevens[12]:
    - Documentnummer;
    - Gerandomiseerde polymorfe pseudoniem;
    - Gerandomiseerde polymorfe identiteit;
    - PIN;
    - PUK;
    - CAN;

[12] Het DH middel zal in de eerste en tweede fase worden gerealiseerd op rijbewijzen respectievelijk Nederlandse Identiteitskaarten (NIK). Doorontwikkeling naar overige wettelijke identiteitsdocumenten, zoals het paspoort, vreemdelingenpaspoort en geprivilegieerdenpas wordt voorzien.

        - Status zoals verstrekt door de MU (uitgereikt, geactiveerd, geblokkeerd of ingetrokken).
    - Accountgegevens:
        - Naam;
        - (Mobiel) telefoonnummer;
        - E-mailadres;
        - Adres;
        - Postcode;
        - Gebruikersnaam;
        - BSN;
        - Status persoonslijst (bijv. overleden);
        - Nationaliteit (alleen nodig voor het balieproces);
        - Gegevens om ingezetenschap of niet-ingezetenschap in de basisregistratie personen vast te kunnen stellen.
    - Gebruiksgegevens:
        - BSN;
        - IP-adres[13];
        - Kenmerken van de gebruikte software en hardware van het apparaat waarmee de gebruiker van DigiD is ingelogd;
        - Handelingen van de gebruiker binnen de DigiD-omgeving;
        - Door de gebruiker gekozen authenticatieniveau;
        - Website van de instelling waar de gebruiker van DigiD een DigiD aanvraagt of met DigiD inlogt;
        - Sessiegegevens, waaronder cookies, tijd van authenticatie, sessie-ID, gekozen document soort, Near Field Communication reader (hierna: NFC-reader) soort, sessie-, verificatie-, en identiteitsbevestigingen (OK/NOK).
    - Gegevens die relevant zijn voor de adequate werking van DigiD, waaronder in ieder geval de kenmerken van de door de gebruiker van DigiD gebruikte software en hardware;
    - Gegevens die noodzakelijk zijn voor de ondersteuning van de gebruiker van DigiD.

Met bovengenoemde opsomming is tevens het belang van de uitvoering van een PIA op DigiD Hoog aangegeven.

[13] Op het moment van het schrijven van deze PIA is nog in onderzoek of het IP-adres in de eindsituatie van DigiD Hoog in de transactielog moet worden opgenomen of dat dit gegeven alleen in de fraude logger wordt verwerkt. Indien het IP-adres wordt opgenomen in de transactielog is de verwachting dat dit in versleutelde vorm zal gebeuren. Zolang aan deze randvoorwaarde is voldaan heeft dat geen invloed op de conclusies van deze PIA.

4. Beschrijving DigiD Hoog

De beschrijvingen in dit hoofdstuk zijn voor een belangrijk deel afkomstig uit de documentatie van de Project Start Architectuur DigiD Hoog. Deze beschrijving vormt de basis van deze PIA. Op deze beschrijving zijn aanvullingen en wijzigen doorgevoerd vanwege veranderingen die zijn doorgevoerd in het ontwerp en vanwege aanvullend verkregen informatie op basis van gevoerde gesprekken met keyfunctionarissen.

4.1. Aanleiding DigiD Hoog

Het kabinet heeft de norm gezet dat gebruikers vanaf 2017, zaken die zij met de overheid doen, digitaal moeten kunnen afhandelen. Daarvoor is een toekomstbestendige identiteitsinfrastructuur nodig die zo veilig mogelijk is en die bestand is tegen de enorme groei aan digitale authenticaties die verwacht wordt. Het gebruik van DigiD stijgt en de behoefte aan een verhoogde betrouwbaarheid neemt toe. Het inloggen met gebruikersnaam en wachtwoord (en optioneel sms) voldoet niet meer aan het gewenste niveau van authenticatie. In de huidige situatie biedt DigiD twee betrouwbaarheidsniveaus om in te loggen bij dienstverleners in het BSN-domein:

- DigiD Basis: inloggen met gebruikersnaam en wachtwoord;
- DigiD Midden:
  - inloggen met gebruikersnaam, wachtwoord en sms;
  - inloggen met gebruikersnaam en de DigiD app (beveiligd met een pincode).

Van DigiD Substantieel is een definitieve Project Start Architectuur beschikbaar en implementatie hiervan vindt eind 2017 plaats. DigiD Substantieel verhoogt het betrouwbaarheidsniveau van DigiD door eenmalig de identiteit van de gebruiker te verifiëren middels een WID. Deze verificatie wordt vervolgens periodiek herhaald. DigiD Substantieel kan worden gezien als de eerste stap in de doorontwikkeling van DigiD.

DigiD Hoog voorziet in de vraag van afnemers naar een authenticatiemiddel met een hoger betrouwbaarheidsniveau waardoor meer online diensten online aangeboden kunnen worden. Met DigiD Hoog wordt gebruikers de mogelijkheid geboden om in te loggen met een hoger betrouwbaarheidsniveau en wordt tevens aan de eIDAS-norm voldaan. De eisen gesteld om het authenticatieniveau van ‘Hoog’ te bereiken zijn vastgelegd in de Europese Uitvoeringsverordening EU2015/1502 van 8 september 2015 (Commissie, 2015). Hierin is onder meer aangegeven dat het aanvraag- en uitgifteproces van een middel met betrouwbaarheidsniveau ‘Hoog’ tenminste één fysiek contactmoment moet kennen waarbij één of meer fysieke kenmerken van de persoon geverifieerd moeten worden door vergelijking met een gezaghebbende bron. Voor het authenticatiemechanisme geldt de eis dat dit voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een hoog aanvalspotentieel.

Het ministerie van BZK streeft ernaar betrouwbaarheidsniveau ‘Hoog’ te behalen waarbij is gekozen voor een aanpak waarbij het WID elektronisch wordt gepersonaliseerd en dit DH-middel bij het inloggen wordt gebruikt om de identiteit van de gebruiker te verifiëren. Deze gegevens worden opgehaald door het scannen van de chip op het WID met een NFC-reader. Het aanvraag-, productie- en uitgifteproces van dit DH-middel maakt gebruik van het bestaande proces van de aanvraag, productie en uitgifte van een WID. In dit proces is tenminste één fysiek contactmoment met de gebruiker aanwezig ter verificatie van de identiteit.

4.2. Doelstellingen DigiD Hoog

De doelstelling van DigiD Hoog is het versterken van het betrouwbaarheidsniveau van DigiD naar eIDAS 'Hoog'. De volgende (sub)doelstellingen worden daarbij onderkend:

- Het bieden van de mogelijkheid aan gebruikers en dienstverleners om voor een hoger betrouwbaarheidsniveau, dat voldoet aan eIDAS Hoog, te kiezen voor diensten in het BSN-domein[14];
- Het creëren van de mogelijkheid om online diensten in het BSN-domein aan te bieden en af te nemen die vanwege de gevoeligheid met het huidige betrouwbaarheidsniveau niet online kunnen worden aangeboden;
- Borgen van de toekomstvastheid van DigiD;
- Verbetering van de privacybescherming voor de gebruiker door het inzetten van Privacy Enhancing Technologies. De gebruiker kan inloggen bij een dienstverlener met DigiD Hoog waarbij dit feit bij de DigiD authenticatiedienst of bij andere tussenliggende partijen in de keten, niet zonder meer herleid kan worden naar de gebruiker;
- Het realiseren van een hoogwaardig proces tegen relatief lage kosten voor de gebruiker en voor de maatschappij, door het meeliften op het al bekende aanvraag- en uitgifteproces van WID.

4.3. Stakeholders DigiD Hoog

Bij dit project zijn stakeholders betrokken met ieder hun eigen belangen en invloed. In dit overzicht beperken wij ons tot de volgende groepen stakeholders:

- Afnemers (dienstverleners);
- Leveranciers;
- Gebruikers;
- Middelenuitgevers en registerhouders (zoals RvIG en RDW);
- Uitgifteloketten (zoals gemeenten);
- Derden (zoals opsporingsdiensten, in verband met een wettelijke verplichting om gegevens te verstrekken).

4.4. Wettelijk kader DigiD Hoog

In *tabel 2* is de relevante wet- en regelgeving opgenomen en de impact hiervan op DigiD Hoog. De tabel geeft geen volledig overzicht van de wet- en regelgeving die van toepassing is voor Logius.

Wets- of beleidsdocument	Impact
Algemene Verordening Gegevensbescherming (AVG)	Europese verordening die vanaf 25 mei 2018 van toepassing zal zijn en waarin eisen worden gesteld aan (persoons)gegevensbescherming. De AVG vervangt de Wbp.
Archiefwet	Wet die het beheer en de toegang van overheidsarchieven regelt.

[14] Het BSN-domein is het domein waarbinnen het gebruik van het BSN wettelijk is voorgeschreven. Hierbij gaat het om publieke taken, uitgevoerd door overheidsinstanties, zorgverzekeraars en zorgaanbieders alsmede pensioenfondsen en onderwijsinstellingen.

Wets- of beleidsdocument	Impact
Besluit verwerking persoonsgegevens GDI	Regels betreffende de verwerking van persoonsgegevens en de bewaartermijnen ervan in de voorziening voor de generieke digitale infrastructuur.
eIDAS-verordening	De eIDAS-verordening van de EU gaat over elektronische identificatie en het opbouwen van een Europees vertrouwenstelsel waarbinnen elkaars identificatiemiddelen worden geaccepteerd om toegang te krijgen tot (grensoverschrijdende) overheidsdienstverlening.
Regeling voorzieningen GDI	Regels met betrekking tot de werking, beveiliging en betrouwbaarheid van de voorzieningen voor elektronisch berichtenverkeer en informatieverschaffing alsmede van voorzieningen voor elektronische authenticatie.
Uitvoeringsverordening tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronisch identificatiemiddelen	Specificaties voor betrouwbaarheidsniveau laag, substantieel, hoog (nr 2015/1502, 8 september 2015).
Wet algemene bepalingen burgerservicenummer (Wabb)	De Wabb stelt eisen aan het gebruik van het burgerservicenummer.
Wet bescherming persoonsgegevens (Wbp)	Wet waarin de bescherming van de privacy van burgers is vastgelegd en waarin is bepaald hoe met persoonsgegevens om moet worden gegaan.
Wet elektronisch berichtenverkeer Belastingdienst (EBV)	De Wet elektronisch berichtenverkeer Belastingdienst (EBV) schept het wettelijk kader voor het verplichten van elektronisch berichtenverkeer in het contact met de Belastingdienst. In artikel X van deze wet is bovendien een grondslag opgenomen voor voorzieningen voor elektronisch berichtenverkeer, elektronische authenticatie en elektronische registratie van machtigingen en het raadplegen ervan, alsmede voor de in dat verband noodzakelijke verwerking van persoonsgegevens.
Meldplicht datalekken	De meldplicht datalekken voegt aan de Wet bescherming persoonsgegevens (Wbp) een meldplicht voor inbreuken op beveiligingsmaatregelen voor persoonsgegevens toe.

Tabel 2: Relevante wet- en regelgeving

4.5. Procesbeschrijving DigiD Hoog

Een gebruiker kan ervoor kiezen zijn account uit te breiden met een middel op betrouwbaarheidsniveau ‘Hoog’. Hiervoor dient de gebruiker reeds in het bezit te zijn van een DH-middel en een NFC-reader. Het DigiD-account kan ook bij het activeren van het DH-middel worden aangemaakt. Het DH-middel is een publiek elektronisch identificatiemiddel (eID) dat op de chip van een WID wordt geplaatst. Dit is een tweede applet, naast de bestaande applet, die op de chip wordt geplaatst. Omdat het DH-middel op een WID wordt geplaatst kan de

aanvraag, productie en uitgifte van dit middel meeliften op de bestaande aanvraag-, productie- en uitgifteprocessen. Logius is niet betrokken in de uitvoering van het aanvraag-, productie- en uitgifteproces van een DH-middel. Voor de volledigheid en voor begripsvorming is dit proces in de volgende subparagraaf wel beschreven. Het DH-middel moet na uitgifte eenmalig geactiveerd worden en wordt iedere keer bij het authenticeren met DigiD Hoog gebruikt om de identiteit van de gebruiker te verifiëren en in te kunnen loggen bij de dienstverlener.

4.5.1. Aanvraag, productie en uitgifte van het DigiD Hoog middel

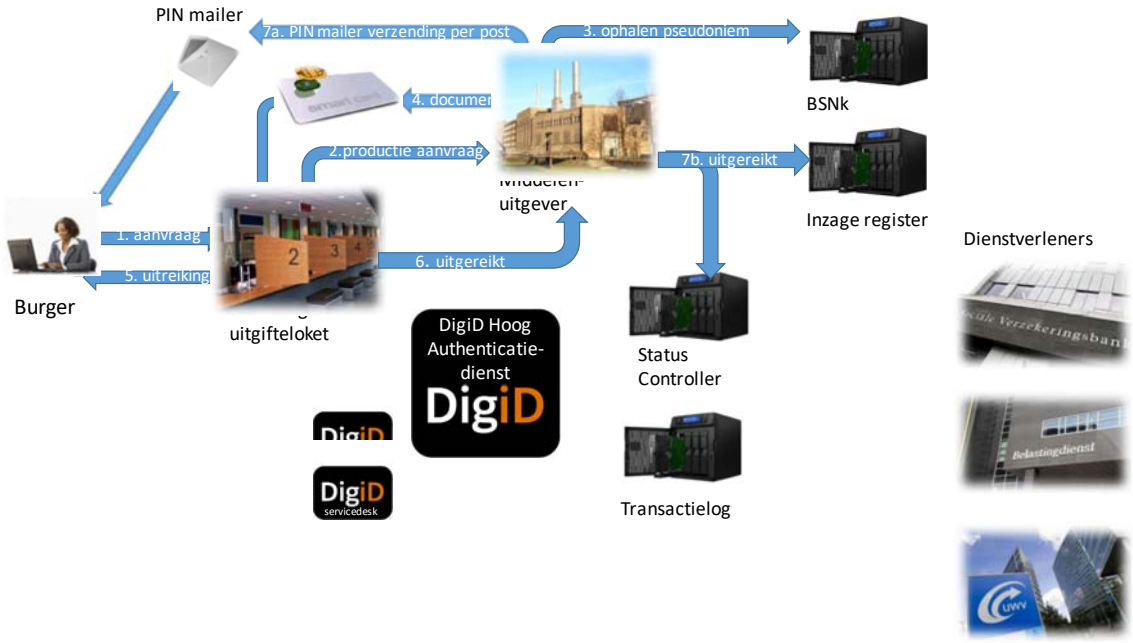
Een gebruiker doet bij een aanvraagloket (meestal een gemeente) een aanvraag voor (vernieuwing van) een WID. Bij dit loket wordt onder meer de identiteit van de gebruiker geverifieerd aan de hand van een WID en de persoons- en adresgegevens in de BRP. Bij juiste authenticatie wordt een aanvraag gedaan bij de MU voor het produceren van het middel. In het geval van een NIK is de MU de RvIG en in het geval van een rijbewijs is dit de RDW. Vanaf de implementatie van DigiD Hoog produceert de RDW een rijbewijs dat is voorzien van een DH-middel. De NIK wordt door de RvIG in een latere release met het DH-middel geproduceerd.

De MU vraagt voor de productie van het DH-middel met het BSN de PI en de PP op bij het BSN-koppelregister (BSNk). Het BSNk is een stelselvoorziening die onder andere de verantwoordelijkheid heeft voor het uitgeven (genereren) van een PI en PP op basis van het BSN. De MU houdt de status van de DH-middelen bij en bewaakt de statusovergangen. De MU werkt deze gegevens bij in de DigiD Hoog Status Controller (DH SC) en het centrale Inzageregister (hierna te noemen: IR). Het IR is gebaseerd op de Uniforme Set van Eisen (hierna te noemen: USvE[15]) en betreft een centraal register waarin de statussen van alle authenticatiemiddelen worden geregistreerd en gebruikers de status van hun eigen authenticatiemiddel(en) in kunnen zien. De MU produceert een NIK of rijbewijs en plaatst de PI, het PP, de Polymorph Card Application (hierna: PCA), de initiële PIN, de CAN (Card Access Number) en de PUK (Personal Unblocking Key) op de NFC chip. Daarmee is het DH-middel geproduceerd. Het DH-middel wordt vervolgens naar het uitgifteloket verstuurd.

De gebruiker wordt bij het ophalen van het document geïnformeerd over het activeren en het gebruik van het DH-middel. Op het moment dat het uitgifteloket (meestal een gemeente) de uitreiking van het document vastlegt, wordt een bericht verstuurd naar de MU. Dat is het signaal voor de MU dat de brief met de unieke en tijdelijke PIN van de gebruiker (PIN-mailer) kan worden verstuurd naar het BRP-adres van de gebruiker. De MU geeft de status ‘uitgereikt’ door aan de DH SC en het IR.

Een visuele weergave van het aanvraag- productie- en uitgifteproces van een DH-middel is weergegeven in *figuur 1*. Zoals is deze afbeelding is weergegeven is Logius als authenticatiedienst niet betrokken in de uitvoering van het aanvraag-, productie- en uitgifteproces van het DH-middel.

[15] Tijdens het schrijven van deze PIA is niet bekend of de term USvE gehanteerd blijft.



Figuur 1: aanvraag-, productie-, en uitgifteproces

4.5.2. Activeren DH middel

Bij de uitreiking van het document is het DH-middel nog niet geactiveerd en kan het dus niet gebruikt worden. De gebruiker kan met de ontvangen PIN-mailer van de MU, waarin de initiële PIN is opgenomen, het DH-middel activeren. De gebruiker activeert het DH-middel via de website van DigiD waar na invoering van de initële PIN controle plaatsvindt met de juiste status van het middel in de DH SC. De gebruiker moet vervolgens een eigen PIN instellen die gebruikt wordt om in te loggen met het DH-middel.

Omdat het DH middel wordt beheerd via het zelfservice portaal Mijn DigiD dient de gebruiker een DigiD account te hebben. Als de gebruiker al over een DigiD account beschikt, wordt het DH-middel aan het account toegevoegd. Indien de gebruiker nog niet over een account beschikt, wordt dit als onderdeel van het initiële activeren aangemaakt. In dat geval zullen aanvullende gegevens worden gevraagd ten behoeve van het aanmaken van het account en het bijbehorende DigiD Basis middel zoals gebruikersnaam en wachtwoord. Aan dit DigiD Basis account kan een DH-middel gekoppeld worden.

4.5.3. Gebruik van DigiD Hoog

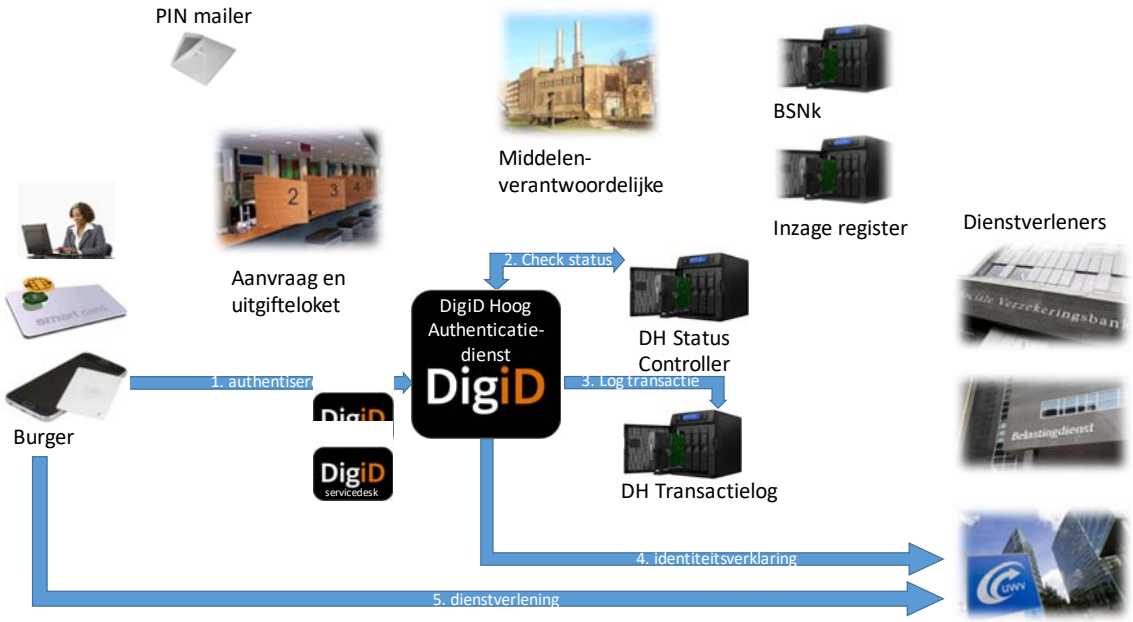
Als de gebruiker op de website van een dienstverlener aangeeft gebruik te willen maken van DigiD kan hij in het openingsscherm van DigiD kiezen om zich te authenticeren met een DH-middel. Vervolgens wordt hij doorgestuurd naar de DigiD Hoog Authenticatiedienst (DH AD) van Logius. De DH AD is verantwoordelijk voor het authenticeren van natuurlijke personen op basis van het DH-middel. De gebruiker scant met een NFC-reader de chip op het WID. Voor het uitlezen van de chip op het WID wordt gebruik gemaakt van middleware. Een beveiligd kanaal wordt opgezet tussen de chip op het WID en de eID server door het gebruik van het Password Authenticated Connection Establishment (hierna: PACE) protocol. Tweezijdige authenticatie vindt plaats tussen applet en eID server via Extended Access Control (EAC), bestaande uit Terminal Authentication (TA), Chip Authentication (CA) en Passive Authentication (PA). EAC is een beveiligingskenmerk van elektronische identiteitskaarten die de toegang tot gevoelige data op de NFC chip beschermt en beperkt. Met TA controleert de

chip of de eID server bevoegd is gegevens uit te lezen, met CA controleert de eID server of de chip authentiek is en met PA wordt aangetoond dat de informatie op de chip authentiek en ongewijzigd is. De gebruiker voert zijn PIN in en indien deze en de uitkomsten van de controles juist zijn bevonden, worden de PI en het PP van het DH-middel afgegeven aan de DH AD. Door de PCA op de chip worden de PI en het PP gerandomiseerd waardoor elke authenticatie een unieke PI en PP oplevert. De DH AD controleert bij de DH SC of het DH-middel nog actief is en niet is geblokkeerd of ingetrokken en schrijft de transactie weg naar de Transactielog (hierna te noemen: TL). Als de controles juist zijn, geeft de DH AD een identiteitsverklaring aan de dienstverlener af, waarmee aan de hand van de versleutelde identiteit (hierna te noemen: VI) het BSN of aan de hand van het versleutelde pseudoniemen (hierna te noemen: VP) het persistente pseudoniem door de dienstverlener kan worden bepaald. Tenslotte wordt de gebruiker teruggeleid naar de dienstverlener en kan de gevraagde dienst worden afgenomen.

Van PI en PP naar VI en VP
De DH AD versleutelt de PI en het PP met de transformatiefunctie in de Hardware Security Module (hierna te noemen: HSM) specifiek voor de ontvangende componenten of partijen door een combinatie van de PI/PP met het overheidsidentificatienummer (hierna te noemen: OIN) van de ontvangende partij. Een component is een technische en organisatorische voorziening binnen de DH AD. Met een ontvangende partij wordt een organisatie bedoeld die geen onderdeel is van de DH AD, bijvoorbeeld het BSNk en een dienstverlener. Aan de hand van het PP worden meerdere VP genereerd, specifiek voor de ontvangende component of partij waarvoor deze bedoeld is. Een VP wordt gegenereerd voor de DH SC, de TL, het fraudeteam van Logius en het IR. Indien de dienstverlener geen BSN mag of wil gebruiken wordt de PP getransformeerd naar een VP, specifiek voor de dienstverlener waar de gebruiker inlogt, zodat alleen deze dienstverlener het persistente pseudoniem kan ontsleutelen. Indien de dienstverlener wel een BSN mag en wil gebruiken wordt de PI getransformeerd naar een VI, specifiek voor de dienstverlener waar de gebruiker inlogt, zodat alleen deze dienstverlener aan de hand van de VI het BSN kan ontsleutelen. Ook wordt een VI gegenereerd voor het fraudeteam van Logius zodat, indien een vermoeden van fraude is gesignaleerd, het BSN ontsleuteld kan worden voor fraudeonderzoek. Dit BSN is benodigd voor overleg met derde partijen of het raadplegen van externe registers.

Van VI en VP naar BSN en persistent pseudoniem
De ontvangende partij kan bij het BSNk Sleutelbeheer (hierna te noemen: BSNk SB) een eigen geheime sleutel opvragen waarmee hij het persistente pseudoniem (hierna: P.xyz) op basis van het VP of het BSN op basis van de VI kan ontsleutelen. Een VI en VP zijn hierdoor alleen leesbaar voor de ontvangende partij. Met het P.xyz kan een DH-middel, door de specifieke partij, uniek worden geïdentificeerd. De identiteitsverklaring wordt afgegeven door de DH AD en bevat de VI of het VP specifiek voor de dienstverlener, waarmee alleen deze dienstverlener, in combinatie met de juiste sleutel van het BSNk, het BSN of het persistente pseudoniem kan ontsleutelen en de gebruiker kan identificeren.

Een visuele weergave van het gebruik van DigiD Hoog is weergegeven in *figuur 2*. Voor een visueel overzicht van de componenten wordt verwezen naar *Bijlage II*.



Figuur 2: authenticatieproces

4.5.4. Rollen en verantwoordelijkheden DigiD Hoog

De afbeeldingen in paragraaf 3.5.1 en 3.5.3 geven weer dat er verschillende rollen en verantwoordelijkheden worden onderscheiden binnen het DigiD Hoog aanvraag-, productie-, uitgifte en authenticatieproces. Een toelichting op de belangrijkste voorzieningen en rollen die worden onderscheiden voor DigiD Hoog is hieronder gegeven.

<u>BSNk</u>

Deze voorziening staat los van de DH AD maar is momenteel in beheer bij Logius. Een besluit ten aanzien van de overdracht van het beheer van het BSNk is nog niet genomen. Het BSNk is een voorziening die onder andere de verantwoordelijkheid heeft voor het genereren van een PI en PP op basis van het BSN. Bij de aanvraag van een NIK of rijbewijs wordt de PI en de PP van de gebruiker door het BSNk specifiek voor dit middel gegenereerd en door de MU op de chip van het WID geplaatst. De dienstverlener krijgt periodiek sleutels van het BSNk, waarmee de VI ontsleuteld kan worden tot het BSN. Door deze opzet, waarbij invulling wordt gegeven aan het privacy by design principe, wordt voorkomen dat het BSN binnen de DigiD-omgeving te achterhalen is. In bijzondere gevallen zoals fraudeonderzoek kan de identiteit van de gebruiker wel achterhaald worden. Het BSNk heeft onderstaande voorzieningen waarmee de volgende functies worden vervuld:

- BSNk Koppelregister (BSNk PP):
- Activatiefunctie: eenmalige activatie van een DH-middel die een gebruiker bij een MU heeft aangevraagd met behulp van het BSN, waarbij de PI en PP aan de MU wordt verstrekt en aan het DH-middel wordt gekoppeld (NIK/rijbewijs);
- Transformatiefunctie: het pseudoniem dat gekoppeld is aan het DH-middel wordt bij het inloggen bij een dienstverlener versleuteld in een VI of VP. De VI of VP kunnen door de dienstverlener ontsleuteld worden tot een BSN of een persistent pseudoniem;
- BSNk Sleutelbeheer (BSNk SB):
- Sleutelbeheerfunctie: het veilig beheren en verstrekken van de cryptografische sleutels;
- BSNk Inzageregister (BSNk IR):

- Inzagefunctie: biedt de gebruiker de mogelijkheid om alle authenticatiemiddelen die hij heeft geactiveerd en die hij gebruikt, in te zien. Het IR wordt gevoed door de MU als bron van de statusinformatie. Het BSNk IR werkt volledig pseudoniem.

Naast deze functies vervult het BSNk de volgende functies die niet specifiek in de PSA worden genoemd (Gegevensbeschermingseffectbeoordeling (GEB) eID-stelsel v1.0, 2017):

- 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.

