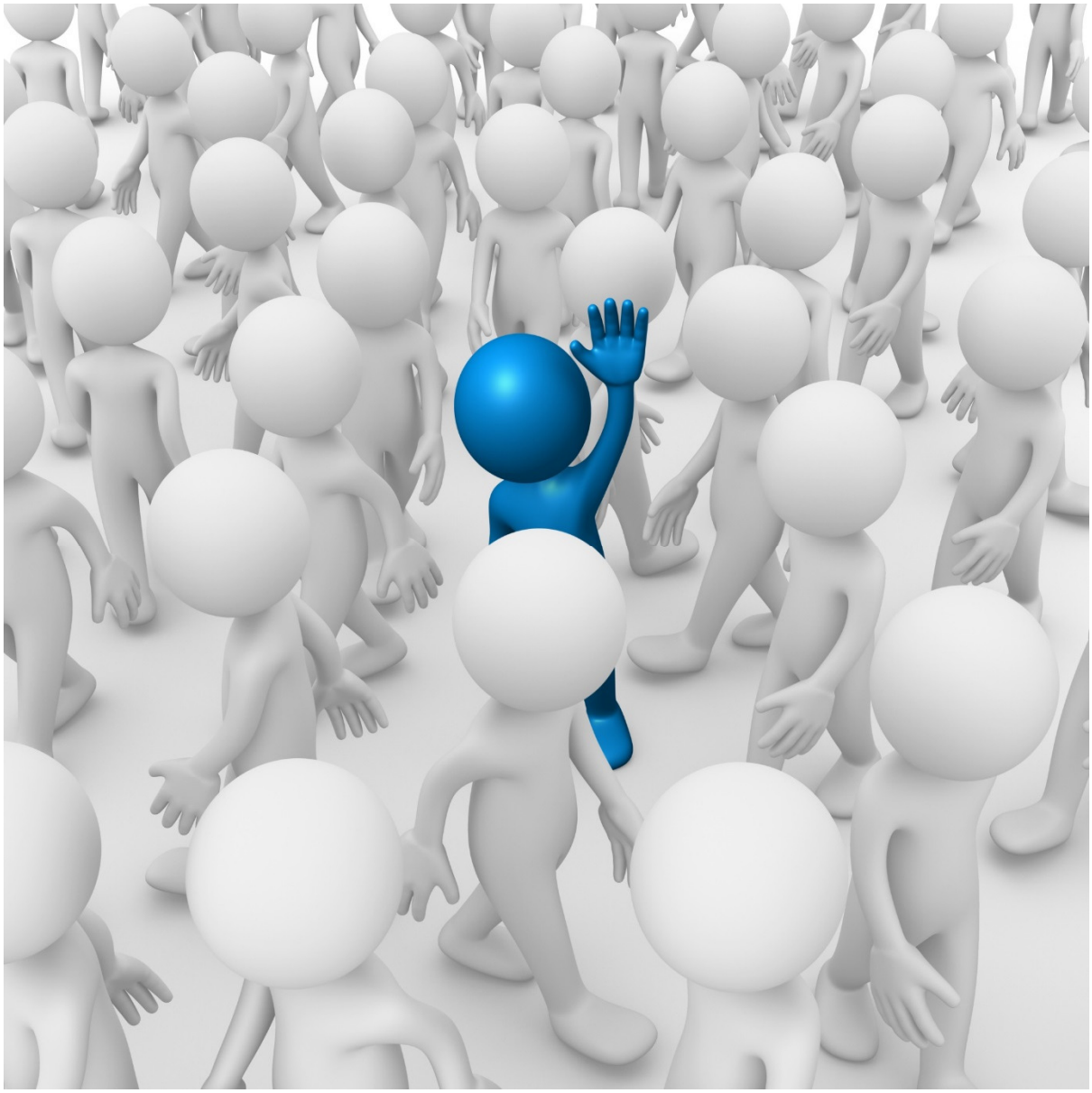
PRIVACY IMPACT ASSESSMENT

DigiD Substantieel

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

6 september 2017



Versie 1.1

MAZARS

INHOUDSOPGAVE

1. Inleiding

1.1. Aanleiding en achtergrond Privacy Impact Assessment

DigiD wordt al geruime tijd gebruikt als middel door gebruikers om in te loggen op online systemen van publieke dienstaanbieders. Dienstaanbieders 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 dienstaanbieders die gebruikers laten inloggen met DigiD.

Het digitale authenticatiesysteem 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.

Met het toenemend gebruik van DigiD stijgt de behoefte aan een versterkte betrouwbaarheid van het bestaande DigiD-inlogmiddel. DigiD is met de komst van Idensys niet langer het enige digitale authenticatiemiddel in het publieke domein. In de toekomst gaan naar alle waarschijnlijkheid ook private organisaties authenticatiemiddelen met een hoger betrouwbaarheidsniveau aanbieden.

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 of in te loggen met de DigiD app. 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 in de toekomst niet meer 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’.[2] [3] De eIDAS-verordening betreft de elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de Europese interne markt. De eIDAS-verordening vervangt de huidige Europese richtlijn voor elektronische handtekeningen, richtlijn 1999/93/EG, en onderscheidt de betrouwbaarheidsniveaus Laag, Substantieel en Hoog.

Het ministerie van BZK wil gebruikers en dienstaanbieders meerdere betrouwbaarheidsniveaus aanbieden voor authenticatie, door het realiseren van DigiD met de betrouwbaarheidsniveaus eIDAS Substantieel en eIDAS Hoog. Door Logius zal via een aantal stappen eerst DigiD Substantieel worden gerealiseerd en in een later stadium DigiD Hoog. Een eerste stap is de realisatie van een betrouwbaar uitgifteproces op het niveau van

[1] Logius Jaarverslag 2016
[2] 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.
[3] Verordening (EU) Nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten en elektronische transacties in de interne markt.

Substantieel, waarna dit middel direct gebruikt kan worden door de dienstaanbieder en de gebruiker.

In de eIDAS-verordening is onder meer aangegeven dat bij de uitgifte van een authenticatiemiddel gegevens gecontroleerd moeten worden aan de hand van een gezaghebbende bron en dat de geldigheid van het bewijs dat gebruikt wordt voor het uitreiken van een digitaal authenticatiemiddel gecontroleerd wordt. Voor het gebruik van het uitgereikte authenticatiemiddel geldt de eis dat beveiligingscontroles worden uitgevoerd ter verificatie van het authenticatiemiddel en maatregelen zijn getroffen ter bestrijding van misbruik, waaronder offline analyse.

Om betrouwbaarheidsniveau 'Substantieel' te behalen is door Logius gekozen voor een aanpak waarbij de identiteit van de gebruiker geverifieerd wordt door het initieel én periodiek scannen van de chip, aanwezig op een wettelijk identiteitsdocument (hierna: WID), met de DigiD app op het mobiele apparaat van de gebruiker.

Het introduceren van DigiD Substantieel 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[4]. 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. Het is daarom van groot belang dat tijdens de ontwerpfase van DigiD Substantieel wordt geïnventariseerd welke privacybedreigende risico's er zijn. Deze door Mazars uitgevoerde privacy impact assessment (Hierna: PIA) gaat uit van de door de OECD/OESO[5] beschreven universele privacyprincipes. Per privacyprincipe zijn in deze PIA de bevindingen, risico's en aanbevelingen opgenomen.

Alvorens in te gaan op de privacyprincipes wordt vastgesteld of de met DigiD Substantieel 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 Substantieel. Deze privacy impact assessment (hierna: PIA) richt zich op de definitieve Project Start Architectuur van DigiD Substantieel van 7 maart 2017, versie 1.0 (hierna: PSA of PSA DigiD Substantieel).

1.2. Doelstelling en scope van de PIA

1.2.1. 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. Door een PIA gedurende het ontwerpproces regelmatig uit te voeren, kunnen

[4] Zie artikel 10, leden 2 en 3 Grondwet, artikel 8 EVRM, artikel 8 EU-Grondrechtenhandvest
[5] OECD / OESO: Organization for Economic Co-operation and Development / Organisatie voor Economische Samenwerking en Ontwikkeling.

(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 DigiD Substantieel bij de diverse stakeholders te creëren, zoals bij verantwoordelijke overheden, gebruikers, betrokken derden en belangenorganisaties. De uitkomsten van de PIA kunnen hergebruikt worden in geval van ontwerp- en systeemaanpassingen en bij verdere doorontwikkeling. Hierbij dient uiteraard kritisch beoordeeld te worden wat de impact is van wijzigingen op de verschillende onderwerpen die zijn behandeld in deze PIA. De PIA-rapportage is een communicatiemiddel.

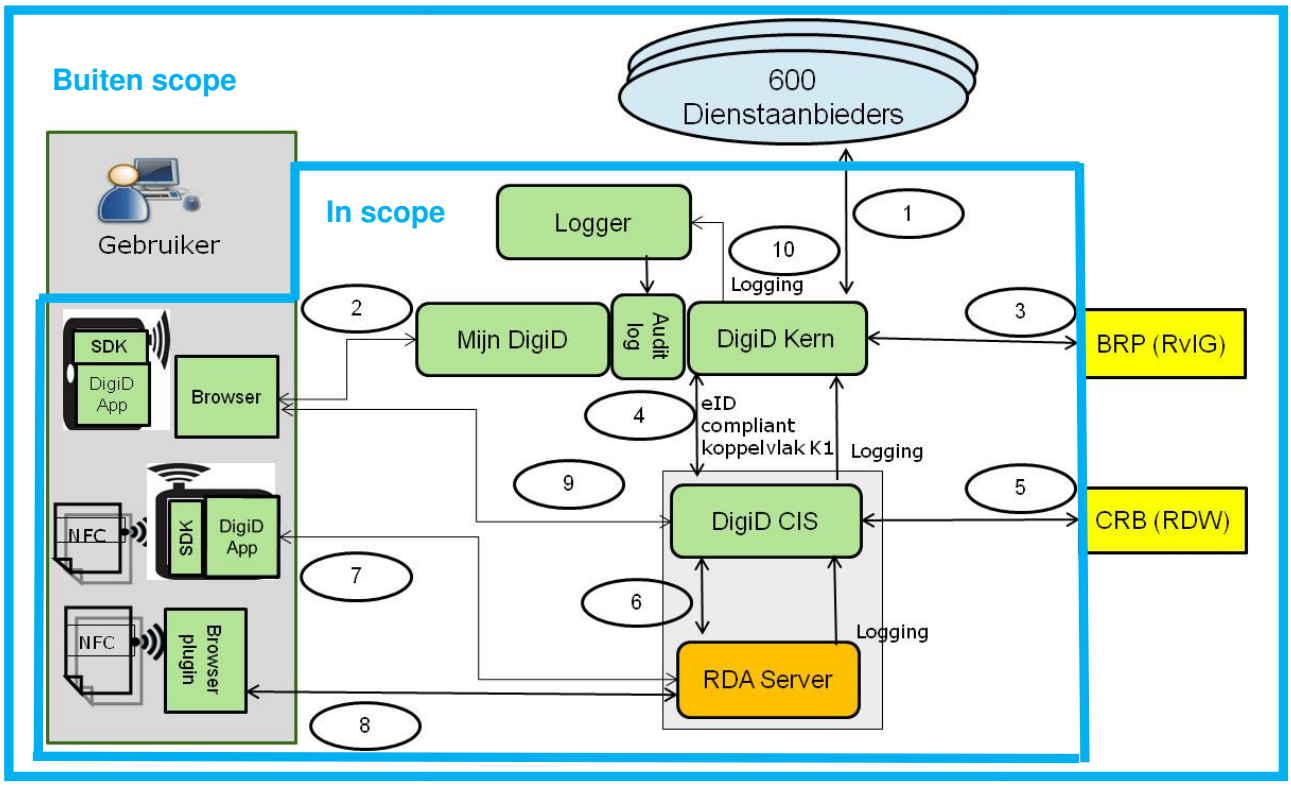
1.2.2. Scope van de PIA DigiD Substantieel

De scope van de PIA op het ontwerp van DigiD Substantieel bestaat uit het versterkingsproces, waarbij de gebruiker zijn bestaande DigiD-account naar betrouwbaarheidsniveau 'Substantieel' verhoogt en het authenticatieproces op basis van DigiD Substantieel. Naast het ontwerp is naar vermogen ook aandacht besteed aan de productieomgeving waarbinnen DigiD Substantieel zal worden geplaatst.

Het versterkingsproces begint met een authenticatie op betrouwbaarheidsniveau 'Midden', waarbij de gebruiker met gebruikersnaam, wachtwoord en sms of gebruikersnaam en app met pincode inlogt op mijn.digid.nl. De gebruiker kiest voor de optie 'inlogniveau verhogen' waarna wordt gevraagd een QR-code te scannen. Deze QR-code is gegenereerd op basis van een accountspecifieke sessie-ID van de gebruiker. Daarna geeft de gebruiker aan met welk WID-soort hij het inlogniveau wil verhogen. Eenmaal gekozen moet de gebruiker zijn WID eenmalig scannen met behulp van de DigiD app. Zodra het WID geverifieerd is, wordt het inlogniveau verhoogd en kan de gebruiker op niveau 'Substantieel' inloggen bij dienstaanbieders. Voor het inloggen kan de gebruiker kiezen uit twee mogelijkheden: via de browser op het mobiele apparaat waar de app op is geïnstalleerd (web to app) of via de browser op een ander apparaat. Bij het inloggen via de browser op het mobiele apparaat waar ook de app op is geïnstalleerd dient de gebruiker zijn gebruikersnaam in te voeren en kan vervolgens met de pincode van de DigiD app worden ingelogd. In dit geval hoeft geen QR-code gescand te worden. Indien de website wordt bezocht via een apparaat waarop de app niet beschikbaar is, moet de gebruiker op dit apparaat zijn gebruikersnaam invoeren en vervolgens met het apparaat waar de DigiD-app op is geïnstalleerd de (getoonde) QR-code scannen en zijn pincode invoeren.

De PSA voor DigiD Substantieel geeft aan dat de ontwikkeling van de DigiD app buiten de scope van de PSA valt aangezien een ander project de verantwoordelijkheid draagt voor de architectuur van de DigiD app. Hoewel de DigiD app strikt genomen buiten de scope van de PSA valt, wordt binnen deze PIA naar vermogen wel aandacht besteed aan de DigiD app aangezien de app onderdeel is van DigiD Substantieel.

De koppelvlakken met de DigiD app en gerelateerde processen zijn in scope van deze PIA meegenomen. In onderstaand schematisch overzicht van het werkingsproces is aangegeven welke componenten en koppelvlakken in scope zijn. Voor een toelichting op de koppelvlakken en gegevensstromen verwijzen wij naar paragraaf 3.6.



1.2.3. Overzicht verwerking persoonsgegevens DigiD Substantieel

In artikel 2 van het Besluit verwerking persoonsgegevens generieke digitale infrastructuur (hierna: Besluit GDI) zijn de persoonsgegevens opgenomen die worden verwerkt door Logius.[6] Echter bevat het Besluit GDI nog niet de gegevens die (additioneel) voor DigiD Substantieel verwerkt zullen worden. In onderstaande opsomming zijn de gegevens die additioneel worden verwerkt voor DigiD Substantieel t.o.v. de bestaande DigiD (DigiD Basis en DigiD Midden) blauw gekleurd en onderstreept:

- 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:
  - Naam;
  - Geboortedatum;
  - Status persoonslijst (bijv. overleden);
  - Nationaliteit (alleen nodig voor het balieproces);
  - Gegevens om ingezetenschap of niet-ingezetenschap in de Basisregistratie Personen (hierna: BRP) vast te kunnen stellen;
  - Adres;
  - Postcode;

[6] Besluit verwerking van persoonsgegevens generieke digitale infrastructuur, Stb. 2016, 195

- BSN;
- Indien gebruik paspoort of identiteitskaart ter verificatie:
  - Documentnummer;
  - Geboortedatum;
  - Einde geldigheidsdatum;
- Indien gebruik rijbewijs ter verificatie:
  - Rijbewijsnummer.
- Datagroepen Near Field Communication (hierna: NFC) chip WID;
- Accountgegevens:
  - (Mobiel) telefoonnummer;
  - E-mailadres;
  - Gebruikersnaam;
  - Wachtwoord (versleuteld).
- Gebruiksgegevens:
  - IP-adres;
  - 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, unieke gepseudonimiseerde BSN[7], sessie-ID, gekozen document soort, 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, waaronder het BSN en andere gegevens die worden verwerkt bij de ondersteuning van de gebruiker van DigiD.

1.3. Aanpak en opbouw van de PIA

Deze PIA heeft betrekking op de PSA van DigiD Substantieel. 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 door de OECD/OESO[9] beschreven universele privacyprincipes. 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. Voor de privacyprincipes en privacyrisico's die wij hebben onderkend verwijzen wij naar Bijlage II en Bijlage III.

[7] Het unieke gepseudonimiseerde BSN is niet te herleiden naar een BSN en wordt niet gebruikt voor authenticatiedoeleinden maar voor het bepalen van het aantal unieke gebruikers van DigiD Substantieel. Dit gegeven vormt de basis voor de facturering t.b.v. de RDA-server.
[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.

Privacyprincipes en -risico's staan onderling tot elkaar in relatie. Zij kunnen elkaar beïnvloeden, versterken, verzwakken en vertonen strijdigheden. 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 van DigiD Substantieel. 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.

1.4. Leeswijzer

In hoofdstuk 2 zijn de uitkomsten van de PIA samengevat in de meest significante bevindingen en risico's van het ontwerp van DigiD Substantieel. Tevens worden in deze managementsamenvatting aanbevelingen gedaan voor de meest relevante mitigerende maatregelen. In hoofdstuk 3 wordt een beschrijving gegeven van DigiD Substantieel, beginnend met de aanleiding en doelstelling van het ontwerp van DigiD Substantieel. Vervolgens zijn de belanghebbenden van DigiD Substantieel benoemd en is het wettelijk kader beschreven, waarna een procesbeschrijving is gemaakt voor het gebruik van DigiD Substantieel. Deze beschrijving is high level en functioneel en beschrijft hoe een gebruiker het betrouwbaarheidsniveau kan verhogen. Tot slot is een beschrijving gemaakt van alle gegevensstromen en koppelingen die aanwezig zijn bij het verhogen van het betrouwbaarheidsniveau van het DigiD-account en de bewaartermijnen van de logging. In hoofdstuk 4 is de noodzaak van de verwerkingen van persoonsgegevens binnen DigiD Substantieel benoemd en zijn vervolgens de bevindingen en aanbevelingen met betrekking tot DigiD Substantieel beschreven per privacyprincipe. In de bijlagen is de literatuurlijst opgenomen met bronnen die gebruikt zijn voor het uitvoeren van deze PIA en de totstandkoming van dit rapport. Ook is hier een overzicht gegeven van de rollen 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 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 III. Bijlage IV geeft ten slotte de betekenis van en een toelichting op de gebruikte afkortingen in het rapport.

