Betaalvereniging Nederland

Ministerie Binnenlandse Zaken en Koninkrijksrelaties
t.a.v. de minister de heer dr. R.H.A. Plasterk
Postbus 20011
2500 EA Den Haag

Gustav Mahlerplein 33-35
1082 MS Amsterdam
Postbus 83073
1080 AB Amsterdam

www.betaalvereniging.nl

T 020 305 19 00
F 020 305 19 12

Datum
31 maart 2017

Telefoon
020 305 19 20

Kenmerk
PM/AK/ 2017-33

E-mail
p.m.mallekoote@betaalvereniging.nl

Betreft
Consultatie reactie Wet Generieke Digitale Infrastructuur en Uniforme Set van Eisen 1.0

Geachte heer Plasterk,

Graag maakt Betaalvereniging Nederland gebruik van de mogelijkheid om te reageren op het conceptvoorstel voor de Wet Generieke Digitale Infrastructuur (Wet GDI) en de Uniforme Set van Eisen 1.0 (USvE). Wij doen dit mede namens een aantal van onze leden: ABNAMRO, ING, Rabobank, de Volksbank (SNS, ASN Bank en Regiobank) en Triodos Bank. Genoemde banken hebben te samen en onder regie van de Betaalvereniging de identificatiedienst iDIN ontwikkeld en deze eind vorig jaar op de markt geïntroduceerd. Met deze online identificatiedienst kunnen natuurlijke personen zich eenvoudig bij organisaties kenbaar maken door de toegangsmiddelen van hun eigen bank te gebruiken.

De Betaalvereniging en de banken onderschrijven van harte de multimiddelenaanpak en de uitgangspunten van de wet GDI en de USvE. Tegelijkertijd merken wij op dat ons inziens de huidige conceptwetgeving en de USvE doorschieten in het voorschrijven van de gedetailleerde wijze waarop de uitgangspunten geïmplementeerd moeten worden. Ons inziens belemmert dit innovatie, die juist op dit gebied nodig is. Ook maken wij ons zorgen over een werkbare governance, een efficiënte inrichting van (onafhankelijk) toezicht en de hoge publieke uitgaven die de uitvoering van de wet en de USvE met zich mee zullen brengen.

Wij hebben vanuit onze kennis en ervaring het wetsvoorstel en de USvE beoordeeld en zijn u erkentelijk voor de geboden mogelijkheid hiertoe. Onze reactie treft u bijgaand aan.

KvK 54048370

Wij zijn zeer bereid tot nader overleg en samenwerking en zijn gemotiveerd om gezamenlijk van de digitale overheid op korte termijn een succes te maken.

Met vriendelijke groeten,

Piet Mallekoote
Algemeen Directeur

Betaalvereniging Nederland

Consultatiereactie banken en Betaalvereniging op de wet GDI en Uniforme Set van Eisen versie 1.0

Consultatiereactie concept wet GDI en USvE van 21 december 2016

30 maart 2017 | Versie 1.0 | Definitief

Auteurs

ABN AMRO
ASN Bank
ING
Rabobank
Regiobank
SNS Bank
Triodos Bank
Betaalvereniging Nederland

Betaalvereniging Nederland

Inhoudsopgave

1. Inleiding

De minister van Binnenlandse Zaken en Koninkrijksrelaties heeft op 21 december 2016 de consultatieversie van het wetsvoorstel voor de Generieke Digitale Infrastructuur (GDI) gepubliceerd. Dit wetsvoorstel geeft invulling aan het voornemen van het kabinet te komen tot een digitaal werkende (semi)overheid. Om digitale dienstverlening in het publieke domein te intensiveren, is een veilige en betrouwbare toegang daartoe door burgers en bedrijven nodig (authenticatie). Dit zal geschieden via erkende publiek en privaat uitgegeven middelen. Onderdeel van de GDI is de Uniforme Set van Eisen (USvE). De USvE beschrijft de aansluitvoorwaarden waaraan partijen moeten voldoen om mee te doen aan authenticatie in het publieke domein (BSN domein). Ook deze zijn gepubliceerd op 21 december jl.

Dit document beschrijft de reactie van zowel Betaalvereniging Nederland, als eigenaar van het product en merk iDIN, als de onder licentie opererende aanbieders van iDIN aan consumenten, bedrijven en organisaties. Deze aanbieders zijn op dit moment: ABN AMRO, ASN Bank, ING, Rabobank, Regiobank, SNS Bank en Triodos Bank (ook wel: de banken).

1.1 Leeswijzer

Dit document is als volgt opgebouwd: Hoofdstuk 2 bevat de samenvatting van ons commentaar. Hoofdstuk 3 geeft de kernpunten van de feedback van de banken en Betaalvereniging op de consultatieversie van de concept wet GDI en USvE versie 1.0 van 21 december 2016. Hoofdstuk 4 geeft een verdieping van de feedback met een uitgebreide toelichting. Hoofdstuk 5 geeft een artikelsgewijze feedback op de in de consultatieversie van de concept wet GDI. Tot slot zijn er twee bijlagen, één die ingaat op de verschillende gewenste koppelvlakken en de functies die daar mee gemoeid zijn. De andere bijlage geeft in een groter detail de resultaten weer van de proof of concept van iDIN met Logius en Polymorfe Encryptie en Pseudonimisering.