Middelenuitgever (MU)

In het geval van een NIK is de MU RvIG en in het geval van een rijbewijs de RDW. De MU stelt het DH-middel beschikbaar en geeft deze op verzoek uit aan de gebruiker. Om een sluitende documentketen te verkrijgen, beheerst de MU de gehele logistieke keten van een WID en voert zij een sluitende administratie naast de productie en personalisatie van het document. De MU is verantwoordelijk voor het uitvoeren van de volgende taken:

- Het borgen van de technisch correcte werking van de chip, het chip OS en de daarop staande applets;
- Het veilig registreren van de verwijzing naar de elektronische identiteit ten behoeve van communicatie met het IR;
- Het veilig registreren van relevante gegevens met betrekking tot de chip op het document, zodat operaties met PIN-mailer, PUK-mailer, intrekken en dergelijke mogelijk zijn;
- Het optreden als authentieke bron van de statussen van het DH-middel: het registreren van statussen van het DH-middel en het doorgeven van deze statussen aan de DH SC en het IR;
- Het aanmaken van een tamper evident PIN-mailer en het versturen daarvan naar het BRP-adres in het binnenland na moment van uitreiking document;
- Het aanmaken van een tamper evident PIN-mailer en het versturen daarvan naar een bij de aanvraag opgegeven adres in het buitenland na moment van inklaring NIK-document;
- Het aanmaken van een tamper evident PUK-mailer en het aangetekend met identiteitscontrole versturen daarvan naar het BRP-adres van de gebruiker;
- De sluitende logistieke beheersing van nieuw aan te vragen documenten;
- De sluitende administratie van nieuw aan te vragen documenten en de statussen van die documenten, alsmede het afgeven van signalen aangaande statuswijzigingen richting DH SC en IR. Signalen betreffen tenminste: uitreiking aan de gebruiker, eventuele schorsing of opheffing van schorsing (alleen rijbewijs) en intrekking;
- Om een sluitende administratie te realiseren is bij de MU een configuratievoorziening gedacht. De invulling door de MU van deze configuratievoorziening is vrij;
- Indien technische problemen daartoe aanleiding geven kan de MU defecte documenten (laten) onderzoeken.

De MU werkt niet gepseudonimiseerd.

De voorziening waarmee Logius de dienst DigiD Hoog realiseert bestaat uit de volgende componenten: DH Authenticatiedienst, DH Status Controller, Transactielog, CTS, HSM, DH Deblokkeringsservice en DH Intrekkingsservice. De drie eerstgenoemde componenten zijn hieronder toegelicht. In paragraaf 3.6 is een toelichting opgenomen van alle componenten.

DigiD Hoog Authenticatiedienst (DH AD)
De DH AD is verantwoordelijk voor het authenticeren van de gebruiker wanneer hij een DH-middel gebruikt om in te loggen bij een dienstverlener. De DH AD maakt gebruik van de DH SC voor het opvragen van de statussen van de DH-middelen en van de TL voor het loggen van transacties. De DH AD maakt voor de toegang tot de DH SC en TL gebruik van gescheiden pseudoniemen (P.sc en P.tl) waardoor de DH AD niet in staat is om, buiten een actieve authenticatiesessie om, deze registers te bevragen. Als de controles juist zijn, geeft de DH AD een identiteitsverklaring aan de dienstverlener af, waarmee aan de hand van de VI het BSN of aan de hand van de VP het persistente pseudoniem door de dienstverlener kan worden bepaald. De DH AD werkt grotendeels gepseudonimiseerd. De DH AD weet bij welke dienstverlener wordt geauthenticeerd, maar niet door welke gebruiker.

DigiD Hoog Status Controller (DH SC)
De DH SC is een geautomatiseerde tabel waarin de statussen van de DH-middelen bij worden gehouden. Technisch gezien is de DH SC onderdeel van de DH AD. De data in de DH SC is technisch gescheiden van overige gegevens binnen de DH AD. Het inhoudelijke beheer (i.c. de data) van de DH SC is de verantwoordelijkheid van de MU. Beheerders van de DH AD kunnen de DH SC raadplegen maar kunnen hier geen mutaties in doorvoeren. Hiervoor dient een aanvraag bij de MU te worden ingediend. De DH SC werkt volledig gepseudonimiseerd en heeft een eigen P.sc waarmee een gebruiker uniek wordt geïdentificeerd binnen de DH SC. De DH SC weet niet van welke persoon het DH-middel is.

Transactielog (TL)
De TL houdt een log bij van het gebruik van DH-middelen ten behoeve van het inzagerecht. De TL wordt beheerd door de DH AD en werkt grotendeels gepseudonimiseerd. Op dit moment is nog in onderzoek of het IP-adres in de eindsituatie van DigiD Hoog in de TL moet worden opgenomen voor bepaalde belangen, waaronder fraudeonderzoek. Indien het IP-adres wordt opgenomen is de verwachting dat dit in versleutelde vorm zal gebeuren. De TL heeft een eigen P.tl waarmee een gebruiker uniek wordt geïdentificeerd binnen de TL. Als de identiteit van een gebruiker is vastgesteld (in Mijn DigiD) kan in de TL opgezocht worden welke handelingen er door deze gebruiker zijn uitgevoerd. Het is niet mogelijk om van een bepaalde handeling vast te stellen welke gebruiker hem heeft uitgevoerd op basis van alleen het TL.

Fraudelog (FL)
Hoewel geen onderdeel van de beschrijvingen in de PSA bestaat er een, in hoofdlijnen beschreven, ontwerp om een Fraudelog (FL) in de architectuur op te nemen voor fraudedetectie, -preventie en -onderzoek. De gebeurtenissen in de keten worden weggeschreven in de FL. In de huidige opzet van het te realiseren systeem wordt onder andere op patroonherkenning geanalyseerd op basis van use cases. Omdat de FL met pseudoniemen werkt moet bij het BSNk een versleuteld pseudoniem opgevraagd worden dat specifiek is voor de FL. Indien hier aanleiding tot is kan toegang verkregen worden tot registraties die op basis van dit pseudoniem zijn aangelegd. Indien vermoeden van fraude wordt gedetecteerd is het fraudeteam in staat de versleutelde identiteit te ontvangen op basis waarvan het BSN kan worden ontsleuteld. Dit is benodigd voor onderzoek, overleg met derde partijen of het raadplegen van externe registers. Naar verwachting wordt het IP-adres in de FL opgenomen.

4.5.5. Verschil eerste fase ten opzichte van laatste fase
De bovenstaande beschrijving geeft de eindsituatie weer van DigiD Hoog. Aangezien DigiD Hoog in fasen geïmplementeerd zal worden, is de situatie in de eerste fase niet gelijk aan

deze eindsituatie. De volgende verschillen zijn aanwezig tussen de implementatie in de eerste en de laatste fase:

- Het DH-middel wordt in de eerste release alleen gerealiseerd op rijbewijzen en later op de Nederlandse Identiteitskaarten. Doorontwikkeling naar overige wettelijke identiteitsdocumenten, zoals het paspoort, vreemdelingenpaspoort en geprivilegieerdenpas wordt voorzien in latere fasen;
- De PI en het PP van de chip op het WID worden in de eerste release vrijwel direct bij ontvangst in de keten vertaald naar een BSN waardoor in de beginsituatie uit de Transactielog te achterhalen is welke gebruiker bij welke dienstverlener heeft ingelogd. In de visuele weergave van het proces in *Bijlage II* worden in de beginsituatie van DigiD Hoog in de eID server nog pseudoniemen verwerkt waarna deze al bij de CTS/CIS-DH component worden vertaald naar een BSN. Vanaf de CTS/CIS-DH is de verwerking niet pseudoniem gebaseerd maar initieel nog BSN gebaseerd. In de eerste fase van DigiD Hoog heeft de DH Authenticatiedienst hierdoor nog wel inzage in welke gebruiker bij welke dienstverlener heeft ingelogd. Naar mate het project vordert zal de vertaling van de PI naar het BSN later in het proces plaatsvinden, totdat in de eindsituatie van DigiD Hoog het pseudoniem pas bij de ontvangende dienstverlener wordt vertaald naar een BSN. De authenticatiedienst heeft dan geen directe herleidingsmogelijkheden om vast te stellen welke gebruiker bij welke dienstverlener heeft ingelogd. Dit kan alleen herleid worden door het fraudeteam bij vermoeden van misbruik; zij zijn de enigen die beschikken over de daarvoor benodigde encryptiesleutels. Gebruik van de sleutels is afgeschermd middels beveiligingsmaatregelen en procedures.

4.6. Componenten, gegevensstromen en koppelingen DigiD Hoog

Om het proces van DigiD Hoog te kunnen realiseren wordt deels gebruik gemaakt van bestaande componenten van DigiD, die al dan niet moeten worden aangepast voor DigiD Hoog, en deels van nieuwe componenten die ontworpen worden voor DigiD Hoog.

In *tabel 3* is een overzicht gegeven van de componenten voor DigiD Hoog, of deze nieuw zijn of al aanwezig zijn in de huidige DigiD, wie de verantwoordelijkheid heeft over deze componenten en wat de functies van deze componenten zijn. Bij de realisatie van DigiD Hoog zijn meerdere partijen betrokken.

Component	Nieuw of bestaand	Verantwoordelijk	Functie
DH Authenticatie-dienst	Nieuw	Afdeling binnen Logius	De kern van de voorzieningen die DH ten behoeve van het gebruik van het DH-middel beschikbaar stelt. De DH AD is verantwoordelijk voor het afhandelen van een authenticatieverzoek van een dienstverlener indien de gebruiker heeft aangegeven met een DH-middel te willen inloggen. Ook heeft de DH AD een apart interface voor het initieel activeren van het DH-middel door de gebruiker. De DH AD maakt gebruik van de DH SC voor het opvragen van de statussen van de DH-middelen en van de TL voor het loggen van transacties. De DH AD maakt voor de toegang tot de DH SC en TL gebruik van gescheiden pseudoniemen (P.sc en P.tl) waardoor de DH AD niet in staat is om, buiten een actieve authenticatiesessie om, deze registers te ondervragen.
DH Status Controller	Nieuw	Technisch: DH AD Inhoudelijk: MU	De DH SC houdt de status van het DH-middel ten behoeve van de authenticaties bij de DH AD bij. Naast statussen houdt de DH SC ook een (status) vlag bij. De DH SC ontvangt de statussen van de MU die de authentieke bron van de statussen is. De DH SC levert op verzoek van de DH

Component	Nieuw of bestaand	Verantwoordelijk	Functie
			AD de actuele status van een DH middel aan de hand waarvan de DH AD de authenticatie afhandelt. De DH SC heeft voor elk DH-middel een eigen pseudoniem P.sc dat alleen voor deze dienst wordt gebruikt.
Transactielog (DigiD Logger)	Nieuw	Afdeling binnen Logius	De Transactielog (TL) slaat de relevante gegevens op van de transacties die door de DH onderdelen worden uitgevoerd. Vanuit de TL zullen, indien vereist, bepaalde opmerkelijke transacties doorgeven worden aan het IR (USvE vereiste). De transactielog is noodzakelijk wegens: ▪ Tonen van transactiehistorie aan de gebruiker; ▪ Tonen van laatste inlogactiviteit aan gebruiker; ▪ Afleggen van verantwoording door de DH Authenticatiedienst; ▪ Eisen vanuit de USvE ten aanzien van het signaleren van opmerkelijke transacties. Indien een separaat systeem voor fraudeonderzoek wordt gerealiseerd zal de logging voor de eerste drie punten (TL) gescheiden worden van de logging voor het vierde punt. Het fraudeonderzoeksysteem maakt hiervoor gebruik van het fraudelog. De TL is door de gebruikers in te zien via Mijn DigiD. Toegang wordt ook voorzien voor het Servicecentrum (zeer beperkt), 3e lijns support en in het kader van wettelijke bindende verzoeken tot inzage. De Transactielog heeft een eigen P.tl waarmee een gebruiker uniek wordt geïdentificeerd binnen de TL. Nieuw aan de TL is dat het een afzonderlijke service is, ontsloten via zijn eigen pseudoniem en dat deze wordt losgekoppeld van de middelen- en accountdatabase. De bestaande transactielog wordt naar de nieuwe structuur geconverteerd (daar zal eenmalig conversieproces voor nodig zijn).
Fraudelog	Nieuw	Afdeling binnen Logius	De Fraudelog (FL) is een aparte component voor fraudedetectie, -preventie en -onderzoek. De gebeurtenissen in de keten worden weggeschreven in de FL. In de huidige opzet van het te realiseren systeem wordt onder andere op patroonherkenning geanalyseerd op basis van use cases.
DH Intrekkings-service	Nieuw	Afdeling binnen Logius	Deze service maakt het mogelijk om een DH-middel op eenvoudige wijze in te trekken met behulp van de Intrekkingscode die in de PIN-mailer (en eventueel opnieuw verzonden PUK-mailer) staat. De intrekking is binnen 60 minuten doorgevoerd conform de eisen daarover in de USvE.
DH Deblokkerings-service	Nieuw	Afdeling binnen Logius	De DH Deblokkeringsservice zorgt ervoor dat gebruikers een geblokkeerd DH-middel weer actief kunnen maken. Daarvoor wordt een Deblokkeringscode gegenereerd door DigiD die naar het BRP-adres per aangetekende post met identiteitsvaststelling wordt verzonden.
DH CTS	Nieuw	Afdeling binnen Logius	De DH Card Test Service stelt gebruikers in staat om hun DH-middel te testen. De teststraat test alle componenten in de authenticatieketen bij de gebruiker tot aan de middleware bij DigiD om te kijken of er problemen zijn (kaart, kaartlezer, drivers, etc). Uit beveiligingsoogpunt staat de CTS los van de andere componenten van DigiD. Uit privacyoverwegingen dient de CTS zo te zijn uitgevoerd dat er geen persoonsgebonden gegevens achterblijven als de test wordt doorlopen.
DH HSM	Nieuw	Logius, levering en onderhoud bij BSNk	De DH HSM versleutelt de PI en PP tot een versleutelde identiteit en pseudoniem (VI/VP). In de uiteindelijke situatie

Component	Nieuw of bestaand	Verantwoordelijk	Functie
			waarbij er grote volumes authenticaties moeten worden verwerkt is het gebruik van een HSM zowel vanuit performance als beveiliging de beste oplossing. De software en de sleutels die in de HSM worden gebruikt, worden geleverd en onderhouden door het BSNk.
Middleware	Nieuw	Afdeling binnen Logius	Voor het uitlezen van de chip op het WID wordt gebruik gemaakt van middleware, waaronder wordt verstaan de eID server en de eID client. De eID client is een apparaat met NFC lezer en DigiD client software.
BSNk (PP)	Nieuw	BSNk, onafhankelijk van DH AD (in huidige situatie ook in beheer van Logius)	Het BSNk PP is een USvE component die onder de gezamenlijke voorzieningen valt. Het BSNk PP is een technische voorziening die de verantwoordelijkheid heeft voor het koppelen van het BSN van een natuurlijk persoon aan het gebruikte pseudoniem (USvE). Het BSNk PP levert een aantal diensten aan AD's en MU's: ▪ Het BSNk PP wordt gebruikt voor het genereren van de PI en PP op grond van het BSN via de functie 'activeren'; ▪ Het BSNk PP wordt gebruikt voor het genereren van de Versleutelde Identiteit (VI) en de Versleutelde Pseudoniem (VP) middels de functie 'transformeren'. Deze functies worden door het BSNk PP als service aangeboden maar ook in alternatieve vorm waarbij lokaal bij de AD een HSM met BSNk PP functionaliteit wordt gebruikt. Op deze HSM worden BSNk PP software en sleutels geplaatst.
BSNk Inzageregister	Nieuw	BSNk, onafhankelijk van DH AD (in huidige situatie ook in beheer van Logius)	Het BSNk IR is een USvE component die onder de gezamenlijke voorzieningen valt. Dit register is erop gericht om het inzagerecht van de gebruiker te ondersteunen. Daartoe moeten alle aangesloten AD's/MU's de actuele status van de middelen bij het IR registreren. In het geval van DigiD Hoog zal de MU als bron van de statusinformatie het IR voeden. Aangezien het DH-middel (bij de MU) andere statussen kent dan het IR (conform USvE) zal daarbij een vertaling plaatsvinden.
BSNk Sleutelbeheer	Nieuw	BSNk, onafhankelijk van DH AD (in huidige situatie ook in beheer van Logius)	Het BSNk SB is een USvE component die onder de gezamenlijke voorzieningen valt. Het specifieke sleutelbeheer voor het stelsel wordt geregeld door het BSNk SB. Vanuit het BSNk SB worden de sleutels voor de HSM bij de DH AD aangemaakt en gedistribueerd.
Mijn DigiD	Bestaand	Afdeling binnen Logius	Mijn DigiD is een bestaand zelfservice portaal van DigiD. Met de implementatie van DigiD Hoog zullen de volgende aanpassingen worden gedaan: 1. De gebruiker krijgt een grote mate van invloed op de hoeveelheid geschiedenis dat getoond wordt t.b.v. het inzagerecht. Afhankelijk van deze instellingen wordt alleen de laatste inlogpoging getoond met het DH-middel of bijvoorbeeld ook de mogelijkheid geboden de geschiedenis van de laatste aantal maanden te tonen; 2. Op dit moment is er binnen (Mijn) DigiD geen onderscheid tussen het accountbeheer en het middelenbeheer. Mijn DigiD zal echter meerdere middelen moeten gaan ondersteunen waardoor het accountbeheer en het middelenbeheer gescheiden moet worden.
DigiD Beheer	Bestaand	Afdeling binnen Logius	Component waarmee de werking van de overige componenten kan worden beïnvloed en inzage kan worden gegeven in deze componenten.

Component	Nieuw of bestaand	Verantwoordelijk	Functie
DigiD Kern	Bestaand	Afdeling binnen Logius	DigiD Kern is de kern van de bestaande DigiD authenticatiedienst. DigiD Kern ondersteunt authenticatiemiddelen op verschillende niveaus. Het DH middel is een middel op het hoogste niveau dat DigiD levert. Ten behoeve van DigiD Hoog worden interfaces van de DigiD Kern aangepast.
DigiD Helpdesk	Bestaand	Extern belegd (eerstelijns) en afdeling binnen Logius (tweedelijns)	De DigiD Helpdesk biedt gebruikersondersteuning per telefoon, email, twitter en per post. In de praktijk bestaat de DigiD Helpdesk uit twee voor de gebruiker zichtbare lagen: ▪ Eerstelijns support door de helpdesk (extern belegd); ▪ Tweedelijns support door het DigiD Servicecentrum. Met de implementatie van DigiD Hoog veranderen voornamelijk de processen van het DigiD Servicecentrum, zie hieronder.
DigiD Servicecentrum	Bestaand	Afdeling binnen Logius	Het DigiD Servicecentrum biedt tweedelijns support. Omdat DigiD Hoog met pseudoniemen gaat werken in plaats van met een BSN dienen er voorzieningen te worden gerealiseerd zodat het Servicecentrum de mogelijkheid behoudt om de gebruiker te ondersteunen. Oplossingen hiervoor kunnen zijn: het identificeren van de gebruiker door controlevragen, het inzetten van feedback kanalen als e-mail en SMS en het registreren van meerdere middelen door de gebruiker.
Publicatiedienst Authenticatie-dienst (DigiD Website)	Bestaand	Afdeling binnen Logius	De Publicatiedienst AD geeft invulling aan eIDAS 2015/1502 2.4.2 sub 1: Er bestaat een gepubliceerde beschrijving van de dienst met alle toepasselijke voorwaarden en vergoedingen, inclusief eventuele gebruiksbeperkingen. De beschrijving van de dienst omvat een privacyverklaring. In essentie kan dit worden ingevuld door de vereiste stukken op de website van DigiD/Logius te publiceren.

Tabel 3: componenten

Onderstaande componenten dragen zorg voor de aanvraag, productie, personalisatie, uitgifte en het beheer van de documenten die drager zijn van het DH-middel. Deze onderdelen dienen een sluitende administratie van documenten en gerelateerde gegevens te realiseren (configuratievoorziening). Deze componenten zijn niet in scope van de PIA:

- Aanvraagsysteem: het systeem dat bij het aanvraag- en uitgifteproces wordt gebruikt voor het aanvragen en beheren van documenten. Dit systeem zal, aan de kant van de MU, ten behoeve van DigiD Hoog een aantal nieuwe functies moeten krijgen voor het doorgeven van statussen. Uitgangspunt is dat het aanvraagsysteem bij het aanvraag- en uitgifteproces uitsluitend koppelingen heeft met de systemen bij de MU;
- Chip: de chip die op een document is geplaatst en waarin de PCA met PI/PP bij het personaliseren wordt geplaatst. De chip wordt gedeeld met reeds bestaande apps als de ICAO EMRTD app voor de NIK en het eDL voor het rijbewijs;
- PCA: de PCA is een smartcard toepassing die gerandomiseerde polymorfe identiteiten en pseudoniemen kan genereren die gebruikt worden door de DH AD. Hiermee wordt voorkomen dat de DH AD inzage krijgt in welke gebruiker bij welke overheid diensten afneemt.

De externe gegevensstromen van DigiD zijn in *tabel 4* weergegeven:

#	Component	Element	Toelichting interface	Attributen/gegevens
1	Dienstverlener	Inloggen	Dienstverleners zullen ten behoeve van de authenticatie met behulp van (versleutelde) pseudoniemen de interface met DigiD moeten aanpassen. Dit zal geleidelijk worden ingevoerd.	▪ Minimaal vereiste authenticatieniveau ▪ OIN van dienstverlener
2	Middelenuit-geversysteem	Activeer BSN		▪ BSN ▪ Documentnummer ▪ Documenttype (NIK, rijbewijs) ▪ Einde geldigheid document signer certificaat ▪ Volgnummer document ▪ VP voor DH Status Controller ▪ Documentstatus ▪ OIN van MU ▪ PUK ▪ Initiële PIN ▪ CAN ▪ Status opmerking ▪ Datum einde geldigheid ▪ PI ▪ PP
		Statuswijzigingsverzoek	Interface waarmee een status-wijzigingsverzoek door de servicedesk of via Mijn DigiD ingediend kan worden. Twee vormen zijn nodig: ▪ Servicedesk (zonder PCA/PI): documentnummer als gedeelde sleutel ▪ Mijn DigiD (met PCA/PI): VI en volgnummer voor de MU als gedeelde sleutel	
		Lever documentgegevens	Interface waarmee DigiD-gegevens van het document waarop een DH-middel is geplaatst opgevraagd kunnen worden. En door de servicedesk of via Mijn DigiD ingediend kan worden. Twee vormen zijn nodig: ▪ Servicedesk (zonder PCA/PI): BSN als gedeelde sleutel ▪ Mijn DigiD (met PCA/PI): VI en volgnummer voor de MU als gedeelde sleutel	
		Registreer Status Controller status		
		Registreer inzageregister status		
		Lever PIN-resetcode	Interface wordt gebruikt om de PUK-code aan te vragen waarmee de gebruiker een PIN-reset kan uitvoeren. De PUK-code wordt digitaal aangeleverd	
		Verzenden PIN-resetmailer	Interface wordt door DigiD gebruikt om een verzending van een PIN-resetmailer aan te vragen. In de PIN-resetmailer staat de PUK-code. De PIN-resetmailer wordt naar het actuele BRP-adres verzonden.	
		Verzenden aanvraag	Interface stelt het aanvraagsysteem in staat om een aanvraag voor een document in te dienen	
		ePersonalisatie		
3	BSNk PP	Activeren BSN	Interface wordt beschikbaar gesteld voor het activeren van het BSN. Als resultaat worden de PI en PP voor de MU (RDW/RvIG) aangemaakt en geretourneerd.	
		Lever VI	Interface wordt aangeboden aan Authenticatiediensten die zelf geen	

#	Component	Element	Toelichting interface	Attributen/gegevens
			VI's kunnen ontsleutelen. De DH Authenticatiedienst kan hier gebruik van maken als (nog) geen HSM ingericht is.	
		Lever VP	Interface wordt aangeboden aan Authenticatiediensten die zelf geen VP's kunnen ontsleutelen. De DH Authenticatiedienst kan hier gebruik van maken als (nog) geen HSM ingericht is.	
4	BSNk IR	Registreer IR- status	Interface wordt door centrale inzageregister aangeboden om status van DH middelen te registreren t.b.v. een centrale inzagedienst. De MU voedt het inzageregister.	▪ Pseudoniem waaronder DH middel bij inzageregister bekend staat ▪ Documenttype ▪ Einde geldigheid document signer certificaat ▪ Volgnummer document ▪ Status DH middel
		Lever IR-status	Interface wordt niet gebruikt door DigiD Hoog. Biedt de mogelijkheid om de status van geregistreerde middelen op te vragen door geautoriseerde partijen.	
5	BSNk SB	BSNk sleutels laden	Sleutels voor de HSM bij de DH Authenticatiedienst worden aangemaakt en gedistribueerd.	

Tabel 4: externe gegevensstromen

4.7. Bewaartermijnen logging

Logging	Maximale bewaartermijn	Toelichting
Transactielog	5 jaar	Logging gegenereerd door applicaties.
Centrale logservers	18 maanden	Centrale vastlegging van de logging.
Back-up termijn	4 maanden	Herstel van DigiD na een grote calamiteit waarbij redundantie over twee sites geen soelaas heeft geboden.
Systeemlog	100 dagen	Technische logging gegenereerd door componenten.
Briefbestanden	6 weken	Gegevens die nodig zijn voor de afhandeling van een aanvraag of verzoek van een gebruiker van DigiD.
Logging infrastructuurcomponenten	1 maand	Deze logging wordt gesynchroniseerd met centrale logservers.
Loadbalancer logging	7 dagen	Deze logging wordt niet met centrale logservers gesynchroniseerd.
Sessiegegevens en cookies	Sessieduur	Gegevens die worden bewaard tot het einde van de sessie.

Tabel 5: bewaartermijnen logging

5. Conclusies en aanbevelingen PIA

5.1. Positionering DigiD Hoog in de ontwikkelcyclus van DigiD

Het voornemen van het ministerie van BZK om DigiD en het bijbehorende authenticatiemechanisme te versterken, wordt gerealiseerd via een aantal stappen die zich in de tijd uitstrekken. De bestaande DigiD (DigiD basis en DigiD midden) biedt de gebruiker de mogelijkheid om met een gebruikersnaam en wachtwoord (optioneel met sms) of gebruikersnaam en DigiD app (met pincode) in te loggen.

De eerste stap in de versterking van DigiD is de realisatie van DigiD Substantieel en betreft de realisatie van een versterkt uitgifteproces en bijbehorend authenticatiemiddel. Om betrouwbaarheidsniveau 'Substantieel' te behalen is door Logius gekozen voor een aanpak waarbij de identiteit van de gebruiker geverifieerd wordt door het initieel en periodiek scannen van de chip aanwezig op een WID met behulp van de DigiD app op het mobiele apparaat van de gebruiker. Een afzonderlijke PIA is op DigiD Substantieel uitgevoerd (Mazars, 2017).

DigiD Hoog bouwt deels voort op componenten van de bestaande DigiD en componenten van DigiD Substantieel. Bestaand DigiD, DigiD Substantieel én DigiD Hoog maken gemeenschappelijk gebruik van componenten, waaronder gemeenschappelijke databases met stamgegevens en transactiegegevens. Op bestaande componenten worden wijzigingen doorgevoerd. Ook worden nieuwe componenten aan het geheel toegevoegd. Op termijn is het de bedoeling dat bestaande componenten van DigiD worden omgebouwd en dat compartimentering, een eigenschap van de architectuur van DigiD Hoog, verregaand wordt doorgevoerd, waardoor het geheel aan verwerkingen vanuit privacyperspectief beter beheersbaar wordt, functiescheidingen kunnen worden ingericht en de data in verschillende componenten niet zondermeer aan elkaar te koppelen zijn. Overigens bestaan er bij het huidige ontwerp van de eindsituatie nog onzekerheden hoe bepaalde onderdelen worden geïmplementeerd. Dit betreft onder meer de wijze waarop onderzoek naar misbruik van DigiD kan worden uitgevoerd en hoe verdere pseudonimisering wordt doorgevoerd binnen de DigiD-systemen en de gekoppelde systemen van de aangesloten dienstveleners, ook voor wat betreft historische gegevens binnen de bestaande DigiD en DigiD Substantieel.

Een andere belangrijke verandering in het ontwerp van DigiD Hoog dat uiteindelijk het gehele DigiD-landschap raakt, is het gebruik van polymorfe identiteiten en pseudoniemen. Het effect van de invoering van deze technologie is dat de authenticatiedienst geen BSN meer ontvangt als gevolg van het inloggen van een gebruiker bij een dienstverlener, maar een polymorfe identiteit en pseudoniem. Deze maatregel heeft als positief effect dat, ook al zou er sprake zijn van een onrechtmatige toegang tot de inloghistorie, het vervaardigen van profielen op basis van BSN of pseudoniemen niet mogelijk is zonder in het bezit te zijn van de encryptiesleutel. Bescherming tegen onrechtmatig gebruik van de inloghistorie wordt hiermee op het niveau van DigiD Hoog aanzienlijk verbeterd.