2. Managementsamenvatting

Met de introductie van DigiD Substantieel versterkt Logius de betrouwbaarheid van DigiD. De bestaande versie van DigiD kent een basisaccount (gebruikersnaam + wachtwoord) en een 2-factor middenaccount (basis + sms of gebruikersnaam + DigiD app). DigiD Substantieel voegt hier een authenticatieniveau aan toe. De gebruiker kan met behulp van de DigiD app zijn WID scannen en daarmee het inlogniveau ophogen naar DigiD Substantieel. Met DigiD Substantieel wordt een authenticatiemiddel verkregen waarvan Logius verwacht dat deze voldoet aan de Europese eisen van eIDAS-niveau 'Substantieel', maar dit kan pas op een later moment (na notificatie) worden vastgesteld. Realisatie van DigiD Substantieel is een belangrijke privacybevorderende maatregel. DigiD Substantieel voorziet bovendien in de wens van bepaalde afnemers van DigiD om een authenticatiemiddel met een hoger betrouwbaarheidsniveau aan te bieden.

De toevoeging van DigiD Substantieel als authenticatiemiddel naast de middelen 'Basis' en 'Midden' heeft geleid tot enkele veranderingen in het DigiD-landschap, waaronder de introductie van de mogelijkheid tot scannen van het WID van de gebruiker met behulp van de DigiD app, inclusief het valideren van WID-gegevens bij de Rijksdienst voor Identiteitsgegevens (hierna: RvIG) op basis van het paspoort en de identiteitskaart, en het valideren van WID-gegevens bij de Rijksdienst Wegverkeer (hierna: RDW) op basis van het rijbewijs. Vastgesteld is dat met deze wijzigingen slechts een zeer beperkte set van aanvullende persoonsgegevens tijdens het controleproces wordt gebruikt ten opzichte van de bestaande authenticatiemiddelen. Bovendien zijn in de DigiD-architectuur maatregelen getroffen waarmee de vastlegging en uitwisseling van gegevens als gevolg van dit nieuwe middel zijn geminimaliseerd.

De uitkomsten van de PIA op de PSA DigiD Substantieel, geven aan dat de introductie van DigiD Substantieel en de daarbij gekozen uitbreiding van de architectuur, slechts een beperkt aantal nieuwe privacyrisico's introduceert voor de gebruiker. Deze privacyrisico's worden enerzijds gemitigeerd door organisatorische en technische beveiligingsmaatregelen die al golden voor de bestaande middelen. Anderzijds geldt dat met de introductie van DigiD Substantieel de kans op misbruik van DigiD sterk verkleind wordt. De PIA onderkent niettemin een aantal resterende privacyrisico's en aandachtspunten aangaande de introductie van DigiD Substantieel.

DigiD Substantieel kan niet los gezien worden van de werking van de bestaande DigiD-omgeving. Doordat DigiD Substantieel een uitbreiding betekent van de bestaande DigiD-componenten en bestaande koppelingen, met uitzondering van de Remote Document Authentication server (hierna: RDA) en de nieuwe koppeling met het Centraal register Rijbewijzen en Bromfietscertificaten (hierna: CRB), blijven risico's die gelden voor bestaande DigiD-componenten nog steeds van kracht voor DigiD Substantieel. Deze risico's zijn niet direct te herleiden uit de PSA waarvoor deze PIA geldt, maar blijken uit nader onderzoek naar het functioneren van de bestaande DigiD-omgeving. De keuze om binnen DigiD Substantieel gebruik te maken van bestaande componenten, is genomen vanuit praktische en bedrijfseconomische motieven, ter beperking van projectrisico's, om bestaande koppelvlakken niet te hoeven vervangen en vanwege het te realiseren tijdpad.

De belangrijkste binnen deze PIA onderkende privacyrisico's en aanbevelingen zijn hierna weergegeven. Hierbij is onderscheid gemaakt naar risico's en aanbevelingen die specifiek te relateren zijn aan het ontwerp van DigiD Substantieel en risico's die voortvloeien uit het gebruik van elementen van de bestaande DigiD.

Risico's en aanbevelingen gerelateerd aan DigiD Substantieel

1. 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.
2. 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.
3. 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.
4. 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.
5. 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

6. 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.

7. 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.
8. Doordat de wettelijke bewaartermijn van transactiegegevens[10] 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 van het combineren van IP-adressen met BSN. Zie hiervoor ook punt 7 van deze managementsamenvatting.
9. 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.

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

3. Beschrijving DigiD Substantieel

3.1. Aanleiding DigiD Substantieel

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 dienstaanbieders in het BSN-domein:

- DigiD Basis: inloggen met gebruikersnaam en wachtwoord;
- DigiD Midden:
  - inloggen met gebruikersnaam, wachtwoord en sms;
  - inloggen met gebruikersnaam en het scannen van de QR-code met de DigiD app (beveiligd met een pincode). De QR-scan is nodig indien de website wordt bezocht via een apparaat waarop de app niet beschikbaar is. De QR-code wordt gescand met het apparaat waar de app wel op is geïnstalleerd;
  - inloggen met gebruikersnaam en de DigiD app (beveiligd met een pincode). De QR-scan is niet nodig als de website wordt bezocht met het apparaat waar de app op is geïnstalleerd (web to app).

Om meer diensten online aan te kunnen bieden, gebruikers op een hoger betrouwbaarheidsniveau te kunnen laten inloggen en te voldoen aan de eIDAS-norm, is DigiD Substantieel ontworpen. Daarnaast is Logius niet (meer) de enige aanbieder van digitale authenticatiemiddelen in het publieke domein. Private organisaties hebben ook de mogelijkheid om middelen aan te bieden om in te loggen bij organisaties in zowel de private als de publieke sector. In de toekomst zullen zij mogelijk de betrouwbaarheidsniveaus verhogen naar eIDAS Substantieel.

De eisen gesteld om het authenticatieniveau van ‘Substantieel’ te bereiken zijn vastgelegd in de eIDAS-verordening. Hierin is onder meer aangegeven dat bij de uitgifte van een authenticatiemiddel gegevens gecontroleerd moeten worden aan de hand van een gezaghebbende bron en dat de geldigheid van het bewijs voor het uitreiken van een digitaal authenticatiemiddel gecontroleerd wordt. Voor het gebruik van het uitgereikte authenticatiemiddel geldt de eis dat er beveiligingscontroles worden uitgevoerd ter verificatie van het authenticatiemiddel en maatregelen zijn getroffen ter bestrijding van misbruik, waaronder offline analyse.

Om betrouwbaarheidsniveau ‘Substantieel’ te behalen is door Logius gekozen voor een aanpak waarbij de identiteit van de gebruiker geverifieerd dient te worden door het initieel en periodiek scannen van de chip op een WID met de DigiD app. De DigiD app is in maart 2017 door Logius in productie genomen, maar dit is nog zonder de functionaliteit om het account te verhogen naar niveau DigiD Substantieel.

3.2. Doelstellingen DigiD Substantieel

De doelstelling van DigiD Substantieel is het versterken van het betrouwbaarheidsniveau van DigiD naar eIDAS ‘Substantieel’. De volgende (sub)doelstellingen worden onderkend:

- Het bieden van de mogelijkheid aan gebruikers en dienstaanbieders om voor een hoger betrouwbaarheidsniveau te kunnen kiezen voor bestaande diensten;
- Het creëren van de mogelijkheid om onlinediensten 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;

- Bijdragen aan de doelen van het programma Versterken DigiD en het programma Impuls eID: een veiliger authenticatiemiddel en de basis leggen voor DigiD Hoog.

De vereisten en criteria van betrouwbaarheidsniveau eIDAS 'Substantieel' verschillen in de volgende punten ten opzichte van betrouwbaarheidsniveau laag voor natuurlijke personen (Commissie, 2015):

- Bewijs en verificatie van identiteit (natuurlijke personen), op basis van één van volgende alternatieven:
  - Er is geverifieerd dat de persoon in het bezit is van het bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat dit de opgegeven identiteit vertegenwoordigt en het bewijs is gecontroleerd op de echtheid ervan; of het bestaan ervan volgens een gezaghebbend bron bekend is en het betrekking heeft op een werkelijk bestaand persoon en er maatregelen getroffen zijn om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat het bewijsstuk verloren, gestolen, geschorst, ingetrokken of verlopen is, of:
  - Er is een identiteitsdocument overlegd tijdens een registratieproces in de lidstaat waar het document is afgegeven en het document lijkt betrekking te hebben op de persoon die het heeft voorgelegd en er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat documenten verloren, gestolen, geschorst, ingetrokken of verlopen zijn, of:
  - Indien procedures die eerder door een publieke of private entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria gelijkwaardig aan die voor betrouwbaarheidsniveau substantieel, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie of een daaraan gelijkwaardige instantie, of:
  - Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau substantieel of hoog, is het, rekening houdend met het risico van een wijziging van de persoonsidentificatiegegevens niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau substantieel of hoog worden bevestigd door een conformiteitsbeoordelingsinstantie of een daaraan gelijkwaardige instantie.
- Beheer van elektronische identificatiemiddelen:
  - Het elektronisch identificatiemiddel maakt gebruik van ten minste twee authenticatiefactoren die tot verschillende categorieën behoren;
  - Het elektronisch identificatiemiddel is zodanig ontworpen dat het kan worden verondersteld slechts te worden gebruikt door of onder controle van de personen aan wie het toebehoort.
- Uitgifte, uitreiking en activering:
  - Na de uitgifte wordt het elektronisch identificatiemiddel uitgereikt via een mechanisme waarmee kan worden verondersteld dat alleen de persoon aan wie het toebehoort in het bezit ervan wordt gesteld.
- Authenticatiemechanisme:

        - Alvorens persoonsidentificatiegegevens worden vrijgegeven, worden het elektronische identificatiemiddel en de geldigheid ervan op betrouwbare wijze geverifieerd door middel van dynamische authenticatie;
        - Het authenticatiemechanisme 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 gematigd aanvalspotentieel.
    - Beheer van informatiebeveiliging:
        - Het beheersysteem voor informatiebeveiliging voldoet aan beproefde normen en beginselen voor het beheer en de beheersing van informatiebeveiligingsrisico's.
    - Technische controles:
        - Gevoelig cryptografisch materiaal dat voor uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, wordt beschermd tegen ongeoorloofde manipulatie.
    - Compliance en audit:
        - Er vinden periodieke onafhankelijke interne of externe audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn, teneinde de naleving van het desbetreffende te waarborgen.

3.3. Stakeholders DigiD Substantieel

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 (dienstaanbieders)
- Leveranciers
- Gebruikers
- Gegevensdiensten (registerhouders zoals: RvIG, RDW)
- Derden (zoals opsporingsdiensten, in verband met een wettelijke verplichting om gegevens te verstrekken)

3.4. Wettelijk kader DigiD Substantieel

In onderstaande tabel is de relevante wet- en regelgeving opgenomen voor DigiD Substantieel en de impact hiervan op DigiD Substantieel. 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.
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.

3.5. Procesbeschrijving gebruik DigiD Substantieel

Een gebruiker kan ervoor kiezen het authenticatieniveau van zijn account te verhogen naar betrouwbaarheidsniveau ‘Substantieel’. Hiervoor dient de gebruiker reeds in het bezit te zijn van een DigiD-account en een geactiveerde DigiD app.

3.5.1. Activeren DigiD app

Voor het activeren van de DigiD app dient ingelogd te worden op mijn.digid.nl op een ander apparaat dan het apparaat waarop de DigiD app is geïnstalleerd. Middels gebruikersnaam, wachtwoord en sms (voor het activeren van de app is vooralsnog het niveau ‘Midden‘ vereist) logt de gebruiker in waarna hij in mijn.digid.nl de app kan activeren. Ter controle dient nogmaals het wachtwoord ingevoerd te worden en wordt een sms-code verstuurd naar het telefoonnummer van de gebruiker. Vervolgens dient de gebruiker de app te openen en de QR-code te scannen die zichtbaar wordt op mijn.digid.nl. Na het scannen van de QR-code met de DigiD app geeft de DigiD app een koppelcode die ingevoerd dient te worden in mijn.digid.nl ter verificatie van het toestel. Ten slotte wordt door de gebruiker een pincode gekozen waarmee in het vervolg (in combinatie met de gebruikersnaam en het scannen van

een QR-code[11]) ingelogd kan worden bij afnemers die gebruik maken van authenticatie met de DigiD app (in de praktijk zijn dit alle dienstaanbieders). Daarnaast is er de mogelijkheid om in te loggen via de webbrowser van het mobiele apparaat waarop de app is geïnstalleerd (web to app).

3.5.2. Inloggen met DigiD app

De functionaliteit van de DigiD app komt algemeen beschikbaar bij alle dienstaanbieders. Voor het inloggen kan de gebruiker kiezen voor twee mogelijkheden: via de browser op het mobiele apparaat waar de app op is geïnstalleerd (web to app) of via de browser op een ander apparaat. Bij het inloggen via de browser op het mobiele apparaat waar ook de app op is geïnstalleerd is een gebruikersnaam en pincode voldoende om in te loggen. Indien een ander apparaat wordt gebruikt moet de gebruiker zijn gebruikersnaam invoeren, de QR-code scannen en zijn pincode invoeren.

3.5.3. Authenticatieniveau verhogen naar DigiD Substantieel

De gebruiker dient in te loggen op mijn.digid.nl met gebruikersnaam en wachtwoord (en sms in geval van DigiD Midden) of met gebruikersnaam en de DigiD app. Vervolgens kan de gebruiker aangeven het inlogniveau te willen verhogen. De gebruiker komt in een scherm waar hij aan kan geven met welk soort WID gewenst wordt het niveau te verhogen. In de eerste release kan dit een Nederlandse identiteitskaart, een Nederlands paspoort of een Nederlands rijbewijs (uitgegeven na 14 november 2014) zijn. Vervolgens dient met de DigiD app de gegenereerde QR-code gescand te worden en dient de gebruiker zijn pincode voor de DigiD app in te voeren. In het volgende scherm op de DigiD app wordt aangegeven dat de gebruiker het toestel (waarop de DigiD app is geïnstalleerd) op het gekozen WID dient te leggen. Het WID wordt vervolgens gecontroleerd en indien deze succesvol geverifieerd is, wordt het inlogniveau opgehoogd naar DigiD Substantieel. De verificatie van het WID om het inlogniveau te verhogen dient eenmalig plaats te vinden en periodiek herhaald te worden.

3.5.4. Inloggen met DigiD Substantieel

Het inloggen met niveau DigiD Substantieel is overeenkomstig het inloggen met de DigiD app. Zie hiervoor 3.5.2.

3.6. Gegevensstromen en koppelingen DigiD Substantieel

Indien de gebruiker beschikt over de DigiD app kan hij via mijn.digid.nl het huidige account uitbreiden met betrouwbaarheidsniveau DigiD Substantieel. Een dienstaanbieder kan de gebruiker verplichten gebruik te maken van betrouwbaarheidsniveau DigiD Substantieel om in te loggen op de betreffende dienst. Om uit te breiden naar dit betrouwbaarheidsniveau dient eenmalig een controle plaats te vinden door het lezen van de chip op het WID met behulp van een NFC-reader. Om niveau DigiD Substantieel te behouden dient de controle van het WID periodiek herhaald te worden zodat de identiteit opnieuw bevestigd wordt.

De gebruiker geeft in mijn.digid.nl aan gebruik te willen maken van DigiD Substantieel. De DigiD app begint vervolgens met het bevragen van de DigiD Kern om de URL te ontvangen waarmee de app de authenticatie kan starten. De RDA-server is een door een leverancier van Logius ingekochte component van een subleverancier. De RDA-server wordt voor DigiD Substantieel gebruikt om het WID via de NFC-chip te authenticeren. De gebruiker kiest in

[11] Indien wordt ingelogd via de browser met het apparaat waar de DigiD app op is geïnstalleerd, hoeft er geen QR-code te worden gescand.

mijn.digid.nl een WID-soort en een NFC-reader soort (type smartphone) waarmee hij zich wil authenticeren. In de eerste release van DigiD Substantieel kan de gebruiker als WID-soort kiezen voor een Nederlandse identiteitskaart, een Nederlands paspoort en een Nederlands rijbewijs (uitgegeven vanaf 14 november 2014). In latere releases zal niveau DigiD Substantieel naar verwachting ook met een of meerdere additionele WID te behalen zijn. In de eerste release van DigiD Substantieel zijn alleen NFC-readers van Android-toestellen geschikt voor het controleren van het WID. In dergelijke toestellen is meestal een NFC-reader ingebouwd. In de iPhone is (vanaf een bepaald modeljaar) tevens een NFC-reader ingebouwd. Echter, deze was op het moment van schrijven nog niet benaderbaar voor derden. In een latere release zal het DigiD-account mogelijk ook versterkt kunnen worden naar DigiD Substantieel met een NFC-reader via een browser plugin (USB) en mogelijk ook met een iOS-toestel, afhankelijk van of Apple de functionaliteit voldoende openstelt. Nadat de gebruiker het WID-soort en het NFC-reader soort heeft gekozen gaat de DigiD app naar de URL die daarbij hoort, om de verbinding te leggen tussen de RDA-server en chip op het WID-document. Afhankelijk van de keuze van het WID-soort wordt informatie opgehaald bij de externe partij RvIG (paspoort of identiteitskaart) of RDW (rijbewijs):

- <u>WID-soort: Nederlandse identiteitskaart of Nederlands paspoort</u>
  Aan de hand van de authenticatie met gebruikersnaam en wachtwoord wordt het BSN van de gebruiker opgezocht in DigiD Kern. Aangezien de gebruiker heeft aangegeven als WID-soort de Nederlandse identiteitskaart of het Nederlandse paspoort te willen gebruiken, wordt op basis van het BSN door DigiD Kern een bevraging gedaan naar de BRP van de RvIG. De BRP geeft van de vier meest recente documenten de gegevens door aan DigiD Kern. DigiD Kern filtert op het gekozen WID-soort (identiteitskaart of paspoort) en geeft vervolgens van de gekozen soort de volgende gegevens door van de geldige en niet ingehouden reisdocumenten aan de DigiD Card Interface Service (hierna: CIS): WID-nummer, geboortedatum van gebruiker en geldigheidsdatum. Dit kunnen meerdere documenten zijn omdat een gebruiker meerdere geldige identiteitskaarten/paspoorten kan hebben. Indien het WID-soort dat de gebruiker gekozen heeft een paspoort is, stuurt DigiD Kern alleen de gegevens van de geldige en niet ingehouden paspoorten die zijn ontvangen van de BRP door aan de RDA-server. Wanneer het WID-soort dat de gebruiker gekozen heeft een identiteitskaart is, worden alleen de gegevens van de geldige en niet ingehouden identiteitskaarten die zijn ontvangen van de BRP doorgegeven aan de RDA-server. Indien meerdere documenten van de gekozen soort geldig en niet ingehouden zijn, geeft DigiD Kern de gegevens door aan de CIS van de meest recente documenten (max. vier identiteitskaarten/paspoorten). De RDA-server berekent op basis van de gegevens uit de BRP de Machine Readable Zone (hierna: MRZ) en genereert de Basic Access Control (hierna: BAC) sleutel op basis van de MRZ. Met de BAC-sleutel kunnen gegevens uit de NFC-chip van de identiteitskaart of het paspoort uitgelezen worden. Indien gegevens van meerdere documenten zijn ontvangen, worden meerdere MRZ-codes en meerdere BAC-sleutels berekend (max. vier).