2. Samenvatting

De Betaalvereniging en de banken onderschrijven de doelen en uitgangspunten die de wetgever beschrijft in de concept Wet generieke digitale infrastructuur en USvE versie 1.0. Echter, samenvattend kan worden gesteld dat de huidige uitwerking te zwaar en te ingrijpend is voor licentie- en certificaathouders om iDIN te kunnen blijven aanbieden aan de overheid.

- De eisen zijn te verplichtend in de wijze waarop een oplossing gerealiseerd dient te worden;
- Er ontstaan te veel technische afhankelijkheden en te veel risico's op het gebied van privacy en haalbaarheid voor alle partijen;
- Er is te veel overlap met bestaande wet- en regelgeving;
- Een rationeel business model met beheersbare kosten voor aanbieders en Dienstverleners en een Europees level playing field worden niet gerealiseerd;
- De doorlooptijd voor invoering van deze uitwerking zal lang zijn waardoor de voortgang voor Gebruikers en Dienstverleners geremd wordt.

Wij zien echter voldoende mogelijkheden om de uitwerking zodanig aan te passen dat deze vraagstukken opgelost kunnen worden. Dit kan onder meer door princple-based eisen te formuleren in plaats van rule based eisen, het drie-lagen model als uitgangspunt te nemen, en door sectoraal toezicht, kunnen alle doelen van de overheid bereikt worden. Daarbij zullen de functionele en technische eisen teruggebracht kunnen worden tot implementeerbare delen, waarbij onderlinge afhankelijkheden en complexiteit geminimaliseerd worden.

We vertrouwen erop dat we deze beweging met elkaar kunnen maken om de kennis, ervaring en innovatiekracht van de Nederlandse markt op die manier ook in dienst te stellen van de ambities van de overheid.

3. Belangrijkste bevindingen

3.1 Algemeen

Belangrijk is om te constateren dat de banken en Betaalvereniging Nederland de doelen en basisuitgangspunten zoals onder meer verwoord in de voorgenomen wet en die ook zijn beschreven in de USvE (pagina 8) en eerder al door de minister zijn aangegeven onderschrijven. Hieronder vallen de uitgangspunten van betrouwbaarheid, privacy-vriendelijkheid en gebruikersvriendelijkheid, maar ook de multimiddelen strategie, level playing field, ruimte voor meerdere technologische oplossingen en het voorkomen van redundante eisen (die elders al zijn vastgelegd in wet- en regelgeving).

Tegelijkertijd constateren we dat de uitwerking van de concept wet GDI en met name van de USvE, dat op veel aspecten niet voldaan wordt aan deze doelen en uitgangspunten. Zo is bijvoorbeeld het verplichte inzageregister een privacy hotspot en zijn de eisen en compliance voor financiële instellingen inzake het identificeren van klanten al in bestaande wetgeving (Wwft) geregeld. Belangrijk is dus om de uitwerking in overeenstemming te brengen met de uitgangspunten en doelen.

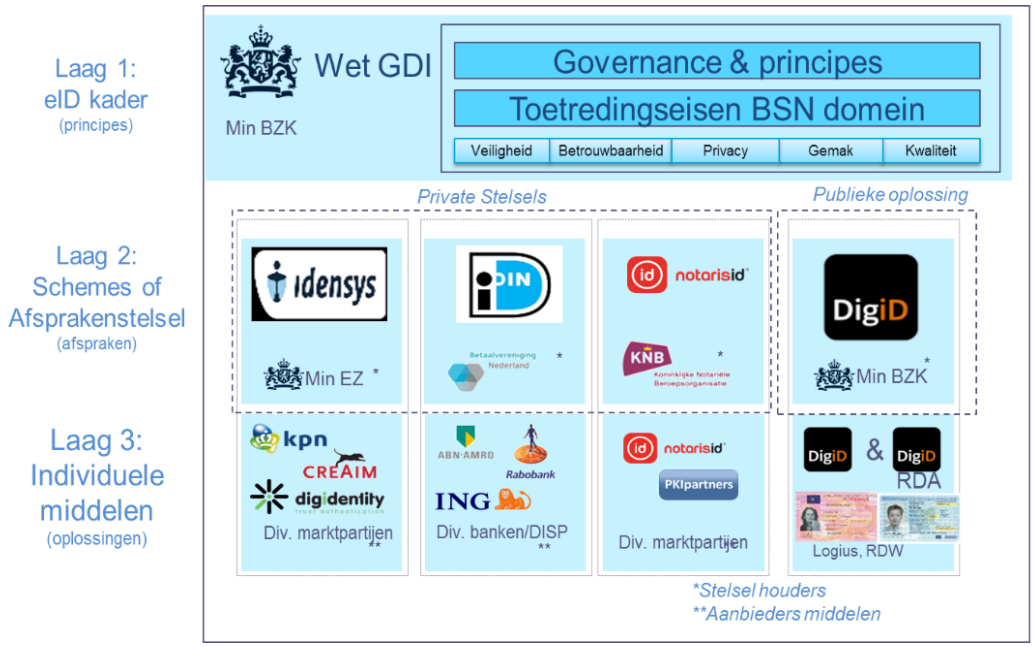
Aanbeveling: Borg dat de uitwerking daadwerkelijk in overeenstemming is met de uitgangspunten.