5.1.1. Bevindingen

Status privacybevorderende maatregelen eerste fase DigiD Hoog

DigiD Hoog wordt in fasen gerealiseerd. In de eerste release wordt het voor gebruikers mogelijk om de beschikking te krijgen over een authenticatiemiddel op het eIDAS-niveau 'Hoog'. Met dit authenticatiemiddel kunnen gebruikers op het hoogst mogelijke betrouwbaarheidsniveau inloggen en hierdoor online diensten afnemen die vanwege de gevoeligheid alleen met dit betrouwbaarheidsniveau kunnen worden afgenomen. Te denken valt hierbij aan het raadplegen van een medisch dossier of strafrechtelijke gegevens.

Vanaf de eerste implementatie van DigiD Hoog zijn een aantal privacybevorderende maatregelen geïmplementeerd, waaronder een hoger betrouwbaarheidsniveau van authenticatie en de organisatorische en technische ontvlechting van het aanvraag-, productie- en uitgifteproces van de authenticatiedienst. De gegevensuitwisseling tussen middelenuitgevers en de authenticatiedienst (onder andere door de inzet van de Status Controller) wordt geminimaliseerd en een verdergaande scheiding in verantwoordelijkheden tussen verschillende rollen wordt gerealiseerd door compartimentering binnen de authenticatiedienst. Het datagebruik per rol wordt hiermee verder geminimaliseerd. In deze fase worden polymorfe identiteiten en pseudoniemen in de keten van eindgebruiker tot de centrale authenticatiedienst gebruikt, waarmee wordt bereikt dat in dit deel van de keten geen BSN meer verwerkt wordt. Het risico van ongewenste herleiding van transacties naar individuen en profiling is binnen dit deel van keten hiermee ook gemitigeerd. Het BSNk functioneert al vanaf de eerste fase als beheerder van de encryptiesleutels (ketensleutel) die benodigd zijn voor het ontsleutelen van de verschillende polymorfe identiteiten en pseudoniemen die zijn gebruikt binnen de componenten van de authenticatiedienst.

De privacybevorderende maatregelen die onderdeel zijn van het totale concept van DigiD Hoog zijn op het eerste releasemoment nog beperkt geëffectueerd. Voor de eerste ingebruikname van DigiD Hoog is hieronder aangegeven welke privacybevorderende maatregelen dan nog niet zijn gerealiseerd.

In de eerste fase van DigiD Hoog vindt het gebruik van pseudoniemen alleen nog plaats op de chip van het WID en in de gegevensstromen en componenten tussen de gebruiker en de authenticatiedienst bij het inlogproces (middleware). Voor de verdere verwerking in het proces wordt het BSN gebruikt, dat vroegtijdig in het authenticatieproces wordt ontsleuteld op basis van de polymorfe identiteit. Hierdoor is bij de authenticatiedienst en andere tussenliggende partijen in de authenticatieketen bekend welke gebruiker inlogt.

Vanaf de eerste implementatie zal de Status Controller een afzonderlijk domein vormen. Volledige compartimentering wordt vanaf 2019 gerealiseerd waarbij onder meer de accountgegevens, transactielog en middelenadministratie van elkaar worden gescheiden. Door compartimentering kan onder meer worden gerealiseerd dat de data in verschillende componenten niet zonder meer te koppelen zijn aan elkaar en de beheersing van privacyrisico's wordt verbeterd. In de eerste fase is de compartimentering nog niet volledig gerealiseerd waardoor onder andere de inloggegevens nog te koppelen zijn aan de accountgegevens. De transactiegegevens bevatten een verwijzing naar de accountgegevens, waaronder het BSN. In deze transactiegegevens is ook vastgelegd bij welke dienst de gebruiker heeft ingelogd. Zolang het gebruik van polymorfe identiteiten en pseudoniemen en de beoogde compartimentering niet volledig is doorgevoerd voor DigiD Hoog én de bestaande DigiD componenten met de daaraan gerelateerde historische gegevensverzamelingen, blijft een privacygevoelige dataset aanwezig op basis waarvan kwaadwillenden profielen van gebruikers op zouden kunnen stellen. Het is een overweging om de historische gegevens aanwezig binnen bestaande DigiD-componenten eveneens te pseudonimiseren. Deze conversie is in de PSA niet beschreven.

Hoewel geen onderdeel van de beschrijvingen in de PSA bestaat er een, in hoofdlijnen beschreven, ontwerp om een afgezonderd compartiment in de architectuur op te nemen voor fraudedetectie, -preventie en -onderzoek. Deze opzet maakt de beheersing van fraudeonderzoek en toegang tot de specifiek daarvoor benodigde informatie beter beheersbaar. Ook biedt deze structuur mogelijkheden voor het realiseren van

controlemechanismen om de integriteit van de data te kunnen toetsen. In de huidige opzet van het te realiseren systeem wordt onder andere op patroonherkenning geanalyseerd op basis van use cases. Indien vermoeden van fraude wordt gedetecteerd is het fraudeteam in staat de versleutelde identiteit te ontvangen op basis waarvan het BSN kan worden ontsleuteld. Dit is benodigd voor onderzoek, overleg met derde partijen of het raadplegen van externe registers. Het ontwerp zal naar verwachting eind 2018 worden geïmplementeerd. De organisatorische opzet rond deze fraudebeheersing is nog niet volledig uitgewerkt.

Op termijn heeft Logius het voornemen om de pseudonimisering niet alleen voor DigiD Hoog te gaan hanteren, maar ook voor de bestaande DigiD en DigiD Substantieel. De bestaande DigiD en DigiD Substantieel kunnen bij het inloggen niet direct een PI/PP genereren. Op basis van het BSN wordt dan voor de verdere verwerking een gerandomiseerd pseudoniem gegenereerd zodat de authenticatiedienst ook bij het gebruik van DigiD en DigiD Substantieel niet weet welke gebruiker inlogt. Deze maatregel wordt in de laatste fase van het project DigiD Hoog gerealiseerd. Dit betekent dat de bestaande privacyrisico's voor de bestaande DigiD en DigiD Substantieel voorlopig blijven bestaan, totdat ook deze onderdelen op basis van pseudoniemen werken.

Het gevolg van de gefaseerde implementatie is dat er slechts beperkt privacybevorderende effecten worden gerealiseerd in de eerste fase van DigiD Hoog, anders dan dat het middelenuitgifteproces en het authenticatieproces naar een hoger zekerheidsniveau is gebracht. De overige privacyrisico's zoals ook beschreven in de PIA DigiD Substantieel blijven voorlopig bestaan. Voor een overzicht van de privacyrisico's en aanbevelingen met betrekking tot DigiD Substantieel en de bestaand DigiD verwijzen wij naar *Bijlage VI*. We willen benadrukken dat de bovenbeschreven risico's van het verzamelen van inloghistorie en de risico's van de beschreven herleiding van gegevens naar natuurlijke personen niet een gevolg zijn van de toegevoegde functionaliteit van DigiD Hoog, maar voortvloeien uit de eigenschappen van de componenten en inrichting van de bestaande DigiD en DigiD Substantieel die gebruikt blijven worden voor DigiD Hoog. Indien de eindsituatie van DigiD Hoog wordt gerealiseerd met de volledige vervanging van het BSN door pseudoniemen en waarbij de pseudonimisering ook wordt doorgevoerd voor de bestaande DigiD en DigiD Substantieel, worden voor DigiD belangrijke privacyrisico's gemitigeerd.

Geconstateerd is dat op de bestaande DigiD nog geen integrale PIA is uitgevoerd. Bij de uitvoering van deze PIA op DigiD Hoog is, vanwege de verwevenheid met het bestaande DigiD-systeem, daarom naar vermogen ook aandacht besteed aan de privacyrisico's die kleven aan de bestaande DigiD en de achterliggende verwerkingen van persoonsgegevens en systeemcomponenten.

5.1.2. Aanbevelingen

Het is belangrijk dat de doorontwikkeling naar de eindsituatie van DigiD Hoog zoals is voorgenomen wordt doorgezet en afgerond en dat uiteindelijk de middelen en concepten van het nu bestaande DigiD-systeem worden omgebouwd en/of de risico's daarvan worden gemitigeerd. Het verdient aanbeveling om een meer concrete uitwerking te maken van hoe en met welke fasering de invoering van de concepten van DigiD Hoog worden gerealiseerd. Besteed hierbij ook aandacht aan de organisatorische inrichting van de verschillende functies en verantwoordelijkheden binnen Logius. De huidige voorgestelde systeemopzet met verregaande compartimentering biedt hier de mogelijkheden toe.

Op de bestaande DigiD is niet eerder een integrale PIA uitgevoerd. Wel is (en wordt) bij het doorvoeren van veranderingen aan DigiD aandacht besteed aan de eisen van de Wbp. Een integraal overzicht van privacyrisico's van de bestaande DigiD is niet voorhanden. Het verdient aanbeveling om bij de doorontwikkeling van DigiD een integrale privacyrisicoanalyse uit te voeren op de organisatorische en technische maatregelen van DigiD Substantieel en DigiD Hoog, inclusief de bestaande DigiD en de onderliggende infrastructuur.

5.2. Noodzakelijke verwerking persoonsgegevens DigiD Hoog

Om te beoordelen of het noodzakelijk is persoonsgegevens te verwerken voor het te bereiken doel voor DigiD Hoog speelt de vraag naar proportionaliteit en subsidiariteit. Het proportionaliteitsbeginsel houdt in dat de inbreuk op de belangen van de bij de verwerking van persoonsgegevens betrokkene niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Ingevolge het subsidiariteitsbeginsel mag het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere, voor de bij de verwerking van de persoonsgegevens gebruiker minder nadelige wijze kunnen worden verwerkelijkt[16].

5.2.1. Bevindingen proportionaliteit

Uit de beschrijving van de PSA DigiD Hoog blijkt dat er geen persoonsgegevens worden verwerkt die niet noodzakelijk zijn voor de werking van DigiD Hoog.

Bij DigiD Hoog wordt het middelenuitgifteproces afgewikkeld buiten de authenticatiedienst van Logius. De authenticatiedienst ontvangt geen persoonsgegevens van middelenuitgevers met betrekking tot dit proces. Voor het verifiëren van de geldigheid van een WID bij het authenticeren wordt een bevraging gedaan naar de Status Controller die gevoed wordt vanuit RvIG en de RDW. In de eindsituatie zijn de gegevens in de Status Controller gepseudonimiseerd en bevatten deze verder alleen documentgegevens en statusinformatie van het WID.

Door het gebruik van PI en PP wordt het BSN gebruik binnen de authenticatiedienst van Logius gereduceerd. De introductie van de Status Controller geeft verdergaande invulling aan het proportionaliteitsprincipe. Dit register kan enkel in een actieve authenticatiesessie door de authenticatiedienst worden bevraagd en geeft alleen de informatie die benodigd is voor verificatie van het DH-middel.

5.2.2. Bevindingen subsidiariteit

Met DigiD Hoog wordt een belangrijke stap gezet in de verdere invulling van het subsidiariteitsprincipe. Dat wil zeggen dat door toepassing van nieuwe werkwijzen en technologieën met minder persoonsgegevens de doelstellingen van de authenticatiedienst met een hoge betrouwbaarheid wordt gerealiseerd, dan bij de overige DigiD-voorzieningen. Belangrijke stappen hierin zijn:

- Reductie van het BSN-gebruik door inzet van pseudonimisering. Door de inzet van deze techniek kunnen de transactiegegevens die worden verwerkt in het authenticatieproces niet meer aan een persoon worden gekoppeld, zonder dat aanvullende gegevens daarvoor benodigd zijn. Alleen met de juiste sleutel kan de identiteit van de gebruiker worden achterhaald.
- Een verdergaande compartimentering van de DigiD-componenten door het technisch scheiden van belangrijke voorzieningen zoals de Status Controller en de

[16] Zie artikel 8 Wet bescherming persoonsgegevens.

Transactielog. De voorzieningen hebben elk hun eigen rollen en verantwoordelijkheden waardoor ongewenste cumulaties van persoonsgegevens wordt voorkomen en dataminimalisatie op componentniveau beter beheersbaar wordt. Deze scheiding van systemen maakt ook de handhaving van functiescheidingen beter mogelijk. In de huidige DigiD is de transactielog gekoppeld aan de accountgegevens en is hierdoor bekend welke gebruiker bij welke dienstverlener inlogt. In het concept van DigiD Hoog is dit niet meer het geval. Daarbij wordt opgemerkt dat analyse van deze gegevens nog wel mogelijk is, maar daar zijn de juiste autorisaties en encryptiesleutels voor benodigd.

Gesteld kan worden dat DigiD Hoog de principes proportionaliteit en subsidiariteit mee weegt en invult. In de eerste fase van DigiD Hoog zijn genoemde privacybevorderende maatregelen deels aanwezig. Pseudonimisering en compartimentering zijn in deze situatie beperkt toegepast waardoor ook de risico's die hiermee samenhangen nog aanwezig zijn. Naarmate de verdere pseudonimisering wordt doorgevoerd binnen DigiD Hoog en de concepten van DigiD Hoog uiteindelijk over de bestaande DigiD en DigiD Substantieel zijn uitgerold, worden de privacyprincipes proportionaliteit en subsidiariteit verdergaand gerealiseerd.

Op dit moment is nog in onderzoek of het IP-adres in de eindsituatie van DigiD Hoog in de transactielog moet worden opgenomen. Indien het IP-adres wordt opgenomen is de verwachting dat dit in versleutelde vorm zal gebeuren. Zolang aan deze randvoorwaarde is voldaan heeft dat geen invloed op de conclusies van deze PIA.

5.2.3. Aanbevelingen

Het verdient aanbeveling om bij het verdere ontwerp van DigiD Hoog specifiek aandacht te besteden aan de afscherming van IP-adressen, na te gaan in welke (ook al bestaande) componenten IP-adressen worden opgeslagen en aan te geven wat de noodzakelijkheid is om deze gegevens te bewaren. Dit onderwerp is nog een onderbelicht aspect in de huidige ontwerpdocumentatie van DigiD Hoog.

5.3. Privacyprincipe: limiteren van het verzamelen van gegevens

Het principe dataminimalisatie, ofwel het limiteren van het verzamelen van gegevens, houdt in dat persoonsgegevens uitsluitend worden verwerkt op basis van de limitatieve grondslagen. Het uitgangspunt is het bereiken van het gestelde doel met minimale gegevensverzameling.

5.3.1. Bevindingen

De DH Authenticatiedienst verwerkt de PI en PP in plaats van het BSN. Het doel is dat de gehele authenticatiedienst pseudoniem-gebaseerd wordt. Het BSN wordt alleen gebruikt indien aanleiding is voor fraudeonderzoek of, door de Servicedesk, om de gebruiker te helpen. In dit laatste geval wordt het BSN door de Servicedesk opgevraagd, maar niet opgeslagen. De Servicedesk maakt in dit geval een uitstap naar een niet-pseudoniem domein, bijvoorbeeld van de middelenuitgever, om technische gegevens van het DH-middel op basis van het BSN op te vragen. Aan de hand van deze gegevens kan een verzoek worden gedaan voor het blokkeren van het DH-middel. Nog onbekend is hoe Logius omgaat met een verzoek waarbij de gebruiker gegevens opvraagt, bijvoorbeeld bij een inzageverzoek. Het is belangrijk de identiteit van de gebruiker vast te stellen alvorens gevoelige gegevens te verstrekken.

Door het gebruik van randomisering wordt in tussenliggende systeemdomeinen voorkomen dat gegevens kunnen worden verzameld voor ongeautoriseerde analyse. Met deze

maatregelen en ook met hetgeen in paragraaf 4.2 is beschreven is invulling gegeven aan het privacyprincipe van limiteren van het verzamelen van gegevens.

De inzet van technische componenten, zoals firewalls en intrusion prevention- en detectionsystemen, DDoS-preventiesysteem en technische logsystemen, wordt in de ontwerpdocumentatie, aanvullend op de PSA, beschreven. In het kader van deze PIA zijn de effecten van deze technische netwerkcomponenten niet in detail onderzocht. Deze technische netwerkcomponenten loggen het gebruik van het DigiD-systeem op verschillende niveaus. Het doel van de systeemlogging is om het systeem te kunnen beheren, de beveiliging te monitoren en het juist functioneren te bewaken. Hiermee worden echter risico's gecreëerd, waaronder risico's voor ongewenste herleiding van gegevens en profiling. Logius geeft nadrukkelijk aan dat profileren geen activiteit is waar zij zich mee bezighoudt of van plan is zich mee bezig te houden. Een integraal overzicht van de gegevens die worden verwerkt door deze componenten is niet aanwezig.

5.3.2. Aanbevelingen

Het verdient aanbeveling om de wijze waarop informatie wordt verzameld en verstrekt nader uit te werken bij de vervolgontwerpen van DigiD Hoog. Het is aan te bevelen procedurebeschrijvingen te maken voor de verschillende activiteiten. Te denken valt aan het achterhalen van de identiteit van de gebruiker door de Servicedesk in een omgeving waar geen BSN wordt verzameld en verwerkt.

Het verdient aanbeveling om bij de verdere detaillering van het DigiD Hoog ontwerp en de verdere realisatie naar de eindsituatie van DigiD Hoog de consequenties van het gebruik van de verschillende loggings bij de inzet van een diversiteit van componenten nader te analyseren en zo nodig additionele privacybeschermende maatregelen te treffen. Dit kan middels additionele beveiligingsmaatregelen of door minimalisatie van de loggegevens. In elk geval is meer duidelijkheid wenselijk over de wijze waarop de loggings in samenhang van de verschillende DigiD voorzieningen en componenten functioneren en welke privacyrisico's dat meebrengt.

5.4. Privacyprincipe: doelbinding / limiteren van het gebruik van gegevens

Het privacyprincipe doelbinding houdt in dat persoonsgegevens alleen voor vooraf welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en niet verder worden verwerkt als dit hiermee onverenigbaar is. Het limiteren van het gebruik van de gegevens houdt in dat persoongegevens niet gedeeld mogen worden met derden of voor andere doeleinden gebruikt mogen worden, tenzij hiervoor expliciet toestemming is verkregen van de gebruiker of hiervoor een wettelijke grondslag is.

Logius verwerkt persoonsgegevens zodat gebruikers op een betrouwbare manier kunnen inloggen bij dienstverleners. De wettelijke grondslagen volgens de Wbp om persoonsgegevens te verwerken ten behoeve van DigiD Hoog zijn de vervulling van een publiekrechtelijke taak en toestemming van de gebruiker.

Het BSN, dat in de huidige DigiD wordt verwerkt in het authenticatieproces, zal uiteindelijk volledig worden vervangen door een PI en PP. De polymorfe identiteit is alleen te herleiden naar het BSN van de gebruiker met een encryptiesleutel die middels een gereguleerd proces kan worden verkregen van het BSNk. Met deze privacybevorderende maatregel wordt bereikt dat bij Logius niet bekend is welke gebruiker bij welke dienstverlener inlogt. Alleen door de

ontvangende dienstverlener of in bijzondere gevallen kan de identiteit van de gebruiker worden ontsleuteld.

Door de compartimentering die wordt gerealiseerd binnen DigiD hebben de verschillende compartimenten hun eigen (versleutelde) polymorf pseudoniem of polymorfe identiteit. Hiermee wordt bereikt dat verschillende componenten, met elk een eigen doelstelling, alleen de benodigde gegevens verkrijgen en gebruiken voor het te realiseren doel. Het aanvraag-, productie- en uitgifteproces van een DH-middel ligt buiten de verantwoordelijkheid van Logius. Door deze processen bij een externe partij te beleggen wordt gerealiseerd dat de gegevens die voor deze verwerking benodigd zijn, gescheiden zijn van de gegevens die worden verzameld of ontstaan bij het gebruik van een DH-middel.

5.4.1. Bevindingen

Logius beschikt over een register van verwerkingen als bedoeld in artikel 30 van de AVG. Een volledig en toegankelijk overzicht van verwerkingen van persoonsgegevens, waarin naast de persoonsgegevens op functioneel niveau ook de verwerkingen van persoonsgegevens op technisch niveau zijn beschreven en gekoppeld aan de specifieke doelen op component- en op overkoepelend niveau, is niet beschikbaar. De verwerkte persoonsgegevens op alle componenten en systeemlagen zijn niet in één overzicht aanwezig en het totaal vormt een complex geheel.

In de huidige ontwerpdocumentatie is weinig aandacht besteed aan de maatregelen voor interne beheersing voor wat betreft het controleren van de toegang tot data, het gebruik van de data en waarborgen die de kwaliteit van de data garanderen. Een beschrijving van deze maatregelen zijn in andere documenten beschreven die in het kader van deze PIA niet zijn bestudeerd. Er wordt weliswaar verwezen naar normen voor informatiebeveiliging waaronder de BIR en ISO27001, maar deze normen zien vooral toe op de procedurele kant van Information Security Management Systemen en niet direct op de werking van de gerealiseerde beveiligingsmaatregelen in de IT werkelijkheid. Beveiligingsmaatregelen zijn door Logius getroffen op de bestaande DigiD, zoals controles op basis van extern systeemgebruik, het uitvoeren van patroonherkenning op gebruikersdata, het beperken van de toegang op basis van toegekende rechten, het monitoren van toegang tot logging en het versturen van alerts indien een onverwachte toegang wordt gedetecteerd. Voor toegang tot de beheermodule is een persoonlijk PKIoverheid-certificaat vereist. Voor het doorvoeren van diverse gevoelige activiteiten op het systeem wordt het vier-ogenprincipe afgedwongen. Voor de vaste schijven waar deze gegevens zijn opgeslagen wordt schijfencryptie toegepast. Dit laat onverlet dat er, met name in de fase van DigiD Hoog waarin het BSN nog in de logging is opgenomen, sprake is van een gevoelig transactiebestand met inloghistorie.

Met de introductie van de PI en PP en door compartimentering wordt het risico op oneigenlijk gebruik van gegevens verlaagd. Adequate domeinscheiding houdt naast de technische compartimentering in dat functiescheiding kan worden gerealiseerd. Deze scheiding van systemen maakt de handhaving van functiescheidingen beter mogelijk, zodat het niet mogelijk is dat één persoon toegang heeft tot meerdere domeinen, anders dan onder specifieke omstandigheden die relevant zijn voor misbruikbestrijding. Organisatorische functiescheiding binnen Logius is in het huidige ontwerp nog niet volledig uitgewerkt. Logius is verantwoordelijk voor het beheer van DigiD en van BSNk. Indien onvoldoende scheiding wordt aangebracht tussen tussen verantwoordelijkheden binnen DigiD en BSNk kan dit leiden tot functievermenging.

5.4.2. Aanbevelingen

De huidige doelstellingen van DigiD Hoog zijn eenduidig en gelimiteerd beschreven. Het verdient aanbeveling om een meer integrale beschrijving te maken van het volledige DigiD-landschap en -infrastructuur, zodat de verwerkingen van DigiD Basis, Midden, Substantieel en Hoog in samenhang kunnen worden geëvalueerd op privacy- en beveiligingsrisico's. Het gaat dan om alle soorten gegevens, waaronder ook de loggegevens per systeemcomponent en de (log)gegevens die bij dienstverleners worden vastgelegd. Daarbij is een eenduidige beschrijving van het doel van deze gegevens per component noodzakelijk vanuit privacyoptiek. De aanbeveling om aandacht te schenken aan de verwerkingen van persoonsgegevens op technische niveaus kan wellicht worden meegenomen als aanvulling op het register van verwerkingen dat reeds aanwezig is.

Wij bevelen aan nadere maatregelen te ontwerpen en te implementeren die de werkelijke toegang tot systemen en gegevens waarborgen én controleerbaar maken zodat periodieke of wellicht permanente monitoring op de beveiligings- en datakwaliteitsaspecten plaatsvindt en rapportage daarover beschikbaar is. Bij periodieke audits of via permanente monitoring kan dan met minder inspanning meer zekerheid worden verkregen over beveiligings- en datakwaliteitsaspecten. Hiermee bedoelen wij andere controles dan de ad hoc controles die uitgevoerd worden in het geval van vermoeden van identiteitsfraude. Hierbij dient niet beperkt te worden tot gebruikersdata van gebruikers, maar dient ook aandacht besteed te worden aan controles op intern gebruik van systemen. Denk hierbij aan het uitvoeren van interne controles en het detecteren en signaleren van afwijkingen in het gebruik en de werking van het systeem.

Het verdient aanbeveling om, naast de technische compartimentering, ook de organisatorische functiescheiding binnen Logius uit te werken. Het is belangrijk de rollen en verantwoordelijkheden van de verschillende compartimenten uit te werken en het doel en gebruik van de gegevensverzameling te beschrijven per compartiment. Besteed hierbij ook aandacht aan de organisatorische scheiding tussen het beheer van DigiD en het beheer van het BSNk. In de huidige situatie is Logius verantwoordelijk voor zowel het beheer van DigiD als van het BSNk.

5.5. Privacyprincipe: gegevenskwaliteit

Een belangrijk onderdeel van de algemene privacyprincipes is het borgen van de datakwaliteit. Een mix van preventieve en repressieve maatregelen is nodig om de kwaliteit van gegevensverwerkende processen te borgen.

Het doel van DigiD Hoog is het bieden van een betrouwbaar middel voor gebruikers om in te kunnen loggen op het BSN-domein. Controle op de kwaliteit van data hoort daar onlosmakelijk bij. Uiteraard staat controle meestal op gespannen voet met het vertrouwelijkheidsaspect van privacy.

5.5.1. Bevindingen

De persoonsgegevens die worden ingevuld door de gebruiker bij de aanvraag van DigiD kunnen door de gebruiker zelf gewijzigd worden indien deze niet (meer) juist of onvolledig zijn. Daarnaast kan de gebruiker een verzoek doen deze gegevens te wijzigen. Logius heeft geen maatregelen geïmplementeerd om de gebruiker te waarschuwen dat hij regelmatig moet controleren of zijn gegevens (zoals het telefoonnummer en het e-mailadres) nog actueel zijn.

De ten behoeve van DigiD Hoog geraadpleegde validatiegegevens in de Status Controller worden door de DH Authenticatiedienst als juist aangenomen. De voeding van de Status

Controller met de juiste statusinformatie is de verantwoordelijkheid van de RvIG en de RDW. Voor deze gegevens gelden controlemechanismen die buiten de verantwoordelijkheid van Logius vallen.

Voor het waarborgen van de kwaliteit van gegevens binnen de bestaande DigiD en DigiD Substantieel wordt vooral gesteund op preventieve toegangsbeveiligingsmaatregelen die de kwaliteit van de persoonsgegevens moeten borgen en bijvoorbeeld manipulatie of andere menselijke of systeemfouten moeten tegengaan of vermijden. Een voorbeeld hiervan is het beperken van de toegang tot de databases en de logging. Deze maatregelen zullen ook voor DigiD Hoog geïmplementeerd worden. Periodieke controles op de juistheid, nauwkeurigheid en actualiteit van binnen DigiD Hoog opgeslagen persoonsgegevens zijn in het huidige ontwerp niet voorzien. Er is geen nadere informatie over welke check and balances aanwezig zijn om de kwaliteit van de verkregen en vastgelegde persoonsgegevens te waarborgen en hoe daar achteraf verantwoording over kan worden afgelegd. Wel logt de database de veranderingen op tabellen, waarbij is na te gaan wat er verandert in de verschillende databases, waaronder de accounts database.

5.5.2. Aanbevelingen

Wij bevelen aan maatregelen te implementeren om de actualiteit van gegevens te waarborgen. Hierbij kan gedacht worden aan het periodiek versturen van een e-mail waarin de gebruiker wordt herinnerd aan het, indien van toepassing, actualiseren van de gegevens.

Het verdient aanbeveling om interne controlemaatregelen gericht op datakwaliteit en de rapportages daarover nader te beschrijven. Ten behoeve van bewijslast achteraf en om verantwoording af te kunnen leggen over datakwaliteit en de integere werking van systemen zijn naast preventieve controles ook repressieve controles relevant. Te denken valt aan het gebruik van hashing op bepaalde gegevensverzamelingen of het gebruik van de bestaande database replica om de integriteit van (historische) data te kunnen valideren. De beoogde interne controle maatregelen zijn dus andere maatregelen dan de bestaande maatregelen om indicaties van fraude te onderzoeken. Deze controlemaatregelen kunnen mogelijk uitgevoerd worden met behulp van de component die voor DigiD Hoog wordt ontworpen ten behoeve van fraudeonderzoek. Het verdient aanbeveling om de hierboven bedoelde interne controle- en verantwoordingsmaatregelen gericht op de kwaliteit van de persoonsgegevens mee te ontwerpen voor de voorziening ten behoeve van fraudeonderzoek.

5.6. Privacyprincipe: verantwoording

De verwerkingsverantwoordelijke dient verantwoording af te kunnen leggen over de beveiliging van de gegevensverwerking en de geïmplementeerde maatregelen en procedures op strategisch-, tactisch- en operationeel niveau. Hieronder vallen ook de verwerkingen die door de verwerkingsverantwoordelijke zijn uitbesteed aan een verwerker.