- <u>WID-soort: Nederlands eRijbewijs (vanaf 14 november 2014)</u>
  Aan de hand van de authenticatie met gebruikersnaam en wachtwoord wordt het BSN van de gebruiker opgezocht in DigiD Kern. Via een artifact binding worden de sessiegegevens meegegeven, zodat DigiD CIS het BSN kan achterhalen. Aangezien de gebruiker heeft aangegeven als WID-soort het Nederlandse rijbewijs te willen gebruiken, wordt op basis van het BSN een bevraging gedaan van DigiD CIS naar het CRB van de RDW. Het CRB geeft de MRZ van het rijbewijs. DigiD CIS kan maximaal één MRZ ontvangen van het CRB omdat maar één rijbewijs geldig kan zijn. De RDA-server berekent op basis van de MRZ de Basic Access Protection

(hierna: BAP) sleutel. Met de BAP-sleutel kunnen gegevens uit de NFC-chip van de rijbewijs uitgelezen worden.

De RDA-server antwoordt aan DigiD CIS door een redirect URL met de sessie-ID en DigiD CIS geeft de redirect URL met Sessie-ID aan DigiD Kern. DigiD Kern geeft een antwoord met de redirect URL aan de DigiD app. De sessie wordt opgezet door de RDA-server met DigiD app waarna de RDA-server het WID kan authenticeren via de NFC-reader. De bevraging om het WID tegen de smartphone te houden start zodra het authenticeren begint.

De DigiD app geeft aan dat de gebruiker het WID in de buurt van de NFC-reader dient te houden zodat de gegevens op de chip via de NFC-reader door de RDA-server gelezen kunnen worden. Met die BAP-/BAC-sleutel wordt een veilig end-to-end kanaal opgezet tussen de RDA-applicatie en de chip of het WID. Met dit beveiligde communicatiekanaal zijn de gegevens vanuit de chip beveiligd en wordt het technisch mogelijk om vast te kunnen stellen dat het aangeboden WID bij die gebruiker hoort en authentiek is. Wanneer het lukt met de BAP of BAC de chip te openen, toont dit aan dat een WID wordt aangeboden dat bij het betreffende BSN in BRP of CRB is geregistreerd. Indien meerdere BAC-sleutels berekend zijn, worden pogingen gedaan totdat de authenticatie succesvol is of dat alle WID zijn gebruikt. Na het opzetten van deze beveiligde verbinding worden de Passive Authentication (hierna: PA) en Active Authentication (hierna: AA) controles uitgevoerd. De RDA-server leest de gegevens uit de chip om onder andere de volgende verificaties te kunnen uit te voeren:

- Controle of de gegevens op de chip niet gewijzigd zijn middels PA;
- Controle of de chip niet gekloond is middels AA;
- Controle van de gegevens op de chip met de controlegetallen in het Document Security Object (SOD);
- Controle van de handtekening met de AA publieke sleutel;
- Controle of het document signer certificaat is uitgegeven door de Country Signing Certificate Authority (CSCA) en geldig is.

In geval van een identiteitskaart of paspoort wordt de datagroep met de MRZ (DG1) uit de chip van het WID uitgelezen. Deze datagroep bevat de volgende gegevens:

- Document code;
- Issuing State or organization;
- Name of holder;
- Document number;
- Nationality;
- Date of birth;
- Seks;
- Date of expiry;
- Optional data;
- Composite check digit.

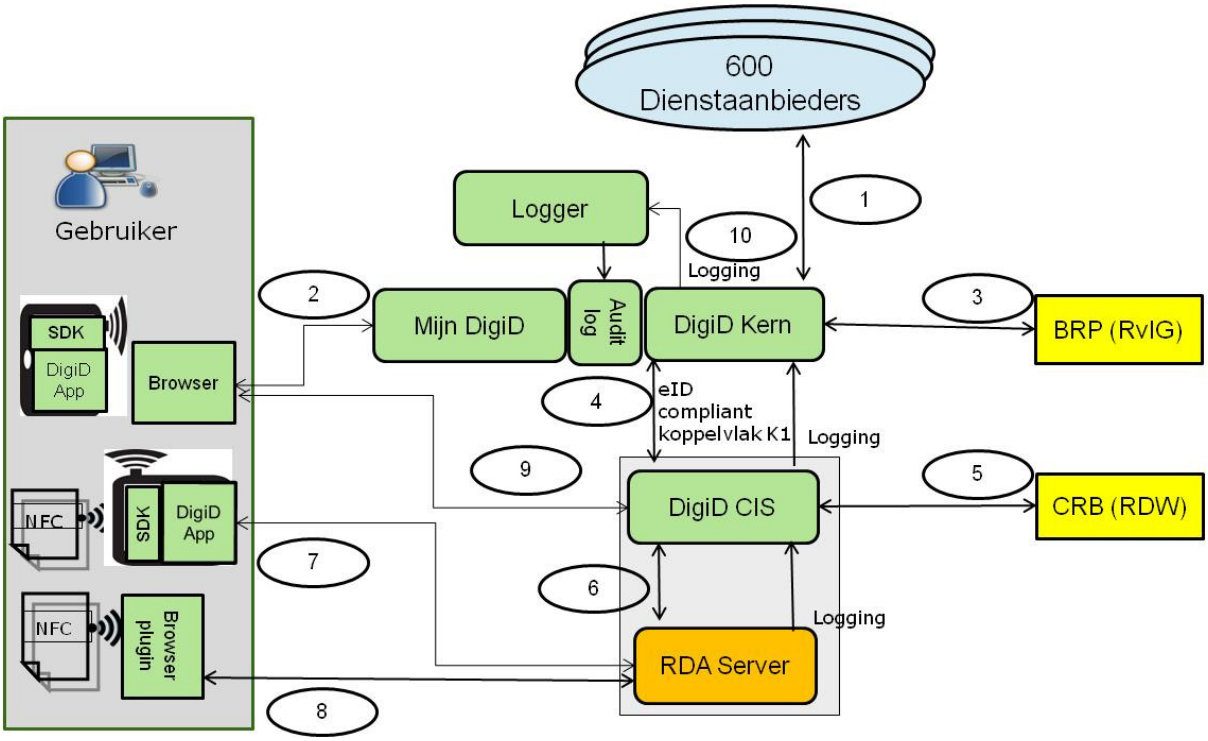
In geval van een rijbewijs wordt de datagroep met de MRZ (DG12) uit de chip van het WID uitgelezen. Deze datagroep met de MRZ bevat de volgende gegevens:

- Identifier;
- Rijbewijs nummer;
- Discretionary data;
- Composite check digit.

De resultaten van de authenticatie verificaties worden uitgewisseld van de RDA-server met DigiD CIS en van DigiD CIS met DigiD Kern. Zodra het resultaat in DigiD Kern is, stopt de

bevraging. De gegevens voor de verificatie blijven alleen voor die sessie bewaard. De gebruiker krijgt te zien of de controle gelukt is of niet en er wordt een advies gegeven aan de gebruiker wat hij kan doen. Hierbij wordt bewust niet gemeld wat er precies fout is gegaan.

Schematisch ziet het proces er als volgt uit:



De koppelvlakken in bovenstaand figuur zijn genummerd en worden toegelicht in onderstaande tabel:

#		Van	Naar	Gegevens/bevraging	Protocol
1	1.1	Dienstaanbieder	Mijn DigiD	Authenticeren (gebruiker, betrouwbaarheidsniveau)	SAML binding met AuthnRequest en AuthResponse
	1.2	Mijn DigiD	Dienstaanbieder	Betrouwbaarheidsniveau DigiD Substantieel, BSN	
2	2.1	Gebruiker	Mijn DigiD	Keuzescherm (account = substantieel)	SAML Redirect binding
	2.2	Mijn DigiD	Gebruiker	Keuzescherm (WID- soort, NFC-reader soort)	
	2.3	Gebruiker	Mijn DigiD	WID-soort, NFC-reader soort	
	2.4	Gebruiker	Mijn DigiD	Polling	
	2.5	Mijn DigiD	Gebruiker	Polling response	
	2.6	Mijn DigiD	Gebruiker	Controle gelukt/niet gelukt	
3	3.1	DigiD Kern	BRP	BSN	Diginetwerk en SOAP

#		Van	Naar	Gegevens/bevraging	Protocol
	3.2	BRP	DigiD Kern	WID-info[12]	
4	4.1	DigiD Kern	DigiD CIS	Sessie-ID, WID-soort, NFC-reader soort, WID- info	SAML met artifact binding[13] (K1 koppelvlak)
	4.2	DigiD CIS	DigiD Kern	URL met Sessie-ID	
	4.3	DigiD CIS	DigiD Kern	Sessie-ID, OK/NOK	
5	5.1	DigiD CIS	CRB	BSN	Diginetwerk en SOAP
	5.2	CRB	DigiD CIS	MRZ of reden ongeldig WID	
6	6.1	DigiD CIS	RDA-server	Sessie-ID, WID-soort, NFC-readersoort, WID- info/MRZ, pseudoniem_user_ID	SAML met SOAP binding (Artifact binding in geval van USB)
	6.2	RDA-server	DigiD CIS	Sessie-ID, URL, OK/NOK	
	6.3	DigiD CIS	RDA-server	Optioneel: cancel Sessie-ID	
	6.4	RDA-server	DigiD CIS	Optioneel: ERR001_CANCELLED	
7	7.1	Mobiel apparaat (NFC)	RDA-server	Polling	APDU commands over TLS
	7.2	Mobiel apparaat (NFC)	RDA-server	MRZ	
	7.3	RDA-server	Mobiel apparaat (NFC)	APDU's	
	7.4	Mobiel apparaat (NFC)	RDA-server	Result APDU's	
8	8.1	USB	RDA-server	Polling	
	8.2	USB (NFC)	RDA-server	MRZ	
	8.3	RDA-server	USB (NFC)	APDU's	
	8.4	RDA-server	USB (NFC)	Sessie-ID, URL, OK/NOK	
9	9.1	Gebruiker	DigiD CIS	WID-soort, NFC-reader soort	SAML Redirect binding
	9.2	DigiD CIS	Gebruiker	Controle gelukt/niet gelukt	

Koppelvlak 10 geeft de koppeling weer tussen een DigiD-component, de Logger en de Auditlog. Op dit moment kan alleen DigiD Kern wegschrijven in de Logger. In de nieuwe release (verwacht september) kan mogelijk iedere DigiD-component logging informatie direct doorgeven aan de Logger. De Logger schrijft de logging weg in de Auditlog.

Technische logging wordt gelogd in de systeemlogging (syslog). De syslog wordt gegenereerd door het systeem en is benodigd voor het onderhouden en het beheren van het systeem. In de syslog worden de volgende gegevens vastgelegd:

- IP-adres;
- Datum;
- Tijd;
- Component / SAML AuthreqID;
- Technische details 'function calls'.

De functionele logging wordt gelogd in de transactielog. In de transactielog van DigiD Substantieel worden de volgende gegevens vastgelegd:

- IP-adres;
- Unieke gepseudonimiseerde BSN[14];

[12] WID-info: WID-nummer, geboortedatum, einddatum geldigheid, datum inhouding/vermissing.
[13] De artifact binding zorgt er voor dat gevoelige data niet via de browser worden verstuurd waardoor kwetsbaarheden zoveel mogelijk op de achtergrond blijven.

- Sessie-ID;
- Sectoraal nummer;
- Dienstaanbieder waar wordt ingelogd;
- Datum en tijd van authenticatie;
- NFC-reader soort;
- WID-soort;
- Resultaat van RDA: OK/NOK;

In de beheermodule is de transactielog gekoppeld aan het account van de gebruiker. De gegevens behorende bij het account zijn vastgelegd in DigiD Kern en bevatten onder andere het BSN van de gebruiker.

De syslog en transactielog zijn van elkaar gescheiden en kunnen middels het IP-adres gekoppeld worden. Bij de syslog kunnen andere personen dan bij de transactielog (functiescheidingen).

3.7. 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	Voor de mogelijkheid tot herstel van DigiD na een grote calamiteit.
Systeemlog	100 dagen	Technische logging gegenereerd door componenten.
Briefbestanden	6 weken	Gegevens die nodig zijn voor het correct weergeven van een aanvraag.
Logging infrastructuurcomponenten	1 maand	Deze logging wordt gesynchroniseerd met centrale logservers.
Loadbalancer logging	7 dagen	Een change is ingediend om deze logging ook naar centrale loservers te synchroniseren.
Sessiegegevens en cookies	Sessieduur	Gegevens die worden bewaard tot het moment van uitloggen.

[14] Het unieke gepseudonimiseerde BSN is niet te herleiden naar een BSN en wordt niet gebruikt voor authenticatiedoeleinden maar voor het bepalen van het aantal unieke gebruikers van DigiD Substantieel. Dit gegeven vormt de basis voor de facturering t.b.v. de RDA-server.

4. Conclusies en aanbevelingen PIA

4.1. Positionering DigiD Substantieel in de ontwikkelcyclus van DigiD en ten opzichte van de bestaande DigiD

Het voornemen van het ministerie van BZK om het DigiD-middel en bijbehorende authenticatiemechanisme te versterken, wordt gerealiseerd via een aantal stappen die zich in de tijd uitstrekken. De PSA DigiD Substantieel en aanvullende ontwerpdocumentatie beschrijven een eerste stap in deze ontwikkelcyclus, namelijk een versterkt uitgifteproces en bijbehorend authenticatiemiddel. Niet alle benodigde functionaliteiten voor een volledig DigiD op het niveau Substantieel zijn in de PSA beschreven. Buiten de scope van de PSA DigiD Substantieel vallen:

- DigiD-accounts van onbekende personen. Deze kunnen voor DigiD Substantieel niet worden gebruikt aangezien een BSN vereist is om gegevens uit de BRP en het CRB op te halen;
- Aanvragen buitenland voor Balie en SVB;
- De mogelijkheid om 7 x 24 uur een identiteitsdocument op te geven als vermist of gestolen en het op basis daarvan blokkeren van een authenticatiemiddel.

De bestaande DigiD biedt de gebruiker de mogelijkheid om met een gebruikersnaam en wachtwoord (optioneel met sms) of gebruikersnaam en DigiD app in te loggen. 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.

In de eerste versie van DigiD Substantieel zal door technische oorzaken buiten het bereik van Logius de DigiD app alleen bruikbaar zijn voor Android-telefoons en nog niet beschikbaar zijn voor iOS/Apple smartphones. In een latere release zal DigiD Substantieel naar verwachting ook bruikbaar zijn met een iOS-toestel, afhankelijk van of Apple de functionaliteit voldoende openstelt.

4.1.1. Bevindingen

Uit de informatie verkregen over het ontwerp van DigiD Substantieel blijkt dat de Remote Document Access (RDA) server een nieuwe technische component is die gerealiseerd is voor DigiD Substantieel. Een nieuw koppelvlak met het CRB is gerealiseerd. Ook is een aantal functionele en technische uitbreidingen doorgevoerd voor de communicatie met nieuwe koppelvlakken op bestaande DigiD-componenten en met al bestaande koppelvakken. Aanpassingen zijn gedaan op de DigiD Kern, DigiD CIS en op de koppelvlakken DigiD Kern - BRP, RDA-server - DigiD app en DigiD CIS - RDA-server. Nieuwe systeemvoorzieningen zijn gerealiseerd voor het gebruik van de DigiD app. Met deze aanpassingen is DigiD Substantieel een systeem dat niet los kan worden gezien van de bestaande DigiD. De bestaande DigiD en DigiD Substantieel zijn onlosmakelijk met elkaar verbonden. DigiD Substantieel maakt voor een belangrijk deel gebruik van bestaande technische voorzieningen en verwerkingen van persoonsgegevens van de bestaande DigiD. Anders geformuleerd: de verwerkingen van persoonsgegevens als gevolg van het gebruik van DigiD Substantieel en de bestaande DigiD zijn voor een belangrijk deel technologisch en functioneel dezelfde verwerkingen en zijn operationeel gezien sterk met elkaar verweven. Dit betekent ook dat de privacyrisico's en de daaraan gerelateerde beveiligingsrisico's van de bestaande DigiD niet los gezien kunnen worden van de risico's gekoppeld aan DigiD Substantieel en vice versa. De privacyrisico’s van de bestaande DigiD, behoudens de

versterking van het uitgifte- en inlogproces, zijn feitelijk ook van toepassing op DigiD Substantieel.

Geconstateerd is dat op de bestaande DigiD nog geen integrale PIA is uitgevoerd. Bij de uitvoering van deze PIA op DigiD Substantieel 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.

DigiD Substantieel is dus een doorontwikkeling en uitbreiding van de bestaande DigiD. Bestaande componenten en beveiligingsmaatregelen worden hergebruikt en de bestaande authenticatiemiddelen blijven voorlopig gehandhaafd en beschikbaar voor gebruikers en dienstaanbieders, naast het authenticatieniveau Substantieel. Hiermee wordt een geleidelijke overgang bewerkstelligd en is de continuïteit van de bestaande administratie en dienstverlening gegarandeerd. Bij deze gekozen aanpak spelen daarnaast afwegingen die de projectrisico's verder beperken en waarbij recht wordt gedaan aan strakke mijlpalen en voorgeschreven tijdpaden. Tot slot spelen ook bedrijfseconomische overwegingen een rol.

In deze PIA op de PSA DigiD Substantieel en de wijze waarop deze versie technisch gerealiseerd wordt, is een aantal bevindingen aangaande privacyrisico's geïdentificeerd. Hierbij zijn naar vermogen aanbevelingen gedaan om deze risico's verder te mitigeren. Deze risico's vloeien echter maar ten dele voort uit de versterking van de bestaande DigiD authenticatiemechanisme naar het niveau Substantieel. Veel van de onderkende privacyrisico's zijn in feite risico's van de bestaande DigiD-opzet en -infrastructuur die hergebruikt worden binnen DigiD Substantieel.