3.2 Drie-lagen model als inrichtingsprincipe met sectoraal Toezicht

IN de voorgenomen multimiddelen aanpak zijn straks meerdere oplossingen actief die allemaal op een andere manier georganiseerd zijn, een andere governance hebben, een andere techniek hebben en waarop toelating en toezicht anders georganiseerd zijn. Dat is de huidige praktijk in de pilot, en dat werkt. Ondanks het gezamenlijk belang voor een veilig en betrouwbaar eID landschap is het niet op voorhand logisch of noodzakelijk dat alle stelselafspraken, regels, technische invulling en doorontwikkeling voor al deze partijen op detail op elkaar afgestemd moeten worden of op dezelfde manier worden toegepast. Dat zijn ze nu ook niet en een keuze voor vergaande uniformering heeft voor de bestaande oplossingen veel impact.
Een drie-lagen model (zie figuur) geeft eenduidige onderverdeling tussen rollen en verantwoordelijkheden van wetgever, afsprakenstelsels (zoals Idensys en iDIN) en deelnemers binnen die stelsels. De huidige inrichting van de USvE is gericht op individuele partijen (leveranciers) waardoor afsprakenstelsels hun verantwoordelijkheid niet kunnen invullen. Hierdoor worden certificeringsprocessen dubbel gedaan, zijn er veel meer partijen waar afspraken mee gemaakt moeten worden en is de producteigenaar/beheerorganisatie niet in staat om haar rol in bijvoorbeeld communicatie of doorontwikkeling goed in te vullen. De maatschappelijke kosten voor die dubbele certificeringslast zijn moeilijk te verantwoorden.

Ook Toezicht is voor de verschillende stelsels en oplossingen nu al anders belegd. Het Bureau Financieel Toezicht (BFT) is verantwoordelijk voor het integrale toezicht op het notariaat (er vanuit

gaande dat die ook gaan participeren), banken vallen onder toezicht van DNB (De Nederlandsche Bank) en de Europese Centrale Bank (ECB), ICT- telecompartijen staan onder toezicht van het Agentschap Telecom.



Aanbeveling: Hanteer het drie-lagen model met sectoraal Toezicht voor de verdere uitwerking van de eisen en maak gebruik van de inrichting en certificering van de bestaande afsprakenstelsels.

3.3 Rule based in plaats van principle based normering maakt niet toekomstbestendig

Samenhangend met het vorige punt (het drie lagen model) is de constatering dat de USvE voor het overgrote deel rule based is opgesteld in plaats van principle based. Oftewel de invulling van de eisen is gedetailleerd voorgeschreven in plaats van dat het beoogde doel wordt geformuleerd en de invulling aan de partijen wordt overgelaten. Omdat er in veel gevallen sprake is van een bestaande praktijk en bestaande wet- en regelgeving die wel principle based is, met toezicht daarop is de impact van rule based normering erg groot en naar onze mening onnodig en daarmee onwenselijk groot.

Bovendien geven rule based eisen maar zeer beperkt ruimte voor eigen invullingen van de eisen, feitelijk alleen op het terrein van de authenticatiestap van de Gebruiker bij zijn Authenticatiedienst is er enige ruimte. Alle andere stappen in het proces zijn deels of geheel voorgeschreven tot en met de technische invulling. Dit leidt uiteindelijk tot gebrek aan innovatie, doorontwikkeling en snelheid om verbeteringen toe te passen. Dit werkt belemmerend vanuit het oogpunt van efficiency en innovatie. In een markteconomie zoeken de spelers altijd naar de meest efficiënte oplossing en innoveren via

creatieve ideeën. In dit geval met als voorwaarden veiligheid, betrouwbaarheid en privacy. Bij de multimiddelen aanpak zou daarvoor ook ruimte moeten zijn. Door de nu geformuleerde inrichting valt de diversiteit aan oplossingen weg, waardoor de technische invulling noodzakelijkerwijs gelijk is. Dit brengt een systeemrisico met zich mee, of single point of failure. Wanneer die ene techniek niet langer betrouwbaar is, heeft dat nadelige gevolgen voor al het inloggen in het BSN domein. Door deze risico's is het model niet toekomstbestendig.

Met het opleggen van rule based eisen vanuit de overheid wordt geen gebruik gemaakt van de uitgebreide expertise / kennis en ervaring van private partijen en wordt de overheid bovendien verantwoordelijk, en daarmee aansprakelijk, voor de invulling van de eisen. Het actualiseren van de rule based eisen is immers de verantwoordelijkheid van de overheid, deze te laat aanpassen kan nadelige gevolgen hebben voor alle erkende eID-middelen en alle partijen die hier gebruik van maken. Bij principle based eisen zijn de marktpartijen verantwoordelijk voor de eigen invulling, waardoor dit probleem veel kleiner is.