De verantwoordelijkheid voor DigiD is duidelijk geregeld. Het ministerie van BZK is verwerkingsverantwoordelijke en de uitvoering is belegd bij Logius, een onderdeel van het ministerie van BZK. Met partijen die de rol van verwerker hebben zijn of worden (sub)verwerker overeenkomsten afgesloten. Voor DigiD Hoog worden geen nieuwe partijen als (sub)verwerker aangesteld.

Voor het aanvraag-, productie- en uitgifteproces zijn de middelenuitgevers (RDW en RvIG) verantwoordelijk. Voor het authenticatieproces is Logius verantwoordelijk. In het authenticatieproces wordt de geldigheid van een WID geverifieerd door een bevraging te doen

naar de Status Controller. De Status Controller wordt door de RvIG en de RDW gevoed met statusinformatie en valt ook onder de verantwoordelijkheid van deze middelenuitgevers.

5.6.1. Bevindingen

Logius maakt op haar beurt gebruik van subverwerkers voor de levering van IT-diensten. Vanuit de ontwerpdocumentatie van DigiD Hoog valt nog niet op te maken in welke mate de realisatie van DigiD Hoog effecten heeft op de verhoudingen met bestaande (sub)verwerkers.

5.6.2. Aanbevelingen

Het verdient aanbeveling om na te gaan of de nieuw beoogde werking van de keten met RvIG en RDW via de Status Controller gevolgen heeft voor de te maken afspraken met deze partijen. Met bestaande (sub)verwerkers moeten overeenkomsten mogelijk aangepast worden en voor eventuele nieuwe (sub)verwerkers moeten (sub)verwerkersovereenkomsten afgesloten worden.

5.7. Privacyprincipe: beveiliging van gegevens

Passende technische en organisatorische beveiligingsmaatregelen dienen te worden genomen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De AVG spreekt van een passend niveau van beveiliging, rekening houdend met de stand van de techniek en de uitvoeringskosten, afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens. De verwerkingsverantwoordelijke moet de beveiliging van de data permanent kunnen garanderen.

5.7.1. Bevindingen

In het huidige ontwerp hanteert Logius de bewaartermijnen zoals opgenomen in paragraaf 3.7. Het doel van het bewaren van deze historische gegevens is het nakomen van wettelijke verplichtingen, het kunnen controleren van de integriteit van de verzamelde data en het afleggen van verantwoording daarover. Een ander doel is het kunnen uitvoeren van onderzoek naar vermeende fraudegevallen op basis van specifieke casusposities of het verrichten van onderzoek naar aanleiding van klachten. De bewaartermijnen hebben een wettelijke grondslag in het Besluit GDI, maar Mazars plaatst hier ook een aantal kanttekeningen bij:

- De reden voor het bewaren van de transactiegegevens ligt in het creëren van de mogelijkheid om tot vijf jaar terug identiteitsfraude te kunnen detecteren en analyseren en inzage te kunnen verschaffen aan betrokkenen in de inloghistorie;
- Een nadeel van het vastleggen van deze transactiegegevens is dat hoe langer ze bewaard worden, hoe meer inloginformatie verzameld wordt over het gedrag van de gebruikers als gevolg van het gebruik van DigiD. Deze inloggegevens kunnen privacygevoelig zijn. Hoe groter het bestand wordt, hoe groter de waarde van het bestand wordt en hoe groter het risico van misbruik wordt voor de gebruikers;
- De bewaartermijnen van transactiegegevens over inloggedrag van gebruikers liggen in de maatschappij gevoelig.

Met de introductie van DigiD Hoog en het gebruik van PI en PP worden de risico's van misbruik van de inloghistorie gemitigeerd. Belangrijk is om te onderkennen dat deze maatregel pas effectief is als DigiD Hoog volledig is gerealiseerd en ook de reeds bestaande DigiD-voorzieningen op dezelfde wijze werken.

Logius heeft beveiligingsmaatregelen getroffen om de persoonsgegevens te beschermen. Voor het uitlezen van de chip op het WID wordt gebruik gemaakt van middleware. End-to-end

encryptie is aanwezig tussen de eID client (apparaat met NFC lezer en DigiD client software) en de eID server. De DigiD client software geeft een redirect url naar de eID server waarna de eID server een beveiligd kanaal opzet om gegevens uit de chip te lezen, door het gebruik van het PACE-protocol. Het PACE-protocol is een Europees protocol voor authenticatiediensten. Tweezijdige authenticatie vindt plaats tussen de applet en de eID server om vast te stellen dat de chip authentiek is en dat de eID server bevoegd is gegevens uit te lezen. Voor het uitwisselen van de PI en het PP tussen de eID server en de CIS wordt gebruik gemaakt van SAML. Dit is een op XML gebaseerde standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen domeinen. In paragraaf 4.4.1 zijn de getroffen beveiligingsmaatregelen opgenomen van de bestaande DigiD. Deze gelden ook voor de nieuwe of gewijzigde componenten voor DigiD Hoog.

In de huidige ontwerpdocumentatie is weinig aandacht besteed aan de maatregelen voor interne beheersing voor wat betreft het controleren van de toegang tot data en het gebruik van de data. Er wordt verwezen naar normen voor informatiebeveiliging die vooral toezien op de procedurele kant van Information Security Management Systemen, waaronder de BIR, en niet direct op de werking van de gerealiseerde beveiligingsmaatregelen in de IT werkelijkheid.

5.7.2. Aanbevelingen

De wettelijke bewaartermijnen zijn in het besluit GDI verhoogd naar vijf jaar voor de inloghistorie van gebruikers. Het gevolg is het ontstaan van een meer risicovolle en omvangrijke dataset. Hierdoor verdient het aanbeveling om na te gaan of de getroffen beveiligingsmaatregelen nog in lijn zijn met de risico's die deze bewaartermijnen met zich meebrengen. Voor het ontwerp van DigiD Hoog geldt dat deze risico's in belangrijke mate worden gemitigeerd als het concept van DigiD Hoog volledig is geïmplementeerd, door het gebruik van polymorfe pseudoniemen en polymorfe identiteiten in plaats van het BSN van de gebruiker. Additionele maatregelen kunnen zijn: encryptie of hashing van gevoelige data zoals IP-adressen en monitoring en periodieke rapportage over de toegang tot gegevens. Onderzoek hierbij ook de risico's van netwerkcomponenten over de hele technologische keten die eveneens metadata genereren die informatie kunnen onthullen over gebruikers. Denk hierbij aan componenten als intrusion detection systemen en firewalls.

Logius is voornemens om de concepten van DigiD Hoog ook toe te gaan passen op DigiD Basis, Midden en Substantieel. Zolang dit niet gerealiseerd is, verdient het aanbeveling om na te gaan of de getroffen beveiligingsmaatregelen in de tussenliggende periode nog in lijn zijn met de risico's die deze bewaartermijnen met zich meebrengen. Onderzoek hierbij of de huidige beveiligingsmaatregelen van DigiD Basis, Midden en Substantieel voldoende recht doen aan de gevoeligheid van de omvangrijke verzameling van inlogacties door gebruikers. Betrek hierbij de risico's van profiling en de gevolgen van datalekken voor de gebruikers. Als alternatieve benadering kan worden nagegaan of de DigiD Hoog concepten versneld, of wellicht in delen versneld, kunnen worden uitgerold over de bestaande DigiD voorzieningen.

5.8. Privacyprincipe: transparantie

Gebruikers dienen geïnformeerd te worden over het gebruik van hun persoonsgegevens in samenhang met de gebruikte technologie. Dit stelt de gebruiker in staat om bepaalde vormen van verwerking of onrechtmatig gedrag in rechte aan te vechten.

5.8.1. Bevindingen

Het ontwerp van DigiD Hoog gaat niet in op de transparantheid en communicatie naar gebruikers over het gebruik van DigiD Hoog. Wij onderschrijven dat transparantie naar

gebruikers voorafgaand aan de implementatie vragen zal oproepen en zal leiden tot onduidelijkheid bij gebruikers. De aanbevelingen hieronder zijn dan ook bedoeld als adviespunten die kunnen worden meegenomen tijdens of na de implementatie van DigiD Hoog.

5.8.2. Aanbevelingen

Het verdient aanbeveling om gebruikers van DigiD Hoog bij het activeren en het gebruik van een DH-middel op de hoogte te stellen van de verwerking en het doel van de gegevensverwerking door een verwijzing op te nemen naar de privacyverklaring. De privacyverklaring dient uitgebreid te worden met de gegevens die additioneel verwerkt worden voor DigiD Hoog. Hierbij is het vooral relevant om aan te geven dat een gebruiker, voordat hij zijn WID scant, op de hoogte wordt gesteld wat er gebeurt bij het scannen van het WID. Aanbevolen wordt transparant te maken dat controle plaatsvindt met statusinformatie uit de BRP of het CRB, welke gegevens worden verwerkt (ook dat dit gepseudonimiseerd gebeurt) en wat het doel van deze verwerking is.

5.9. Privacyprincipe: rechten van betrokkenen

Gebruikers hebben, naast het recht van transparantie, het recht op inzage, correctie, aanvulling, afscherming of verwijdering van hun persoonsgegevens of zich tegen de verwerking ervan te verzetten.

De gebruiker van DigiD kan zijn gebruikersnaam, telefoonnummer, BSN, e-mailadres en gebruiksgeschiedenis inzien door in te loggen op mijn.digid.nl. Het telefoonnummer, e-mailadres en wachtwoord kunnen hier door de gebruiker zelf worden gewijzigd. Ook kan de gebruiker een inzageverzoek indienen bij Logius en een verzoek doen voor het verbeteren, aanvullen, verwijderen of afschermen van gegevens, tenzij dit niet is toegestaan op grond van een wettelijke bepaling.

De gebruiker kan zelf zijn account verwijderen of een verzoek doen het DigiD-account op te heffen. Indien een dergelijk verzoek wordt gedaan wordt het account, inclusief alle bijbehorende gegevens verwijderd. In de transactielog blijven de gegevens uiteraard wel beschikbaar conform de vastgestelde bewaartermijn. Bij kritieke activiteiten in de beheermodule, zoals het verwijderen van een account, wordt het vier-ogenprincipe afgedwongen. Het DigiD-account kan geblokkeerd worden op verzoek van de gebruiker, bijvoorbeeld ter voorkoming van fraude. Indien de gebruiker een DH-middel wil blokkeren of verwijderen verstrekt de gebruiker zijn BSN aan de Servicedesk. De Servicedesk vraagt met het BSN van de gebruiker bij het niet-pseudonieme domein informatie op die benodigd is om het DH-middel te blokkeren of te verwijderen. Een harde opt-out is mogelijk door gebruik te maken van de intrekkingscode die al voor initiële activering gebruikt kan worden. Een intrekkingsverzoek leidt altijd direct tot het niet meer kunnen gebruiken van het DH-middel. Een intrekking door de gebruiker heeft alleen betrekking op het DH-middel en niet op het WID.

5.9.1. Bevindingen

Het ontwerp van DigiD Hoog beschrijft niet gedetailleerd hoe invulling wordt gegeven aan het inzagerecht dat gebruikers hebben. Het is nog niet bekend hoe een verzoek tot inzage, verbetering of aanvulling van gegevens in behandeling zal worden genomen in een pseudoniem-gebaseerde omgeving. In de huidige DigiD wordt de gebruiker geïdentificeerd door het verstrekken van het BSN en het beantwoorden van een aantal persoonlijke vragen. In DigiD Hoog kan de identiteit van de gebruiker niet worden vastgesteld aan de hand van het BSN.

5.9.2. Aanbevelingen

Het verdient aanbeveling gedetailleerd te beschrijven hoe invulling wordt gegeven aan het inzagerecht dat gebruikers hebben tot hun eigen gegevens en hoe de identiteit van de gebruiker in een pseudoniem-gebaseerde omgeving wordt vastgesteld.

6. Bronnen

Literatuurlijst

College Bescherming Persoonsgegevens. (2013, februari). *CBP Richtsnoeren - Beveiliging van persoonsgegevens.* Opgehaald van https://www.autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

Commissie. (2015, september 8). Uitvoeringsverordening (EU) 2015/1502 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronisch identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014. *Publicatieblad van de Europese Unie*.

DigiD. (2016). *Privacyverklaring DigiD en DigiD Machtigen*. Opgehaald van DigiD: https://www.digid.nl/privacyverklaring/

Europees Parlement en de Raad. (2014, juli 23). Verordening (EU) Nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG. *Publicatieblad van de Europese Unie*.

(2017). *Gegevensbeschermingseffectbeoordeling (GEB) eID-stelsel v1.0.*

Logius. (2015). *Bewerkersovereenkomst Logius - Capgemini Nederland BV.*

Logius. (2016). *DigiD Beveiligingsvoorschrift - Logische Toegangsbeveiliging.*

Logius. (2016). *DigiD Beveiligingsvoorschrift - Omgang met informatie.*

Logius. (2016). *DigiD Beveiligingsvoorschrift - Transport Layer Security (TLS).*

Logius. (2016). *DigiD Beveiligingsvoorschrift - Vulnerability Management.*

Logius. (2016). *DigiD Informatiebeveiligingsbeleid.*

Logius. (2017). *DigiD Hoog Koppelvlakspecificatie - DH AH voor MU v0.9.*

Logius. (2017). *Fraude detectie en onderzoek in een polymorfe omgeving.*

Logius. (2017, april 7). *Jaarverslag 2016*. Opgehaald van Logius online-magazine: https://logius.online-magazine.nl/nl/magazine/11769/818894/cover.html

Logius. (2017). *Project Start Architectuur - DigiD Hoog versie 0.99.*

Logius. (2017). *PvA - Programma DigiD Hoog met eRijbewijs & eNIK v0.5.*

Mazars. (2017). *Privacy Impact Assessment DigiD Substantieel v1.1.*

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2017). *Procedurebeschrijvingen Logius - Melden datalekken.*

OECD. (2013). *OECD Guidelines on the protection of privacy and transborder flows of personal data*. Opgehaald van OECD: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

RDW. (2017). *DigiD Hoog Koppelvlakspecificatie - RDW als MU voor DH v0.95.*

RDW. (2017). *eID statussen en daaraan gerelateerde berichtuitwisseling v13.*

RDW, & Logius. (2017). *DigiD Hoog Koppelvlakspecificatie - BSNk-PP voor MU v0.84.*

Rijksoverheid. (2013). *Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst.*

Staatsblad van het Koninkrijk der Nederlanden. (2016, mei 17). 195 Besluit verwerking persoonsgegevens generieke digitale infrastructuur.

Staatscourant. (2015, februari 26). Autorisatiebesluit DigiD, Rijksdienst voor Identiteitsgegevens.

Staatscourant. (2015, april 15). Instellingsbesluit besturing elektronische toegangsdiensten nr. WJZ/15023462.

Staatscourant. (2015, oktober 23). Regeling voorzieningen GDI, nr. 2015-609536.

Staatscourant. (2017, maart 27). Aanwijzigingsbesluit Logius als belanghebbende van het Reglement rijbewijzen.

7. Interviews

Naast het raadplegen van bovenstaande bronnen zijn met de volgende functionarissen van Logius interviews gehouden:

- Architect
- Beleidsmedewerker
- Communicatiemedewerker
- Functioneel ontwerper DigiD Hoog
- Informatiebeveiliger
- Jurist
- Ketenbeheerder
- Productmanager Implementatie
- Productmanager Toegangsdiensten
- Projectleider DigiD Hoog
- Technisch projectleider

Bijlage I: Vragenlijst PIA

Per privacy principe worden bij benadering de volgende risico's gesignaleerd:

Privacy principe		Privacyrisico's								
		ID	DD	FC	IV	NT	NE	DL	OB	GC
II	Limiteren van het verzamelen van gegevens	x	x	x				x		x
III	Doelbinding / limiteren van het gebruik van gegevens	x	x	x		x	x	x		x
IV	Gegevenskwaliteit	x							x	
V	Verantwoording		x	x	x	x	x	x		
VI	Beveiliging van gegevens	x	x	x			x		x	
VII	Transparantie					x	x	x	x	
VIII	Rechten van betrokkenen					x	x	x	x	x

De afkorting in de tabel hebben de volgende betekenis:

- ID: Identiteitsfraude
- DD: 'Data deluge'-effect
  - Waardestijging van persoonsgegevens
- FC: 'Function creep'
  - Gebruik van persoonsgegevens voor andere doeleinden dan waarvoor deze oorspronkelijk verzameld zijn
  - Profileren
- IV: Inconsistente implementatie en naleving verantwoordingsbeginsel
- NT: Geheime (niet transparante) verwerking van persoonsgegevens
- NE: Niet toegestane verwerking van persoonsgegevens buiten de EU
- DL: Data lekken
- OB: Omkering van de bewijslast voor de betrokkene
- GC: Consumenten worden gedwongen om in te stemmen met het gebruik van hun gegevens

Voor een gedetailleerde uitleg van de universele privacy principes verwijzen wij naar Bijlage III en Bijlage IV.

In de linker kolom van onderstaande tabel zijn de vragen opgenomen, geordend naar privacy principe, die behandeld zijn in de PIA. De rechter kolom geeft de bevindingen en eventuele risico's en aanbevelingen weer.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
I	**Basisinformatie: type persoonsgegevens, type verwerking en verantwoordelijke(n)**	Inherent aan de doelstellingen van DigiD Hoog worden persoonsgegevens verwerkt waaronder inloggegevens, (in de toekomst gepseudonimiseerde) burgerservicenummers, (in de toekomst versleutelde) IP-adressen, kenmerken van identiteitsdocumenten en andere tot een natuurlijk persoon te herleiden gegevens. De minister van BZK is verwerkingsverantwoordelijke voor deze verwerkingen en heeft de uitvoering hiervan belegd bij Logius. Hiermee is de relevantie van de PIA aangetoond. Een PIA heeft betrekking op de bescherming van de privacy van gebruikers. Het recht op privacy is onder meer geregeld in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) en artikel 10 van de Grondwet. In een PIA heeft privacy vooral betrekking op de bescherming van persoonsgegevens. Het gaat hier om de zogenaamde 'informationele privacy'. Voordat met de uitvoering van de onderhavige PIA wordt gestart, dient de vraag te worden beantwoord of persoonsgegevens van gebruikers worden verwerkt. Artikel 1 van de Wbp geeft aan wat onder een persoonsgegeven moet worden verstaan: 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'. DigiD Hoog is een doorontwikkeling en uitbreiding van de bestaande DigiD. Bestaande componenten en beveiligingsmaatregelen worden hergebruikt en de bestaande authenticatiemechanismen op basis van gebruikersnaam en wachtwoord (en optioneel sms) en gebruikersnaam en DigiD app blijven voorlopig gehandhaafd en beschikbaar voor gebruikers en dienstverleners, naast het authenticatieniveau Hoog. Hiermee wordt een geleidelijke overgang bewerkstelligd en is de continuïteit van de bestaande administratie van de inloghistorie van gebruikers gegarandeerd. Het is de bedoeling van Logius om de cryptografische en andere aanvullende maatregelen die in de doorontwikkeling van DigiD Hoog worden gerealiseerd ook in te voeren voor DigiD Substantieel en de bestaande DigiD. Hierdoor worden bestaande privacyrisico's van DigiD Substantieel en de bestaande DigiD gereduceerd en ook beter beheersbaar. Naast de eindsituatie van DigiD Hoog richt deze PIA zich ook op de verwachte beginsituatie van DigiD Hoog. In de eerste fase zijn privacybevorderende maatregelen nog in beperkt mate geïmplementeerd. **Conclusie** Een belangrijke conclusie uit deze PIA is dat de realisatie van de eindsituatie van DigiD Hoog privacyrisico's in DigiD doet afnemen. De cryptografische en andere aanvullende maatregelen die in de doorontwikkeling van DigiD Hoog worden gerealiseerd gelden voor zowel DigiD Hoog als DigiD Substantieel en de bestaande DigiD en beperken de privacyrisico's verder.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		Aanbevelingen Ten tijde van de eerste implementatie van DigiD Hoog zullen de privacyrisico's van de bestaande DigiD grotendeels nog van toepassing zijn en door het gebruik van gemeenschappelijke systeemcomponenten en -functies ook gelden voor DigiD Hoog. Het is daarom belangrijk dat de doorontwikkeling zoals is voorgenomen wordt doorgezet en afgerond en dat uiteindelijk de middelen en concepten van het nu bestaande DigiD systeem worden omgebouwd en/of de risico's daarvan worden gemitigeerd. Op de bestaande DigiD is niet eerder een integrale PIA uitgevoerd. Wel is (en wordt) bij het doorvoeren van veranderingen aan DigiD aandacht besteed aan de eisen van de Wbp. Een integraal overzicht van privacyrisico's van de bestaande DigiD is niet voorhanden. Het verdient aanbeveling om bij de doorontwikkeling van DigiD een integrale privacyrisicoanalyse uit te voeren op de organisatorische en technische maatregelen van DigiD Substantieel en DigiD Hoog, inclusief de bestaande DigiD en de onderliggende infrastructuur.
I.1	Is sprake van een verwerking van persoonsgegevens (volgens de definities van de Wbp?)	Ja, in het domein van DigiD Hoog worden persoonsgegevens verzameld en verwerkt van gebruikers die een DH-middel gebruiken. De gegevens die worden verwerkt zijn onder andere: PI en PP, BSN (in de eindsituatie niet meer), WID-nummer (in de eindsituatie niet meer) en IP-adres (in de eindsituatie naar verwachting in versleutelde vorm). Genoemde gegevens zijn persoonsgegevens volgens de Wbp en AVG. Een belangrijke eigenschap van DigiD Hoog is het gebruik van PI en PP binnen verschillende componenten. De PI is alleen te herleiden naar het BSN van de gebruiker met een encryptiesleutel die middels een gereguleerd proces kan worden verkregen van het BSNk, een externe bron die buiten de verantwoordelijkheid van Logius ligt. Er is sprake van persoonsgegevens omdat het mogelijk is, dan wel met behulp van een sleutel verkregen van een externe bron, de identiteit van de gebruiker te bepalen. In de eerste fase vindt het gebruik van pseudoniemen alleen nog plaats op de chip van het WID en in de gegevensstromen en componenten tussen de gebruiker en de authenticatiedienst bij het inlogproces (middleware). Voor de verdere verwerking in het proces wordt het BSN gebruikt, dat vroegtijdig in het authenticatieproces wordt ontsleuteld op basis van de polymorfe identiteit. Hierdoor is bij de authenticatiedienst en andere tussenliggende partijen in de authenticatieketen bekend welke gebruiker inlogt. Naarmate het project vordert zal het BSN steeds later in het authenticatieproces ontsleuteld worden. In de toekomst is bij de DH Authenticatiedienst en het BSNk niet bekend welke gebruiker bij welke dienstverlener inlogt. De PI en het PP worden in de eindsituatie pas bij de ontvangende dienstverlener ontsleuteld naar een BSN. DigiD maakt gebruik van sessie en persistente cookies en deze zijn niet specifiek voor DigiD Hoog. In deze cookies worden geen persoonsgegevens gebruikt. De cookies zijn nodig om te zorgen dat DigiD kan werken met de verschillende applicatie servers die gebruikt worden. Teneinde het gebruik van de app te kunnen

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		volgen en analyseren wordt gebruik gemaakt van Piwik. Piwik is een opensourceprogramma om bezoekersstatistieken bij te houden. Piwik houdt hiervoor geanonimiseerde gebruiksgegevens bij. Ook voor Piwik wordt voor de DigiD app niets met cookies gedaan ten aanzien van gebruiksgegevens. Voor de DigiD-website gaan in de toekomst wel cookies gebruikt worden voor Piwik met gebruiksgegevens, alleen zullen de gegevens niet te herleiden zijn naar een persoon. De sessie en persistente cookies zijn van tijdelijke aard: de sessie cookies worden opgeruimd na de sessie en de persistente cookies nadat het proces van aanvragen is beëindigd of totdat de loadbalancer die opruimt. Op dit moment is nog in onderzoek of het IP-adres in de eindsituatie van DigiD Hoog in de transactielog moet worden opgenomen of niet. Indien het IP-adres wordt opgenomen is de verwachting dat dit in versleutelde vorm zal gebeuren. Zolang aan deze randvoorwaarde is voldaan heeft dat geen invloed op de conclusies van deze PIA.
I.2	Kan uw organisatie als verantwoordelijke worden aangemerkt voor de verwerking of treedt u op als verwerker (uw organisatie verwerkt de persoonsgegevens in opdracht en onder verantwoordelijkheid van een andere organisatie)?	De minister van BZK is verwerkingsvantwoordelijke en de uitvoering is belegd bij Logius, een onderdeel van het ministerie van BZK. Ten opzichte van de bestaande DigiD en DigiD Substantieel heeft DigiD Hoog nieuwe stakeholders, namelijk de middelenuitgevers en registerhouders waaronder RvIG en RDW.
I.3	Andere specifieke persoonsgegevens?	
I.3a	Is het de bedoeling om gegevens over de financiële of economische situatie van betrokkenen of andere gegevens met een verhoogde gevoeligheid of die kunnen leiden tot stigmatisering of uitsluiting te verwerken?	Nee, dit is niet het doel. DigiD facilitieert dat bij dienstverleners kan worden ingelogd. Het inloggen bij specifieke dienstverleners kan, vanwege de aard van de activiteiten van deze dienstverleners, leiden tot de verwerking van gevoelige gegevens. DigiD Hoog wordt geplaatst op het bestaande DigiD-systeem en de bestaande technische componenten. Ten tijde van de eerste implementatie wordt in de transactielogging van het gebruik van DigiD nog het BSN vastgelegd. Hierdoor is bekend bij welke dienst de gebruiker heeft ingelogd en ontstaat een omvangrijke cumulatie van inloghistorie. Deze inloghistorie is een gevoelig en waardevol bestand op basis waarvan profielen van gebruikers opgesteld zouden kunnen worden (bijvoorbeeld via offline analyse). Hiermee kan indirect een beeld worden verkregen over mogelijk stigmatiserende situaties van een gebruiker. Denk hierbij aan gebruikers die met hun DigiD inloggen bij dienstverleners voor schuldhulpverlening of uitkeringsinstanties. Logius geeft nadrukkelijk aan dat profileren geen activiteit is waar zij zich mee bezighoudt of van plan is zich mee bezig te houden. In de doorontwikkeling van DigiD Hoog zullen huidige DigiD systemen omgebouwd worden en de transactielog volledig pseudoniem werken. Het BSN kan alleen via een gecontroleerd proces ontsleuteld worden voor specifieke doeleinden zoals fraudeonderzoek. Hierdoor is niet zondermeer bekend welke gebruiker bij welke