Een belangrijke conclusie uit deze PIA is dat de realisatie van de PSA DigiD Substantieel maar beperkte additionele privacyrisico's met zich meebrengt ten opzichte van de bestaande DigiD. Het feit dat DigiD Substantieel gerealiseerd wordt met gemeenschappelijke systeemcomponenten en -functies van de bestaande DigiD zorgt ervoor dat de privacyrisico's van de bestaande DigiD overerft worden in DigiD Substantieel.

Het is belangrijk te onderkennen dat DigiD Substantieel nog verder wordt doorontwikkeld. De PSA DigiD Substantieel is slechts een eerste stap in een breder versterkingsproces van DigiD. Uiteindelijk is het de bedoeling van het ministerie van BZK en Logius om, naast de realisatie van Substantieel, door te gaan met het ontwikkelen naar DigiD Hoog. Inmiddels is bekend dat in DigiD Hoog cryptografische en andere aanvullende maatregelen voor zowel de bestaande DigiD als DigiD Substantieel zijn voorzien om de privacyrisico's verder te beperken. Het uiteindelijke doel is dat het huidige DigiD-stelsel overgaat van een BSN-gebaseerde verwerking naar een pseudoniem-gebaseerde verwerking waarbij alleen de dienstaanbieder in staat is het pseudoniem te herleiden tot de identiteit van de gebruiker. Met deze technologische maatregelen die op termijn ook voor DigiD Substantieel gaan gelden wordt invulling gegeven aan de eis vanuit de AVG om beveiligingsmaatregelen te treffen naar de stand van de techniek.

Op basis van de huidige plannen van het ministerie van BZK om de authenticatiemechanismen en -middelen te versterken, valt te concluderen dat het belangrijk is dat de doorontwikkeling, zoals is voorgenomen door het ministerie van BZK, wordt doorgezet en afgerond en dat uiteindelijk de middelen en concepten van het nu bestaande DigiD-systeem worden afgebouwd en/of de privacyrisico's daarvan worden gemitigeerd. In de volgende paragraaf wordt nader ingegaan op de specifieke privacyrisico's.

4.1.2. Aanbevelingen

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.

4.2. Noodzakelijke verwerking persoonsgegevens DigiD Substantieel

Om te beoordelen of het noodzakelijk is persoonsgegevens te verwerken voor het te bereiken doel voor DigiD Substantieel speelt de vraag naar proportionaliteit en subsidiariteit. Het proportionaliteitsbeginsel houdt in dat de inbreuk op de belangen van de betrokkene bij de verwerking van persoonsgegevens, 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 betrokkene, minder nadelige wijze kunnen worden verwerkelijkt[15].

Voor het realiseren van DigiD Substantieel is door Logius voor een aanpak gekozen waarbij in een aantal fasen vanuit de bestaande DigiD wordt doorontwikkeld naar een hoger betrouwbaarheidsniveau. Hierbij spelen zowel bedrijfseconomische en dienstverlenende afwegingen als ook afwegingen om de projectafbreukrisico's te beperken. Bij de verdere doorontwikkeling na de realisatie van DigiD Substantieel is Logius voornemens om binnen een periode van één tot drie jaar te starten met het afbouwen van het rechtstreeks gebruik van het BSN binnen de DigiD-systeemomgeving en worden additionele cryptografische maatregelen geïntroduceerd, waardoor DigiD in de toekomst voorziet in onder meer een betere beheersing van het BSN.

4.2.1. Bevindingen proportionaliteit

Voor het verifiëren van een identiteitskaart/paspoort wordt een bevraging gedaan naar de BRP van de RvIG. De gegevens van de meest recente paspoorten en identiteitskaarten behorende bij het BSN worden ontvangen door Logius en niet alleen de strikt noodzakelijke gegevens. De gegevensaanvraag is niet specifiek voor Substantieel waardoor alle gegevens waar DigiD autorisatie voor heeft worden ontvangen. De huidige bevraging is daarmee als niet-proportioneel te beschouwen. De gegevens die benodigd zijn voor DigiD Substantieel (de geboortedatum van de gebruiker, het WID-nummer, de geldigheidsdatum en de aanduiding op of datum van inhouding/vermissing) kunnen door Logius wel gespecifieerd worden zodat alleen deze gegevens worden ontvangen. De huidige functionaliteit geboden door RvIG biedt echter niet de mogelijkheid om de gegevensaanvraag RvIG specifiek te maken op basis van het documentsoort (paspoort/identiteitskaart). Als compenserende maatregel worden conform het ontwerp ontvangen gegevens bij Logius na maximaal een uur geautomatiseerd gewist. De privacyrisico's zijn voor dit onderdeel hiermee geminimaliseerd.

[15] Zie artikel 8 Wet bescherming persoonsgegevens.

4.2.2. Bevindingen subsidiariteit

Logius heeft de beschikking over persoonsgegevens, waaronder BSN's en IP-adressen van gebruikers. Deze gegevens zijn afgeschermd door organisatorische en technische beveiligingsmaatregelen maar worden zelf niet versleuteld of gepseudonimiseerd. De transactiegegevens bevatten onder andere accountgegevens, BSN's en IP-adressen. In deze transactiegegevens is ook vastgelegd bij welke dienst de gebruiker heeft ingelogd. Gezien de wettelijke bewaartermijnen (1,5 jaar systeemlogging en 5 jaar van transactielogging) is de totale dataset in volumes groot. Uitgaande van de bewaartermijn van vijf jaar en een aantal van 250 miljoen transacties per jaar gaat dat aantal, zeker gezien het toenemend gebruik, over de 1,25 miljard records heen. Hierdoor ontstaat een cumulatie van inloghistorie van gebruikers. Dit transactiebestand met inloghistorie is een gevoelig en waardevol bestand op basis waarvan (hoewel onrechtmatig) profielen van gebruikers opgesteld zouden kunnen worden. Het gaat hier om het risico van profileren. Denk hierbij aan gebruikers die met hun DigiD inloggen bij dienstaanbieders die zich inzetten voor ondersteuning bij jeugdzorg, bij reclassering of binnen het sociaal domein. De inloghistorie geeft daarbij mogelijk indicaties prijs dat gebruikers behoren tot kwetsbare groepen. Kwetsbare groepen hebben conform de privacywetgeving meer rechten op privacybescherming. De potentiële impact van eventueel misbruik van deze gevoelige dataset is hoog. Logius geeft uitdrukkelijk aan dat zij niet aan profilering doet. Binnen Logius zijn diverse beveiligingsmaatregelen getroffen om de risico's van profiling te beperken.

Binnen de beheeromgeving van Logius zijn verscheidene maatregelen getroffen om de toegang en het gebruik van deze gevoelige gegevens te beperken en te beheersen. De transactielog is toegankelijk voor ketenbeheer en het servicecentrum en de inloggegevens zijn alleen toegankelijk voor daartoe bevoegde functionarissen. Beide gegevensverzamelingen zijn ook toegankelijk voor analisten van het fraudeteam, mits daar aanleiding toe is. 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 (middels validatie door een geautoriseerde collega). Voor de vaste schijven waar deze gegevens zijn opgeslagen wordt schijfencryptie toegepast. Met deze maatregelen zijn de risico's van dit transactiebestand verminderd.

Deze risico's van de cumulerende inloghistorie, waaronder profiling en toenemende waarde en gevoeligheid van het bestand zijn niet in de ontwerpdocumentatie van PSA DigiD Substantieel geadresseerd. De hierboven genoemde risico's zijn niet nieuw of specifiek voor DigiD Substantieel. Ze gelden ook voor het al bestaande DigiD-systeem en technische componenten waarop DigiD Substantieel wordt geplaatst.

De inloghistorie en transactiegegevens bieden mogelijkheden voor gebruikersondersteuning, noodzakelijke controle en fraudeonderzoek. Deze controlewerkzaamheden kunnen over het algemeen ook uitgevoerd worden op versleutelde, gepseudonimiseerde of geanonimiseerde gegevens. Gesteld kan worden dat DigiD Substantieel nog niet geheel in overeenstemming is met het subsidiariteitsbeginsel vanwege het niet encrypten of pseudonimiseren van gevoelige gegevens. Waarbij de opmerking geplaatst wordt dat wachtwoorden gehasht worden opgeslagen en er sprake is van schijfencryptie, zoals ook nu toegepast wordt in de huidige DigiD.

4.2.3. Aanbevelingen

Op basis van deze bevindingen kan worden gesteld dat in de ontwerparchitectuur voor de eerste fase van DigiD Substantieel de principes proportionaliteit en subsidiariteit zijn meegewogen en tot op zekere hoogte zijn ingevuld, maar dat naar de toekomst toe verdere optimalisaties mogelijk zijn.

De huidige uitvraag naar de BRP is niet specifiek voor DigiD Substantieel waardoor naast de benodigde gegevens voor DigiD Substantieel ook overige gegevens van de meest recente paspoorten en identiteitskaarten behorende bij het BSN worden ontvangen. Aanbevolen wordt de gegevensaanvraag voor Substantieel te specifiëren zodat alleen de gegevens worden ontvangen die benodigd zijn voor DigiD Substantieel (geboortedatum, WID-nummer, geldigheidsdatum en aanduiding op of datum van inhouding/vermissing). Het verdient aanbeveling om bij de doorontwikkeling van DigiD Substantieel de RvIG te verzoeken om de mogelijkheid te bieden voor het specifiëren van de BRP bevraging, zodat alleen de gegevens van het voor de verificatie gebruikte WID worden ontvangen.

Verwerking van persoonsgegevens en logging van de (goede) werking is noodzakelijk en inherent aan de authenticatiedienstverlening. Gezien het geconstateerde risico van het ontstaan van een omvangrijke dataset is het van belang ervoor te zorgen dat gegevens die mogelijk inzicht kunnen geven in het inloggedrag van een gebruiker tot een minimum worden beperkt en dat aanvullende maatregelen worden getroffen om onbevoegd/onbedoeld gebruik en misbruik tegen te gaan.

Bij de vervolgontwerpfasen verdient het aanbeveling de risico's van het transactiebestand met inloghistorie en de hieraan gerelateerde profilingrisico's nader te beschouwen en na te gaan welke additionele maatregelen getroffen kunnen worden om de risico's van dit transactiebestand nog verder te reduceren. Te denken valt aan verdere toepassing van encryptie van data, pseudonimiseringstechnieken en verdere limitering van de opslag en toegang tot de data. Het aanbrengen van een 'Chinese muur' tussen accountgegevens (BSN) en transactiegegevens (inloghistorie) en netwerkgegevens (IP-adressen) is daarbij een belangrijk handvat. Het ontwerp van DigiD Hoog biedt hiervoor aanknopingspunten.

We willen nogmaals benadrukken dat de bovenbeschreven risico's van het transactiebestand met inloghistorie en de risico's van de beschreven herleiding van gegevens naar natuurlijke personen niet een gevolg zijn van de toegevoegde functionaliteit van DigiD Substantieel, maar voortvloeien uit de eigenschappen van de componenten en inrichting van het bestaande DigiD-systeem die gebruikt blijven worden voor DigiD Substantieel. Anders gezegd: door de introductie van DigiD Substantieel krijgt de gebruiker een inlogmiddel met een hogere betrouwbaarheid en wordt een belangrijke versterking gerealiseerd, maar de overige al bestaande privacyrisico's worden er niet direct beter op, maar ook niet materieel slechter.

In de plannen voor de doorontwikkeling van DigiD Substantieel en de realisatie van DigiD Hoog zijn verdere optimalisaties voorzien. Een belangrijke voorgenomen optimalisatie is het terugdringen van het BSN-gebruik door het gebruik van gerandomiseerde polymorfe pseudo-identiteiten. Hiermee wordt de scheiding tussen IP-adressen en BSN's gerealiseerd. Deze technische voorzieningen zullen gebruikt gaan worden voor de verdere doorontwikkeling van DigiD. Het is belangrijk te onderkennen dat de voordelen van deze maatregelen pas volledig effectief zijn als DigiD Hoog volledig geïmplementeerd is.

4.3. 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.

In de DigiD app worden in een beveiligde zone het app ID en een private key opgeslagen. Op het functionele niveau van DigiD Substantieel is het principe van gegevenslimitering toegepast, waarbij zoals in paragraaf 4.2.3 is aangegeven optimalisaties mogelijk zijn. 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 op de PSA van DigiD Substantieel zijn de effecten van deze technische netwerkcomponenten niet in detail nader 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. Vastgesteld is dat loggegevens op basis van het IP-adres en andere (interne of externe) bronnen zoals de transactiegegevens kunnen worden herleid tot een BSN.

In de bestaande DigiD zijn de technische loggings gedecentraliseerd naar componenten. Dezelfde benadering geldt voor de nieuwe componenten van DigiD Substantieel (waaronder de RDA-server) en voor de aanpassingen in koppelvlakken en interfaces (waaronder het CIS) en bestaande DigiD-onderdelen (waaronder DigiD Kern). De eerder beschreven beveiligingsregimes gelden ook voor deze nieuwe componenten. De componenten zelf genereren de syslogs en de applicaties genereren de transactielogs. De afzonderlijke decentrale loggings worden samengebracht in een centrale DigiD logging- en monitoringomgeving. Vanuit deze omgeving gaat alleen relevante logging naar het Security Information and Event Management (hierna: SIEM). Het SIEM is een bij een externe partij afgenomen dienst ingericht op infrastructuurniveau waarin de logging voor specifieke doelstellingen wordt gemonitord (op basis van use cases). De monitoringomgeving is apart te bereiken en extra beveiligd (veilig opgeslagen en encrypted). Deze beveiligingsmaatregelen gelden ook voor de back-up van de logbestanden.

4.3.1. Bevindingen

Het stelsel van loggings en de centralisatie van logging is voorzien van preventieve beveiligingsmaatregelen en signaleringen van eventueel onbevoegde toegang. Er is sprake van een limitering van dataverzameling in het SIEM op basis van use cases. Dit laat onverlet dat de geconstateerde herleiding van IP-adressen naar BSN deze loggings nog steeds gevoelig maken voor (onrechtmatige) profiling. Daarbij ontbreekt een integraal en toegankelijk overzicht van alle verwerkingen van persoonsgegevens op dit technische niveau.

Door het gebruik van DigiD kan niet worden uitgesloten dat er gegevensverzamelingen ontstaan waarmee privacygevoelige informatie kan worden verkregen over individuen. Bijvoorbeeld over hun sociaal maatschappelijke situatie of dat zij deel uitmaken van kwetsbare groepen. Deze bijzondere gegevens zouden kunnen worden afgeleid uit de inloghistorie van gebruikers indien zij bij specifieke dienstaanbieders inloggen waarvan de diensten te koppelen zijn aan kwetsbare groepen of andere bijzondere omstandigheden van

de gebruiker die stigmatiserend zijn. Denk hierbij aan het inloggen bij organisaties voor schuldhulpverlening, medisch gerelateerde diensten en uitkeringsinstanties.

4.3.2. Aanbevelingen

Voor bijzondere gegevens en gegevens over kwetsbare groepen moet rekening gehouden worden met een verzwaard privacyregime. Aanbevolen wordt in kaart te brengen welke persoonsgegevens worden verwerkt die hogere privacy waarborgen verlangen en additionele maatregelen te implementeren om de beveiliging van deze gegevens te waarborgen. In de voorafgaande paragrafen is al aangegeven dat de voorgenomen maatregelen binnen het ontwerp van DigiD Hoog aanknopingspunten bieden om ongewenste herleiding van gegevens tegen te gaan.

4.4. 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.

De ontwikkeling van DigiD Substantieel heeft tot doel het bieden van een betrouwbaar middel voor gebruikers om in te kunnen loggen op het BSN-domein, waarbij wordt voldaan aan de eisen van het eIDAS betrouwbaarheidsniveau ‘Substantieel’ (Commissie, 2015). Deze ontwikkeling moet gezien worden als een stap in de uiteindelijke doorontwikkeling naar een middel met het eIDAS betrouwbaarheidsniveau ‘Hoog’. Om meer diensten online aan te kunnen bieden, gebruikers op een hoger betrouwbaarheidsniveau te kunnen laten inloggen en te voldoen aan de eIDAS-norm, is DigiD Substantieel ontworpen. Logius verwerkt persoonsgegevens om gestelde doelen te kunnen bereiken. Ten opzichte van het huidige DigiD-stelsel (DigiD Basis en DigiD Midden) vinden voor DigiD Substantieel meer gegevensverwerkingen plaats. Als voorbeeld noemen wij de controle die gedaan wordt bij externe bronnen, de BRP en het CRB, waarbij gegevens over het WID worden opgehaald.

4.4.1. Bevindingen

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. DigiD Substantieel zorgt slechts voor een beperkte uitbreiding van de typen van persoonsgegevens bovenop de al bestaande gegevensverwerkingen van de bestaande DigiD. Een totaal overzicht van alle verwerkte persoonsgegevens op alle componenten en systeemlagen is niet in één overzicht aanwezig en het totaal vormt een complex geheel.

In de huidige ontwerpdocumentatie DigiD Substantieel 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. Er wordt weliswaar verwezen naar normen voor informatiebeveiliging waaronder de Baseline Informatiebeveiliging Rijksdienst (hierna: BIR) en ISO27001. Deze normen zien echter 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 sprake is van een gevoelig transactiebestand met inloghistorie. Additionele controles worden nog ontwikkeld met betrekking tot DigiD Substantieel.

Voor het uitvoeren van de controles van het WID maakt Logius gebruik van de RDA-server van een subleverancier. Controles van persoonsgegevens van de chip op het WID vinden plaats in de RDA-server. Alleen het IP-adres wordt gelogd in de database van de RDA-server (syslog). Centraal bij de applicatielogging van DigiD Substantieel wordt verder het volgende gelogd:

- IP-adres;
- Unieke gepseudonimiseerde BSN;
- Dienstaanbieder waar wordt ingelogd;
- NFC-reader soort;
- WID-soort;
- Resultaat van RDA: OK/NOK.

Vastgesteld is dat geen subverwerkersovereenkomst is opgesteld met de subleverancier van de RDA-server. Aangezien deze partij in verband met de werking van DigiD Substantieel wel persoonsgegevens verwerkt, dient dit nog gerealiseerd te worden. Dit is door Logius onderkend en de actie om de subverwerkersovereenkomst te realiseren is onderhanden.

4.4.2. Aanbevelingen

De huidige doelstellingen van DigiD Substantieel zijn eenduidig en gelimiteerd beschreven. DigiD Substantieel zorgt voor een uitbreiding van de typen van persoonsgegevens bovenop de al bestaande gegevensverwerkingen van DigiD Basis en Midden. Voorts verdient het aanbeveling om een meer integrale beschrijving te maken van het volledige DigiD landschap en infrastructuur, zodat de verwerkingen van DigiD Basis, Midden en Substantieel 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 dienstaanbieders 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 én rapportage over de beveiligings- en datakwaliteitsaspecten plaatsvindt. Hierbij dient dit 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 werking van het systeem en vermoedens van

identiteitsfraude. Uiteraard zijn deze maatregelen bedoeld ter bescherming van de belangen van de gebruikers en gelden er voor de onderzoeken van het fraudeteam strikte procedures.