Principle based eisen zijn nationaal en internationaal een algemene werkwijze die in allerlei sectoren gebruikt wordt, waaronder in het betalingsverkeer, en waar overheden, toezichthouders en bedrijven veel ervaring mee hebben. Door van principle based eisen uit te gaan wordt het gebruik van een schat aan kennis, mogelijkheden en innovatie mogelijk gemaakt in plaats van gehinderd.

Aanbeveling: beschrijf de eisen principle based, waarbij partijen nadrukkelijk vrij gelaten worden in hoe ze invulling geven aan de eisen.

3.4 Nederlandse eisen vs. eIDAS eisen

eIDAS heeft o.a. als doel een Europese interne (gelijke) markt voor elektronische identificatie te creëren. De USvE met al haar extra rule-based eisen is strijdig met dit doel. Als je de eisen vanuit Europa zoals verwoord in de eIDAS Uitvoeringsverordening 2015/1502 vergelijkt met de USvE dan staan Nederlandse additionele eisen niet in verhouding tot de eisen in verschillende lidstaten binnen de EU. De Nederlandse USvE gaat veel verder dan een invulling van de noodzakelijke puntjes op de i binnen een nationale context en betekent een aanzienlijke verzwaring ten opzichte van de oorspronkelijke Europese verordening. Hierdoor ontstaat er een onbalans in Europa waarin:

- eIDAS genotificeerde middelen uit andere lidstaten die aan veel minder zware eisen hoeven te voldoen verplicht ondersteund moeten worden binnen de Nederlandse publieke sector.
- Er een onbalans ontstaat voor de betrouwbaarheidsniveaus tussen verschillende landen. "Substantieel" in het ene land betekent heel wat anders dan "Substantieel" in een ander land.
- Nederlandse (private) oplossingen die gekozen hebben om te voldoen aan de invulling van de USvE deze kostbare en zware oplossingen niet competitief kunnen aanbieden buiten Nederland.

Hierdoor verhindert de Nederlandse overheid de vorming van een level playing field in Europa en worden Nederlandse private partijen binnen Europa op achterstand gezet.

Aanbeveling: zoek aansluiting bij de uitvoeringsverordening eIDAS, in detaillering en zwaarte van het proces om een ongelijk speelveld binnen Europa te voorkomen.

3.5 Financiering en verplichtende werking

Een verplichte acceptatie van erkende middelen is per definitie marktverstorend. Omdat hier ook middelen of oplossingen geaccepteerd moeten worden met bijvoorbeeld een heel klein bereik, of die niet gebruiksvriendelijk zijn, is het de vraag of de afnemer hierop zit te wachten.

Wanneer de verplichte acceptatie vervolgens ook gebeurt in samenhang met een door de minister opgelegde prijs werkt dit bijzonder marktverstorend. Niet alleen kan een oplossing binnen het BSN domein dan niet op basis van marktwerking worden aangeboden, ook buiten het BSN domein heeft dit verregaande gevolgen. De private sector zal zeker kijken naar de door de minister vastgestelde prijs en voorwaarden, waardoor private aanbieders niet meer op eigen merites hun oplossing in de private markt kunnen aanbieden.

Ook op het gebied van (juridische) voorwaarden is het kunnen ingrijpen van de minister een te zwaar middel.

In het huidige voorstellen wordt aangegeven dat de kosten voor de centrale voorzieningen doorbelast worden aan de Authenticatiediensten of Toegangsdiensten. Daarmee worden de private partijen geconfronteerd met de hoge kosten van inefficiënte centrale systemen. Private partijen moeten vervolgens deze hoge kosten doorbelasten aan hun klanten, die de private partijen zullen aanspreken op de kosten en functionaliteit. Dit zal de acceptatie van de diensten niet ten goede komen. Dit vertroebelt de dienstverlening en bemoeilijkt het ontwikkelen van een normale business case.

Wij realiseren ons dat de eIDAS verordening een verplichte acceptatie van genotificeerde middelen vereist en dat dit logischerwijs ook zou moeten gelden voor door Nederland genotificeerde middelen binnen Nederland. We stellen echter wel voor deze stappen van elkaar te scheiden, waardoor *erkenning* niet automatisch leidt tot *notificeren* en daarmee ook niet tot verplichte acceptatie.

Aanbeveling: maak de acceptatie van erkende middelen/oplossingen niet verplicht. Schrap de doorbelasting van kosten van centrale voorzieningen en het kunnen opleggen van prijzen en voorwaarden door de minister.

3.6 Techniek - algemeen

Het uitgangspunt van eIDAS is dat dit technologieneutraal is. Dit om meerdere invullingen te ondersteunen die leiden tot een zelfde betrouwbaarheidsniveau. De nu voorliggende uitwerking is dat bepaald niet. Er wordt juist erg veel techniek voorgeschreven. Doordat in de voorgeschreven techniek geen rekening is gehouden met de mogelijkheden van iDIN is de impact voor alle participanten, ook voor de overheids-dienstverleners, onnodig complex. Bovendien wordt hiermee de facto één (technisch) stelsel gecreëerd (anders dan in de MvT, pag. 16 wordt gesuggereerd), met erg veel onderlinge afhankelijkheden, waarbij het uitgangspunt vanuit eIDAS is dit te vermijden.