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		dienstverlener heeft ingelogd. Deze maatregelen reduceren de risico's op mogelijke stigmatisering of uitsluiting verregaand. Op dit moment is nog in onderzoek of het IP-adres in de eindsituatie van DigiD Hoog in de transactielog moet worden opgenomen. Indien het IP-adres wordt opgenomen is de verwachting dat dit in versleutelde vorm zal gebeuren. Indien het IP-adres niet versleuteld wordt opgenomen en het bestand in handen komt van kwaadwillenden bestaat het risico dat met externe bronnen de identiteit van de gebruiker herleid kan worden en op deze manier een beeld kan worden verkregen over welke gebruiker bij welke dienstverlener heeft ingelogd. **Aanbevelingen** Het is belangrijk dat de doorontwikkeling zoals is voorgenomen wordt doorgezet en afgerond en dat uiteindelijk de middelen en concepten van het bestaande DigiD-systeem worden omgebouwd en de risico's daarvan worden gemitigeerd. Om privacyrisico's nog verder te reduceren verdient het aanbeveling in de vervolgontwerpfasen het IP-adres te versleutelen indien dit gegeven opgenomen is de transactielog. Indien het bestand met inloghistorie in handen komt van kwaadwillenden neemt de impact hierdoor af. Onderzoek hierbij ook de risico's van netwerkcomponenten over de hele technologische keten die eveneens metadata genereren die informatie kunnen onthullen over gebruikers. Denk hierbij aan intrusion detection en prevention systemen, DDoS systemen en firewalls. In de ontwerpdocumentatie, aanvullend op de PSA, worden deze componenten beschreven. In het kader van deze PIA op de PSA van DigiD Hoog is dit niet nader onderzocht.
I.3b	Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?	Nee, dit is niet de bedoeling. Door de inloghistorie die ontstaat, zoals beschreven in I.3a, is het onvermijdelijk dat bij het gebruik van DigiD Hoog ook gegevens over kwetsbare personen worden verwerkt, aangezien de gebruikers alle Nederlandse burgers kunnen zijn. Als een gebruiker DigiD gebruikt om in te loggen bij een dienstverlener die specifiek diensten aanbiedt aan een kwetsbare groep kan in de huidige situatie via data-analyse en profiling achterhaald worden welke gebruikers tot welke kwetsbare groepen behoren. Denk hierbij aan de inloghistorie van gebruikers die met hun DigiD inloggen bij organisaties voor schuldhulpverlening, medisch gerelateerde diensten en uitkeringsinstanties. Zoals ook bij 1.3a genoemd zal in de doorontwikkeling van DigiD Hoog de huidige DigiD systemen worden omgebouwd worden en de transactielog volledig pseudoniem werken. Het BSN kan in de eindsituatie van DigiD Hoog alleen via een gecontroleerd proces ontsleuteld worden voor specifieke doeleinden zoals fraudeonderzoek. Hierdoor kan niet zondermeer achterhaald worden welke gebruikers tot kwetsbare groepen behoren. **Aanbevelingen** Zie de tekst onder I.3a.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
I.3c	Is het de bedoeling gebruikersnamen, wachtwoorden of andere inloggegevens te verwerken?	Ja, in het domein van DigiD Hoog worden accountgegevens van een gebruiker van DigiD verzameld, waaronder het e-mailadres en de gebruikersnaam van het account. Voorts worden ook andere gegevens vastgelegd welke gebruikt zijn bij het inlogproces en de validatie van gegevens. Zie antwoorden bij vraag 1.3e.
I.3d	Is het de bedoeling om uniek identificerende gegevens, zoals biometrische gegevens, te verwerken?	Nee, het is niet de bedoeling om uniek identificerende gegevens te verwerken.
I.3e	Is het de bedoeling om het BSN-nummer of een ander persoonsgebonden nummer te verwerken?	Ja, in de eerste implementatie van DigiD Hoog is het de bedoeling om het BSN te verwerken. In de eindsituatie van de doorontwikkeling van DigiD Hoog zal het BSN uiteindelijk niet meer worden verwerkt, maar vervangen worden door PI en PP. Om in te loggen met DigiD Hoog wordt een WID gescand waar een PI en PP op staat, gebaseerd op het BSN van de gebruiker. Ten tijde van de eerste implementatie wordt bij het verkregen PI en PP vroeg in het proces vertaald naar een BSN. De accountgegevens en de transactielogging bevatten in deze situatie nog het BSN. Met de doorontwikkeling van DigiD Hoog zal het BSN-gebruik sterk teruggedrongen worden. Het uiteindelijke doel is dat alleen de ontvangende dienstverlener het BSN kan herleiden uit het PI en PP. Hiermee wordt bereikt dat de DH Authenticatiedienst geen beschikking heeft over het BSN en het niet eenvoudig mogelijk is om de inloggeschiedenis van een gebruiker te achterhalen. In bijzondere gevallen kan met sleutelmateriaal de pseudonimisering van een BSN opgeheven worden. Overigens is het gebruik van DigiD Hoog alleen geschikt om gebruikt te worden binnen het BSN-domein. Verder gebruik in het private domein is uitgesloten. Het is nadrukkelijk niet de doelstelling van de PSA DigiD Hoog om de gehele authenticatiedienst pseudoniem te maken in de zin dat deze de gebruiker niet meer kent. Op termijn zou een dergelijke architectuur wel te realiseren zijn en de beschreven PSA kan ook gezien worden als een eerste plateau op weg naar een dergelijk lange termijn einddoel. Een dergelijk einddoel is nu echter niet geformaliseerd, aangezien het niet duidelijk is hoe de verdere evolutie van privacybescherming in de USvE zal worden vormgegeven. **Aanbevelingen** Het is belangrijk dat de doorontwikkeling zoals is voorgenomen wordt doorgezet en afgerond en dat uiteindelijk de middelen en concepten van het bestaande DigiD-systeem worden omgebouwd en de risico's daarvan worden gemitigeerd. De overgang van een BSN-gebaseerde transactielog naar een volledig pseudoniem-gebaseerde transactielog leidt tot de afname van privacyrisico's.
I.3f	Is het de bedoeling om andere bijzondere persoonsgegevens te verzamelen of te verwerken (zoals gegevens omtrent godsdienst, ras, politieke of seksuele voorkeur, strafrechtelijk verleden, etc.)?	Nee, het is niet de bedoeling om gegevens omtrent godsdienst, ras, politieke of seksuele voorkeur en strafrechtelijk verleden te verzamelen of te verwerken. In de metadata die wordt verzameld door middel van transactielogging is het niet uitgesloten dat dit soort gegevens echter wel herleid kunnen worden. De doorontwikkeling van DigiD Hoog draagt bij aan reducering van dit risico. Zie de voorafgaande opmerkingen en toelichting hierover bij vraag I.3a.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		Aanbevelingen Het is belangrijk dat de doorontwikkeling van DigiD Hoog wordt doorgezet en afgerond zodat het herleiden van de gegevens tot een natuurlijk persoon bemoeilijkt worden.
I.4	Gaat het bij het project/systeem om het gebruik van nieuwe/andere technologieën of informatiesystemen of de invoer van bestaande technologie in een nieuwe context?	Ja, nieuwe technologieën en informatiesystemen worden gebruikt om het inlogproces met een DH middel mogelijk te maken. Ook worden bestaande componenten van DigiD aangepast voor DigiD Hoog. De gebruiker dient iedere keer bij het inloggen met DigiD Hoog de NFC chip van een WID-document te scannen voor het uitlezen van PI en PP. De volgende componenten zijn nieuwe componenten die ontworpen worden voor DigiD Hoog: ▪ Middleware (eID Server en eID Client) ▪ CIS-DH ▪ CTS ▪ Transactielogger (DigiD Logger) ▪ Fraudelogger ▪ DH Authenticatiedienst ▪ DH Status beheer koppelvlak ▪ DH Status Controller ▪ DH Intrekkingsservice ▪ DH Deblokkeringsservice ▪ HSM De volgende componenten zijn bestaande componenten die aangepast worden voor DigiD Hoog: ▪ Mijn DigiD ▪ DigiD Beheer ▪ DigiD Kern ▪ DigiD Helpdesk ▪ DigiD Servicecentrum ▪ Publicatiedienst Authenticatiedienst (DigiD Website) De volgende componenten van het BSNk zijn gezamenlijke voorzieningen die in het kader van de USvE worden gerealiseerd. Deze vallen niet onder de verantwoordelijkheid van Logius: ▪ BSNk PP ▪ BSNk IR ▪ BSNk Sleutelbeheer Voorgaande opsomming is beperkt tot de componenten die benodigd zijn voor het kunnen inloggen met een DH-middel. De componenten die benodigd zijn bij de MU en de dienstverlener voor het aanvragen, produceren en uitreiken van een DH-middel zijn in voorgaande opsomming niet meegenomen.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
I.5	Is er sprake van gebruik van technologie die bij het publiek vragen of weerstand op kan roepen (zoals locatie- of volgsystemen op basis van GPS, mobiele technologie, gezichtsherkenning in samenhang met cameratoezicht)?	Ja, er wordt gebruik gemaakt van nieuwe technologie om het BSN te pseudonimiseren en te randomiseren. Voor het uitlezen van de chip op het WID wordt nieuwe technologie gebruikt: de eID server en de eID client. De eID client is een apparaat met NFC lezer en DigiD client software. Het gebruik van polymorfe identiteiten en polymorfe pseudoniemen is in de praktijk nog niet eerder geïmplementeerd en weinig getest. Doordat er weinig bekend is over deze technologie zal dit vragen oproepen bij het publiek. Het is ook niet uit te sluiten dat het gebruik van deze technologie bij een gedeelte van het publiek tot weerstand zou kunnen leiden.
I.6	Is er sprake van (andere) grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij wordt gebruikt?	Ja, de ontwikkeling van DigiD Hoog is op zichzelf een verschuiving in zowel de manier waarop persoonsgegevens worden verwerkt als in de technologie die daarvoor wordt gebruikt. De middelenuitgevers (RvIG en RDW) zijn verantwoordelijk voor de productie van het WID met de NFC chip. De stelselvoorzieningen BSNk PP, BSNk IR en BSNk SB zijn nieuwe voorzieningen die ook bijbehorende organisatorische veranderingen vereisen. Ook de gemeenten als aanvraag- en uitgifteloket krijgen aanvullende taken. Logius blijft verantwoordelijk voor het authenticatieproces. Een belangrijke verschuiving is dat geen WID-gegevens direct van de RvIG en de RDW worden opgehaald maar dat de statusinformatie van documenten wordt opgehaald bij de Status Controller. De Status Controller wordt gevoegd en geactualiseerd door de RvIG en RDW. Een directe koppeling met de middelenuitgevers voor het ophalen van statusinformatie in het authenticatieproces is bij DigiD Hoog niet aanwezig. De wijze waarop persoonsgegevens worden verwerkt verschuiven gedurende de implementatie van DigiD Hoog. DigiD Hoog wordt geplaatst op de huidige systemen en componenten van DigiD. Ook worden nieuwe componenten voor DigiD Hoog gerealiseerd. In de beginsituatie van DigiD Hoog vindt de vertaling van het PI en PP al vroeg in het proces plaats. In een groot deel van de keten, waaronder in de transactielog, wordt in deze situatie nog het BSN verwerkt. Gedurende de implementatie wordt de polymorfe identiteit steeds op een later moment in de keten ontsleuteld naar het BSN. Uiteindelijk zal in de gehele keten bij Logius geen BSN meer worden verwerkt bij het gebruik van een DH-middel en wordt de polymorfe identiteit pas bij de ontvangende dienstverlener het BSN ontsleuteld van de gebruiker.
I.7	Kan de manier waarop de gegevens worden verzameld worden opgevat als privacygevoelig?	Nee, de invoering van geavanceerde cryptografische beschermingen en de compartimentering van domeinen maken het geheel minder privacygevoelig. In de eerste fase zal nog niet in de gehele keten met pseudoniemen gewerkt worden en is compartimentering nog niet volledig gerealiseerd waardoor deze privacybevorderende maatregelen op het moment van de eerste release nog niet worden gerealiseerd. De Status Controller zal bijvoorbeeld al een afzonderlijk domein vormen maar de transactielog zal nog niet gescheiden zijn van de accountgegevens. De gegevensverzameling zal in de eerste fase worden opgevat als privacygevoelig omdat het BSN wordt verzameld. Het BSN is op zichzelf al een privacygevoelig gegevens aangezien het een unieke identifier is. Naar mate het project vordert zal de privacygevoeligheid van de gegevensverzameling afnemen. Dit wordt gerealiseerd door de inzet van Privacy Enhancing Technologies waarmee burgerservicenummers worden gepseudonimiseerd en de verdere compartimentering van systemen.
I.8	Zijn er veel maatschappelijk belanghebbenden?	Ja, alle Nederlandse burgers kunnen gebruikmaken van DigiD en daarmee ook van DigiD Hoog. Voor DigiD Hoog is een (nieuw) WID met een gepersonaliseerde chip met PI en PP benodigd die geproduceerd zal worden door de middelenuitgever ten tijde van de eerste implementatie van DigiD Hoog. Om DigiD Hoog te

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		kunnen gebruiken moet de gebruiker eerst over dit DH-middel beschikken door deze aan te vragen bij een aanvraagloket (meestal een gemeente). Een NIK en rijbewijs zijn 10 jaar geldig en het verlengen of aanvragen van een document brengt kosten voor de gebruiker met zich mee. De verwachting is dat DigiD Hoog vooral in de beginfase door een aanzienlijk kleiner deel van de bevolking gebruikt zal worden dan de huidige DigiD. DigiD zelf is van maatschappelijk en economisch groot belang, aangezien het één van de belangrijkste (publieke) eID-middelen zal blijven. De komst van een eID-middel met een hoger betrouwbaarheidsniveau zal bij veel belanghebbenden onder de aandacht vallen. Logius is onderdeel van het ministerie van BZK met een eindverantwoordelijke minister. DigiD staat zowel maatschappelijk als politiek in de schijnwerpers. Ook vanuit dit perspectief zijn er veel verschillende belanghebbenden.
I.9	Hebben de gegevens betrekking op de gehele of grote delen van de bevolking?	De gegevens hebben betrekking op een groot deel van de bevolking. DigiD wordt op dit moment gebruikt door 13,4 miljoen gebruikers. De verwachting is dat DigiD Hoog vooral in de beginfase door een aanzienlijk kleiner deel van de bevolking gebruikt zal worden dan de huidige DigiD. Dit komt doordat de gebruiker beschikking moet krijgen over een nieuw WID alvorens gebruik te kunnen maken van DigiD Hoog. Ook de gebruiksvriendelijkheid is voor DigiD Hoog lager dan voor de huidige DigiD en DigiD Substantieel. De verwachting is dat niet alle dienstverleners het betrouwbaarheidsniveau 'Hoog' zullen aanbieden of pas in een later stadium aanbieden aan gebruikers. Uiteindelijk is het de bedoeling dat de gehele Nederlandse bevolking de mogelijkheid heeft om gebruik te maken van DigiD Hoog. Voorwaarde voor het gebruik van een DH-middel is dat de gebruiker een BSN heeft en het juiste adres in de BRP is geregistreerd omdat hier de PIN-mailer naartoe gezonden wordt die benodigd is voor het activeren van het DH-middel.
I.10	In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene beleid/databestand/informatiesysteem ontwikkeld en wat voor soort(en) verwerking(en) van persoonsgegevens gaat/gaan hiervan deel uitmaken bij het voorziene traject?	Het wettelijk kader voor de verwerking van de persoonsgegevens is het Besluit GDI. Verwerkingen van persoonsgegevens vinden plaats om de identiteit van de gebruiker vast te stellen zodat op een betrouwbare manier ingelogd kan worden bij dienstverleners. Additioneel worden bij DigiD Hoog, ten opzichte van DigiD Substantieel, de volgende gegevens verwerkt: ▪ gerandomiseerde polymorfe pseudoniemen en polymorfe identiteiten; ▪ diverse noodzakelijke gegevens benodigd voor statusbeheer en beheer van operationele processen rond het DH middel. Bij de doorontwikkeling van DigiD Hoog zal het BSN uiteindelijk verdwijnen in de accountgegevens en de transactielog waardoor de authenticatiedienst volledig pseudoniem werkt. De ontwikkeling van DigiD Hoog vloeit verder voort uit een aantal Europese verordeningen, waaronder: ▪ eIDAS: de verplichting dat Europese lidstaten elkaars digitale authenticatie middelen accepteren en toelaten (nr. 910/2014, 23 juli 2014) ▪ minimale technische specificaties voor betrouwbaarheidsniveaus authenticatiediensten (laag, substantieel, hoog), (nr. 2015/1502, 8 september 2015)
I.11	Worden de gegevens verzameld op basis van een van de wettelijke grondslagen volgens de Wbp?: ▪ U vraagt toestemming	De wettelijke grondslagen volgens de Wbp/AVG om persoonsgegevens te verwerken onder de verantwoordelijkheid van het ministerie van BZK/Logius ten behoeve van DigiD Hoog zijn aanwezig: vervulling publiekrechtelijke taak en toestemming.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
	▪ De gegevens zijn noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene een partij is ▪ De gegevens zijn nodig voor het volgen van een wettelijke verplichting ▪ De betrokkene heeft er een vitaal belang bij dat u de gegevens verzamelt ▪ De gegevens zijn nodig voor de goede vervulling van een publiekrechtelijke taak ▪ U heeft een gerechtvaardigd belang bij de verwerking	De persoonsgegevens worden verwerkt als onderdeel van de publiekrechtelijke taak van DigiD, zoals opgenomen in het Besluit GDI. Het Besluit GDI biedt een adequate grondslag voor de verwerking. Uit de toelichting van het Besluit GDI volgt dat met de verwerkingsdoelen wordt beoogd om gegevensverwerking mogelijk te maken voor identificatie en authenticatie. In een aanstaande wijziging van het Besluit GDI zal de exacte werking van DigiD Hoog opgenomen worden.
I.12	Welke (overige) wet- en regelgevingen zijn relevant voor deze PIA?	De volgende wet- en regelgevingen zijn relevant voor de PIA op DigiD Hoog. Wij hebben niet getracht een volledig overzicht van relevante wet- en regelgeving voor Logius te geven. De belangrijkste wetgeving is hieronder genoemd: ▪ Algemene verordening gegevensbescherming, 25 mei 2018 (AVG) ▪ Archiefwet ▪ Besluit verwerking persoonsgegevens GDI ▪ eIDAS: de verplichting dat Europese lidstaten elkaars digitale authenticatie middelen accepteren en toelaten (nr 910/2014, 23 juli 2014) ▪ Regeling voorziening GDI ▪ Uitvoeringsverordening tot vaststelling van minimale technische specificaties voor betrouwbaarheidsniveaus authenticatiediensten (laag, substantieel, hoog), (nr 2015/1502, 8 september 2015) ▪ Wet algemene bepalingen burgerservicenummer (Wabb) ▪ Wet bescherming persoonsgegevens (Wbp) ▪ Wet elektronisch berichtenverkeer (EBV) ▪ Meldplicht datalekken (onderdeel van de Wbp)
II	**Noodzaak / gegevensminimalisering** **Privacy Principe:** **Limiteren van het verzamelen van gegevens**	
II.1	Kan van elk van de onder vraag I.3 en vraag I.4 opgevoerde typen persoonsgegevens worden gesteld dat zij beleidsmatig of technisch direct van belang en onontbeerlijk zijn voor het bereiken van de beleidsdoelstelling? Wat zou er precies niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? Licht per te verwerken persoonsgegeven toe.	Ja, een belangrijke verbetering die gerealiseerd wordt bij de doorontwikkeling van DigiD Hoog is de vervanging van het BSN door een pseudoniem en de compartimentering. Door het pseudoniem te randomiseren en te versleutelen kan alleen de ontvangende component of partij de gegevens die benodigd zijn voor het te realiseren doel ontsleutelen. Hiermee wordt gerealiseerd dat de authenticatiedienst niet weet welke gebruiker bij welke dienstverlener inlogt. Alleen voor specifieke doelen, zoals fraudeonderzoek, is het mogelijk om achter de identiteit van de gebruiker te komen. In de eerste release van DigiD Hoog wordt het BSN nog wel verwerkt omdat de ontsleuteling al vroegtijdig in het authenticatieproces plaatsvindt. In het laatste stadium van het project vindt de vertaling van de polymorfe identiteit naar het BSN plaats in de koppelvlak module (zie 'Afnemer

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		koppelvlakken' in Bijlage II), met behulp van de afnemerspecifieke sleutel. In feite decrypt DigiD dan het BSN namens de afnemer. In de eindsituatie kan alleen de dienstverlener zelf het BSN ontsleutelen. Een ontwerp is beschikbaar van een dedicated subsysteem ten behoeve van fraudebestrijding. De gebeurtenissen in de keten worden weggeschreven in een afzonderlijk bestand, de fraudelog. Aan de hand van dit bestand wordt patroonherkenning geanalyseerd op basis van use cases. Voor fraudeonderzoek moet een concrete aanleiding bestaan. Dit kan zijn: 1. Aangifte van de gebruiker. De gebruiker machtigt in dit geval om zijn gegevens te gebruiken; 2. Onderkenning van een voorgedefinieerd patroon in geregistreerde gebeurtenissen. Hiervoor worden use cases gedefinieerd; 3. Verzoek om gegevens van een bevoegde (opsporings)instantie Maatregelen zijn getroffen om onbevoegde toegang en oneigenlijk gebruik van deze fraudelog te beperken. Omdat de fraudelog met pseudoniemen werkt moet bij het BSNk een versleuteld pseudoniem opgevraagd worden dat specifiek is voor de fraudelog en kan aan de hand hiervan toegang worden verkregen tot registraties die op basis van dit pseudoniem zijn aangelegd (als hier aanleiding tot is). De handelingen van het fraudeteam worden gelogd en zijn een onderdeel van een dossier. De gegevens ten behoeve van fraudeopsporing en onderzoek worden gescheiden van de gegevens ten behoeve van verantwoording. Voor fraudeopsporing wordt de fraudelog gebruikt en voor verantwoording de transactielog. Een dergelijke voorziening voor fraudeonderzoek maakt dat het geheel beter beheersbaar wordt en toegang tot gevoelige data beperkt kan worden. Op het niveau van de inzet van technische componenten, zoals firewalls en intrusion prevention- en detectionsystemen, DDoS-preventiesysteem en technische logsystemen wordt in de PSA het verwerken van persoonsgegevens onvoldoende belicht. Deze technische netwerkcomponenten loggen het gebruik van het DigiD systeem op verschillende niveaus. Het doel van de logbestanden is om het systeem te kunnen beheren, de beveiliging te monitoren en het bewaken van juist functioneren. Hiermee worden echter risico's gecreëerd waaronder risico's voor ongewenste herleiding van gegevens en profiling. **Conclusie en aanbevelingen** Het subsysteem ten behoeve van fraudebestrijding geeft mogelijkheden om op een beheerste wijze onderzoek te doen naar fraude zonder de privacy van gebruikers te schaden. Ten tijde van de PIA is dit systeem slechts een ontwerp en bestaat onduidelijkheid over de implementatie hiervan. Een integraal en toegankelijk overzicht van alle verwerkingen van persoonsgegevens op technisch niveau ontbreekt. Het verdient aanbeveling om een dergelijk integraal overzicht te maken van alle gegenereerde loggegevens en eventuele metadata door de componenten die in gebruik zijn voor DigiD, naast de functionele beschrijvingen van het huidige ontwerp van DigiD Hoog. Ook in het kader van het principe van transparantie is dit overzicht relevant.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
II.2	Kan, als het gaat om gevoelige persoonsgegevens, hetzelfde beleidseffect of technisch resultaat worden bereikt op een van de volgende wijzen: (a) door (gecombineerd) gebruik van normale persoonsgegevens of (b) door gebruik van geanonimiseerde of gepseudonimiseerde gegevens?	Ja, DigiD Hoog maakt gebruik van gepseudonimiseerde gegevens. In de eindsituatie van DigiD Hoog kan alleen met een sleutel het BSN worden ontsleuteld op basis van de polymorfe identiteit. Logius kan dan alleen in bijzondere gevallen, zoals fraudeonderzoek, achterhalen welke gebruiker bij welke dienstverlener heeft ingelogd. Deze verbetering vanuit privacyoptiek kan pas worden gerealiseerd als de volledige DigiD pseudoniem werkt, de transactielog geen BSN meer bevat en de transactielog is losgekoppeld van de accountgegevens. Hiervoor moeten ook de huidige DigiD en DigiD Substantieel overgaan naar een pseudoniem-gebaseerde verwerking en moet historische data geconverteerd worden. Tot deze realisatie blijven de privacyrisico's van de huidige DigiD gelden. In de transactielogging van het gebruik van DigiD is in de huidige DigiD door registratie van het BSN bekend welke gebruiker bij welke dienst heeft ingelogd. Hierdoor ontstaat een gevoelig en waardevol bestand op basis waarvan profielen van gebruikers opgesteld zouden kunnen worden (bijvoorbeeld via offline analyse). Het pseudonimiseren van het BSN leidt tot een afname van de privacygevoeligheid van dit bestand. Het toepassen van randomisering leidt er toe dat patroonherkenning op basis van dit bestand bemoeilijkt wordt. **Conclusie en aanbevelingen** Het BSN-gebruik wordt sterk gereduceerd in de doorontwikkeling naar de eindsituatie van DigiD Hoog door de inzet van cryptografische maatregelen. Het is belangrijk dat de doorontwikkeling zoals is voorgenomen BZK wordt doorgezet en afgerond en dat uiteindelijk de middelen en concepten van het bestaande DigiD-systeem worden omgebouwd om de privacyrisico's verder te beperken. Dit wordt pas gerealiseerd als ook de huidige DigiD en DigiD Substantieel gebruik maken van gepseudonimiseerde gegevens, de historische data is geconverteerd en de transactielog is losgekoppeld van de accountgegevens.
III	**Doelbinding, koppeling en profilering** **Privacy principe:** **Doelbinding / Limitering van gebruik van gegevens**	
	Doeleinden/doelbinding en koppeling	
III.1	Hebt u het/de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld? Geldt hiervoor één en hetzelfde specifieke doel?	Ja, Logius beschikt over een register van verwerkingen als bedoeld in artikel 30 van de AVG. Vastgesteld is dat Logius nog niet beschikt over een volledig en toegankelijk register van verwerkingen van persoonsgegevens, waarin naast de persoonsgegevens op functioneel niveau ook de verwerkingen van persoonsgegevens op technisch niveau zijn beschreven en gekoppeld aan de specifieke doelen op component- en op overkoepelend niveau.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		Aanbevelingen Het verdient aanbeveling om een integraal overzicht te maken van het volledige DigiD landschap en de infrastructuur, zodat de verwerkingen van bestaand DigiD, DigiD Substantieel en DigiD Hoog in samenhang kunnen worden geëvalueerd op privacy en beveiligingsrisico's. Aanbevolen wordt in dit overzicht naast de functionele- ook de technische gegevensverwerkingen op te nemen. Daarbij is een eenduidige beschrijving van het doel van deze gegevens per component noodzakelijk vanuit privacyoptiek.
III.2	Gaat het bij het project/systeem om gebruik/verzameling van nieuwe, meer of andere persoonsgegevens voor een bestaand doel of bestaande doelen binnen al bestaande systemen? (scenario toevoeging nieuwe persoonsgegevens)	Voor het bestaande doel van DigiD, namelijk het bieden van een betrouwbaar authenticatiemiddel voor gebruikers om in te loggen in het BSN-domein, worden voor DigiD Hoog beperkte aanvullende persoonsgegevens verwerkt. DigiD Hoog bouwt voort op het ontwerp en de bestaande componenten van DigiD Substantieel. DigiD Hoog verwerkt binnen het DigiD systeemdomein, waar Logius verantwoordelijk voor is, de volgende additionele persoonsgegevens ten opzichte van DigiD Substantieel: ▪ gerandomiseerde polymorfe pseudoniemen en polymorfe identiteiten; ▪ diverse noodzakelijke gegevens benodigd voor statusbeheer en beheer van operationele processen rond het DH-middel. **Aanbevelingen** Het verdient aanbeveling om bij de verdere ontwerpstappen een integraal overzicht op te stellen van welke persoonsgegevens worden verwerkt over de verschillende DigiD-voorzieningen heen en dit ook per technische DigiD-component te doen. Het gaat dan om alle soorten gegevens, ook de loggegevens per systeemcomponent. Daarbij is een eenduidige beschrijving van het doel van deze gegevens per component noodzakelijk vanuit privacy optiek. Deze actie draagt ook bij aan de verplichtingen van de AVG om een register van verwerkingen aan te leggen waarbij deze informatie ook dient te worden vastgelegd. In het bijzonder verdient het aanbeveling om periodiek te evalueren of alle loggings gegenereerd door de verschillende technische systeemcomponenten niet meer gegevens bevatten dan noodzakelijk is en daarbij ook de privacyrisico's af te wegen die deze loggings introduceren.
III.3	Gaat het bij het project/systeem om het nastreven van nieuwe/aanvullende doeleinden door bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, vergelijken, delen, koppelen of anderszins verder te verwerken? (scenario toevoeging doeleinden) Zo ja, hebben alle personen/instanties/systemen die betrokken zijn bij de verwerking dezelfde doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang? Gelden dezelfde doelen voor het hele proces?	Ten opzichte van de huidige DigiD streeft DigiD Hoog een aanvullend doel na, namelijk het ter beschikking stellen van een authenticatiemiddel op het hoogst mogelijke betrouwbaarheidsniveau: eIDAS Hoog. Om dit doel te bereiken wordt onder andere gebruik gemaakt van bestaande persoonsgegevens, zoals de accountgegevens van de gebruiker. Er zijn vanuit privacy optiek geen strijdige belangen of doelstellingen te verwachten bij de betrokken stakeholders in de DigiD-keten en bij het gebruik van DigiD Hoog.
III.4	Is het gebruik van de gegevens in lijn en verenigbaar met het doel van verzamelen? Worden de gegevens gebruikt	Ja, de verzamelde gegevens bij Logius zijn passend binnen de doelstellingen van DigiD Hoog. De gegevens die door Logius worden opgeslagen worden niet gebruikt voor andere doeleinden dan het identificeren en