4.5. 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 Substantieel 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.

4.5.1. 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 Substantieel opgevraagde persoonsgegevens bij de BRP en het CRB worden als juist aangenomen. 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. In het huidige ontwerpdocument zijn geen (periodieke) controles op de juistheid, nauwkeurigheid en actualiteit van binnen DigiD Substantieel opgeslagen persoonsgegevens voorzien. Er is geen nadere informatie over welke check 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 accounts database.

4.5.2. 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. In toekomstige ontwerpen van DigiD ten behoeve van fraudeonderzoek en -detectie worden mogelijk separate afgeschermde voorzieningen

gerealiseerd, waarbij op basis van polymorfe pseudoniemen niet zonder meer te herleiden gegevens uit systeem- en transactielogs worden verzameld. Het verdient aanbeveling om bij deze toekomstige ontwerpen hierboven bedoelde interne controle- en verantwoordingsmaatregelen gericht op de kwaliteit van de persoonsgegevens mee te ontwerpen.

4.6. Privacyprincipe: verantwoording

De verantwoordelijke 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 verantwoordelijke zijn uitbesteed aan een verwerker.

De verantwoordelijkheid voor DigiD is duidelijk geregeld. Het ministerie van BZK is verantwoordelijke 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.

Over de ketenverantwoordelijkheid RDW <> Logius <> RvIG in relatie tot DigiD Substantieel bestaan de volgende afspraken. Logius is verantwoordelijk voor de ad hoc gegevensuitvraag en voor het daartoe bedoelde bericht. Dit bericht wordt aangeleverd via Diginetwerk. Dit wordt beheerd door een separate afdeling. RvIG en RDW zijn verantwoordelijk voor de voorzieningen aan hun zijde en de aanlevering van de juiste berichten ook weer via Diginetwerk. Logius, RDW en RvIG zijn dus operationeel elk verantwoordelijk voor haar eigen ‘end point’. De verbinding geregeld via Diginetwerk is encrypted (SSL/TLS). Diginetwerk is een voorziening van de Rijksoverheid. Diginetwerk kent eigen logging en genereert metadata (gegevens die ontstaan als gevolg van het gebruik van Diginetwerk), maar deze zijn niet te herleiden naar gebruikersniveau.

4.6.1. Bevindingen

Logius maakt op haar beurt gebruik van subverwerkers voor de levering van IT-diensten. Zoals in paragraaf 4.4.1 genoemd dient de subverwerkersovereenkomst met de subleverancier nog opgesteld te worden. Door Logius is dit onderkend en is dit actiepunt onderhanden. Op de verwerkingen bij derde partijen in relatie tot de realisatie van DigiD Substantieel en specifiek de verwerkingen met betrekking tot de RDA-server is het toezicht nog onvoldoende geformaliseerd.

4.6.2. Aanbevelingen

Aanbevolen wordt om ook vanuit de eigen verantwoordelijkheid periodiek controles uit te voeren op de gegevens(verwerkingen) die bij derden zijn ondergebracht.

4.7. 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 verantwoordelijke moet de beveiliging van de data permanent kunnen garanderen.

4.7.1. 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. De beleidsmatige en technische gronden op basis waarvan deze bewaartermijn wordt gerealiseerd en wat de consequenties daarvan zijn, zijn echter onvoldoende belicht in de wetgeving;
- Een nadeel van het vastleggen van deze transactiegegevens is dat hoe langer ze bewaard worden, hoe meer informatie verzameld wordt over het gedrag van de gebruikers, wat gebruikt kan worden voor profileren. 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 bij burgerrechtenorganisaties. Vanuit die hoek zouden dus bezwaren kunnen komen op de bewaartermijn van vijf jaar.

Logius draagt naast de verantwoordelijkheid over gegevensverwerkingen die intern plaatsvinden ook verantwoordelijkheid voor de beveiliging van de gegevensverwerkingen die bij verwerkers zijn ondergebracht. Met derden dienen tevens afspraken gemaakt te worden teneinde de beveiliging bij deze partijen te waarborgen. De softwarecode van de RDA-server is door de subleverancier van de RDA-server en software, gescand op kwetsbaarheden middels HP Fortify. Deze partij heeft verder hardening uitgevoerd waarmee kwetsbaarheden zijn gereduceerd. Inzicht in de code wordt alleen ter plekke gegeven. De RDA-server staat fysiek in een extern datacenter, waar ook de overige hardware van DigiD staat, in een beveiligde omgeving. Op de verwerkingen bij derde partijen in relatie tot de realisatie van DigiD Substantieel en specifiek de verwerkingen met betrekking tot de RDA-server is het toezicht nog onvoldoende geformaliseerd.

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. In paragraaf 4.4.1 zijn de getroffen beveiligingsmaatregelen opgenomen van het bestaande DigiD-stelsel.

4.7.2. 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 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. 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. Additionele maatregelen kunnen zijn: verdere compartimentering (scheiding) van systemen waardoor risico's beter beheersbaar kunnen worden, encryptie van gevoelige data, reductie van bewaartermijnen waar toegestaan 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.

Aanbevolen wordt om ook vanuit de eigen verantwoordelijkheid periodiek controles uit te voeren op de geïmplementeerde beveiligingsmaatregelen van de gegevens(verwerkingen) die bij verwerkers zijn ondergebracht.

Het verdient aanbeveling om, voor zover nog niet aanwezig, maatregelen te ontwerpen en te implementeren die de werkelijke toegang tot systemen en gegevens waarborgen en deze maatregelen controleerbaar te 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.

4.8. 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.

4.8.1. Bevindingen

In de privacyverklaring van DigiD, die te vinden is op de website, staat beschreven welke persoonsgegevens van de gebruiker van DigiD worden verwerkt en met welk doel (DigiD, 2016). Gebruikers worden bij de aanvraag of het gebruik van DigiD niet expliciet gewezen op de privacyverklaring. De gebruiker wordt dus niet op de hoogte gesteld van het doel van de verwerking van zijn persoonsgegevens vóór het moment van verwerking. Voordat een gebruiker zijn WID scant om DigiD Substantieel te behalen wordt hij ook niet op de hoogte gesteld wat er gebeurt bij het scannen van het WID, dat controle plaatsvindt met de gegevens uit de BRP of het CRB, welke gegevens worden verwerkt en wat het doel van deze verwerking is. In de privacyverklaring ontbreekt tevens expliciet de bewaartermijn van vijf jaar en is niet opgenomen hoe gebruikers het gebruik van DigiD Substantieel kunnen beëindigen en het account kunnen laten opheffen met in acht name van de gehanteerde bewaartermijnen van historische gegevens.

4.8.2. Aanbevelingen

Het verdient aanbeveling om gebruikers van DigiD bij het aanmaken van het authenticatiemiddel en het gebruik hiervan op de hoogte te stellen van de verwerking en het doel van de gegevensverwerking door een verwijzing op te nemen naar de privacyverklaring. Dit verzoek is reeds door Logius in behandeling genomen en wordt doorgevoerd voor de in productie name van DigiD Substantieel.

4.9. Privacyprincipe: 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 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. Tevens heeft de gebruiker de mogelijkheid om zijn account te verwijderen. De gebruiker kan tevens een inzageverzoek indienen bij Logius en een verzoek indienen voor het verbeteren, aanvullen, verwijderen of afschermen van gegevens, tenzij dit niet is toegestaan op grond van een wettelijke bepaling.

Ook kan de gebruiker 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. De gebruiker kan het DigiD-account laten blokkeren of zijn BSN op een afmeldlijst laten plaatsen, zodat geen DigiD aangemaakt kan worden met het betreffende BSN. Dit kan bijvoorbeeld gebruikt worden ter voorkoming van fraude. Bij een verzoek tot inzage, verbetering, aanvulling of verwijdering zal de gebruiker gevraagd worden zich te identificeren door het verstrekken van het BSN en het beantwoorden van een aantal persoonlijke vragen. Bij kritieke activiteiten in de beheermodule, zoals het verwijderen van een account, wordt het vier-ogenprincipe afgedwongen.

4.9.1. Bevindingen

Zoals benoemd in paragraaf 4.8.1 is in de privacyverklaring (nog) niet duidelijk opgenomen hoe het gebruik van DigiD beëindigd kan worden en/of het account opgeheven kan worden.

4.9.2. Aanbevelingen

Het verdient aanbeveling om de gebruikers op de hoogte te stellen van de beëindigingsprocedure door deze op te nemen in de privacyverklaring.

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*.

Integrale Veiligheid Hoger Onderwijs. (2016). *Privacy Impact Assessment - DigiD App Logius.*

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, 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 Substantieel versie 1.0.*

Logius. (2017). *Project Start Architectuur Bijlagen - DigiD Substantieel versie 1.0.*

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

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.

Interviews

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

- Architect
- Beleidsmedewerker
- Communicatiemedewerker
- Fraudemedewerker
- Functioneel ontwerper DigiD Substantieel
- Informatiebeveiliger
- Jurist
- Ketenbeheerder
- Productmanager DigiD app
- Productmanager DigiD Kern
- Productmanager Implementatie
- Productmanager Toegangsdiensten
- Projectleider DigiD

Bijlage I: Vragenlijst PIA

Per privacyprincipe worden bij benadering de volgende risico's gesignaleerd:

Privacyprincipe		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'
  - 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 gebruiker
- GC: Consumenten worden gedwongen om in te stemmen met het gebruik van hun gegevens

Voor een gedetailleerde uitleg van de universele privacyprincipes verwijzen wij naar Bijlage II: Universele privacyprincipes en Bijlage III: Algemene privacyrisico's.
In de linker kolom van onderstaande tabel zijn de vragen opgenomen, geordend naar privacyprincipe, 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)**	**Vaststellen Privacyrelevantie van de PIA** Alvorens de PIA op te starten zal eerst de privacyrelevantie van het object van onderzoek moeten worden vastgesteld. 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'. Uit de informatie verkregen over het ontwerp van DigiD Substantieel blijkt dat de Remote Document Authentication (RDA) server een nieuwe technische component is die wordt gerealiseerd voor DigiD Substantieel. Een nieuw koppelvlak met het CRB wordt gerealiseerd. Ook zijn een aantal functionele en technische uitbreidingen benodigd voor de communicatie met nieuwe koppelvlakken op bestaande DigiD-componenten en bestaande koppelvakken. Aanpassingen worden gedaan op de DigiD Kern, DigiD CIS en op de koppelvlakken DigiD Kern - BRP, RDA-server - DigiD app en DigiD CIS - RDA-server. Nieuwe systeemvoorzieningen zijn gerealiseerd voor het gebruik van de DigiD app. DigiD Substantieel is een systeem dat niet los kan worden gezien van de bestaande DigiD. DigiD Substantieel maakt voor een belangrijk deel gebruik van bestaande technische voorzieningen en verwerkingen van persoonsgegevens van de bestaande DigiD. Anders geformuleerd: de verwerkingen van persoonsgegevens als gevolg van het gebruik van DigiD Substantieel en de bestaande DigiD zijn voor een belangrijk deel technologisch en functioneel dezelfde verwerkingen en zijn operationeel gezien sterk met elkaar verweven. Dit betekent ook dat de privacyrisico's en de daaraan gerelateerde beveiligingsrisico's van de bestaande DigiD niet los gezien kunnen worden van de risico's gekoppeld aan DigiD Substantieel en vice versa. De privacyrisico's van de bestaande DigiD, behoudens de versterking van het uitgifte- en inlogproces, zijn feitelijk ook van toepassing op DigiD Substantieel. Geconstateerd is dat op de bestaande DigiD nog geen integrale PIA is uitgevoerd. Bij de uitvoering van deze PIA op DigiD Substantieel 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. DigiD Substantieel is dus 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 dienstaanbieders, naast het authenticatieniveau

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		Substantieel. Hiermee wordt een geleidelijke overgang bewerkstelligd en is de continuïteit van de bestaande administratie van de inloghistorie van gebruikers gegarandeerd. Bij deze gekozen aanpak spelen daarnaast afwegingen die de projectrisico's beperken, recht wordt gedaan aan strakke mijlpalen en voorgeschreven tijdpaden en een kostenaspect. In deze PIA op de PSA DigiD Substantieel en de wijze waarop deze versie technisch gerealiseerd wordt, is een aantal belangrijke privacyrisico's onderkend. Hierbij zijn naar vermogen aanbevelingen gedaan om deze risico's verder te mitigeren. Deze risico's vloeien echter maar ten dele voort uit de versterking van het bestaande DigiD-authenticatiemechanisme naar het niveau Substantieel. Veel van de onderkende privacyrisico's zijn in feite risico's van de bestaande DigiD-opzet en -infrastructuur die hergebruikt worden binnen DigiD Substantieel. **Conclusie** Een belangrijke conclusie uit deze PIA is dat de realisatie van de PSA DigiD Substantieel maar beperkte additionele privacyrisico's met zich meebrengt ten opzichte van de bestaande DigiD. Het feit dat DigiD Substantieel gerealiseerd wordt met gemeenschappelijke systeemcomponenten en -functies van de bestaande DigiD zorgt ervoor dat de privacyrisico's van de bestaande DigiD overerft worden in DigiD Substantieel. Het is belangrijk te onderkennen dat DigiD Substantieel nog verder wordt doorontwikkeld. De PSA DigiD Substantieel is slechts een eerste stap in een breder versterkingsproces van DigiD. Uiteindelijk is het de bedoeling van het ministerie van BZK en Logius om, naast de realisatie van Substantieel, door te gaan met het ontwikkelen naar DigiD Hoog. Inmiddels is bekend dat in DigiD Hoog cryptografische en andere aanvullende maatregelen zijn voorzien om de privacyrisico's verder te beperken. Het uiteindelijke doel is dat de huidige BSN-gebaseerde verwerking wordt vervangen door een pseudoniem-gebaseerde verwerking waarbij alleen de dienstaanbieder in staat is het pseudoniem te herleiden tot de identiteit van de gebruiker. Dit laat onverlet dat ook voor DigiD Hoog zal gelden dat de eerdere, minder sterke authenticatiemethoden van DigiD voorlopig blijven bestaan en daarmee tevens de daaraan gerelateerde risico's. Op basis van de huidige plannen van het ministerie van BZK om de authenticatiemechanismen en -middelen te versterken is het belangrijk dat de doorontwikkeling zoals is voorgenomen door het ministerie van BZK wordt doorgezet en afgerond en dat uiteindelijk de middelen en concepten van het nu bestaande DigiD-systeem worden afgebouwd en/of de risico's daarvan worden gemitigeerd. In de volgende paragraaf wordt nader ingegaan op de specifieke privacyrisico's. Inherent aan de doelstellingen van DigiD Substantieel worden persoonsgegevens verwerkt waaronder inloggegevens, IP-adressen, BSN's, kenmerken van wettelijke identiteitsdocumenten en andere tot een natuurlijk persoon te herleiden gegevens. Hiermee is de relevantie van de PIA aangetoond.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		Aanbevelingen Op de bestaande DigiD is niet eerder een integrale PIA uitgevoerd. Wel is 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 Substantieel een integrale privacyrisicoanalyse uit te voeren op de organisatorische en technische maatregelen van de bestaande DigiD en de onderliggende infrastructuur.
I.1	Is sprake van een verwerking van persoonsgegevens (volgens de definities van de Wbp?)	Er worden in het domein van DigiD Substantieel persoonsgegevens verzameld en verwerkt van gebruikers die een DigiD-middel aanvragen en gebruiken. De gegevens die worden verwerkt zijn onder andere: <u>Voor paspoort en ID-kaart:</u> ▪ BSN; ▪ Geboortedatum van de gebruiker; ▪ WID-nummer; ▪ Geldigheidsdatum; ▪ Aanduiding resp. datum van inhouding/vermissing; ▪ IP-adres. <u>Voor het rijbewijs:</u> ▪ BSN; ▪ MRZ; ▪ Reden ongeldig rijbewijs; ▪ IP-adres. Dit zijn persoonsgegevens volgens de Wbp en de AVG. Daarnaast worden gegevens verwerkt die ontstaan door het gebruik van DigiD door de gebruiker, zogeheten metadata. Bij het gebruik van een DigiD-middel bij dienstaanbieders worden in een transactielog gegevens vastgelegd, waaronder het IP-adres van de gebruiker, de tijd van inloggen en de website van de instelling waar de gebruiker inlogt. Netwerkcomponenten genereren loggings waarin metadata (waaronder IP-adressen) zitten die informatie kunnen onthullen over gebruikers. IP-adressen worden aangemerkt als digitale *identifiers*, wat gevoelige gegevens zijn waar extra voorzichtig mee moeten worden omgegaan, omdat deze gebruikt kunnen worden om te profileren en mogelijk voor identiteitsfraude. De genoemde metadata kunnen ook informatie onthullen over inloggedrag en in potentie misbruikt worden voor profiling met mogelijk negatieve gevolgen voor de gebruikers. **Conclusie** Er is sprake van het verwerken van persoonsgegevens zoals bedoeld in de Wbp en de AVG. Bovendien is naast het verwerken van gewone persoonsgegevens ook sprake van de verwerking van gevoelige persoonsgegevens. Zie I.3.
I.2	Kan uw organisatie als verantwoordelijke worden aangemerkt voor de verwerking of treedt u op als verwerker	De minister van BZK is verantwoordelijke en de uitvoering is belegd bij Logius, een onderdeel van het ministerie van BZK. Logius maakt op haar beurt gebruik van (sub)verwerkers voor de levering van IT-diensten.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
	(uw organisatie verwerkt de persoonsgegevens in opdracht en onder verantwoordelijkheid van een andere organisatie)?	Met deze partijen zijn of worden (sub)verwerkersovereenkomsten afgesloten. Het technisch applicatiebeheer van de RDA-omgeving heeft Logius uitbesteed aan een leverancier. Met deze partij is een verwerkersovereenkomst afgesloten. De RDA-server is door deze leverancier ingekocht bij een subleverancier. Een subverwerkersovereenkomst met deze partij is niet aanwezig en is ook geen onderdeel van de verwerkersovereenkomst van de leverancier. Aangezien de subleverancier in verband met de werking van DigiD Substantieel wel persoonsgegevens verwerkt, dient een subverwerkersovereenkomst nog opgesteld te worden. **Conclusie en aanbevelingen** Ten tijde van de uitvoering van de PIA bleek dat de subverwerkersovereenkomst tussen Logius en de subleverancier van de RDA-server nog niet was geformaliseerd. Het verdient aanbeveling om de verwerkersovereenkomsten te formaliseren met alle relevante partijen. Dit is door Logius onderkend en de actie om de subverwerkersovereenkomst te realiseren is onderhanden.
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 de bedoeling. Het verwerken van gegevens met een verhoogde gevoeligheid die kunnen leiden tot stigmatisering of uitsluiting is geen onderdeel van het ontwerp van DigiD Substantieel. De beschrijving van de PSA DigiD Substantieel geeft dit niet aan. Logius heeft de beschikking over persoonsgegevens, waaronder BSN's en IP-adressen van gebruikers. Deze gegevens worden niet versleuteld of gepseudonimiseerd. Daarbij blijkt uit waarnemingen dat de accountgegevens gekoppeld kunnen worden aan transactiegegevens. Het is daarmee onder meer bekend welk IP-adres hoort bij welk BSN. In de transactielogging van het gebruik van DigiD wordt onder andere vastgelegd bij welke dienst de gebruiker heeft ingelogd. Hierdoor 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). Denk hierbij aan gebruikers die met hun DigiD inloggen bij dienstaanbieders voor schuldhulpverlening of uitkeringsinstanties. DigiD maakt gebruik van sessie en persistente cookies en deze zijn niet specifiek voor DigiD Substantieel. In deze cookies worden geen persoonsgegevens gebruikt. De cookies zijn nodig om te zorgen dat DigiD kan werken met de verschillende applicatieservers die gebruikt worden. Teneinde het gebruik van de app te kunnen 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.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		Conclusie Binnen het concept van DigiD Substantieel is een cumulatie aanwezig met inloghistorie waarmee een beeld kan worden verkregen over welke dienstaanbieders door welke gebruikers worden bezocht. Hiermee kan indirect een beeld worden verkregen over mogelijk stigmatiserende situaties van een gebruiker. Dit is niet nieuw of specifiek voor DigiD Substantieel. Ze gelden ook voor het al bestaande DigiD-systeem en technische componenten waarop DigiD Substantieel wordt geplaatst. **Aanbevelingen** Bij de vervolgontwerpfasen verdient het aanbeveling de risico's van de inloghistorie en profilingrisico's nader te beschouwen en aanvullende maatregelen te treffen. Te denken valt aan verdere toepassing van encryptie van data, pseudonimiseringstechnieken en verdere limitering van de opslag en toegang tot de data. Het aanbrengen van een 'Chinese muur' tussen accountgegevens (BSN) en transactiegegevens (inloghistorie) en netwerkgegevens (IP-adressen) is daarbij een belangrijk handvat. 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. Dit wordt in de ontwerpdocumentatie, aanvullend op de PSA, beschreven. In het kader van deze PIA op de PSA van DigiD Substantieel 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 er in DigiD Substantieel 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 dienstaanbieder die specifiek diensten aanbiedt aan een kwetsbare groep, vanwege de eigenschap van DigiD dat de inloghistorie wordt bewaard, waaronder ook de gegevens over bij welke dienstaanbieder een gebruiker inlogt, kan 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. **Conclusie** Via de DigiD-inloghistorie kan een relatie gelegd worden tussen welke gebruikers tot welke kwetsbare groepen behoren. De DigiD-dataset biedt de analysemogelijkheden hiertoe. Het ligt in de lijn van de verwachting dat DigiD Substantieel gebruikt gaat worden voor het inloggen bij meer gevoelige webdiensten van dienstaanbieders in het BSN-domein. Dus juist deze gevoeligheid maakt de risico's van profling en stigmatisering groter. **Aanbeveling** Aanbevolen wordt in kaart te brengen welke persoonsgegevens worden verwerkt die hogere