Ook pleiten we voor het gebruik van open standaarden, waarbij we vaststellen dat de USvE invulling van het polymorf pseudoniem, daar in ieder geval niet aan voldoet (zie o.a. ook bijlage 2).

Aanbeveling: beschrijf de architectuur meer high level, schrijf geen technische invulling voor en houd rekening met de mogelijkheden die er al zijn binnen een bestaande oplossing.

3.7 Techniek - polymorfe encryptie en pseudonimisering

Uit de Proof of Concept op de techniek van polymorfe encryptie en pseudonimisering die we vanuit iDIN hebben uitgevoerd met Logius blijkt dat de techniek op dit moment nog niet het volwassenheidsniveau heeft om het verantwoord in te voeren. Ook wordt de veronderstelde privacy winst niet gehaald en is de invoering voor met name de Dienstverlener te complex, technische kennis die nodig is voor de voorgestelde grootschalige uitrol niet voorhanden, en is de techniek dermate specifiek dat er op dit moment nog geen open source libraries (standaard software, nodig voor software ontwikkeling), HSM's (Hardware Security Modules) of andere oplossingen voorhanden zijn.

De implementatie van polymorfe encryptie en pseudonimisering kent ook in haar sleutelbeheer nog steeds een single point of failure, een 'masterkey' waar alle stelsels van afhankelijk zijn. Dit lijkt op een 'Diginotar'-achtige afhankelijkheid met alle risico's van dien. De opzet staat erg ver af van de 'open standaarden' ambitie zoals verwoord in de uitgangspunten.

Aanbeveling: kies (nu) niet voor polymorfe encryptie en pseudonimisering, kies voor een open standaard.

3.8 Centrale voorzieningen

De twee centrale voorzieningen die verplicht worden voor participanten, het inzageregister en het misbruikregister, zijn onzes inziens niet nodig en zorgen voor extra afhankelijkheden, complexiteit en risico's.
De functie van beide registers worden al vervuld door de systemen van de banken.

- De banken houden zelf al de status van de authenticatiemiddelen bij. Het is niet erg aannemelijk dat Gebruikers via de overheid middelen gaan inzien en/of blokkeren. Het is veel logischer dat de Gebruiker direct contact opneemt met zijn/haar Authenticatiedienst.
- Ook fraudedetectie vindt plaats in de systemen van de banken. Deze systemen en processen vertegenwoordigen jaren ervaring in fraudebeperking en hierover publiceren de banken ook de resultaten. Als het gaat om het delen van fraudepatronen om opsporing te bevorderen dan zijn er al bestaande samenwerkingsverbanden tussen banken, politie en justitie die die rol vervullen.

De risico's die ontstaan bij het inrichten van de centrale systemen worden niet benoemd maar die zijn er wel. Het inzageregister zal een nieuwe rijke gegevensverzameling worden die grote privacy en veiligheidsrisico's (ook voor banken) met zich mee brengen en die aantrekkelijk is voor phishing aanvallen. Het goed inrichten van een centraal misbruikregister zal, naast dat de functie voor het authenticatie deel dat al bestaat, veel tijd vergen en het systeem zal tot die tijd onduidelijke boodschappen geven aan Gebruikers.

Aanbeveling: richt het inzageregister en het misbruikregister niet als centraal systeem in, maar laat de verantwoordelijkheid waar hij al ligt: bij de Authenticatiedienst.

3.9 Dubbel toezicht

Naast voor veel andere producten en diensten worden de betaalinfrastructuur, de Wwft en in het bijzonder de eisen ten aanzien van Anti Money Laundering (AML), als belangrijkste kader voor identificatie van klanten, en de bestaande systemen en processen ten behoeve van bijvoorbeeld risicobeheersing en informatiebeveiliging nu ook voor iDIN gebruikt. Deze componenten hebben ook al een Toezichthouder. Naast de Autoriteit Persoonsgegevens voor alle privacy gerelateerde vraagstukken is dat De Nederlandsche Bank (DNB). In het geval van de vier grote Nederlandse banken is die Toezichtstaak inmiddels voor een groot deel overgenomen door de Europese Centrale Bank (ECB), waar internationale teams de banken in kwestie beoordelen op onder meer deze dossiers. Ook de PSD2 (Payment Services Directive) en de RTS (Regulatory Technical Standards) vallen hier straks onder, wederom nieuwe regelgeving die ook eisen stellen aan de authenticatie van klanten en vallend binnen het toezicht domein van DNB.

Wanneer er naast deze bekende Toezichthouders een nieuwe Toezichthouder benoemd wordt zal er spanning ontstaan in de verschillende compliance regimes, de toelichting daarop en de ontwikkeling binnen dit veld. Dit genereert extra kosten uit hoofde van doublures in dit toezicht. Wanneer DNB niet alleen impliciet maar ook expliciet de (sectorale) Toezichthouder voor iDIN wordt, is daarmee tevens het toezicht voor het gebruik van iDIN in de private sector geborgd. Iets wat de GDI wetgeving niet zal afdekken.