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
	voor andere bedrijfsprocessen of doelen dan waar ze oorspronkelijk voor zijn verzameld? Zo ja, past het doel van dit bedrijfsproces bij het oorspronkelijke doel van verzamelen?	authenticeren van gebruikers met DigiD. Gegevens zijn wel benaderbaar indien aanleiding is tot fraudeonderzoek of voor verantwoordingsdoeleinden. Compartimentering leidt tot een betere beheersing van het gebruik van en de toegang tot persoonsgegevens. Alleen met een afnemerspecifieke sleutel van het BSNk kunnen persoonsgegevens ontsleuteld worden op basis van de polymorfe identiteit. De organisatorische inrichting van de verschillende functies en verantwoordelijkheden binnen Logius moet nog uitgewerkt worden. De huidige voorgestelde systeemopzet biedt hier de mogelijkheden toe. Adequate domeinscheiding houdt naast de compartimentering in dat functiescheiding wordt geïmplementeerd zodat het niet mogelijk is dat één persoon toegang heeft tot meerdere domeinen, anders dan onder specifieke omstandigheden die relevant zijn voor misbruikbestrijding. **Aanbevelingen** Om de privacybescherming te waarborgen en functiescheidingen adequaat in te richten bevelen wij aan de verschillende functies en verantwoordelijkheden binnen Logius te beschrijven, organisatorisch in te richten en hier toezicht op uit te oefenen. Functies en verantwoordelijkheden kunnen overzichtelijk in een autorisatiematrix weergegeven worden. Aanbevolen wordt periodieke controle uit te voeren op de overeenkomst tussen de geformaliseerde autorisatiematrix (soll-situatie) en de daadwerkelijke autorisaties in de verschillende domeinen (ist-situatie). Voorkomen moet worden dat één persoon toegang heeft tot meerdere domeinen/compartimenten.
III.5	Indien u positief hebt geantwoord op de vragen III.2, III.3 III.4, hoe wordt een dergelijk voorgenomen gebruik dan gemeld aan: (a) de functionaris voor de gegevensbescherming, of (b) het Cbp indien er geen FG is?	Logius meldt de verwerkingen aan de functionaris voor de gegevensbescherming (FG). De persoonsgegevens die verwerkt worden in de huidige DigiD zijn reeds gemeld bij de FG. De melding bij de FG voor de verwerking van persoonsgegevens voor DigiD Hoog zal worden gedaan wanneer DigiD Hoog in productie is.
III.6	Indien u positief hebt geantwoord op de vragen III.2, III.3 of III.4, welke (nadere) controles op een dergelijk gebruik zijn dan ingebouwd?	Binnen de beheeromgeving van Logius zijn verscheidene maatregelen getroffen om de toegang en het gebruik van de gevoelige gegevens te beperken. Deze maatregelen zijn aanwezig in de huidige DigiD en gelden ook voor de nieuwe of gewijzigde componenten voor DigiD Hoog. Gegevens zijn alleen toegankelijk op basis van toegekende rechten, toegang tot logging wordt gemonitord en alerts worden verstuurd indien een onverwachte toegang wordt gedetecteerd. Voor toegang tot de beheermodule is een persoonlijk PKIoverheid-certificaat vereist. Voor het doorvoeren van diverse gevoelige activiteiten op het systeem wordt toepassing van het vier-ogenprincipe afgedwongen. Voor de vaste schijven waar deze gegevens zijn opgeslagen wordt schijfencryptie toegepast. Voor het uitlezen van de chip op het WID wordt gebruik gemaakt van middleware, waaronder wordt verstaan de eID server en eID client. De eID client is een apparaat met NFC lezer en DigiD client software. End-to-end encryptie is aanwezig tussen de chip, de app en de eID server. De DigiD app DH geeft een redirect url naar de eID server waarna de eID server een beveiligd kanaal opzet om gegevens uit de chip te lezen, door het gebruik van het PACE protocol. Het PACE protocol is een Europees protocol voor authenticatiediensten. Tweezijdige authenticatie vindt plaats tussen de applet en de eID server om vast te stellen dat de chip

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		authentiek is en dat de eID server bevoegd is gegevens uit te lezen. Voor het uitwisselen van de PI en het PP tussen de eID server en de CIS wordt gebruik gemaakt van SAML. Dit is een op XML gebaseerde standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen domeinen. In de huidige ontwerpdocumentatie is weinig aandacht besteed aan de additionele controles die zijn ingebouwd op het gebruik van en de verwerking van de gegevens voor DigiD Hoog. Er wordt verwezen naar normen voor informatiebeveiliging die vooral toezien op de procedurele kant van Information Security Management Systemen (BIR) en niet direct op de werking van de gerealiseerde beveiligingsmaatregelen in de IT werkelijkheid. Hiermee bedoelen wij andere controles dan de ad hoc controles die uitgevoerd worden in het geval van identiteitsfraude. **Conclusie en aanbevelingen** Het verdient aanbeveling om maatregelen te ontwerpen en te implementeren die de werkelijke toegang tot systemen en gegevens en het gebruik van de gegevens waarborgen en deze maatregelen controleerbaar maken zodat periodieke of wellicht permanente monitoring op de beveiligings- en datakwaliteitsaspecten plaatsvindt en rapportage daarover beschikbaar is.
	Profilering	
III.7	Kunnen de verzamelde/verwerkte persoonsgegevens gebruikt worden om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen, te beoordelen, te voorspellen, of om beslissingen over de betrokkenen te nemen? Ofwel, kunnen met behulp van de gegevens profielen worden opgesteld van de betrokkenen, al dan niet geanonimiseerd?	In DigiD Hoog zijn maatregelen genomen om het risico op profiling verder te reduceren. Deze risicoafname wordt pas gerealiseerd in laatste fase van DigiD Hoog en geldt nog niet in de eerste fase. Compartimentering wordt toegepast waardoor de accountgegevens niet zondermeer aan de transactiegegevens gekoppeld kunnen worden. Met het gebruik van pseudoniemen is alleen de ontvangende component of partij in staat het BSN te ontsleutelen. Door het randomiseren en pseudonomiseren kan aan de hand van de transactielogging herleid worden bij welke dienstverlener is ingelogd maar niet direct door welke gebruiker. Het risico op mogelijke profiling wordt hierdoor gemitigeerd.
III.8	Zijn de betrokkenen op de hoogte van het gebruik van de gegevens voor profiling? Zijn de gegevens die hiervoor worden gebruikt afkomstig uit verschillende (eventueel externe) bronnen en zijn zij oorspronkelijk voor andere doelen verzameld? Leveren de gegevens die hiervoor worden gebruikt een volledig en actueel beeld van de betrokkenen op? Kunnen de opgestelde profielen leiden tot uitsluiting of stigmatisering?	Profileren is niet aan de orde. Gegevens die Logius verzamelt en verwerkt hebben niet tot doel gebruikers te profileren.
III.9	Wordt bij deze analyse/beoordeling/voorspelling gebruik gemaakt van een vergelijking van persoonsgegevens die technisch geautomatiseerd is (d.w.z. niet door mensen zelf wordt uitgevoerd)? Zo ja, hoe wordt geregeld dat, indien dit	De vergelijking van persoonsgegevens op de chip met de DH Status Controller, die wordt gevoed door de MU, vindt geautomatiseerd plaats. De persoon wordt middels deze vergelijking niet beoordeeld/voorspeld maar er vindt een verificatie plaats op het WID van de gebruiker waar eventuele foutmeldingen uit voortkomen. Uit deze foutcodes kan bijvoorbeeld worden opgemaakt of een WID geblokkeerd is of dat er andere afwijkingen

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
	geautomatiseerde proces tot een beoordeling of voorspelling over een bepaalde persoon leidt, hierop pas concrete actie wordt ondernomen na tussenkomst en (tweede) controle van (menselijk) personeel?	zijn. Aan de hand van de foutcodes kunnen medewerkers van Logius actie ondernemen en zo nodig contact opnemen met de gebruiker. **Aanbevelingen** Het verdient aanbeveling ter waarborging van de rechten van betrokkenen en ter beperking van eventuele nadelige effecten voor de betrokkenen om aan het huidige ontwerp DigiD Hoog een procedure toe te voegen met hierin hoe afwijkingen worden geconstateerd, hoe medewerkers daarmee omgaan en hoe, indien nodig, de gebruiker wordt geïnformeerd over de geconstateerde afwijkingen.
IV	**Kwaliteit** **Privacy Principe:** **Gegevenskwaliteit**	
IV.1	Welke periodieke en incidentele controles zijn voorzien om de juistheid, nauwkeurigheid en actualiteit van de in het ICT-systeem verwerkte persoonsgegevens na te gaan?	In het huidige ontwerpdocument zijn geen (periodieke) controles op de juistheid, nauwkeurigheid en actualiteit van binnen DigiD Hoog opgeslagen persoonsgegevens voorzien. Voor het waarborgen van de kwaliteit van gegevens binnen de bestaande DigiD en DigiD Hoog wordt vooral gesteund op preventieve toegangsbeveiligingsmaatregelen die de kwaliteit van de persoonsgegevens moeten borgen en bijvoorbeeld manipulatie of andere menselijke of systeemfouten moeten tegengaan of vermijden. Een voorbeeld hiervan is het beperken van de toegang tot de databases en de logging. Er is geen nadere informatie over welke checks and balances zijn ingevoerd in de bestaande DigiD om de kwaliteit van de verkregen en vastgelegde persoonsgegevens te waarborgen en hoe daar achteraf verantwoording over kan worden afgelegd. Wel logt de database de veranderingen op tabellen, waarbij is na te gaan wat er verandert in de verschillende databases, waaronder de accountdatabase. De persoonsgegevens die worden ingevuld door de gebruiker bij de aanvraag van DigiD kunnen door de gebruiker zelf gewijzigd worden indien deze niet (meer) juist of onvolledig zijn. Daarnaast kan de gebruiker een verzoek doen deze gegevens te wijzigen. Logius heeft geen maatregelen geïmplementeerd om de gebruiker erop te attenderen dat hij regelmatig dient te controleren of zijn gegevens (zoals het telefoonnummer en het e-mailadres) nog actueel zijn. Bij de aanvraag van een DH-middel wordt de BRP aangeroepen om de persoonsgegevens en adresgegevens te verifiëren. Ten behoeve van het gebruik van DigiD Hoog wordt de status van het gebruikte WID geverifieerd aan de hand van de Status Controller, die wordt gevoed door de RvIG en RDW. Deze gegevens worden als juist aangenomen. Voor deze gegevens gelden controlemechanismen die buiten de verantwoordelijkheid van Logius vallen.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		Aanbevelingen Het verdient aanbeveling om interne controlemaatregelen gericht op datakwaliteit en de rapportages daarover nader te beschrijven. Ten behoeve van bewijslast achteraf en om verantwoording af te kunnen leggen over datakwaliteit en de integere werking van systemen zijn naast preventieve controles ook repressieve controles relevant. Te denken valt aan het gebruik van hashing op bepaalde gegevensverzamelingen en het gebruik van de bestaande database replica om de integriteit van (historische) data te kunnen valideren. De beoogde interne controle maatregelen zijn dus andere maatregelen dan de bestaande maatregelen om indicaties van fraude te onderzoeken. Deze controlemaatregelen kunnen mogelijk uitgevoerd worden met behulp van de component die voor DigiD Hoog wordt ontworpen ten behoeve van fraudeonderzoek. Het verdient aanbeveling om de hierboven bedoelde interne controle- en verantwoordingsmaatregelen gericht op de kwaliteit van de persoonsgegevens mee te ontwerpen voor de voorziening ten behoeve van fraudeonderzoek. Wij bevelen aan maatregelen te implementeren om de actualiteit van gegevens te waarborgen. Hierbij kan gedacht worden aan het periodiek (jaarlijks) versturen van een e-mail naar gebruikers waarin de gebruiker wordt herinnerd aan het, indien van toepassing, actualiseren van de gegevens
IV.2	Kunnen de verwerkte persoonsgegevens gecorrigeerd, aangepast of verwijderd worden en zo ja, door wie kan dat worden gedaan?	Ja, op verzoek van de gebruiker kunnen zijn of haar persoonsgegevens worden verbeterd, aangevuld, verwijderd of afgeschermd, tenzij dit niet is toegestaan op grond van een wettelijke bepaling. Het telefoonnummer en e-mailadres kunnen door de gebruiker zelf worden gewijzigd op mijn.digid.nl. De eerstelijns helpdesk is uitbesteed aan 'Webhelp' en deze partij heeft geen toegang tot de beheeromgeving en dus geen toegang tot accountgegevens.
V	**Betrokken instanties/systemen en verantwoordelijkheid** **Privacy principe:** **Verantwoording**	
V.1	Welke interne en externe instanties en/of systemen zijn betrokken bij de voorziene verwerkingen in elk van de fasen en de uitvoering van het project en aan welke derde partijen worden de gegevens verstrekt? Welke verstrekkers zijn er en welke ontvangers? Welke bestanden of deelbestanden en welke infrastructuren?	Anders dan bij DigiD Substantieel worden gegevens van het WID niet rechtstreeks gecontroleerd met gegevens van de middelenuitgevers (RvIG en RDW). De Status Controller wordt door de middelenuitgever gevoed en geactualiseerd met de statusinformatie van het WID. Indien de gebruiker inlogt met een DH middel wordt met behulp van de Status Controller geverifieerd of het WID geldig is om te gebruiken voor de authenticatie. De RvIG en RDW ontvangen bij het gebruik van DigiD Hoog geen gegevens van Logius. De dienstaanbieder waar de gebruiker inlogt ontvangt van Logius het (gepseudonimiseerde) BSN en het authenticatieniveau dat gebruikt is voor het inloggen.
V.2	Is (in ieder stadium) duidelijk wie verantwoordelijk is voor de verwerking van de persoonsgegevens? Zo ja, is deze persoon of organisatie daarop voldoende voorbereid en geëquipeerd wat betreft de nodige voorzieningen en	Ja, de verantwoordelijkheid voor het aanvraag-, productie- en uitgifteproces ligt bij de middelenuitgever. De Status Controller is een component die technisch gezien onderdeel is van de authenticatiedienst. Deze is raadpleegbaar vanuit de authenticatiedienst maar het inhoudelijk beheer van deze component is de verantwoordelijkheid van de middelenuitgever. De verantwoordelijkheid voor het authenticatieproces ligt bij de authenticatiedienst (Logius). DigiD Hoog maakt gebruik van een nieuwe voorziening, namelijk het BSNk. Het

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
	maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht?	BSNk is een technische stelselvoorziening die de verantwoordelijkheid heeft voor het koppelen van het BSN van een natuurlijk persoon aan een PI en PP. Het BSNk is daarnaast verantwoordelijk voor het sleutelbeheer en het inzageregister. Het BSNk en de authenticatiedienst staan volledig los van elkaar.
V.3	Is het duidelijk wie na afloop van het project verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen?	Ja, Logius verwerkt namens de minister van BZK voor de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van DigiD persoonsgegevens. De minister van BZK is verantwoordelijke voor de verwerking van persoonsgegevens door zijn departement. De minister kan zijn verplichtingen op grond van de Wbp mandateren aan een beheerder. Voor de verwerkingen van persoonsgegevens waarvoor Logius bij de uitvoering de verantwoordelijkheid draagt heeft de minister het beheer overgedragen aan Logius. Hiermee is duidelijk wie na afloop van het project verantwoordelijk is voor de uitvoering en evaluatie.
V.4	Wie binnen uw organisatie en elk van de andere betrokken organisaties/buiten uw organisatie krijgen precies toegang tot de persoonsgegevens? Bestaat de kans dat bij het gebruik ervan de gegevens ter beschikking komen van onbevoegden? Is de verstrekking van de gegevens aan derde partijen in lijn met het doel van verzameling?	De toegang tot persoonsgegevens wordt in de doorontwikkeling van DigiD Hoog beter beheersbaar door compartimentering. Organisatorische functiescheiding is in de ontwerpdocumentatie nog onvoldoende belicht. In de huidige situatie en in de eerste fase van DigiD Hoog hebben beheerders, de tweedelijns helpdesk en het fraudeteam toegang tot de beheermodule. Om toegang te verkrijgen tot deze beheermodule is een persoonlijk PKIoverheid-certificaat vereist. Een pasje is benodigd om in te kunnen loggen. De kans dat deze gegevens ter beschikking komen van onbevoegden wordt hierdoor als laag beschouwd. Nieuw voor DigiD Hoog is dat de gebeurtenissen in de keten worden weggeschreven in een afzonderlijk bestand, de fraudelog. Aan de hand van dit bestand wordt patroonherkenning geanalyseerd op basis van use cases. Voor fraudeonderzoek moet een concrete aanleiding bestaan. Maatregelen zijn getroffen om onbevoegde toegang en oneigenlijk gebruik van deze fraudelog te beperken. Omdat de fraudelog met pseudoniemen werkt moet bij het BSNk een versleuteld pseudoniem opgevraagd worden dat specifiek is voor de fraudelog en kan aan de hand hiervan toegang worden verkregen tot registraties die op basis van dit pseudoniem zijn aangelegd (als hier aanleiding tot is). De handelingen van het fraudeteam worden gelogd en zijn een onderdeel van een dossier. In de eindsituatie werkt de keten bij Logius met pseudoniemen en wordt een VI en VP aan de dienstverlener verstrekt waarmee de dienstverlener de identiteit van de gebruiker kan achterhalen. Verder worden er geen persoonsgegevens aan derden verstrekt zonder voorafgaande ondubbelzinnige toestemming van de gebruiker. Een uitzondering hierop is een wettelijke verplichting om gegevens te verstrekken. **Conclusie en aanbevelingen** De kans dat de gegevens ter beschikking komen van onbevoegden wordt verlaagd door de compartimentering van systemen. Adequate domeinscheiding houdt naast compartimentering in dat functiescheiding ingericht moet worden om te voorkomen dat één persoon toegang heeft tot meerdere domeinen. Uit de PSA blijkt niet duidelijk hoe deze functiescheiding gerealiseerd zal worden en welke interne controles uitgevoerd worden op de daadwerkelijke toegang tot persoonsgegevens. Om de privacybescherming te waarborgen en functiescheidingen adequaat in te richten bevelen wij aan de verschillende functies en verantwoordelijkheden

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		binnen Logius te beschrijven, organisatorisch in te richten en hier toezicht op uit te oefenen. Het verdient aanbeveling om een mix van preventieve en repressieve maatregelen te beschrijven met daarbij ook eventuele rapportages over de werking van deze maatregelen over een bepaalde periode.
V.5	Worden de gegevens doorgegeven of verkocht aan derde partijen? Is het verkopen van de gegevens in lijn met de regels van de Wbp? Is het doorgeven van de gegevens aan partijen buiten de organisatie in lijn met de verwachtingen van het individu?	Nee, er worden geen persoonsgegevens aan derden verstrekt zonder voorafgaande ondubbelzinnige toestemming van de gebruiker, een uitzondering hierop is een wettelijke verplichting om gegevens te verstrekken. Aan dienstverleners die aangesloten zijn op DigiD, verstrekt Logius in de huidige situatie het BSN en het authenticatieniveau. Het BSN wordt verstrekt aan de dienstverlener om de identiteit van de gebruiker vast te kunnen stellen. Het gekozen authenticatieniveau wordt verstrekt zodat de dienstverlener een beeld heeft van de mate waarin er zekerheid is over de identiteit van de gebruiker die heeft ingelogd. Dit is overeenkomstig de verwachtingen van het individu en tevens zo opgenomen in de privacyverklaring van DigiD (DigiD, 2016). In de eindsituatie wordt in plaats van het BSN het VI en VP aan de dienstverlener verstrekt. Het koppelvlak met de dienstverleners moet hiervoor aangepast worden.
V.6	Geldt voor een of meer van de betrokken instanties een beperking van de mogelijkheid om persoonsgegevens te verwerken als gevolg van geheimhoudingsplichten (in verband met functie/wet)?	Ja, de geheimhoudingsplicht is geregeld in artikel 2:5 van de Algemene wet bestuursrecht (Awb). Deze wet is van toepassing op alle overheidsinstanties, dus ook op de RDW, de RvIG en de publieke dienstverleners. Door de RDW en de RvIG worden echter geen persoonsgegevens ontvangen van Logius waarover deze partijen nog niet beschikken. Met dienstverleners zijn of worden verwerkersovereenkomsten afgesloten waarvan de geheimhoudingsplicht onderdeel is.
V.7	Zijn alle stappen van de verwerking, in de zin van soorten gegevens en uitwisselingen, in kaart gebracht of te brengen, zodanig dat daardoor voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt?	Ja, de verwerkingen van persoonsgegevens zijn in kaart gebracht door Logius en onder andere benoemd in de privacyverklaring (DigiD, 2016). Voor de gebruikers is op dit moment nog niet inzichtelijk welke gegevens additioneel verwerkt zullen worden voor DigiD Hoog. Naar verwachting worden deze gegevens ook opgenomen in de privacyverklaring voor de in productie name van DigiD Hoog. **Conclusie en aanbevelingen** Een verduidelijking van alle loggegevens die gegenereerd worden door de betrokken technische componenten van DigiD en vooral een integraal overzicht van de verwerkingen van persoonsgegevens van alle DigiD-voorzieningen is wenselijk. Verwerk deze inzichten in de nog aan te passen privacyverklaring voor DigiD Hoog.
V.8	Zijn er beleid en procedures voor het creëren en bijhouden van een verzameling van de persoonsgegevens die gebruikt gaan worden? Zo ja, hoe vaak en door wie zal de verwerking worden gecontroleerd? Omvat de verzameling een verwerking die namens u wordt uitgevoerd (bijvoorbeeld door een onderaannemer)?	Ja, beveiligingsvoorschriften zijn aanwezig voor onder andere de omgang met informatie (Logius, 2016). Hierin is de classificatie van informatie en het behandelen van informatie opgenomen. De BIR stelt tevens vereisten voor het beschermen van persoonsgegevens. De jaarlijkse in control verklaring (hierna te noemen: ICV) geeft aan of Logius voldoet aan de BIR. Overige interne controles op de verwerking en de handhaving van het beleid en procedures vinden niet plaats. **Conclusie en aanbevelingen** Zie ook de al eerder gedane aanbevelingen om de interne controle maatregelen nader te beschrijven en periodiek te toetsen op effectiviteit op werking. Besteed daarbij vooral ook aandacht aan maatregelen die zekerheid verschaffen over de daadwerkelijke functionering van de technische systemen (IT werkelijkheid).

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
V.9	Is er sprake van overdracht van persoonsgegevens naar een (overheids)instantie buiten de EU/EER? Heeft dit land een niveau van gegevensbescherming dat als passend is beoordeeld door een besluit van de Europese Commissie of de minister van Veiligheid en Justitie?	Nee, persoonsgegevens worden niet doorgegeven aan landen buiten de Europese Unie en er is geen voornemen dit te gaan doen. **Conclusie en aanbevelingen** Deze PIA richt zich op de ontwerpdocumentatie van DigiD Hoog. Hoewel strikt genomen buiten de scope van dit onderzoek is wel duidelijk dat de gehele DigiD-keten uit een reeks van componenten bestaat die van verschillende leveranciers betrokken worden. Wij bevelen aan om de gehele keten periodiek te controleren om te beoordelen of er geen sprake is van ongewenste doorgifte van persoonsgegevens buiten de EER, bijvoorbeeld als gevolg van onderhoudswerkzaamheden door leveranciers. Deze controle kan onderdeel uitmaken van het eerder al aanbevolen te realiseren stelsel van interne controle maatregelen gericht op beveiliging en datakwaliteit.
VI	**Beveiliging en bewaring/vernietiging** **Privacy principe:** **Beveiliging van gegevens** **(Privacy by Design)** **(Privacy Enhancing Technologies)**	
	<u>Beveiliging</u>	
VI.1	Is het beleid met betrekking tot gegevensbeveiliging binnen uw organisatie op orde? Zo ja, wie/welke afdeling(en) is/zijn binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan? Is dit beleid specifiek gericht op gegevensbescherming en gegevensbeveiliging? Hoe wordt het beveiligingsbeleid getoetst?	Ja, een informatiebeveiligingsbeleid is beschreven en geformaliseerd (Logius, 2016). Het afdelingshoofd Toegangsdiensten is eindverantwoordelijk over informatiebeveiliging binnen de afdeling Toegangsdiensten. De teamleiders DigiD Levering en Productontwikkeling zijn verantwoordelijk voor de implementatie van het informatiebeveiligingsbeleid binnen de teams DigiD Levering en Productontwikkeling en het toezien op de juiste toepassing hiervoor. De informatiebeveiligingsspecialist is verantwoordelijk voor de uitvoering van het informatiebeveiligingsproces en het opstellen, onderhouden, bewaken en naleven van het informatiebeveiligingsbeleid voor de teams binnen zijn verantwoordelijkheidsgebied. Het informatiebeveiligingsbeleid is niet specifiek gericht op gegevensbescherming, maar dit onderwerp vormt wel onderdeel van het beveiligingsvoorschrift omgang met informatie (Logius, 2016). Jaarlijks wordt een ICV afgegeven voor het voldoen aan de BIR. Overige interne controles op handhaving van het beveiligingsbeleid worden niet uitgevoerd. **Conclusie en aanbevelingen** Zie eerdere aanbevelingen over het opzetten van een stelsel van interne beheersmaatregelen met checks and balances om de gegevensbeveiliging en de datakwaliteit te monitoren en permanent te garanderen.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
VI.2	Indien (een deel van) de verwerking bij een bewerker plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging, en het toezicht daarop, bij die bewerker?	DigiD Hoog introduceert geen nieuwe verwerkingen bij verwerkers. Uiteindelijk is het de bedoeling dat ook de RDA-server die wordt gebruikt voor DigiD Substantieel in eigen beheer van Logius wordt genomen.
VI.3	Welke technische en organisatorische beveiligingsmaatregelen zijn getroffen om te voldoen aan de gestelde eisen in het beveiligingsbeleid en ter voorkoming van niet-geautoriseerde of onrechtmatige verwerking/misbruik van (a) gegevens die in een geautomatiseerd format staan (bv. wachtwoordbescherming, versleuteling, encryptie) en (b) gegevens die handmatig zijn opgetekend (bv. sloten op kasten)? Is er een hoger beschermingsniveau om gevoelige persoonsgegevens te beveiligen? Is bij het vaststellen van de maatregelen rekening gehouden met de Richtsnoeren Beveiliging van Persoonsgegevens, gepubliceerd door het College Bescherming Persoonsgegevens (College Bescherming Persoonsgegevens, 2013)?	De voorzieningen van Logius (en daarmee DigiD) dienen te handelen conform het informatieveiligheidsbeleid van Logius. Voor DigiD is een separaat informatiebeveiligingsbeleid opgesteld en een informatiebeveiligingsplan (Logius, 2016). DigiD heeft reeds een deel van de beveiligingsmaatregelen opgenomen in het informatiebeveiligingsplan DigiD. Dit plan is nog in bewerking en zal de komende tijd verder uitgewerkt worden voor DigiD Substantieel en DigiD Hoog. Daarnaast zijn beveiligingsmaatregelen in de beveiligingsvoorschriften (Logius, 2016) opgenomen. In de applicatie- en infrastructuur architectuur is aandacht besteed aan beveiligingsmaatregelen voor interne beheersing. Verder wordt bij elk increment de opgeleverde applicatie door externe auditors gecontroleerd op information leakage, aanvallen en zwakheden. Er wordt weliswaar verwezen naar normen voor informatiebeveiliging waaronder de BIR en ISO27001. Deze normen zien echter voor al toe op de procedurele kant van Information Security Management Systemen en niet direct op de werking van de gerealiseerde beveiligingsmaatregelen in de IT werkelijkheid. Dit geldt overigens niet voor de normen die vanuit het ICT beveiligingsassessment komen. Daar staan wel normen in die toezien op de technische beveiliging van webapplicaties. Beveiligingsmaatregelen zijn door Logius getroffen op de bestaande DigiD zoals controles op basis van extern systeemgebruik, het uitvoeren van patroonherkenning op gebruikersdata, het beperken van de toegang op basis van toegekende rechten, het monitoren van toegang tot logging en het versturen van alerts indien een onverwachte toegang wordt gedetecteerd. Voor de uitvoering van gevoelige activiteiten op het systeem geldt een vier-ogenprincipe en wordt minimaal 2-factor authenticatie toegepast. Daarnaast maakt het Beheer & Servicecentrum Logius gebruik van PKI-O certificaten. Voor de vaste schijven waar gegevens zijn opgeslagen wordt schijfencryptie toegepast. Er worden periodiek externe audits uitgevoerd. Deze maatregelen gelden ook voor de nieuwe of gewijzigde componenten voor DigiD Hoog. Voor het uitlezen van de chip op het WID wordt gebruik gemaakt van middleware, waarodner wordt verstaan de eID server en eID client. De eID client is een apparaat met NFC lezer en DigiD client software. End-to-end encryptie is aanwezig tussen de chip, de app en de eID server. De DigiD app DH geeft een redirect url naar de eID server waarna de eID server een beveiligd kanaal opzet om gegevens uit de chip te lezen, door het gebruik van het PACE-protocol. Het PACE protocol is een Europees protocol voor authenticatiediensten. Tweezijdige authenticatie vindt plaats tussen de applet en de eID server om vast te stellen dat de chip authentiek is en dat de eID server bevoegd is gegevens uit te lezen. Voor het uitwisselen van de PI en het PP tussen de eID server en de CIS wordt gebruik gemaakt van SAML. Dit is een op XML gebaseerde standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen domeinen. Met de introductie van DigiD Hoog, het gebruik van PI en PP en compartimentering van systemen worden de risico's van misbruik van de inloghistorie beperkt, maar het niet bezitten van deze gegevens is altijd nog