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		privacywaarborgen verlangen en additionele maatregelen te implementeren voor de beveiliging van deze gegevens.
I.3c	Is het de bedoeling gebruikersnamen, wachtwoorden of andere inloggegevens te verwerken?	In het domein van DigiD Substantieel worden volgens het Besluit GDI de accountgegevens van een gebruiker van DigiD verzameld, waaronder het e-mailadres, de gebruikersnaam van het account en het bijbehorende wachtwoord, dat versleuteld wordt verwerkt. De pincode, die werd geïntroduceerd bij de DigiD app, wordt - gemaskeerd (niet herleidbaar tot de echte pincode) opgeslagen conform cryptografisch ontwerp. 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 biometrische gegevens te verwerken.
I.3e	Is het de bedoeling om het BSN-nummer of een ander persoonsgebonden nummer te verwerken?	Het huidige DigiD-stelsel en DigiD Substantieel verwerken BSN's van gebruikers. Het BSN wordt in het DigiD-domein gebruikt als uniek identificeerbaar gegeven om gebruikers van elkaar te scheiden, de uniciteit van identiteiten te waarborgen en gegevens te valideren op juistheid en geldigheid om vervolgens aan dienstaanbieders kenbaar te maken en zekerheid te verschaffen met welke persoon zij te maken hebben. Daarnaast wordt in DigiD Substantieel het BSN gebruikt om gegevens van de gebruikers uit de BRP of het CRB op te halen als zij het WID scannen om DigiD Substantieel te behalen. Door middel van het BSN worden de gegevens van de (vier) meest recente paspoorten en identiteitskaarten van die specifieke persoon uit de BRP of van het rijbewijs uit het CRB verkregen. Overigens is het gebruik van DigiD Substantieel alleen geschikt om gebruikt te worden binnen het BSN-domein. Verder gebruik in het private domein is uitgesloten. Het BSN wordt onversleuteld en niet-gepseudonimiseerd opgeslagen in de accountdatabase van de gebruiker, die via de beheermodule van DigiD te bereiken is. Slechts een beperkt aantal medewerkers van Logius heeft toegang tot deze beheermodule. Het BSN wordt tevens gebruikt als een gebruiker de helpdesk van Logius benadert met vragen over of problemen met het account. Gezien de vertrouwelijkheid van het BSN is er wel voor gekozen om het BSN te vervangen door een tijdelijk en niet persistent sessie-ID bij de gegevensuitwisseling tussen de endpoint van de gebruiker (in casu een smartphone of usb-reader) met de RDA-server. De roadmap om naar DigiD Hoog te komen is de doorontwikkeling van het huidige DigiD-systeem, om van een BSN-gebaseerde verwerking naar een pseudoniem-gebaseerde verwerking te komen. **Conclusie** Het BSN is het kerngegeven binnen DigiD Substantieel. In de toekomst zal DigiD Substantieel doorontwikkeld worden waarbij het huidige DigiD-systeem afgebouwd zal worden. Naast DigiD Hoog zullen uiteindelijk ook de huidige DigiD en DigiD Substantieel gebruik maken van een pseudoniem-gebaseerde verwerking ter vervanging van de huidige BSN-gebaseerde verwerking.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
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.)?	DigiD Substantieel verwerkt het BSN voor de bevraging van de BRP en het CRB. Gegevens omtrent godsdienst, ras, politieke of seksuele voorkeur en strafrechtelijk verleden worden niet door DigiD verwerkt en zijn ook niet in de ontwerpen beschreven. In de metadata die worden verzameld door middel van transactielogging is het niet uitgesloten dat dit soort gegevens echter wel herleid kunnen worden. In de transactielogging worden namelijk IP-adressen van gebruikers opgeslagen en wordt informatie opgeslagen over wanneer gebruikers bij welke dienstaanbieders hebben ingelogd. Zie de voorafgaande opmerkingen en toelichting hierover bij vraag I.3a en I.3b. **Conclusie** Gegevens omtrent godsdienst, ras, politieke of seksuele voorkeur en strafrechtelijk verleden worden niet door DigiD verwerkt. Echter is indirecte herleiding van deze gegevens niet uitgesloten vanwege de gegenereerde metadata. **Aanbeveling** Aanbevolen wordt in kaart te brengen welke persoonsgegevens worden verwerkt die hogere privacywaarborgen verlangen en additionele maatregelen te implementeren voor de beveiliging van deze gegevens.
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?	Nieuw in DigiD Substantieel, ten opzichte van het huidige DigiD-systeem, is dat een gebruiker de NFC-chip in een WID scant met een NFC-reader, om zijn identiteit te laten verifiëren. Om de NFC-chip van een WID uit te lezen en de informatie daarin te controleren, wordt gebruik gemaakt van een RDA-server. De RDA-server maakt gebruik van nieuwe technologie ten opzichte van de bestaande middelen gebruikt bij DigiD. Deze technologie is wel al toegepast in een pilot bij de RDW. Naast de toevoeging van de RDA-server zijn aanpassingen gedaan in koppelvlakken en interfaces (CIS) en bestaande DigiD-onderdelen. Ook moet de gebruiker, om DigiD Substantieel te gebruiken, beschikken over de DigiD app. De DigiD app is al beschikbaar, maar nog niet met de functionaliteiten om niveau 'Substantieel' te behalen. Aanpassingen worden gedaan voor deze app voor het kunnen behalen van dit niveau.
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)?	Er wordt gebruik gemaakt van nieuwe technologie, de RDA-server. Daarnaast wordt de mobiele technologie, namelijk de DigiD app, aangepast voor DigiD Substantieel. Via de app wordt met behulp van de NFC-reader de chip van een WID gescand. Het is 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?	De ontwikkeling van DigiD Substantieel is op zichzelf een verschuiving in zowel de manier waarop persoonsgegevens worden verwerkt als in de technologie die daarvoor wordt gebruikt. Het verschil in de verwerking van persoonsgegevens met het huidige DigiD-systeem is dat in DigiD Substantieel een WID uitgelezen en geverifieerd zal gaan worden door middel van een nieuwe technologie (de RDA-server). Er worden tevens meer gegevens verwerkt dan voor de huidige DigiD Basis en DigiD Midden, zie hiervoor III.2. Belangrijk is te onderkennen dat de achterliggende systemen en dataverwerkingen van DigiD Basis en DigiD Midden dezelfde systemen en databases zijn als die gebruikt worden voor DigiD Substantieel en dat de gebruikte dataverzamelingen ook blijven bestaan. Het is belangrijk te onderkennen dat DigiD Substantieel nog

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		verder wordt doorontwikkeld. De PSA DigiD Substantieel is slechts een eerste stap in een breder versterkingsproces van DigiD. Uiteindelijk is het de bedoeling van het ministerie van BZK en Logius om, naast de realisatie van Substantieel, door te gaan met het ontwikkelen naar DigiD Hoog. Inmiddels is bekend dat in DigiD Hoog cryptografische en andere aanvullende maatregelen zijn voorzien om de privacyrisico's verder te beperken. Het uiteindelijke doel is dat de huidige BSN-gebaseerde verwerking wordt vervangen door een pseudoniem-gebaseerde verwerking waarbij alleen de dienstaanbieder in staat is het pseudoniem te herleiden tot de identiteit van de gebruiker.
I.7	Kan de manier waarop de gegevens worden verzameld worden opgevat als privacygevoelig?	Voor het verzamelen en verwerken van de persoonsgegevens van gebruikers wordt gebruik gemaakt van het BSN. Het BSN is op zichzelf al een privacygevoelig gegeven aangezien het een unieke identifier is. Daarnaast worden gegevens verzameld over het inloggen door gebruikers bij dienstaanbieders. Dit levert privacygevoelige data op aangezien personen hiermee geprofileerd kunnen worden.
I.8	Zijn er veel maatschappelijk belanghebbenden?	Alle Nederlandse burgers kunnen gebruikmaken van DigiD en daarmee ook van DigiD Substantieel. Daarmee is de groep maatschappelijk belanghebbenden dus erg groot. Daarnaast kan gezegd worden dat DigiD zelf van maatschappelijk en economisch groot belang is, aangezien het één van de belangrijkste (publieke) eID-middelen zal blijven. 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?	DigiD wordt op dit moment gebruikt door 13,4 miljoen gebruikers. De verwachting is dat 0,5 miljoen tot 1,5 miljoen van deze gebruikers in de eerste fase zal overgaan naar DigiD Substantieel. Een beperking daarbij is dat in eerste instantie enkel Android-telefoons gebruikt kunnen worden voor het scannen van de NFC-chip op het WID. DigiD Substantieel zal daarmee betrekking hebben op en gebruikt worden door een aanzienlijk kleiner deel van de bevolking dan DigiD Basis/Midden. Uiteindelijk is het echter de bedoeling dat de gehele bevolking de mogelijkheid heeft om gebruik te maken van DigiD Substantieel.
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 dienstaanbieders. Additioneel worden bij DigiD Substantieel, ten opzichte van DigiD Basis en DigiD Midden, de gegevens van het WID verwerkt. De ontwikkeling van DigiD Substantieel 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) Daarbij is het initiatief tot de ontwikkeling van DigiD Substantieel een voortvloeisel van het beleid van Kabinet Rutte om de betrouwbaarheid van DigiD te versterken en het realiseren van een multimiddelenstrategie. Het

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		uitvoeringsprogramma om dit te realiseren heet 'eID Impuls' en wordt uitgevoerd onder verantwoordelijkheid van het ministerie van BZK waarvan de uitvoering is belegd bij Logius.
I.11	Worden de gegevens verzameld op basis van een van de wettelijke grondslagen volgens de Wbp?: ▪ U vraagt 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 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 Substantieel (en Hoog) opgenomen worden. **Conclusie** De wettelijke grondslagen volgens de Wbp en AVG om persoonsgegevens te verwerken onder de verantwoordelijkheid van het ministerie van BZK/Logius ten behoeve van DigiD Substantieel zijn aanwezig: vervulling publiekrechtelijke taak en toestemming.
I.12	Welke (overige) wet- en regelgevingen zijn relevant voor deze PIA?	De volgende wet- en regelgevingen zijn relevant voor de PIA op DigiD Substantieel. 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** **Privacyprincipe:** **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	Om betrouwbaarheidsniveau DigiD Substantieel te behalen wordt een bevraging gedaan naar de BRP of het CRB. Het raadplegen van gezaghebbende bronnen is een eIDAS-vereiste voor authenticatiebetrouwbaarheidsniveau Substantieel. In het ontwerp van DigiD Substantieel is de bevraging naar de BRP specifiek. In de implementatie is hier geen rekening mee gehouden waardoor de gegevens waar

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
	er precies niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? Licht per te verwerken persoonsgegeven toe.	DigiD autorisatie voor heeft, worden ontvangen van de vier meest recente paspoorten/identiteitskaarten. De gegevens die benodigd zijn voor DigiD Substantieel (geboortedatum van de gebruiker, WID-nummer. geldigheidsdatum en aanduiding op of datum van inhouding/vermissing) kunnen door Logius wel gespecifieerd worden zodat alleen de gegevens worden ontvangen die benodigd zijn voor DigiD Substantieel. De huidige functionaliteit geboden door RvIG biedt echter niet de mogelijkheid om de gegevensaanvraag RvIG specifiek te maken op basis van het documentsoort (paspoort/identiteitskaart). Als compenserende maatregel wordt conform het ontwerp de onnodig ontvangen gegevens bij Logius na een uur geautomatiseerd gewist. De privacyrisico's zijn voor dit onderdeel hiermee geminimaliseerd. 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. In de Detailed Level Design worden deze technische componenten wel genoemd. 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 juist functioneren te bewaken. Hiermee worden echter risico's gecreëerd waaronder risico's voor ongewenste herleiding van gegevens en profiling. Vastgesteld is dat loggegevens op basis van IP-adres kunnen worden herleid tot een BSN. In de bestaande DigiD zijn de technische loggings gedecentraliseerd naar componenten. Dezelfde benadering geldt voor de nieuwe componenten van DigiD Substantieel (waaronder de RDA-server) en voor de aanpassingen in koppelvlakken en interfaces (waaronder het CIS) en bestaande DigiD-onderdelen (waaronder DigiD Kern). De DigiD app zelf legt geen gegevens vast over het gebruik. De eerder beschreven beveiligingsregimes gelden ook voor deze nieuwe componenten. De componenten zelf genereren de syslogs en de applicatie/databases genereren de transactielogs. De afzonderlijke decentrale loggings worden samengebracht in een centrale logging- en monitoringomgeving. Vanuit deze omgeving gaat alleen relevante logging naar het SIEM. Het SIEM is een bij een externe partij afgenomen dienst ingericht op infrastructuurniveau waarin de logging voor specifieke doelstellingen wordt gemonitord (op basis van use cases). De monitoringomgeving is apart te bereiken en extra beveiligd (veilig opgeslagen en encrypted). Deze beveiligingsmaatregelen gelden ook voor de back-up van de logbestanden. **Conclusie en aanbevelingen** De huidige uitvraag naar de BRP is niet specifiek voor DigiD Substantieel waardoor naast de benodigde gegevens voor DigiD Substantieel ook overige gegevens van de gebruiker waar DigiD autorisatie voor heeft worden ontvangen. Aanbevolen wordt de gegevensaanvraag voor Substantieel te specifiëren zodat alleen de gegevens worden ontvangen die benodigd zijn voor DigiD Substantieel (geboortedatum, WID-nummer, geldigheidsdatum en aanduiding op of datum van inhouding/vermissing). Het verdient aanbeveling om bij de doorontwikkeling van DigiD Substantieel de RvIG te verzoeken om de mogelijkheid te bieden voor het specifiëren van de BRP bevraging zodat alleen de gegevens van het voor de verificatie gebruikte WID worden ontvangen. Logius heeft als maatregel ingesteld dat deze gegevens, na uitvraag en indien ze niet nodig zijn