Aanbeveling: richt toezicht sectoraal in en volg de bestaande toezicht relaties. Formaliseer de rol van DNB hierin.

3.10 Definities en Rollenmodel

In de concept van de wet GDI wet en van de USvE is in belangrijke mate het gedachtegoed van Idensys en eHerkenning gevolgd in het definiëren van rollen en begrippen. Doordat deze rollen en begrippen bij banken soms anders ingevuld of gehanteerd worden, ontstaat hierdoor een verwarring en extra complexiteit bij het bespreken van de impact.

In het rollenmodel is de filosofie gevolgd dat alle rollen beschreven, gedefinieerd en erkend moeten worden en dat zij het hele huidige en toekomstige bereik en mogelijke toepassingen moeten afdekken, zowel de authenticatie van systemen (machine to machine), als van burgers en bedrijven (zie bijvoorbeeld USvE, pag. 59). Dit leidt in de praktijk tot een complex geheel waarbij een bank straks in plaats van één drie rollen lijkt te hebben waar erkenning voor nodig is, die ook nog eens samenhangen met nog niet uitgewerkte rollen.

Door de wet GDI en de USvE te beperken tot alleen het noodzakelijke, het gebruik van het BSN door burgers in het overheidsdomein, zijn veel rollen niet noodzakelijk. Dit verhoogt de haalbaarheid van het geheel. De verschillende stelsels zouden ook vrij moeten zijn om binnen hun eigen stelsel hun eigen rollen te definiëren. Daarmee kan het ene stelsel zich onderscheiden van een ander en worden er geen oneigenlijke verplichtingen aan alle participanten opgelegd.

Aanbeveling: beperk de wet GDI en de USvE tot alleen het noodzakelijke: het gebruik van BSN voor authenticatie in het overheidsdomein. Laat stelsels vrij in het hanteren van het eigen rollenmodel. Erken oplossingen op stelsel-niveau in plaats van de individuele rollen en partijen daarbinnen. Vermijd afhankelijkheden tussen rollen.

3.11 Rol als verantwoordelijke voor het BSN

De Authenticatiediensten hebben voor de vastgelegde persoonsgegevens de rol van verantwoordelijke in de zin van de Wet Bescherming Persoonsgegevens. Momenteel zijn de banken bewerker voor de verwerkingen in het kader van iDIN in het BSN-stelsel. Voor de banken is dit een bijzondere rol gezien hun rol als verantwoordelijke ten opzichte van de BSN-verwerkingen buiten het iDIN-stelsel (bijv. renseignering bij de Belastingdienst). Gezien de belangen van gebruikers en banken lijkt het in de rede te liggen dat de banken een even grote verantwoordelijkheid krijgen met betrekking tot het verwerken van BSN in het kader van iDIN.
Onderdeel van die verantwoordelijkheid is ook de validatie van het BSN. Dat kan via de Basisregistratie Persoonsgegevens (BRP) of nu ook via het BSN koppelregister. Naast BSN zouden ook andere persoonsgegevens gevalideerd moeten kunnen worden om gebruiksgemak te bevorderen en misverstanden te voorkomen. Een gegevensuitwisseling tussen banken en de BRP met dat doel kan op veel dossiers helpen de datakwaliteit over en weer te vergroten, en daarmee de verschillende taken goed uit te voeren, waaronder het voorkomen van witwassen of uitkeringsfraude.

Aanbeveling: wijs de (bancaire) Authenticatiedienst aan als verantwoordelijke voor het verwerken van het BSN bij identificatie en authenticatie. Verruim de mogelijkheden voor gegevensuitwisseling ter validatie en fraudepreventie.

3.12 Overlap met andere wet- en regelgeving

In de USvE zijn veel regels terecht gekomen die elders al een wettelijke regeling kennen. Heel specifiek gaat dat bij banken om de Wwft, en voor alle participanten om de Wbp. Bijvoorbeeld op het terrein van bescherming van gegevens van de Gebruiker, bewaartermijnen etc. is de Wbp duidelijk genoeg en volstaat een verwijzing daarnaar, in plaats van de uitwerking in de USvE. Dit is dan ook in overeenstemming met het uitgangspunt om geen eisen te formuleren die al in andere wet- en regelgeving zijn vastgelegd.

Aanbeveling: schrap alle bepalingen die elders al in wet- en regelgeving geregeld zijn, en verwijs daarnaar.

4. Themagewijze toelichting op de belangrijkste bevindingen

In dit hoofdstuk zullen we langs een aantal kernthema's aangeven welke bezwaren we zien in de huidige concept versie van de wet GDI en de USvE, welke achtergrond die hebben en welke oplossing we voorstaan.