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		sterker. Belangrijk is te onderkennen dat deze maatregelen pas effectief zijn als DigiD Hoog volledig is gerealiseerd en ook de bestaande DigiD voorzieningen op deze zelfde wijze werken. **Conclusie en aanbevelingen** Recent heeft de Algemene Rekenkamer geconstateerd dat de versleuteling waar DigiD gebruik van maakt niet toereikend is en niet voldoet aan de wettelijke eisen. De Algemene Rekenkamer heeft overigens wel geconstateerd dat de informatiebeveiliging DigiD voldoet aan de normen. Het verdient aanbeveling om de encryptie van gevoelige verzamelingen van persoonsgegevens verder te realiseren, op onderdelen te evalueren en zo nodig aan te scherpen. Wij bevelen aan maatregelen te ontwerpen en te implementeren die de werkelijke toegang tot systemen en gegevens waarborgen en controleerbaar maken zodat periodieke of wellicht permanente monitoring op de beveiligings- en datakwaliteitsaspecten plaatsvindt. Hierbij dient niet beperkt te worden tot gebruikersdata door betrokkenen, maar dient ook aandacht besteed te worden aan controles op intern gebruik van systemen. Het uitvoeren van interne controles en het detecteren en signaleren van vermoedens van identiteitsfraude hebben karakteristieken van profiling. Uiteraard is dit bedoeld ter bescherming van de betrokkenen en gelden er strikte procedures voor onderzoeken door het fraudeteam. Een verkeerd gebruik of een verkeerde interpretatie kan er toe leiden dat een gebruiker als een soort 'verdachte' wordt gezien. Het verdient aanbeveling om bij het verdere ontwerp en implementatie strikte procedures op te stellen hoe met deze, al dan niet geautomatiseerde, interne controles wordt omgegaan zodat de rechten van betrokkenen blijven gerespecteerd. Betrokkenen dienen onverwijld geïnformeerd te worden indien hun gegevens gecompromitteerd zijn en zij mogelijk nadelige gevolgen daarvan hebben of kunnen ondervinden.
VI.4	Welke procedures bestaan er in geval van inbreuken op beveiligingsvoorschriften en voor het detecteren ervan? Is er een calamiteitenplan om het gevolg van een onvoorziene gebeurtenis, waarbij persoonsgegevens worden blootgesteld aan onrechtmatige verwerking, of verlies van persoonsgegevens af te handelen?	Een incidentmanagementprocedure en een calamiteitenplan is aanwezig in geval van inbreuk op de beveiligingsvoorschriften. In de procedurebeschrijving "melden datalekken" zijn de procedurestappen beschreven in geval sprake is van een potentieel datalek (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2017). **Conclusie en aanbevelingen** Procedureel zijn er geen aanbevelingen. In het ontwerp is geen informatie beschikbaar over het eventueel kunnen detecteren van een datalek. Het verdient aanbeveling om te verkennen of er gestructureerde technische maatregelen mogelijk zijn om datalekken of beveiligingsincidenten te kunnen detecteren. Zie ook de eerdere aanbevelingen over het verder ontwikkelen van een stelsel van interne beheersmaatregelen die direct toezien op effectieve werking van de beveiliging van de technische systemen en datakwaliteit.
VI.5	Welke procedures en maatregelen bestaan er in geval van datalekken om deze te melden aan de Autoriteit Persoonsgegevens en aan de betrokkenen van wie de gegevens zijn gelekt? (Zie ook meldplicht datalekken Wbp en Richtsnoeren die de AP daarover heeft gepubliceerd)	In de procedurebeschrijving "melden datalekken" zijn de stappen opgenomen die gevolgd dienen te worden bij een (potentieel) datalek. Ten eerste wordt bepaald of het informatiebeveiligingsincident een potentieel datalek kan zijn en het incident in geval van een potentieel datalek wordt opgeschaald naar calamiteit. Vervolgens wordt een adviesformat ingevuld om te bepalen of het datalek gemeld dient te worden bij de Autoriteit Persoonsgegevens (hierna te noemen: AP) en/of gebruikers indien ongunstige gevolgen voor de

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		persoonlijke levenssfeer waarschijnlijk worden geacht. Het datalek wordt ten slotte via een registratieformulier, binnen 72 uur, gemeld aan de AP (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2017).
	Bewaring/vernietiging	
VI.6	Hoe lang worden de persoonsgegevens bewaard? Geldt dezelfde bewaartermijn voor elk van de typen van verzamelde persoonsgegevens? Is het project onderworpen aan enige wettelijke/sectorale eisen met betrekking tot bewaring?	In het huidige ontwerp hanteert Logius de wettelijke bewaartermijnen van 18 maanden voor verzamelde persoonsgegevens via systeemlogging en vijf jaar voor gebruiksgegevens via transactielogging. Het doel van het bewaren van deze historische gegevens is het nakomen van wettelijke verplichtingen, het kunnen controleren van de integriteit van de verzamelde data en het afleggen van verantwoording daarover. Een ander doel is het kunnen uitvoeren van onderzoek naar vermeende fraudegevallen op basis van specifieke casusposities of het verrichten van onderzoek naar aanleiding van klachten. Het gevolg van het hanteren van een bewaartermijn van vijf jaar leidt tot een transactiebestand met naar verwachting minstens 1,25 miljard records gebaseerd op het DigiD-gebruik over 2016. Bij een toenemend gebruik van DigiD wordt dit aantal records uiteraard nog hoger. In het Besluit GDI is de wettelijke grondslag met betrekking tot de bewaartermijn van persoonsgegevens vastgelegd (Staatsblad van het Koninkrijk der Nederlanden, 2016). Deze bewaartermijnen hebben een wettelijke grondslag, maar hebben ook een aantal kanttekeningen: ▪ De reden voor het bewaren van de transactiegegevens ligt in het creëren van de mogelijkheid om tot vijf jaar terug identiteitsfraude te kunnen detecteren en analyseren en inzage te kunnen verschaffen aan betrokkenen in de inloghistorie; ▪ Een nadeel van het vastleggen van deze transactiegegevens is dat hoe langer ze bewaard worden, hoe meer inloginformatie verzameld wordt over het gedrag van de gebruikers als gevolg van het gebruik van DigiD. Deze inloggegevens kunnen privacygevoelig zijn. Hoe groter het bestand wordt, hoe groter de waarde van het bestand wordt en hoe groter het risico van misbruik wordt voor de gebruikers. **Conclusie en aanbevelingen** Vanuit het perspectief van controlemogelijkheden, het afleggen van verantwoording, fraudeonderzoek en afwikkeling van klachten kan de vraag gesteld worden of een bewaartermijn van vijf jaar daarvoor noodzakelijk is, mede gelet op het ontstaan van een risicovolle en omvangrijke dataset. De bewaartermijnen zijn onlangs verhoogd door wettelijke besluiten, waar Logius zich aan dient te houden. Hierdoor verdient het aanbeveling om na te gaan of de getroffen beveiligingsmaatregelen nog in lijn zijn met de risico's die deze bewaartermijnen met zich meebrengen. De invoering van polymorfe pseudoniemen in DigiD Hoog zorgt ervoor dat uit de transactielog niet direct te herleiden is door wie bepaalde transacties zijn uitgevoerd. Op deze manier wordt de dataset minder privacygevoelig. Dit is echter de eindsituatie voor DigiD Hoog. Bij de eerste release van DigiD Hoog zal het koppelvlak om de polymorfe identiteit te vertalen in het BSN zich aan de voorkant bij Logius bevinden, waardoor het BSN bij transacties nog wel bekend is.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
VI.7	Op welke beleidsmatige en technische gronden is deze termijn van bewaring gebaseerd?	Zoals bij de vorige vraag beschreven is de bewaartermijn bepaald op basis van een wettelijke grondslag. De beleidsmatige en technische gronden op basis waarvan deze bewaartermijn is bepaald zijn echter onvoldoende belicht. **Conclusie en aanbevelingen** Door pseudonimisering is het risico op het ontstaan van een steeds groter wordende privacygevoelige set aan historische data reeds ingeperkt. In de transactielog is niet direct te herleiden welke gebruiker een bepaalde transactie heeft uitgevoerd. Dit geldt echter pas in de eindsituatie van DigiD Hoog, wanneer ook de huidige DigiD en DigiD Substantieel gepseudonimiseerd werken en de historische data geconverteerd is. Ga bij de verdere ontwikkeling en implementatie van DigiD Hoog na in welke mate de nu gehanteerde wettelijke bewaartermijnen ook daadwerkelijk voor alle betreffende gegevens gelden, inclusief de technische logbestanden. Betrek bij de afwegingen voor bewaartermijnen ook het feit dat terwijl de inloghistorie ook, zij het gedistribueerd, bij de dienstverleners waar gebruikers uiteindelijk inloggen beschikbaar is.
VI.8	Welke maatregelen zijn voorzien om de persoonsgegevens na afloop van de bewaartermijn te vernietigen of verwijderen? Worden alle persoonsgegevens, inclusief loggegevens, vernietigd? Is er controle op de vernietiging en zo ja, door wie? Kan deze vernietiging (of verwijdering) ongedaan worden gemaakt?	Persoonsgegevens worden na afloop van de bewaartermijn automatisch verwijderd door middel van batch jobs. Hierbij worden ook de loggegevens verwijderd. De automatische batch jobs zouden ongedaan kunnen worden gemaakt, maar dit wordt ook gelogd en gesignaleerd mocht de werking stagneren..
VII	**Transparantie** **Privacy principe:** **Transparantie**	
VII.1	Is het doel van het verwerken van de gegevens bij de betrokkenen en/of publiekelijk bekend of kan het bekend worden gemaakt? Wat is de procedure om betrokkenen, indien nodig, te informeren over het doel van de verwerking van hun persoonsgegevens? Zouden de betrokkenen kunnen worden verrast door de verwerking op het moment dat zij daarover worden geïnformeerd?	Het ontwerp van DigiD Hoog gaat niet in op de transparantheid en communicatie naar gebruikers over het gebruik van DigiD Hoog. Wij onderschrijven dat transparantie naar gebruikers voorafgaand aan de implementatie vragen zal oproepen en zal leiden tot onduidelijkheid bij gebruikers. De aanbevelingen hieronder zijn dan ook bedoeld als adviespunten die kunnen worden meegenomen tijdens of na de implementatie van DigiD Hoog. **Aanbevelingen** Het verdient aanbeveling om gebruikers van DigiD Hoog bij het activeren en het gebruik van een DH-middel op de hoogte te stellen van de verwerking en het doel van de gegevensverwerking door een verwijzing op te nemen naar de privacyverklaring. De privacyverklaring dient uitgebreid te worden met de gegevens die additioneel verwerkt worden voor DigiD Hoog. Hierbij is het vooral relevant om aan te geven dat een gebruiker, voordat hij zijn WID scant, op de hoogte wordt gesteld wat er gebeurt bij het scannen van het WID. Aanbevolen

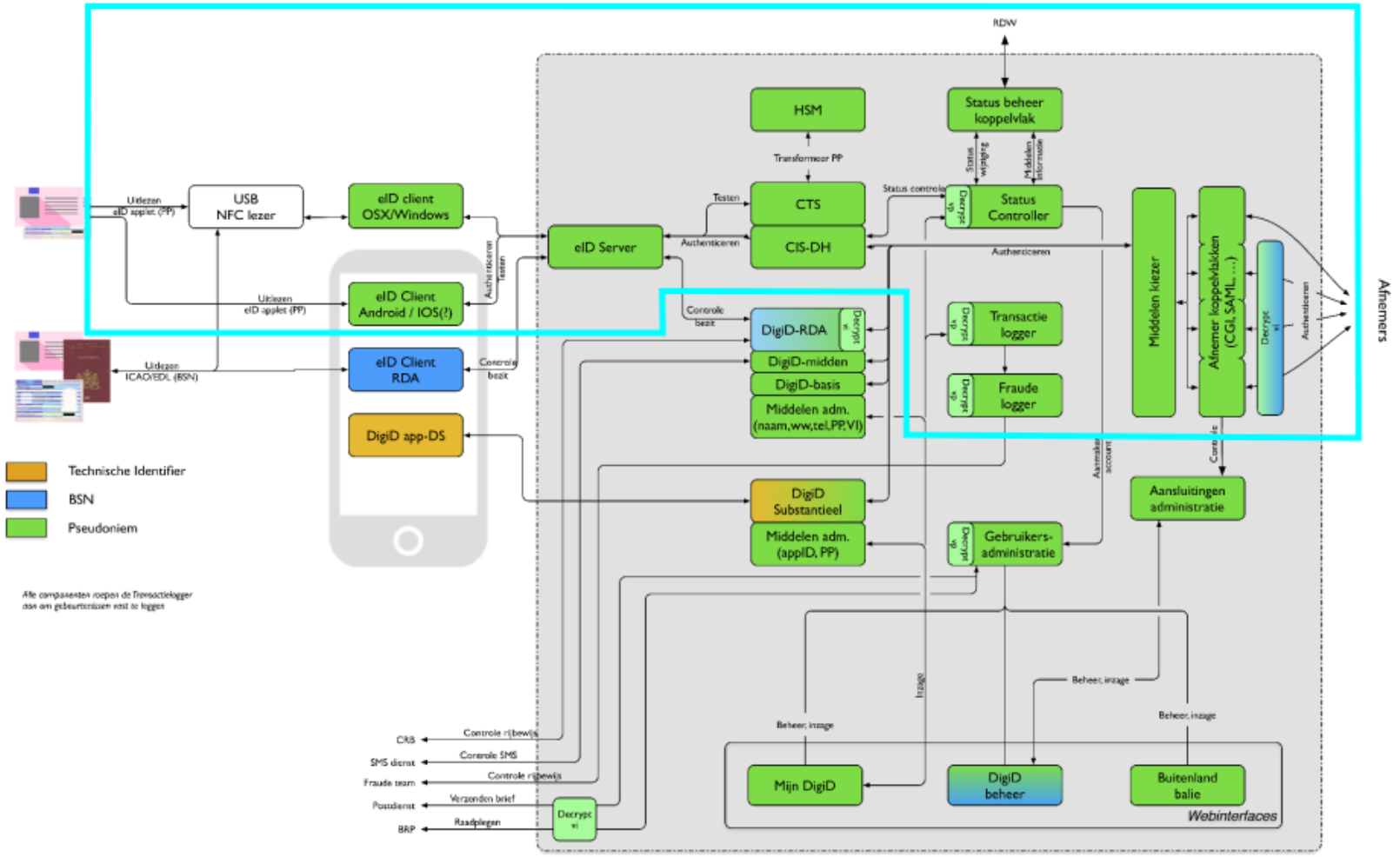
Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		wordt transparant te maken dat controle plaatsvindt met statusinformatie uit de BRP of het CRB, welke gegevens worden verwerkt (ook dat dit gepseudonimiseerd gebeurt) en wat het doel van deze verwerking is.
VII.2	Indien u de persoonsgegevens direct van de betrokkenen verkrijgt, hoe stelt u hen van uw identiteit en het doel van de verwerking op de hoogte vóór het moment van verwerking?	De website van DigiD is beveiligd door middel van een beveiligingscertificaat. Op de inlogpagina van de website staat niet vermeld dat Logius de eigenaar en beherende partij van DigiD is. Dit staat wel in de privacyverklaring vermeld. **Aanbevelingen** Zie de aanbevelingen onder VII.1
VII.3	Indien u de persoonsgegevens via een andere (overheids)organisatie verkrijgt, hoe zullen de betrokkenen daarvan op de hoogte worden gesteld op het moment van verwerking?	Zie VII.1
VII.4	(Hoe) meldt u de betrokkenen aan wie de gegevens worden verstrekt (waar dit geen wettelijke verplichting is)?	DigiD verstrekt in het kader van de authenticatie het VI/VP en het authenticatieniveau aan dienstverleners waarbij de gebruiker op dat moment wenst in te loggen en zich te authenticeren. Verder worden geen gegevens aan derden verstrekt zonder voorafgaande, ondubbelzinnige toestemming van de gebruiker, m.u.v. wettelijke verplichtingen om gegevens te verstrekken. Dit wordt middels de privacyverklaring van DigiD gemeld aan gebruikers (DigiD, 2016).
VIII	**Rechten van betrokkenen** **Privacy principe:** **Rechten van betrokkenen**	
VIII.1	Verzamelt u de gegevens op basis van opt-in (verzameling uitsluitend als de betrokkene daarvoor toestemming heeft gegeven) of op basis van opt-out (verzameling tenzij de betrokkene daartegen bezwaar heeft gemaakt) en zijn de betrokkenen daarvan op de hoogte?	Om de gebruiker zelfbeschikkingsrecht te geven en derhalve een opt-in model te implementeren, moet de gebruiker het DH-middel middels een bewuste handeling activeren bij DigiD. Hiervoor dient de gebruiker de initiële PIN te gebruiken die de gebruiker krijgt toegezonden in een tamper evident PIN-mailer. Indien de gebruiker ervoor kiest een DigiD aan te vragen om deze te gebruiken als authenticatiemiddel worden persoonsgegevens verwerkt. De gebruiker geeft geen expliciete toestemming voor de verzameling van gegevens maar wordt via de privacyverklaring wel op de hoogte gesteld van de gegevens die worden verzameld (DigiD, 2016). De gebruiker wordt hier echter niet op gewezen bij het aanvragen of gebruiken van DigiD. Op verzoek van de gebruiker kunnen persoonsgegevens worden verbeterd, aangevuld, verwijderd of afgeschermd, tenzij dit niet is toegestaan op grond van een wettelijke bepaling. Overigens is het gebruik van DigiD niet verplicht voor de gebruiker. Echter gezien de ontwikkelingen dat overheidsdiensten steeds minder toegankelijk worden buiten de digitale kanalen om is feitelijk sprake van dwang tot het gebruik van DigiD en dus dwang tot opt-in.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
VIII.2	Indien u toestemming tot verwerking van persoonsgegevens aan de betrokkene vraagt (opt-in), kan de betrokkene deze toestemming dan op een later tijdstip weer intrekken (opt-out)? Bij een weigering toestemming te geven of een dergelijke intrekking, wat is dan de implicatie voor de betrokkene?	De gebruiker kan zelf zijn account verwijderen of een verzoek doen het DigiD-account op te heffen. Indien een dergelijk verzoek wordt gedaan wordt het account, inclusief alle bijbehorende gegevens verwijderd. In de transactielog blijven de gegevens uiteraard wel beschikbaar conform de vastgestelde bewaartermijn. Bij kritieke activiteiten in de beheermodule, zoals het verwijderen van een account, wordt het vier-ogenprincipe afgedwongen. Het DigiD-account kan geblokkeerd worden op verzoek van de gebruiker, bijvoorbeeld ter voorkoming van fraude. Indien de gebruiker een DH-middel wil blokkeren of verwijderen verstrekt de gebruiker zijn BSN aan de Servicedesk. De Servicedesk vraagt met het BSN van de gebruiker bij het niet-pseudonieme domein informatie op die benodigd is om het DH-middel te blokkeren of te verwijderen. Een harde opt-out is mogelijk door gebruik te maken van de intrekkingscode die al voor initiële activering gebruikt kan worden. Een intrekkingsverzoek leidt altijd direct tot het niet meer kunnen gebruiken van het DH-middel. Een intrekking door de gebruiker heeft alleen betrekking op het DH-middel en niet op het WID. Op dit moment is er binnen (Mijn) DigiD geen onderscheid tussen het accountbeheer en het middelenbeheer. Mijn DigiD zal echter meerdere middelen moeten gaan ondersteunen waardoor het accountbeheer en het middelenbeheer gescheiden moet worden. Dit werpt ook de vraag op wat de regels worden voor het opheffen van een DigiD-account als er meerdere actieve middelen zijn binnen het account. Een mogelijk uitgangspunt is dat een DigiD -account slechts kan worden verwijderd als er geen actieve middelen zijn gekoppeld aan het account..
VIII.3	Via welke procedure hebben betrokkenen de mogelijkheid zich tot de verantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt? Hoe worden derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, in de gelegenheid gesteld hun zienswijze te geven?	Gebruikers kunnen zich tot Logius wenden middels e-mail, telefoon, per post, via een digitaal formulier op de website en via Twitter. Op verzoek van de gebruiker kunnen zijn persoonsgegevens worden verbeterd, aangevuld, verwijderd of afgeschermd, tenzij dit niet is toegestaan op grond van een wettelijke bepaling.
VIII.4	Hoe kunnen betrokkenen een verzoek indienen voor het inzien van hun (verzamelde) gegevens? Hoe kan een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling worden genomen?	Gebruikers hebben, naast het recht van transparantie, het recht op inzage, correctie, aanvulling, afscherming of verwijdering van hun persoonsgegevens of zich tegen de verwerking ervan te verzetten. De gebruiker van DigiD kan zijn gebruikersnaam, telefoonnummer, BSN, e-mailadres en gebruiksgeschiedenis inzien door in te loggen op mijn.digid.nl. Het telefoonnummer, e-mailadres en wachtwoord kunnen hier door de gebruiker zelf worden gewijzigd. Ook kan de gebruiker een inzageverzoek indienen bij Logius en een verzoek doen voor het verbeteren, aanvullen, verwijderen of afschermen van gegevens, tenzij dit niet is toegestaan op grond van een wettelijke bepaling. Ongeacht met welk authenticatieniveau is ingelogd op mijn.digid.nl kunnen de geactiveerde middelen en de gebruikersgeschiedenis worden ingezien door de gebruiker. Indien ingelogd is met DigiD Basis, DigiD Midden of DigiD Substantieel kan ook de inloghistorie worden ingezien van DigiD Hoog.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		Het ontwerp van DigiD Hoog beschrijft niet gedetailleerd hoe invulling wordt gegeven aan het inzagerecht dat gebruikers hebben. Het is nog niet bekend hoe een verzoek tot inzage, verbetering of aanvulling van gegevens in behandeling zal worden genomen in een pseudoniem-gebaseerde omgeving. In de huidige DigiD stelsel wordt de gebruiker geïdentificeerd door het verstrekken van het BSN en het beantwoorden van een aantal persoonlijke vragen. In DigiD Hoog kan de identiteit van de gebruiker niet worden vastgesteld aan de hand van het BSN. **Aanbevelingen** Het verdient aanbeveling gedetailleerd te beschrijven hoe invulling wordt gegeven aan het inzagerecht dat gebruikers hebben tot hun eigen gegevens en hoe de identiteit van de gebruiker in een pseudoniem-gebaseerde omgeving wordt vastgesteld.
VIII.5	Is er een geschillenregeling of een partij waar de betrokkenen terecht kunnen bij vragen of klachten?	Ja, gebruikers kunnen zich tot Logius wenden middels e-mail, telefoon, per post, via een digitaal formulier op de website en via Twitter. Voor klachten geldt de klachtenregeling van het ministerie van BZK. Het ministerie van BZK beschikt voorts over het Centraal Meldpunt Identiteitsfraude en -fouten (CMI). Deze dienst is op werkdagen zowel via internet als per telefoon bereikbaar om identiteitsfraude en -fouten te melden.

Tabel 6: vragenlijst PIA

Bijlage II: Scope PIA gevisualiseerd



Figuur 3: authenticatieproces

MAZARS

Bijlage III: Universele privacy principes

De basis voor een PIA ligt in het identificeren van de zogenaamde privacyprincipes. Op basis van een literatuurstudie zijn uit verschillende documenten de privacyprincipes geïnventariseerd, welke relevant zijn voor de toetsing van het ontwerp van DigiD Hoog. De aanpak van Mazars gaat uit van onderstaande beschreven universele privacyprincipes door de OECD/OESO[17].

Limiteren van het verzamelen van gegevens
De inrichting van een informatiesysteem is op het ondersteunen van het specifieke doel toegespitst. Identificatie en traceerbaarheid van het individu duurt niet langer dan strikt noodzakelijk is. Minimale gegevensverzameling is het uitgangspunt. Persoonsgegevens worden uitsluitend verwerkt op basis van de limitatieve grondslagen in de Wet bescherming persoonsgegevens (Wbp). De Wbp kent de volgende wettelijke grondslagen op basis waarvan gegevens mogen worden verwerkt:

- De betrokkene geeft expliciete toestemming;
- De gegevens zijn noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene een partij is;
- De gegevens zijn nodig voor het volgen van een wettelijke verplichting;
- De betrokkene heeft er een vitaal belang bij dat de gegevens worden verzameld;
- De gegevens zijn nodig voor de goede vervulling van een publiekrechtelijke taak;
- De organisatie heeft een gerechtvaardigd belang bij de verwerking.

Doelbinding / limiteren van het gebruik van gegevens
Persoonsgegevens worden alleen voor vooraf welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld en niet verder verwerkt als dit hiermee onverenigbaar is. De mogelijkheid om grote hoeveelheden gegevens binnen en buiten de organisatie te verspreiden wordt beperkt door gefragmenteerde opslag in plaats van het concentreren van alle gegevens in één database.

Gegevenskwaliteit
Vooraf wordt in een procedure vastgelegd aan welke kwaliteitseisen een verwerking moet voldoen. Kwaliteitseisen worden zoveel mogelijk via de functionaliteit van een informatiesysteem afgedwongen.

Verantwoording
Verantwoordelijken nemen maatregelen om materiële beginselen in de Wbp te vertalen naar differentieerbare programma's (nalevingsprogramma's). De nalevingsprogramma's worden gebaseerd op PIA's om privacyrisico's te elimineren of te mitigeren. Het geheel wordt vertaald naar concrete maatregelen en procedures op strategisch-, tactisch- en operationeel niveau. De borging kan aan externe belanghebbenden, met inbegrip van de Autoriteit Persoonsgegevens (AP), worden bewezen door monitoring, interne of externe audits.

Beveiliging van gegevens (privacy by design / privacy enhancing technologies)
Passende technische en organisatorische beveiligingsmaatregelen worden genomen tegen verlies of tegen enige vorm van onrechtmatige verwerking op basis van een risico-analyse. Daarbij wordt rekening gehouden met de stand van de techniek en de kosten van de

[17] OECD / OESO: Organization for Economic Co-operation and Development / Organisatie voor Economische Samenwerking en Ontwikkeling.

implementatie. Onnodige verzameling en verdere verwerking van persoonsgegevens wordt voorkomen. Privacy by design en privacy enhancing technologies (PET) zijn hierbij essentieel:

- **Privacy by design** houdt in dat al bij het ontwerp van de architectuur van het informatiesysteem de beginstelen van de **noodzakelijkheid, proportionaliteit en subsidiariteit** worden meegenomen. Tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) wordt ten eerste aandacht besteed aan privacyverhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Ten tweede wordt rekening gehouden met dataminimalisatie. Privacy by design verlaagt het risico dat achteraf noodzakelijke aanpassingen moeten worden gedaan die vaak tijdrovend en kostbaar zijn.
- **Privacy enhancing technologies (PET)** omvat alle technische maatregelen om de privacy te waarborgen. Het is een samenhangend systeem van maatregelen dat privacy beschermt door het elimineren, verminderen of voorkomen van onnodige en/of ongewenste verwerking van persoonsgegevens zonder dat hierbij de functionaliteit van een informatiesysteem wordt aangetast.

Transparantie

Gebruikers worden geïnformeerd over het gebruik van hun persoonsgegevens in samenhang met de gebruikte technologie en kunnen daarover controle uitoefenen. De gebruiker is hierdoor in staat om bepaalde vormen van verwerking of onrechtmatig gedrag in rechte aan te vechten.

Rechten van betrokkenen

Gebruikers hebben naast het recht van transparantie, het recht om inzage, correctie, aanvulling, afscherming of verwijdering van hun persoonsgegevens te vragen of zich tegen de verwerking ervan te verzetten. De gebruiker mag periodiek vragen aan welke instanties zijn persoonsgegevens zijn verstrekt en hiervan een overzicht ontvangen. De functionaliteit van de IT-infrastructuur is op het effectueren van deze rechten toegerust.

Bijlage IV: Algemene privacy risico's

Het verwerken van persoonsgegevens kan risico's voor de privacy van de burger opleveren. Risico's staan meestal niet op zich zelf, zijn soms in elkaar verweven, kunnen elkaar sterk beïnvloeden en laten zich daarom niet scherp afbakenen. De onderstaande risico's die zich in de maatschappij kunnen voordoen, zijn ontleend aan literatuuronderzoek.