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		voor de controle, maximaal één uur nadien worden verwijderd. Het stelsel van loggings en de centralisatie van logging is voorzien van preventieve beveiligingsmaatregelen en signaleringen van eventueel onbevoegde toegang. Er is sprake van een limitering van dataverzameling in het SIEM op basis van use cases. Dit laat onverlet dat de geconstateerde herleiding van IP-adressen naar BSN's deze loggings nog steeds gevoelig maken voor profiling. Daarbij ontbreekt een integraal en toegankelijk overzicht van alle verwerkingen van persoonsgegevens op dit technische niveau. Het verdient aanbeveling om een dergelijk integraal overzicht te maken van alle gegenereerde loggegevens en eventuele metadata (gegevens die ontstaan als gevolg van het gebruik van DigiD), naast de functionele beschrijvingen van het huidige ontwerp van DigiD Substantieel. Ook in het kader van het principe van transparantie is dit overzicht relevant.
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?	Logius heeft de beschikking over persoonsgegevens, waaronder BSN's en IP-adressen van gebruikers. Deze gegevens worden niet versleuteld of gepseudonimiseerd. Daarbij blijkt uit waarnemingen dat de accountgegevens gekoppeld kunnen worden aan transactiegegevens. Het is daarmee onder meer bekend welke IP-adres hoort bij welk BSN. In de transactielogging van het gebruik van DigiD wordt onder andere vastgelegd bij welke dienst de gebruiker wenst in te loggen. Hierdoor ontstaat een gevoelig en waardevol bestand op basis waarvan profielen van gebruikers opgesteld zouden kunnen worden (bijvoorbeeld via offline analyse). Denk hierbij aan gebruikers die met hun DigiD inloggen bij dienstaanbieders die zich inzetten voor ondersteuning bij jeugdzorg, bij reclassering of binnen het sociaal domein. De inloghistorie geeft daarbij mogelijk indicaties prijs dat gebruikers behoren tot kwetsbare groepen. Kwetsbare groepen hebben conform de privacywetgeving meer rechten op privacybescherming. Het is hierbij belangrijk te onderkennen dat DigiD Substantieel nog verder wordt doorontwikkeld. De PSA DigiD Substantieel is slechts een eerste stap in een breder versterkingsproces van DigiD. Uiteindelijk is het de bedoeling van het ministerie van BZK en Logius om, naast de realisatie van Substantieel, door te gaan met het ontwikkelen naar DigiD Hoog. Inmiddels is bekend dat in DigiD Hoog cryptografische en andere aanvullende maatregelen zijn voorzien om de privacyrisico's verder te beperken. Het uiteindelijke doel is dat de huidige BSN-gebaseerde verwerking wordt vervangen door een pseudoniem-gebaseerde verwerking waarbij alleen de dienstaanbieder in staat is het pseudoniem te herleiden tot de identiteit van de gebruiker. **Conclusie en aanbevelingen** Op de bestaande DigiD is niet eerder een integrale PIA uitgevoerd. Wel is 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 Substantieel een integrale privacyrisicoanalyse uit te voeren met inachtneming van de getroffen organisatorische en technische maatregelen van de bestaande DigiD en de onderliggende infrastructuur.
III	**Doelbinding, koppeling en profilering**	

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
	Privacyprincipe: **Doelbinding / Limitering van gebruik van gegevens**	
	<u>Doeleinden/doelbinding en koppeling</u>	
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?	Het doel van het ontwikkelen van DigiD Substantieel is het bieden van een betrouwbaar middel voor gebruikers om in te kunnen loggen op het BSN-domein, waarbij wordt voldaan aan de eisen van het eIDAS betrouwbaarheidsniveau 'Substantieel' (Commissie, 2015). De huidige DigiD (DigiD Basis en DigiD Midden) voldoet daar niet aan. De ontwikkeling van DigiD Substantieel moet gezien worden als een stap in de uiteindelijke doorontwikkeling naar een middel met het eIDAS betrouwbaarheidsniveau 'Hoog'. **Conclusie en aanbevelingen** 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. Het verdient aanbeveling om een integraal overzicht te maken van het volledige DigiD landschap en de infrastructuur, zodat de verwerkingen van bestaand DigiD en DigiD Substantieel 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)	Het doel van DigiD is het bieden van een authenticatiemiddel voor gebruikers om in te loggen in het BSN-domein. Ten opzichte van DigiD Basis en DigiD Midden worden voor DigiD Substantieel de volgende nieuwe persoonsgegevens verwerkt om de betrouwbaarheid van het authenticatiemiddel te verhogen: <u>Koppelvlak BRP</u>: Van de BRP worden de volgende velden aanvullend voor DigiD Substantieel ontvangen en verwerkt van een identiteitskaart of paspoort: ▪ Soort Nederlands reisdocument ▪ Nummer Nederlands reisdocument ▪ Datum einde geldigheid Nederlands reisdocument ▪ Datum inhouding dan wel vermissing Nederlands reisdocument ▪ Aanduiding inhouding dan wel vermissing Nederlands reisdocument ▪ Geboortedatum houder identiteitsdocument <u>Koppelvlak CRB:</u>

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		Van het CRB wordt de MRZ of de reden van een ongeldig rijbewijs ontvangen. Dit betreft een nieuw koppelvlak. <u>Tunnel RDA-server en NFC-chip op WID (met DigiD app of USB Reader):</u> In geval van een identiteitskaart of paspoort wordt de MRZ uit de chip van het WID uitgelezen. Deze datagroep bevat de volgende gegevens: ▪ Document code ▪ Issuing State or organization ▪ Name of holder ▪ Document number ▪ Check digit - Document number ▪ Nationality ▪ Date of birth ▪ Check digit - Date of birth ▪ Sex ▪ Date of expiry ▪ Check digit - Date of expiry or valid until date ▪ Optional data ▪ Check digit ▪ Composite check digit In geval van een rijbewijs wordt de MRZ uit de chip van het WID uitgelezen. Deze MRZ bevat de volgende gegevens: ▪ Identifier ▪ Rijbewijsnummer (persoonsgegeven) ▪ Discretionary data ▪ Composite check digit De DigiD app zelf legt geen gegevens vast over het gebruik. De DigiD app genereert ook geen aanvullende loggings. Op het mobiele apparaat met de DigiD app worden alleen het app ID en de private key vastgelegd op een beveiligde wijze. Aan de backend zijde voor de communicatie met de DigiD app worden de volgende gegevens vastgelegd: <u>Gemaskeerde pincode van de gebruiker:</u> ▪ Public key ▪ App ID ▪ Naam van het mobiele apparaat ▪ Symmetrische sleutel De historie van de sessie tussen de DigiD app en de backend wordt cryptografisch beschermd opgeslagen.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		Nadat de controles zijn afgerond worden de gegevens uit de BRP of het CRB en van de NFC-chip niet bewaard in DigiD. <u>Logging:</u> In de log van de RDA-server wordt het unieke gepseudonimiseerde BSN, de tijd van authenticatie, de NFC-reader soort, het WID-soort en het resultaat van de verificatie (OK/NOK) opgeslagen. In bovenstaand overzicht worden BSN, IP-adres, telefoonnummer, hardware kenmerken van devices en andere gegevens van gebruikers niet genoemd omdat deze in de huidige DigiD Basis en Midden al worden vastgelegd. Belangrijk is te onderkennen dat deze gegevens wel ook verwerkt worden bij DigiD Substantieel. Teneinde het gebruik van de app te kunnen volgen en analyseren wordt gebruik gemaakt van Piwik. Piwik is een opensourceprogramma om bezoekersstatistieken bij te houden. Piwik houdt hiervoor geanonimiseerde gebruiksgegevens bij. **Conclusie en aanbevelingen** DigiD Substantieel zorgt voor een uitbreiding van de typen van persoonsgegevens bovenop de al bestaande gegevensverwerkingen van DigiD Basis en Midden. Het verdient aanbeveling om bij de verdere ontwerpstappen een integraal overzicht op te stellen van welke persoonsgegevens worden verwerkt over de verschillende DigiD-varianten 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 privacyoptiek. 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?	Een nieuw doel dat wordt bereikt met DigiD Substantieel ten opzichte van DigiD Basis en DigiD Midden is het verhogen van de betrouwbaarheid van het authenticatiemiddel. Dit wordt bereikt door het verifiëren van de identiteit door middel van gegevens op het WID. Hiervoor worden aanvullende gegevens verkregen van de BRP en is een nieuw koppelvlak gecreëerd met het CRB. De RvIG en de RDW hebben geen belang bij de verwerking van deze gegevens. Logius is aangewezen als belanghebbende voor het verkrijgen van de gegevens uit de BRP en het CRB. Dienstaanbieders die gebruik maken van DigiD Substantieel zullen dezelfde doelstelling hebben als Logius, namelijk het bieden van een betrouwbaar authenticatiemiddel om gebruik te maken van de dienst. **Conclusie**

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		Er zijn vanuit privacyoptiek geen strijdige belangen of doelstellingen te verwachten bij de betrokken stakeholders in de DigiD-keten en bij het gebruik van DigiD Substantieel.
III.4	Is het gebruik van de gegevens in lijn en verenigbaar met het doel van verzamelen? Worden de gegevens gebruikt 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?	In het aanwijzingsbesluit van RDW is opgenomen dat de gegevens die worden verkregen van het CRB voor identiteitsverificatie uitsluitend gebruikt mogen worden om: ▪ Te verifiëren dat de persoon van wie het BSN is verstrekt in het bezit is van een rijbewijs; ▪ Het WID op echtheid te controleren. Het autorisatiebesluit van RvIG voor de verstrekking en verzameling van gegevens van het paspoorten/identiteitskaarten voor de doelstellingen van DigiD Substantieel is nog niet definitief. De verwachting is echter dat in dit besluit gelimiteerd wordt op het gebruik van de gegevens door Logius. De gegevens die beschikbaar worden gesteld door RvIG aan Logius in het kader van de validatie van WID-informatie worden niet opgeslagen. De verstrekte informatie betreft validatie-informatie en niet de persoonsgegevens zelf van het WID. Uit de loggegevens aanwezig bij Logius zijn de gegevens wel herleidbaar. Deze gegevens worden niet voor andere doeleinden gebruikt dan authenticatiedoelstellingen, maar zijn wel benaderbaar in geval er aanleiding is tot fraudeonderzoek. **Conclusie** De verzamelde gegevens bij Logius zijn passend binnen de doelstellingen van DigiD Substantieel.
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 bij het gebruik van DigiD Basis, DigiD Midden en de DigiD app zijn reeds gemeld bij de FG. De melding bij de FG voor de verwerking van persoonsgegevens voor DigiD Substantieel zal worden gedaan wanneer DigiD Substantieel 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?	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 Substantieel. Er wordt verwezen naar normen voor informatiebeveiliging die vooral toezien op de procedurele kant van Information Security Management Systemen 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. Binnen de beheeromgeving van Logius zijn verscheidene maatregelen getroffen om de toegang en het gebruik van deze gevoelige gegevens te beperken. 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. Dit laat onverlet dat er sprake is van een cumulatie van inloghistorie met hoog gevoelige data en dat IP-adressen naar een BSN worden herleid. Deze maatregelen gelden voor de huidige DigiD en blijven gelijk voor DigiD Substantieel. **Conclusie en aanbevelingen**

Nr.	Vraag	Bevindingen / Risico's / 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 Gebruikers te nemen? Ofwel, kunnen met behulp van de gegevens profielen worden opgesteld van de Gebruikers, al dan niet geanonimiseerd?	In de metadata die worden verzameld door middel van logging kunnen deze gegevens herleid worden. In de transactielogging worden onder meer het BSN en het IP-adres van de gebruiker opgeslagen en wordt informatie opgeslagen over wanneer de gebruiker bij welke dienstaanbieders heeft ingelogd. De inloghistorie kan vertrouwelijke informatie bevatten waarmee gebruikers geprofileerd kunnen worden. Zoals eerder benoemd is het belangrijk te onderkennen dat DigiD Substantieel nog verder wordt doorontwikkeld. De PSA DigiD Substantieel is slechts een eerste stap in een breder versterkingsproces van DigiD. Uiteindelijk is het de bedoeling van het ministerie van BZK en Logius om, naast de realisatie van Substantieel, door te gaan met het ontwikkelen naar DigiD Hoog. Inmiddels is bekend dat in DigiD Hoog cryptografische en andere aanvullende maatregelen zijn voorzien om de privacyrisico's verder te beperken. Het uiteindelijke doel is dat de huidige BSN-gebaseerde verwerking wordt vervangen door een pseudoniem-gebaseerde verwerking waarbij alleen de dienstaanbieder in staat is het pseudoniem te herleiden tot de identiteit van de gebruiker. **Conclusie en aanbevelingen** Het is belangrijk te onderkennen dat de privacyrisico's steeds verder toenemen naarmate de hoeveelheid van opgeslagen persoonsgegevens groter wordt naarmate er meer historie wordt opgeslagen én het gebruik van DigiD stijgt. Met de transactielogging en systeemlogging die ontstaat kunnen profielen opgesteld worden van de gebruikers. Het verdient aanbeveling om de privacyrisico's die hierdoor ontstaan te mitigeren door sterke technische beveiligingsmaatregelen te implementeren. Te denken valt aan verdere toepassing van encryptie van data, pseudonimiseringstechnieken en verdere limitering van de opslag en toegang tot de data. Ook het compartimenteren van systemen en het afscheiden van deze gevoelige datasets verdient overweging. Het aanbrengen van een Chinese muur tussen accountgegevens (BSN) en transactiegegevens (inloghistorie) en netwerkgegevens (IP-adressen) is daarbij een belangrijk handvat. Deze maatregelen zijn nu niet voorzien in de ontwerpdocumentatie.
III.8	Zijn de Gebruikers 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 Gebruikers op? Kunnen de opgestelde profielen leiden tot	Profileren is niet aan de orde. Gegevens die Logius verzamelt en verwerkt hebben niet tot doel gebruikers te profileren.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
	uitsluiting of stigmatisering?	
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 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?	De vergelijking van persoonsgegevens met de BRP of het CRB en de chip vindt geautomatiseerd plaats. De persoon wordt middels deze vergelijking niet beoordeeld/voorspeld maar er vindt wel een verificatie plaats op basis van deze gegevens waar eventuele foutcodes uit voortkomen. Uit deze foutcodes kan bijvoorbeeld worden opgemaakt of een chip gewijzigd of gekloond is of dat er andere afwijkingen zijn. Aan de hand van de foutcodes kunnen medewerkers van Logius actie ondernemen en zo nodig contact opnemen met de gebruiker. **Conclusie en aanbevelingen** Het verdient aanbeveling ter waarborging van de rechten van gebruikers en ter beperking van eventuele nadelige effecten voor de gebruikers om aan het huidige ontwerp DigiD Substantieel 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*** ***Privacyprincipe:*** **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?	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. De ten behoeve van DigiD Substantieel opgevraagde persoonsgegevens bij de BRP en het CRB worden als juist aangenomen. 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. In het huidige ontwerpdocument zijn geen (periodieke) controles voorzien op juistheid, nauwkeurigheid en actualiteit van binnen DigiD Substantieel opgeslagen persoonsgegevens. 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 loggen de databases de veranderingen in de tabellen, waaronder de accountdatabase.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		Conclusie en aanbevelingen 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. 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 data te kunnen valideren. De beoogde interne controle maatregelen zijn dus andere maatregelen dan de bestaande maatregelen om indicaties van fraude te onderzoeken. In toekomstige ontwerpen van DigiD worden ten behoeve van fraudeonderzoek en detectie separate mogelijk afgeschermde voorzieningen getroffen, waarbij op basis van polymorfe pseudoniemen niet zonder meer te herleiden gegevens uit systeem- en transactielogs worden verzameld. Het verdient aanbeveling om bij deze toekomstige ontwerpen ook de mogelijkheden voor de hier bedoelde maatregelen van interne controle gericht op de kwaliteit van de persoonsgegevens mee te ontwerpen.
IV.2	Kunnen de verwerkte persoonsgegevens gecorrigeerd, aangepast of verwijderd worden en zo ja, door wie kan dat worden gedaan?	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. 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** **Privacyprincipe:** **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?	Gegevens uit de BRP en het CRB worden opgehaald door Logius op basis van het BSN ter verificatie van het WID. De verwerking van de gegevens wordt uitgevoerd door een leverancier, die voor het leveren van diensten voor DigiD Substantieel gebruik maakt van een onderaannemer. De dienstaanbieder ontvangt van Logius het BSN en het authenticatieniveau dat gebruikt is voor het inloggen. De verantwoordelijkheid voor DigiD is duidelijk geregeld. Het ministerie van BZK is verantwoordelijke en de uitvoering is belegd bij Logius, een onderdeel van het ministerie van BZK. Mits sprake is van een gerechtelijk bevel kunnen persoonsgegevens ter beschikking worden gesteld aan opsporingsdiensten voor strafrechtelijk onderzoek. Dit is via de bestaande wet- en regelgeving gereguleerd. De infrastructuren en betrokken bestanden zijn beschreven in de PSA van DigiD Substantieel. Uit interviews is gebleken dat er op componentniveau sprake is van diverse logfiles. Als voorbeeld noemen wij het Intrusion Detection Systeem van Logius. Strikt genomen is dit geen specifiek onderdeel van het ontwerp van DigiD Substantieel, maar van

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		DigiD in brede zin. Deze deelcomponent genereert ook data over het gebruik van DigiD door gebruikers. Over de ketenverantwoordelijkheid RDW <> Logius <> RvIG in relatie tot DigiD Substantieel bestaan de volgende afspraken. Logius is verantwoordelijk voor de ad hoc gegevensuitvraag en voor het daartoe bedoelde bericht. Dit bericht wordt aangeleverd aan Diginetwerk. Dit wordt beheerd door een separate afdeling. RvIG en RDW zijn verantwoordelijk voor de voorzieningen aan hun zijde en de aanlevering van de juiste berichten ook weer via Diginetwerk. Logius, RDW en RvIG zijn dus operationeel elk verantwoordelijk voor haar eigen 'end point'. De verbinding geregeld via Diginetwerk is encrypted (SSL/TLS). Diginetwerk kent eigen logging en genereert metadata maar deze zijn niet te herleiden naar gebruikersniveau en zijn alleen in te zien door de beheerder van Diginetwerk. **Conclusie en aanbevelingen** Uit de huidige ontwerpdocumentatie blijkt niet duidelijk welke interne beheersingsmaatregelen zijn getroffen om de daadwerkelijke toegang tot persoonsgegevens gerelateerd aan DigiD Substantieel te waarborgen. 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. Hierbij hoort dan ook een werkprogramma hoe intern de effectieve werking van deze maatregelen wordt getoetst.
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 maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht?	Ja, zie V.1 **Conclusie en aanbevelingen** Aanbevolen wordt om ook vanuit de eigen verantwoordelijkheid periodiek controles uit te voeren op de gegevens(verwerkingen) die bij derden zijn ondergebracht.
V.3	Is het duidelijk wie na afloop van het project verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen?	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?	Binnen de organisatie hebben beheerders, de tweedelijns helpdesk en het fraudeteam toegang tot de persoonsgegevens. 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. Echter, indien door onbevoegden toegang wordt verkregen is de impact hoog. In de beheermodule staan de persoonsgegevens van de gebruiker en de transactielog die is ontstaan door het inloggen bij een dienstaanbieder. DigiD verstrekt in het kader van de authenticatie het BSN aan de dienstaanbieder waar de gebruiker op dat moment inlogt en het authenticatieniveau. Dit is in lijn met het doel van de verzameling van de gegevens.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		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** Het is nooit geheel uit te sluiten dat onbevoegden toegang krijgen tot persoonsgegevens of dat een bevoegd persoon verkeerde handelingen uitvoert waardoor gegevens in onbevoegde handen vallen. Op basis van de nu ter beschikking gestelde ontwerpdocumentatie wordt aanbevolen om bij het verdere ontwerp en de implementatie de mogelijkheden van een bredere inzet van encryptie, pseudonimisering, compartimentering van systemen en gegevensverzamelingen te overwegen en ook monitoring en rapportage over toegang en gebruik van systemen aan te scherpen. Bedoeld wordt in dit geval het gebruik en toegang door eigen medewerkers en/of medewerkers van leveranciers.
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?	Aan dienstaanbieders die aangesloten zijn op DigiD, verstrekt Logius het BSN en het authenticatieniveau. Het BSN wordt verstrekt aan de dienstaanbieder om de identiteit van de gebruiker vast kan stellen. Het gekozen authenticatieniveau wordt verstrekt zodat de dienstaanbieder een beeld heeft van de mate van zekerheid betreffende 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 deze verklaring is nog niet opgenomen dat gegevens van het WID uit de BRP en het CRB worden opgehaald en dat persoonsgegevens worden verwerkt in de RDA-server. Echter is dit voor de huidige DigiD ook nog niet het geval. 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. **Conclusie en aanbevelingen** Voor de ingebruikname van DigiD Substantieel dient de privacyverklaring van de bestaande DigiD te worden aangepast op de verwerkingen gerelateerd aan DigiD Substantieel.
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)?	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 dienstaanbieders. Door de RDW en de RvIG worden echter geen persoonsgegevens ontvangen van Logius waarover deze partijen nog niet beschikken. Met dienstaanbieders 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?	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 Substantieel. Naar verwachting worden deze gegevens ook opgenomen in de privacyverklaring voor de in productie name van DigiD Substantieel. **Conclusie en aanbevelingen** Een verduidelijking van alle loggegevens die gegenereerd worden door de betrokken technische componenten