4.1 Drie - lagen model

Zoals gezegd zijn de partijen binnen het iDIN-scheme een voorstander van het inrichten van het eID landschap door het erkennen van het bestaan van drie lagen, die er feitelijk al zijn:

- De wetgevende laag (level 1), waar de kaders en spelregels (principes) gezet worden en waarbinnen de oplossingen die binnen het BSN domein opereren aan moeten voldoen.
- De afsprakenstelsel / oplossing laag (level 2), waar nadere voorwaarden zijn opgenomen voor onder meer het product, de techniek, en operationele afspraken, naast afspraken over innovatie en doorontwikkeling. Maar ook de product governance, toelating en toezicht, veiligheid en privacy, merkenbeleid en communicatie zijn hier geborgd, waardoor de invulling van DigiD en iDIN verschillen. De oplossingen kunnen zich onafhankelijk van elkaar doorontwikkelen, maar passen beiden wel binnen dezelfde (wettelijke) kaders (level 1). De regels op dit niveau moeten passen binnen de principes van Level 1.
- De aanbieder laag (level 3). Hier bevinden zich de aanbieders van een specifieke oplossing die in het geval van iDIN bijvoorbeeld gecertificeerd worden op basis van alle governance eisen binnen het stelsel. Maar ook andere invullingen zijn denkbaar. Dit is het commerciële domein waar de daadwerkelijke contracten gesloten worden over de levering van het product.

Het proces van certificeren op basis van generieke eisen en principes (level 1), dat op de verschillende oplossingen een andere invulling kent, maar wel aan dezelfde belangrijke principes van veiligheid, betrouwbaarheid, privacy, gemak en kwaliteit voldoet, leidt ertoe dat er een level playing field ontstaat, waarbij de ruimte voor innovatie en doorontwikkeling voldoendeaanwezig blijft, en ook voor concurrentie. Kortom: er is behoefte aan een wettelijk kader, maar niet aan een invulling daarvan. Deze invulling kan prima op stelsel- of oplossing-niveau. In onze visie adresseert level 1 de "wat" vraag, level 2 de "hoe" vraag. In de concept wet lopen deze vragen nu door elkaar.

Dat deze laag (level 2) ontbreekt in de concept wet en in de uitwerking in de USvE, blijkt ook uit het verkeerde voorbeeld dat wordt gegeven bij punt 4.3 in de Memorie van Toelichting. iDEAL wordt daar aangedragen als voorbeeld van een Ontsluitende dienst terwijl hier juist iDEAL moet worden gezien als een voorbeeld van een afsprakenstelsel met daar achter de verschillende Licentiehouders als verschillende "Authenticatiediensten". In dit voorbeeld zou een pagina waarop wordt getoond dat kan worden gekozen uit verschillende betaalmogelijkheden - PayPal, Mastercard, Acceptgiro en iDEAL – juist zijn geweest. Van de Ontsluitende dienst, indien nodig, wordt verwacht de gebruiker te laten kiezen uit een aantal opties, bijvoorbeeld DigiD, Idensys en iDIN.

4.2 Rule based versus principle based

In de kamerbrief van minister Plasterk van 21 december jl. geeft de minister het volgende aan “De uniforme set van eisen richt zich met name op voorschriften t.a.v. veiligheid, privacy en betrouwbaarheid.” De eIDAS-verordening, met name de uitvoeringsverordening (2015/1502) en de Wet Bescherming Persoonsgegevens (WBP) (en straks de Algemene verordening gegevensbescherming 2016/679 en de daarop gebaseerde Uitvoeringswet Algemene verordening gegevensbescherming) benoemen ook deze terreinen en schrijven daarmee voor aan welke eisen eID-partijen dienen te voldoen, zonder specifiek te maken hoe deze eisen ingevuld dienen te worden.

De USvE beschrijft wel één invulling, en gaat daarmee veel verder en dieper (op een veel groter detail-niveau) dan Europees gevraagd wordt en wenselijk of noodzakelijk is voor de Nederlandse situatie. Alle oplossingen dienen zich op basis van deze versie te conformeren aan die ene invulling, die wettelijk is verankerd.

Waarom de overheid zoveel aanvullende eisen stelt is onduidelijk. Ze lijkt hiermee risico’s (hoe klein dan ook) af te willen vangen, maar:

1) Het is vaak onduidelijk welk risico de overheid probeert te verkleinen en hoe groot deze risico’s zijn. Welk risico wordt verkleind met een centraal inzageregister? Wat is het doel? Is dit überhaupt wel een effectieve maatregel?

2) Sommige maatregelen creëren nieuwe risico’s, zoals haalbaarheidsrisico’s (financieel maar ook operationeel) en privacyrisico’s. Het centrale inzageregister is bijvoorbeeld een privacy hotspot waar ook frauderisico’s aan kleven. Rechtvaardigt het doel van een centraal inzageregister deze nieuwe risico’s?

Er zijn diverse bezwaren tegen rule-based eisen.