Identiteitsfraude
Bij identiteitsfraude wordt misbruik gemaakt van valse of gestolen identiteitsgegevens. Deze gegevens gebruiken criminelen bijvoorbeeld voor het aanvragen van toeslagen of voor het kopen van spullen op naam van een ander. Naarmate meer persoonsgegevens worden verwerkt, neemt het risico op identiteitsfraude toe. Burgers en organisaties moeten terughoudend zijn met de uitwisseling van persoonsgegevens.

'Data deluge'-effect
Het 'data deluge'-effect houdt in dat de hoeveelheid persoonsgegevens die beschikbaar is, wordt verwerkt en wordt doorgegeven blijft groeien. Dit fenomeen wordt versterkt door zowel technologische ontwikkelingen, de groei van informatie- en communicatiesystemen, als door het feit dat individuen steeds beter in staat zijn gebruik te maken van en te reageren op technologieën. Naarmate er meer gegevens beschikbaar zijn en mondiaal worden uitgewisseld, neemt ook het risico voor de privacy toe.

Waardestijging van persoonsgegevens
Toenemende hoeveelheden persoonlijke informatie gaat gepaard met een waardestijging in sociaal, politiek en economisch opzicht. In bepaalde sectoren, met name in onlineomgevingen, zijn persoonsgegevens de facto een betaalmiddel geworden voor toegang tot onlinecontinent.

'Function creep'
Function creep is het risico van het verschuiven van de doeleinden waarvoor de persoonsgegevens aanvankelijk mogen worden gebruikt. Dit risico kan ontstaan bij steeds groter groeiende database met persoonsgegevens: In de loop van de tijd kan het inzicht of de behoefte ontstaan om die gegevens voor heel andere doeleinden te gaan gebruiken, dan ooit bij de aanleg van de database de bedoeling was.

Profiling
Het van overheidswege uitgegeven BSN als uniek identificerend gegeven voor een persoon, zorgt voor ongekende mogelijkheden om hiermee ingeval van een breed maatschappelijk gebruik personen te volgen en te profileren. Profileren houdt in dat van personen profielen worden gemaakt op basis van bijvoorbeeld hun leefpatroon, bestedingspatroon, betaalgedrag, eetgewoonten op basis waarvan zij worden gekarakteriseerd, in maatschappelijke klassen worden ingedeeld of op een bepaalde manier in het maatschappelijk verkeer worden bejegend.

Dit gevolg kan optreden als het BSN wordt gebruikt om de effectiviteit, efficiency en betrouwbaarheid van administratieve processen te bevorderen door hieraan allerlei andere soorten van persoonsgegevens te koppelen. Identificatie via het BSN opent voor de burger in toenemende mate de poort naar dienstverleners door de overheid en het bedrijfsleven.

Het BSN mag alleen worden gebruikt als daarvoor een wettelijke basis aanwezig is. Dit geldt ook voor uniek identificerende gegevens als biometrische gegevens en persistente pseudo-

identiteiten die tot op personen herleid kunnen worden. Naarmate dergelijke uniek identificeerbare gegevens meer in het maatschappelijk verkeer worden verspreid, neemt het risico van het gebruik ervan buiten de wettelijk gestelde grenzen toe.

Inconsistente implementatie en naleving verantwoordingsbeginsel
Vanwege de veelheid van partijen die bij de verwerking van persoonsgegevens (verwerkingsverantwoordelijken en verwerkers) zijn betrokken, varieert het niveau van privacybescherming bij de betrokken verantwoordelijkheden en verwerkers. Hierdoor kan de bescherming van de persoonlijke levenssfeer op onderdelen worden aangetast. Hierdoor ontstaan zwakke schakels in de keten van de verwerkingen van persoonsgegevens. Zwakke schakels kunnen een cumulatief effect veroorzaken waardoor het niveau van de bescherming van persoonsgegevens in een neerwaartse spiraal terecht komt.
Het kan ook zijn, dat door de inconsistentie of niet correcte toepassing van de privacyprincipes door een partij in de keten, de verwerking van persoonsgegevens wordt belemmerd. Dit leidt niet alleen tot privacyrisico's maar ook tot onnodige bureaucratie en additionele kosten.

Geheime (niet transparante) verwerking van persoonsgegevens
Indien een verwerking niet transparant is voor de burger kan de verwerking onder omstandigheden zonder zijn toestemming, tegen zijn voorkeuren of anderszins onrechtmatig plaatsvinden. Doordat burgers niet op de hoogte zijn van het gebruik van hun persoonsgegevens, kunnen zij de impact ervan in het sociaal maatschappelijk verkeer niet overzien. Zij hebben hier niet of nauwelijks controle meer over. Dit kan betekenen dat zij, zonder zich hiervan bewust te zijn, worden gestigmatiseerd en/of uitgesloten van sociaal maatschappelijke voorzieningen. Ingeval dit bewustzijn ontstaat, is soms zonder buitengewone inspanningen niet te achterhalen wat de oorzaak van de nadelige effecten is. Hierdoor is de burger ook niet of nauwelijks meer in staat om zijn wettelijke privacyrechten te effectueren. Net als bij onrechtmatig gebruik van uniek identificerende gegevens, kunnen de gevolgen onomkeerbaar en onherstelbaar zijn.

Niet toegestane verwerking van persoonsgegevens buiten de EU
Doorgifte van persoonsgegevens naar landen buiten de EU en EER naar landen zonder adequaat privacybeschermingsniveau herbergt op voorhand een hoog risico van onrechtmatige verwerkingen van persoonsgegevens, alsmede het niet kunnen effectueren van rechten van betrokkenen.

Datalekken
Ten gevolge van datalekken of breuken in de informatiebeveiliging kunnen persoonsgegevens in handen komen van onbevoegden en onrechtmatige verwerkingen tot gevolg hebben. Grote databases van overheidsdiensten en private partijen zijn gevoelig voor datalekken en onbevoegde uitwisseling van persoonsgegevens. Burgers hebben in de regel geen weet van dergelijke datalekken. Hierdoor zijn zij vatbaar voor de gevolgen van alle hiervoor genoemde risico's, die afhankelijk van de aard en omvang van het datalek, progressief in omvang kunnen toenemen.

Omkering van de bewijslast voor de betrokkene
Doordat persoonsgegevens in een database voorkomen en door de verwerkingsverantwoordelijke als juist worden bestempeld bestaat het risico dat bewijslast omgekeerd wordt.

Consumenten worden gedwongen om in te stemmen met het gebruik van hun persoonsgegevens

Voor diverse doelen en met het oog op het bijvoorbeeld het verkrijgen van diensten, gunsten of direct marketing doeleinden worden consumenten haast gedwongen in te stemmen met de verwerking van persoonsgegevens. De risico's die verbonden zijn aan deze verwerkingen worden onvoldoende benadrukt.

Bijlage V: Afkortingen en begrippen

Afkorting	Betekenis	Toelichting
AP	Autoriteit Persoonsgegevens	De Autoriteit Persoonsgegevens houdt toezicht op het gebruik van persoonsgegevens door organisaties en op de naleving van de Wbp en in de toekomst de AVG.
BIR	Baseline Informatiebeveiliging Rijksdienst	Biedt één normenkader voor de beveiliging van de informatiehuishouding van de Rijksoverheid.
BRP	Basisregistratie Personen	BRP wordt beheerd door de RvIG. Voor de controle van de identiteitskaart of het paspoort wordt een bevraging naar de BRP gedaan.
BSNk PP	BSNk Koppelregister	Het BSNk PP is een technische voorziening die de verantwoordelijkheid heeft voor het koppelen van het BSN van een natuurlijk persoon aan een polymorfe identiteit (PI) en een polymorfe pseudoniem (PP). Het BSNk PP levert een aantal diensten aan Authenticatiediensten/MU's.
BSNk IR	BSNk Inzageregister	Het Inzageregister is een component die in de USvE wordt beschreven. Dit register is erop gericht om het inzagerecht van de gebruiker te ondersteunen. Daartoe moeten alle aangesloten Authenticatiediensten/MU's de actuele status van de middelen bij het IR registreren. In het geval van DigiD Hoog zal de MU als bron van de statusinformatie het IR voeden. Aangezien het DH-middel (bij de MU) andere statussen kent dan het IR (conform USvE) zal daarbij een vertaling plaatsvinden.
BSNk SB	BSNk Sleutelbeheer	Het specifieke sleutelbeheer voor het stelsel wordt geregeld door het BSNk Sleutelbeheer. Vanuit het BSNk Sleutelbeheer worden de sleutels voor de HSM bij de DH Authenticatiedienst aangemaakt en gedistribueerd.
BZK	Binnenlandse Zaken en Koninkrijksrelaties	Logius is de dienst digitale overheid en onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De minister van BZK is eindverantwoordelijke.
CA	Chip Authentication	Controle uitgevoerd om vast te stellen dat de chip authentiek is. Met CA wordt ook een hoog beveiligd communicatiekanaal opgezet.
CAN	Card Access Number	Een nummer dat noodzakelijk is om een veilige communicatie op te zetten tussen de middleware en het DH-middel.
CIS	Card Interface Service	De middelen waar DigiD app geactiveerd is worden gekoppeld middels een CIS aan de DigiD kern.
CSCA	Country Signing Certificate Authority	Het DS-certificaat in de chip, waarmee de digitale handtekening is geverifieerd, dient te zijn uitgegeven door een CSCA.
--	Diginetwerk	Diginetwerk is een afsprakenstelsel voor het koppelen van besloten netwerken van de overheid. Via deze gekoppelde netwerken kunnen

Afkorting	Betekenis	Toelichting
		overheidsorganisaties onderling gegevens uitwisselen.
DigiD	Digitale Identiteit	Met DigiD kan worden ingelogd op websites van dienstverleners in het BSN-domein.
DH Authenticatiedienst / DH AD	DigiD Hoog Authenticatiedienst	De DH Authenticatiedienst is een vereiste rol binnen de USvE die de verantwoordelijkheid heeft voor het authenticeren van natuurlijke personen op basis van het door de natuurlijk persoon gebruikte authenticatiemiddel. In geval van DigiD Hoog is dit het DH-middel.
DH CTS	DigiD Hoog Card Test Service	Stelt gebruikers in staat om hun DH-middel te testen. De teststraat test alle componenten in de authenticatieketen. Uit beveiligingsoogpunt is de CTS losgekoppeld van de andere componenten van DigiD.
DH-middel	DigiD Hoog middel	Een middel dat gebruikt kan worden om te authenticeren/identificeren in het BSN-domein op het hoogst mogelijke betrouwbaarheidsniveau. Het DH-middel is een publiek middel dat wordt geplaatst op een WID. In eerste instantie zal het DH-middel op de NIK en het rijbewijs worden geplaatst in de vorm van een PCA.
DH Status Controller / DH SC	DigiD Hoog Status Controller	De DigiD Hoog Status Controller houdt de status van de DH-middelen bij en bewaakt de statusovergangen.
Transactielog / TL	Transactielog	De Transactielog houdt een log bij van het gebruik van DH middelen ten behoeve van het inzagerecht.
DIO	Directie Informatiesamenleving en Overheid	Onderdeel van het ministerie van BZK. Houdt zich bezig met concretiseren van de visie op de rol van de overheid in de informatiesamenleving.
EAC	Extended Access Control	Een beveiligingskenmerk van elektronische identiteitskaarten die de toegang tot gevoelige data op de NFC chip beschermt en beperkt.
eIDAS	Electronic Identity and Signature	De eIDAS-verordening gaat over elektronische identificatie en heeft de betrouwbaarheidsniveaus Laag, Substantieel en Hoog bepaald.
HSM	Hardware Security Module	Verantwoordelijk voor het genereren van versleutelde pseudoniemen. De software en de sleutels die in de HSM worden gebruikt, worden geleverd en onderhouden door het BSNk.
ICV	In control verklaring(en)	Jaarlijks intern self-assessment van controles, waaronder in relatie tot informatiebeveiliging, die aan het management van Logius en BZK wordt gerapporteerd.
IR	Inzageregister	Zie BSNk IR.
MCC	Mobile Competence Center	Ontwikkelt apps voor gebruikers, leverancier van DigiD app, in beheer van Belastindienst.
MRZ	Machine Readable Zone	Code dat is opgebouwd uit persoonlijke nummers en een algoritme ter verificatie (vanaf november 2014 aan de voorkant van het rijbewijs).
MU	Middelenuitgever	De uitgever van het DH-middel. In het geval van een NIK is de MU RvIG en in het geval van een rijbewijs de RDW.

Afkorting	Betekenis	Toelichting
NFC	Near Field Communication	Een draadloze manier om kleine hoeveelheden informatie uit te wisselen binnen een straal van 10 centimeter. Met de NFC reader wordt de NFC chip op het WID uitgelezen.
NIK	Nederlandse Identiteitskaart	Geldig Nederlands identiteitsbewijs dat voor DigiD Hoog kan worden gebruikt om het DH-middel op te plaatsen in de vorm van een PCA.
OIN	Overheidsidentificatienummer	Het OIN is een uniek identificerend nummer dat gebruikt wordt door overheidspartijen of organisaties met een publieke taak in de digitale communicatie met andere publieke of private partijen.
P.xyz	Persistent pseudoniem	Het pseudoniem waaronder een gebruiker uniek wordt geïdentificeerd bij de ontvangende partij (xyz).
PACE	Password Authenticated Connection Establishment	Het DH-middel maakt gebruik van het PACE-protocol voor het opzetten van een beveiligd kanaal tussen de chip en de middleware (eID server en eID client) voor het voorkomen van skimming en afluisteren.
PCA	Polymorph Card Application	Een smartcard toepassing die het mogelijk maakt om op de smartcard gerandomiseerde polymorfe identiteiten en pseudoniemen te gebruiken.
PI	Gerandomiseerde polymorfe identiteit	De publieke polymorfe identiteit is een identiteit gebaseerd op versleuteling van het BSN van de gebruiker. De PI wordt verkregen van het BSNk en tijdens de personalisatie in het document geplaatst. Met de juiste sleutels kan met de PI het BSN verkregen worden.
PIN	Personal Identification Number	Een persoonlijk nummer dat door de gebruiker is gekozen en is gekoppeld aan het DH-middel. Door de invoering van de PIN kunnen gegevens van het DH-middel afgegeven worden aan de DH AD.
PP	Gerandomiseerd polymorfe pseudoniem	Het private polymorfe pseudoniem is een versleuteling van een ‘one-way’ afgeleide van het BSN. Het BSN kan niet worden ontsleuteld op basis van het PP. Het PP wordt verkregen van het BSNk PP en tijdens de personalisatie in het document geplaatst. Het PP wordt versleuteld door de DH AD tot een VP zodat alleen de ontvangende partij het persistente pseudoniem (P.xyz) kan verkrijgen via een VP.
PUK	Personal Unblocking Key	De PUK maakt het mogelijk om een chipkaart die is geblokkeerd, door het meermaals invoeren van een verkeerde PIN, te deblokkeren. Na invoer van de PUK dient de gebruiker een nieuwe PIN in te voeren.
RDW	Dienst Wegverkeer	RDW is de MU van rijbewijzen. De RDW beheert het CRB.
RvIG	Rijksdienst voor Identiteitsgegevens	RvIG is de MU van Nederlandse identiteitsbewijzen. De RvIG beheert de BRP.
SAML	Security Assertion Markup Language	Een op XML gebaseerde standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen domeinen.

Afkorting	Betekenis	Toelichting
TA	Terminal Authentication	Controle uitgevoerd om vast te stellen dat de Inspection System de gevoelige data mag lezen van de chip. TA is gebaseerd op digitale certificaten.
USVE	Uniforme Set van Eisen	De Uniforme Set van Eisen 1.0 bevat de eisen voor publieke en private Authenticatiemiddelen, op Betrouwbaarheidsniveau Laag, Substantieel en Hoog.
VI	Versleuteld gerandomiseerd identiteit	Door de DH Authenticatiedienst wordt de PI versleuteld in een VI specifiek voor de dienstverlener, zodat alleen de betreffende dienstverlener het BSN kan ontsleutelen.
VP	Versleuteld gerandomiseerd pseudoniem	Door de DH Authenticatiedienst wordt de PP versleuteld in een VP, zodat alleen de ontvangende partij het persistente pseudoniem (P.xyz) kan ontsleutelen met de juiste sleutel van het BSNk SB.
WID	Wettelijk Identiteitsdocument	Documenten genoemd in artikel 1 van de Wet op de identificatieplicht waarmee in bij de wet aangewezen gevallen de identiteit van personen kan worden vastgesteld. In de eerste release van DigiD Hoog kan alleen de NIK of het rijbewijs als WID gebruikt worden. Voor de producenten van de documenten verwijzen wij naar MU.

Tabel 7: afkortingen en begrippen

Bijlage VI: Privacyrisico's DigiD Substantieel

In deze bijlage zijn de privacyrisico's en aanbevelingen opgenomen die zijn geïdentificeerd met betrekking tot DigiD Substantieel en de bestaande DigiD. De risico's en aanbevelingen zijn afkomstig uit de samenvatting van de PIA op DigiD Substantieel (Mazars, 2017).

Risico's en aanbevelingen gerelateerd aan DigiD Substantieel

- Voor het verifiëren van een paspoort of identiteitskaart worden BRP-gegevens van RvIG gebruikt. In de huidige systematiek worden meer gegevens ontvangen door Logius dan strikt noodzakelijk is, namelijk de gegevens van de meest recente paspoorten en identiteitskaarten behorend bij een BSN. De gegevensaanvraag is niet specifiek voor Substantieel waardoor alle gegevens waar DigiD autorisatie voor heeft, worden ontvangen. De gegevens die benodigd zijn voor DigiD Substantieel kunnen door Logius wel nader gespecificeerd worden. De huidige functionaliteit geboden door RvIG biedt echter niet de mogelijkheid om de gegevensaanvraag specifiek te maken op basis van het documentsoort (paspoort/identiteitskaart). Als maatregel bij Logius is voorzien dat na uitvraag van gegevens deze, indien niet nodig voor de controle, per direct tot maximaal één uur nadien worden verwijderd waardoor het risico van het niet voldoen aan dataminimalisatie is geminimaliseerd. Aanbevolen wordt de gegevensaanvraag voor Substantieel te specificeren, zodat alleen de gegevens worden ontvangen die benodigd zijn voor DigiD Substantieel. Het verdient aanbeveling om bij de doorontwikkeling van DigiD Substantieel de RvIG te verzoeken om de functionaliteit te bieden voor het specifiëren van de BRP bevraging, zodat alleen de noodzakelijke gegevens van het voor de verificatie gebruikte WID worden ontvangen.
- De huidige privacyverklaring DigiD vereist nog aanpassing naar de specifieke verwerkingen van persoonsgegevens en doelstellingen welke gekoppeld zijn aan DigiD Substantieel. Ook een aanpassing in de verklaring aangaande de bewaartermijnen en hoe een account van DigiD Substantieel kan worden beëindigd is nog nodig. Dit is door Logius onderkend en de actie om de privacyverklaring te actualiseren is onderhanden.
- Voor het uitvoeren van de controles van het WID maakt Logius gebruik van de RDA-server van een subleverancier. De DigiD backend voert controles uit op de gegevens van de chip op het WID om te verifiëren dat het aangeboden WID bij die gebruiker hoort en authentiek is. Nadat de controles zijn afgerond zijn de gegevens uit de BRP of het CRB en van de NFC chip niet meer beschikbaar in DigiD. Vastgesteld is dat geen subverwerkersovereenkomst is opgesteld met deze subleverancier. Aangezien de subleverancier in verband met de werking van DigiD Substantieel persoonsgegevens kan verwerken, dient dit nog gerealiseerd te worden. Dit is door Logius onderkend en de actie om de subverwerkersovereenkomst te realiseren is onderhanden.
- In de bestaande applicatiearchitectuur en het high level design is aandacht geschonken aan maatregelen van interne controle die zich richten op het achteraf controleren en afleggen van verantwoording over de werking van gerealiseerde beveiligingsmaatregelen. In de ontwerpdocumentatie van DigiD Substantieel zijn dit soort maatregelen niet expliciet opgenomen. Het verdient aanbeveling om naast de al aanwezige vooral preventief gerichte beveiligingsmaatregelen meer aandacht te schenken aan controls waarmee achteraf verantwoording kan worden afgelegd over de effectiviteit van de geïmplementeerde beveiligingsmaatregelen over een bepaalde periode. Hierbij kan gedacht worden aan het verkrijgen van inzicht in de effectiviteit van de gerealiseerde beveiligingsmaatregelen op basis van rapportages vanuit o.a. IT security audits, vulnerability- en penetratietesten en periodieke monitoring.

- In de huidige ontwerpdocumentatie is nog beperkt aandacht geschonken aan maatregelen van interne controle die zich richten op het borgen van de datakwaliteit waarmee achteraf de betrouwbaarheid van de binnen Logius aanwezige gegevensverzamelingen kan worden aangetoond. Het verdient aanbeveling om maatregelen hiervoor te ontwerpen. Denk hierbij aan periodieke verbandcontroles, gebruik van de bestaande replica database, gebruik van hashing technieken en rapportages over de werking van deze controlemaatregelen.

Risico's en aanbevelingen gerelateerd aan bestaand DigiD

- Een bestaand risico is dat Logius beschikt over persoonsgegevens vanuit de inlogtransacties van gebruikers. De transactiegegevens bevatten een verwijzing naar de accountgegevens, BSN's en IP-adressen. In deze transactiegegevens is ook vastgelegd bij welke dienst de gebruiker heeft ingelogd. Hierdoor ontstaat een privacygevoelige dataset op basis waarvan kwaadwillenden profielen van gebruikers op zouden kunnen stellen. Denk hierbij aan gegevens van gebruikers die met hun DigiD inloggen bij dienstaanbieders die zich inzetten voor ondersteuning bij jeugdzorg, bij reclassering of binnen het sociaal domein. De potentiële impact van ongewenste profiling van deze gevoelige dataset is hoog. Logius geeft nadrukkelijk aan dat profileren geen activiteit is waar zij zich mee bezighoudt of van plan is zich mee bezig te houden. Logius heeft diverse beveiligingsmaatregelen getroffen waardoor toegang tot deze gevoelige gegevens is beperkt tot alleen functionarissen die daar rechten toe hebben. Daarnaast zijn maatregelen aanwezig die misbruik kunnen detecteren. Het verdient aanvullend aanbeveling om een sterke scheiding aan te brengen tussen het verwerken van BSN's en IP-adressen waarmee eventueel misbruik wordt bemoeilijkt.
- De huidige DigiD maakt gebruik van encryptie op het niveau van harddisks en wachtwoorden. Het gebruik van verdergaande encryptie van gevoelige gegevens en het gebruik van gerandomiseerde polymorfe pseudo-identiteiten zijn in het ontwerp van DigiD Substantieel nog niet voorzien. Logius is voornemens om deze technologieën in de toekomst wel te gaan gebruiken en deze technologieën zijn onderdeel van het voorlopige ontwerp voor DigiD Hoog. Het verdient aanbeveling om deze technische maatregelen uiteindelijk ook te realiseren voor DigiD Substantieel. Met deze maatregelen wordt voorkomen dat het BSN gebruikt wordt binnen de authenticatiedienst van DigiD. Door deze voorgenomen technische voorzieningen worden de bevindingen bij de punten 2 en 7 van deze managementsamenvatting in positieve zin geraakt.
- Doordat de wettelijke bewaartermijn van transactiegegevens[18] door wettelijke besluitvorming is opgeschroefd naar vijf jaar ontstaat een omvangrijke cumulatie van inloghistorie van gebruikers. Deze cumulatie van inloghistorie neemt in kwantiteit toe en kan in samengevoegde vorm privacygevoelige informatie opleveren en eventueel gebruikt worden voor profiling. Hierbij merken we overigens op dat Logius zich niet met profiling bezighoudt. Ter beheersing van dit risico zijn de bestaande, compenserende gegevensbeveiligingsmaatregelen getroffen bij Logius. Het verdient aanbeveling om de risico's van deze cumulatie van gevoelige informatie bij de verdere ontwikkeling van DigiD Substantieel opnieuw te evalueren en te onderzoeken of de gestelde bewaartermijnen aanpassing behoeven. Ter indicatie: op basis van het huidige DigiD gebruik ontstaat over een periode van vijf jaar naar verwachting een dataset van 1,25 miljard records aan inloghistorie. Dit is een voorzichtige inschatting. Deze risico's van cumulerende inloghistorie dient ook in relatie te worden gezien met het risico

[18] Bewaartermijnen hebben een wettelijke grondslag in het besluit verwerking persoonsgegevens GDI (Staatsblad van het Koninkrijk der Nederlanden, 2016)

van het combineren van IP-adressen met BSN. Zie hiervoor ook punt 7 van deze managementsamenvatting.

- Tijdens ons onderzoek bleek dat er nog niet eerder een integrale PIA was uitgevoerd op de bestaande DigiD. In de ontwikkelcycli van de bestaande DigiD zijn per fase de eisen van de Wbp meegenomen. Een hanteerbaar integraal overzicht van alle verwerkingen van persoonsgegevens op zowel functioneel als technisch niveau, inclusief de verwerkingen van persoonsgegevens gekoppeld aan technische systemen en een beschrijving van de bijbehorende doelstellingen, is nog niet volledig voorhanden. Het verdient aanbeveling om bij de doorontwikkeling van DigiD Substantieel een dergelijk overzicht op te stellen en de privacyrisico's hiervan integraal te analyseren. Dit punt is onderkend door Logius en wordt opgepakt.

Bijlage VII: Privacybevorderende maatregel per fase

Met de release van DigiD Hoog blijven de bestaande privacyrisico's van de bestaande DigiD en DigiD Substantieel vrijwel ongewijzigd. In onderstaande tabel zijn op hoofdlijnen de effecten van de privacybevorderende maatregelen van DigiD Hoog, in de eerste fase, van de laatste fase van DigiD Hoog en van de bestaande DigiD voorzieningen tegen elkaar afgezet.

Onderwerp	Bestaand DigiD & DigiD Substan-tieel	DigiD Hoog eerste fase	DigiD Hoog laatste fase	Toelichting
Betrouwbaarheid authenticatie				Met DigiD Hoog wordt een hoger betrouwbaarheidsniveau van authenticatie bereikt.
Functiescheiding uitgifte en gebruik authenticatiemiddel				De middelenuitgever is verantwoordelijk voor de uitgifte van een DH-middel en het authenticatieproces is de verantwoordelijkheid van Logius. De authenticatiedienst van Logius krijgt alleen die gegevens die strikt noodzakelijk zijn.
Randomisering				Randomisering van de PI en het PP heeft als positief effect dat iedere keer een ander PI/PP wordt gegenereerd waardoor onrechtmatig gebruik van de data voor profiling bemoeilijkt wordt. De risico's van een onverhoopt datalek wordt geminimaliseerd.
Beheersing systemen				Door de afbouw en/of compartimentering van bestaande systemen en de implementatie van nieuwe compartimenten wordt de privacybescherming in de eindsituatie beter beheersbaar.
Fraudeonderzoek				Een separate voorziening voor fraudeonderzoek wordt ontwikkeld waardoor de toegang tot de specifiek daarvoor benodigde informatie beter beheersbaar wordt.
Dataminimalisatie				DigiD Hoog verzamelt en gebruikt minder gegevens door onder andere het gebruik van pseudoniemen en het scheiden van het uitgifteproces met het authenticatieproces.
Compartimentering				Compartimentering wordt gerealiseerd door technische scheiding van systemen. In de beginsituatie zal dit nog niet volledig gerealiseerd zijn.
BSN-gebruik vs. Pseudonimisering				Het BSN-gebruik neemt af door het gebruik van polymorfe identiteiten en pseudoniemen. De authenticatiedienst zet in de eerste fase het pseudoniem vroegtijdig om naar het BSN. In de eindsituatie wordt dit pas laat in het proces, door de dienstverlener, gedaan. Het BSN wordt dan niet meer binnen de authenticatiedienst van Logius verwerkt.
Cumulatie persoonsgegevens				Door compartimentering neemt de cumulatie van inloghistorie, waaruit is te herleiden welke persoon bij welke dienstverlener heeft ingelogd, af. Risico's van onrechtmatige profiling worden hiermee gemitigeerd.
Impact datalek				In de eindsituatie van DigiD Hoog is een encryptiesleutel van het BSNk benodigd om uit de inloghistorie te kunnen herleiden welke gebruiker bij welke dienstverlener heeft ingelogd. De impact van een datalek neemt af indien deze gegevens niet herleid kunnen worden zonder sleutel.
IP-adressen				Op dit moment is nog in onderzoek of het IP-adres in de eindsituatie van DigiD Hoog in de transactielog moet worden opgenomen. Indien het IP-adres wordt opgenomen is de verwachting dat dit in versleutelde vorm zal gebeuren.

Tabel 8: privacybevorderende maatregelen per fase

Legenda

	Privacybevorderende maatregel op laag niveau
	Privacybevorderende maatregel deels geïmplementeerd
	Privacybevorderende maatregel op hoog niveau