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		van DigiD en vooral een integraal overzicht van de verwerkingen van persoonsgegevens van alle DigiD varianten is wenselijk. Verwerk deze inzichten in de nog aan te passen privacyverklaring voor DigiD Substantieel.
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)?	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: 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).
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?	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 Substantieel. 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** **Privacyprincipe:** **Beveiliging van gegevens** **(Privacy by Design)** **(Privacy Enhancing Technologies)**	
	<u>Beveiliging</u>	
VI.1	Is het beleid met betrekking tot gegevensbeveiliging binnen	Een informatiebeveiligingsbeleid is beschreven en geformaliseerd (Logius, 2016). Het afdelingshoofd

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
	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?	Toegangsdiensten is eindverantwoordelijk voor 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.
VI.2	Indien (een deel van) de verwerking bij een verwerker plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging, en het toezicht daarop, bij die verwerker?	Logius draagt naast de verantwoordelijkheid over gegevensverwerkingen die intern plaatsvinden ook verantwoordelijkheid voor de beveiliging van de gegevensverwerkingen die bij verwerkers zijn ondergebracht. Met derden dienen tevens afspraken gemaakt te worden teneinde de beveiliging bij deze partijen te waarborgen. Het rapport dat de kwetsbaarheden op de RDA-server code heeft geïdentificeerd is door Logius geanalyseerd. Uit de bevindingen zijn geen issues naar voren gekomen. De subleverancier van de RDA-server en software, heeft hardening uitgevoerd waarmee kwetsbaarheden zijn gereduceerd. Inzicht in code wordt alleen ter plekke bij deze partij zelf gegeven. De RDA-server staat in een virtual private cloud bij Logius met een eigen beveiligde omgeving. Op de verwerkingen bij derde partijen in relatie tot de realisatie van DigiD Substantieel en specifiek de verwerkingen met betrekking tot de RDA-server is het toezicht nog onvoldoende geformaliseerd. Logius is voornemens om de RDA-server geheel in eigen beheer te nemen. Dit is echter een plan voor de langere termijn. **Conclusie en aanbevelingen** Vastgesteld is dat geen subverwerkersovereenkomst is opgesteld met de subleverancier. Aangezien deze partij in verband met de werking van DigiD Substantieel wel persoonsgegevens verwerkt, dient dit nog gerealiseerd te worden. Dit is door Logius onderkend en de actie om de subverwerkersovereenkomst te realiseren is onderhanden. Aanbevolen wordt om ook vanuit de eigen verantwoordelijkheid periodiek controles uit te voeren op de gegevens(verwerkingen) die bij derden zijn ondergebracht.
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.	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. Daarnaast zijn beveiligingsmaatregelen in de beveiligingsvoorschriften (Logius, 2016) opgenomen.

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
	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)?	In de applicatie- en infrastructuurarchitectuur 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. Gezien de vertrouwelijkheid van het BSN is ervoor gekozen om het BSN te vervangen door een sessie-ID bij de gegevensuitwisseling met de RDA-server. In het ontwerp is echter nog niet gekozen voor het gebruik van (polymorfe) pseudoniemen waardoor Logius en dienstaanbieders wel beschikking hebben over BSN's van gebruikers. De ontwerpdocumentatie van DigiD Hoog maakt wel gebruik van polymorfe pseudoniemen en naar verwachting gaat dit ook doorgevoerd worden voor DigiD Substantieel. Daarnaast worden door het gebruik van DigiD sessiegegevens gelogd, waaronder het IP-adres, de tijd van inloggen en de dienst waar de gebruiker heeft ingelogd. Deze IP-adressen worden niet gehasht opgeslagen. De loggegevens zijn te koppelen aan de accountgegevens. Transactiegegevens zijn in te zien door een beperkt aantal personen. Dit laat onverlet dat er sprake is van een cumulatie van inloghistorie met gevoelige data. Additionele controles worden ontwikkeld met betrekking tot DigiD Substantieel. **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. Ook de mogelijkheden van het pseudonimiseren van opgeslagen gegevens verdient nader onderzoek om de privacyrisico's te beperken. De AVG geeft een aantal aanwijzingen over het gebruik van identificerende persoonsgegevens aangaande encryptie en pseudonimisering. 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

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		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: AP) en/of gebruikers indien ongunstige gevolgen voor de 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	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

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
	aan enige wettelijke/sectorale eisen met betrekking tot bewaring?	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. De beleidsmatige en technische gronden op basis waarvan deze bewaartermijn wordt gerealiseerd en wat de consequenties daarvan zijn, zijn echter onvoldoende belicht in de wetgeving; ▪ Een nadeel van het vastleggen van deze transactiegegevens is dat hoe langer ze bewaard worden, hoe meer informatie verzameld wordt over het gedrag van de gebruikers, wat gebruikt kan worden voor profileren. 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 bij burgerrechtenorganisaties. Vanuit die hoek zouden dus bezwaren kunnen komen op de bewaartermijn van vijf jaar. **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.
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** Ga bij de verdere ontwikkeling en implementatie van DigiD Substantieel na in welke mate de nu gehanteerde wettelijke bewaartermijnen ook daadwerkelijk voor alle betrokken gegevens gelden inclusief de technische logbestanden. Tref aanvullende maatregelen om de risico's van de steeds groter wordende set aan historische data te beperken. Bijvoorbeeld door compartimentering, pseudonimisering en encryptie. Betrek bij de afwegingen inzake bewaartermijnen het feit dat de inloghistorie, zij het gedistribueerd, ook bij de

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		dienstaanbieders 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** **Privacyprincipe:** **Transparantie**	
VII.1	Is het doel van het verwerken van de gegevens bij de Gebruikers en/of publiekelijk bekend of kan het bekend worden gemaakt? Wat is de procedure om Gebruikers, indien nodig, te informeren over het doel van de verwerking van hun persoonsgegevens? Zouden de Gebruikers kunnen worden verrast door de verwerking op het moment dat zij daarover worden geïnformeerd?	Op de website van DigiD is een privacyverklaring te vinden. Daarin staat opgesomd welke gegevens van gebruikers van DigiD worden verwerkt, met welke doelen dat wordt gedaan, hoe lang de gegevens worden bewaard en aan welke derde partijen deze worden verstrekt (DigiD, 2016). Gebruikers worden bij de aanvraag of het gebruik van DigiD niet expliciet gewezen op de privacyverklaring. De gebruiker wordt dus niet op de hoogte gesteld van het doel van de verwerking van zijn persoonsgegevens vóór het moment van verwerking. Voordat een gebruiker zijn WID gaat scannen om DigiD Substantieel te behalen wordt hij ook niet op de hoogte gesteld dat controle plaatsvindt met de gegevens uit de BRP of het CRB, welke gegevens worden verwerkt en wat het doel van deze verwerking is. In de privacyverklaring ontbreekt tevens de bewaartermijn van vijf jaar en is niet opgenomen hoe gebruikers het gebruik van DigiD Substantieel kunnen beëindigen en het account kunnen laten opheffen met in acht name van de gehanteerde bewaartermijnen van historische gegevens. **Conclusie en aanbevelingen** De huidige privacyverklaring DigiD vereist nog actualisering op de voorgenomen bewaartermijnen. In het kader van transparantie verdient het ook aanbeveling om een communicatieplan op te stellen omtrent de verdere introductie van DigiD Substantieel en wat er precies met de gegevens van gebruikers gebeurt per verwerkingsstap. Dit verzoek is reeds door Logius in behandeling genomen en wordt doorgevoerd voor de in productie name van DigiD Substantieel.
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. De privacyverklaring is te vinden op de website van DigiD, maar de gebruikers worden daar niet op gewezen bij het aanvragen of gebruiken van DigiD. De gebruiker wordt dus niet op de hoogte gesteld van het doel van de verwerking van zijn persoonsgegevens vóór het moment van verwerking. Er is initiatief nodig van de gebruiker om achter de identiteit van Logius te komen. Voor het scannen van een WID met de DigiD app wordt de gebruiker geïnformeerd dat het identiteitsbewijs

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		wordt gecontroleerd op basis van onder meer het documentnummer en de geldigheidsdatum. De gebruiker wordt er echter niet van op de hoogte gesteld dat deze controle plaatsvindt met de gegevens uit de BRP of het CRB en met welk doel dat wordt gedaan. **Conclusie en aanbevelingen** Aanbevolen wordt een verwijzing toe te voegen naar de privacyverklaring bij in elk geval het aanvragen van een nieuwe DigiD, eventueel ook bij het inloggen met DigiD. Een nadere toelichting op de wijze waarop controles worden uitgevoerd op een WID en de controles bij derde partijen is eveneens een belangrijke aanbeveling om misverstanden en wantrouwen te voorkomen. Dit verzoek is reeds door Logius in behandeling genomen en wordt doorgevoerd voor de in productie name van DigiD Substantieel.
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?	Voor het scannen van een WID met de DigiD app wordt de gebruiker geïnformeerd dat het identiteitsbewijs wordt gecontroleerd op basis van onder meer het documentnummer en de geldigheidsdatum. De gebruiker wordt er echter niet van op de hoogte gesteld dat deze controle plaatsvindt met de gegevens uit de BRP of het CRB en met welk doel dat wordt gedaan. **Conclusie en aanbevelingen** In aanvulling op de aanbevelingen bij vraag VII.2 wordt aanbevolen een melding aan de gebruiker te presenteren bij het scannen van een WID dat persoonsgegevens worden opgevraagd bij de BRP/het CRB en met welk doel dit wordt gedaan.
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 BSN en het authenticatieniveau aan de dienstaanbieder waar de gebruiker op dat moment wenst in te loggen. Verder worden geen gegevens aan derden verstrekt zonder voorafgaande ondubbelzinnige toestemming van de gebruiker, met uitzondering van wettelijke verplichtingen om gegevens te verstrekken. Dit wordt middels de privacyverklaring van DigiD gemeld aan gebruikers (DigiD, 2016).
VIII	**Rechten van betrokkenen** **Privacyprincipe:** **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?	Indien de gebruiker ervoor kiest een DigiD aan te vragen om deze te gebruiken als authenticatiemiddel worden persoonsgegevens verwerkt. De gebruiker vult zelf gegevens in zoals het BSN en het e-mailadres waarna overige gegevens worden verzameld. 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

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		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. **Conclusie en aanbevelingen** Het verdient aanbeveling de privacyverklaring te actualiseren met de gegevensverwerking van DigiD Substantieel. Logius heeft aangegeven dat dit is opgepakt en wordt gerealiseerd voor in productiename van DigiD Substantieel.
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 een verzoek doen bij de tweedelijns helpdesk het DigiD-account op te heffen. Indien een dergelijk verzoek wordt gedaan wordt het account geblokkeerd. In de transactielog blijven de gegevens wel beschikbaar conform de bewaartermijn. Ook kan de gebruiker zijn BSN op een afmeldlijst laten plaatsen zodat geen DigiD aangemaakt kan worden met het betreffende BSN. Dit kan bijvoorbeeld gebruikt worden ter voorkoming van fraude. **Conclusie** Geef duidelijk aan in de privacyverklaring hoe gebruikers het gebruik van hun DigiD Substantieel kunnen beëindigen en hun account kunnen laten opheffen met in acht name van de gehanteerde bewaartermijnen van historische gegevens.
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?	De gebruiker van DigiD kan zijn gebruikersnaam, telefoonnummer, BSN, e-mailadres en gebruiksgeschiedenis inzien door in te loggen op mijn.digid.nl. Het telefoonnummer en e-mailadres kunnen hier door de gebruiker zelf worden gewijzigd. De gebruiker kan tevens een inzageverzoek indienen bij Logius en een verzoek indienen voor het verbeteren, aanvullen, verwijderen of afschermen van gegevens, tenzij dit niet is toegestaan op grond van een wettelijke bepaling, door een e-mail te sturen aan info@digid.nl of een brief te sturen. Bij een verzoek tot inzage, verbetering, aanvulling of verwijdering zal de gebruiker gevraagd worden zich te identificeren door het verstrekken van het BSN en het beantwoorden van een aantal persoonlijke vragen. Bij kritieke activiteiten in de beheermodule, zoals het verwijderen van een account, is het vier-ogenprincipe toegepast. De gebruiker kan een verzoek doen bij de tweedelijns helpdesk het DigiD-account op te heffen. Indien een dergelijk verzoek wordt gedaan wordt het account, inclusief alle gegevens in de beheermodule verwijderd. In de transactielog blijven de gegevens wel beschikbaar conform de nu gestelde bewaartermijnen. Ook kan de gebruiker zijn BSN op een afmeldlijst laten plaatsen zodat geen DigiD aangemaakt kan worden met het

Nr.	Vraag	Bevindingen / Risico's / Aanbevelingen
		betreffende BSN. Dit kan bijvoorbeeld gebruikt worden ter voorkoming van fraude. Daarnaast kan de gebruiker het DigiD-account laten blokkeren bij de tweedelijns helpdesk. In dit geval wordt een brief verstuurd naar het geregistreerde adres van de gebruiker met de mededeling dat schriftelijk bevestigd dient te worden dat het account geblokkeerd moet blijven. Indien de schriftelijke bevestiging niet wordt ontvangen, wordt het account na twee weken automatisch weer geactiveerd.
VIII.5	Is er een geschillenregeling of een partij waar de betrokkenen terecht kunnen bij vragen of klachten?	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.

Bijlage II: Universele privacyprincipes

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 Substantieel. De aanpak van Mazars gaat uit van onderstaande beschreven universele privacyprincipes door de OECD/OESO[16].

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 implementatie. Onnodige verzameling en verdere verwerking van persoonsgegevens wordt

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

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 III: Algemene privacyrisico'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 en zijn niet specifiek voor DigiD Substantieel.

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, in geval 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. Hiermee kunnen 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 dienstaanbieders 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 (verantwoordelijken 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 verantwoordelijke 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 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 IV: Afkortingen en begrippen

Afkorting	Begrip	Betekenis / toelichting
AA	Active Authentication	Controleert of het een originele NFC-chip betreft en dat deze niet gekloond is.
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.
APDU	Application Protocol Data Unit	Communicatie tussen de NFC-chip op het WID-document en de NFC-reader.
BAC	Basic Access Control	Sleutel waarmee NFC-chip geopend kan worden (m.b.v. MRZ) in geval van identiteitskaart of paspoort (BRP). Geldt als een authenticatie richting de chip. Met de BAC-sleutel kan de RDA-server bewijzen kennis te hebben van de WID-gegevens.
BAP	Basic Access Protection	Sleutel waarmee NFC-chip geopend kan worden (m.b.v. MRZ) in geval van rijbewijs (CRB). Geldt als een authenticatie richting de chip. Met de BAP kan de RDA-server bewijzen kennis te hebben van de WID-gegevens.
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.
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.
CIS	Card Interface Service	De middelen waar DigiD app geactiveerd is worden gekoppeld middels een CIS aan de DigiD Kern. De CIS geeft informatie van de RDA-server naar DigiD Kern en visa versa.
CRB	Centraal register Rijbewijzen en Bromfietscertificaten	CRB wordt beheerd door de RDW. Voor de controle van het rijbewijs wordt een bevraging naar het CRB gedaan.
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 overheidsorganisaties onderling gegevens uitwisselen.
DigiD	Digitale Identiteit	Met DigiD kan worden ingelogd op websites van dienstaanbieders in het BSN-domein.
eIDAS	Electronic Identity and	De eIDAS-verordening gaat over

Afkorting	Begrip	Betekenis / toelichting
	Signature	elektronische identificatie en heeft de betrouwbaarheidsniveaus Laag, Substantieel en Hoog bepaald.
ICV	In control verklaring(en)	Jaarlijks intern self-assessment van controles, waaronder in relatie tot informatiebeveiliging, die aan het management van Logius en het ministerie van BZK wordt gerapporteerd.
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).
NFC	Near Field Communication	Een draadloze manier om kleine hoeveelheden informatie uit te wisselen binnen een straal van 10 centimeter. De chip communiceert met een ander NFC-apparaat. Met de NFC-reader wordt de chip op het WID gecontroleerd middels de RDA-controle (controle met RDA-server).
PA	Passive Authentication	Controleert of de gegevens op de chip van het WID zijn gewijzigd.
RDA	Remote Document Authentication	Techniek waarmee een gebruiker, na een geslaagde inlog met zijn DigiD gebruikersnaam en wachtwoord, m.b.v. een Nederlands identiteitsdocument, in combinatie met een kaartlezer toegang krijgt tot digitale diensten. De kaartlezer communiceert hiertoe met de contactloze chip in het reisdocument en stelt via cryptografische processen vast dat de chip authentiek en onveranderd is en toebehoort aan de persoon die inlogt.
RDW	Dienst Wegverkeer	RDW is de middelenuitgever van rijbewijzen. De RDW beheert het CRB.
RvIG	Rijksdienst voor Identiteitsgegevens	RvIG is de middelenuitgever 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.
SIEM	Security Information and Event Management	Software die real-time de beveiliging analyseert (in casu op infrastructuurniveau).
SOD	Document Security Object	Onderdeel van de chip dat door de staat van afgifte digitaal ondertekend wordt. Het SOD bevat de representatie van de LDS-inhoud (Logical Data Structure) in hash-code.
TLS	Transport Layer Security	Encryptieprotocol die de communicatie beveiligt.
WID	Wettelijk Identiteitsdocument	Nederlands paspoort, Nederlandse ID-kaart en Nederlands Rijbewijs.