- Ten eerste betreft dit reeds bestaande processen en procedures, met bestaande wettelijke kaders en bestaande normen en toezicht daarop. Bijvoorbeeld het proces aanvraag en registratie (USvE 1.4.1.1.2.1.1) en Bewijs en verificatie identiteit (USvE 1.4.1.1.2.1.2) zijn gevat in het “klant worden” proces bij een bank, waarbij op basis van de Wwft eisen worden gesteld aan identificatie en registratie van de klant. Deze eisen, die wereldwijd in de financiële sector gebruikt worden, zijn Principle Based geformuleerd en vallen onder toezicht van de Centrale Bank. De eisen beogen voor elke transactie die een bank kan uitvoeren ten behoeve van de klant de identiteit van die klant betrouwbaar (en veilig) vast te stellen. Dit gebeurt met behulp van een uitgebreide risico-gebaseerde classificatie, waardoor er meerdere invullingen van deze eisen bestaan, die allemaal voldoen aan de internationale kwaliteits- en betrouwbaarheids-eisen. Door hier nu een veel beperkender invulling voor te schrijven zullen de instellingen die daaraan moeten voldoen hun processen aan moeten passen, waarbij de betrouwbaarheid of kwaliteit van de identificatie niet per sé verbetert, terwijl die aanpassing wel grote impact zal hebben op de werkprocessen van de bank en de

manier waarop zij voldoet aan andere (inter-)nationale eisen. Met andere woorden, als enkel het doel is te voldoen aan de rule based eisen dan spreken we over een significante investering zonder toegevoegde waarde.

- Technologische ontwikkelingen staan nooit stil. Een groot deel van de USvE is gewijd aan de technische inrichting van het eID-landschap en de componenten daarin. Door dit in deze regelgeving vast te leggen, worden tevens de systemen en oplossingen voor eID-dienstverlening bevroren en is er minimaal een ministerieel besluit nodig voor aanpassingen. Dit mechanisme kan er gemakkelijk toe leiden dat innovatie onder de participanten geremd wordt en men wacht tot de overheid zelf weer initiatief neemt tot wijziging, bij voorkeur inclusief de benodigde financiële ruimte om deze aanpassing door te voeren. Er is daarmee geen inherente prikkel meer voor het nastreven van efficiëntere, veiligere of betrouwbaardere oplossingen die tegen lagere kosten geleverd kunnen worden. Bij het nalaten de eisen tijdig te actualiseren lopen we in Nederland zelfs het risico dat alle eID oplossingen een kwetsbaarheid gaan vertonen, waarbij de overheid het eventuele risico draagt, door nalatig te zijn in het tijdig actualiseren.

Het is onze aanbeveling om hier een andere strategie te kiezen, een strategie die ook door andere toezichthouders in Nederland veel gebruikt wordt om enerzijds kwaliteit en betrouwbaarheid te borgen en anderzijds meerdere invullingen toe te staan, zodat de sector zich kan blijven innoveren. Die strategie komt erop neer dat in plaats van voor te schrijven *hoe* de invulling moet zijn van de eID-oplossing (in het Engels: rule based) vooral gekeken wordt naar wat er beoogd wordt te *bereiken* met de oplossing (principle based). De manier waarop dat dan bereikt wordt, wordt vrijgelaten aan de partijen die het invullen en wordt daarna beoordeeld door de bevoegde toezichthouder. Dit is de werkwijze van o.a. AP, DNB, AFM en ACM op veel dossiers waar partijen goed mee om kunnen gaan. Ook internationaal wordt dit veel gebezigd en zijn bijvoorbeeld ook de eisen die in de RTS (*Regulatory Technical Standards*) van de PSD 2 (*Payment Services Directive*) Principle Based opgesteld. Deze eisen worden naar verwachting in 2018 op banken van toepassing en betreffen ook de processen rond authenticatie en identificatie.

Door te kiezen voor principle based eisen wordt ook dichter bij de oorspronkelijke Europese tekst gebleven en zijn de verschillen met andere Europese landen minder groot. De consequentie is mogelijk wel dat de participant meer moeite zal moeten doen in het aantonen of toelichten waarom de gekozen methode een correcte invulling is, maar dit weegt niet op tegen de voordelen van de ruimte voor invulling en de prikkel voor innovatie die er dan is. Dit komt ook de slagkracht van een Nederlandse oplossing in het Europese landschap ten goede en zullen de implementatiekosten voor de overheid om het eID-stelsel te faciliteren drastisch worden teruggebracht.

4.3 Level playing field in Europa

Ten opzichte van de oorspronkelijke Europese eisen zoals geformuleerd in de eIDAS uitvoeringsverordening (EU, 2015/1502 van 8 september 2015), is de Nederlandse invulling erg omvattend en gedetailleerd. Dit steekt des te meer omdat andere Europese landen geen (wezenlijke) aanvullende eisen stellen. Dit creëert niet alleen binnen Europa een ongelijk speelveld, maar

verzwaart ook een Nederlandse invulling zodanig dat de kosten voor gebruik van eID-middelen zelfs binnen een uitsluitend Nederlandse context erg hoog worden. Dit blijkt ook uit de gepubliceerde business case (Business Case Inloggen in het BSN-domein) van 9 november 2016, waar de jaarlijkse kosten voor het beheren van de (complexe) stelselvoorziening € 36,8 miljoen euro per jaar bedragen, ten opzichte van de verwachte variabele kosten voor gebruik € 7,6 miljoen bedragen.

De mate waarin (private) Nederlandse eID oplossingen hierdoor in Europa concurrerend kunnen zijn in het private domein lijkt daardoor vrijwel nihil te zijn. Ook zullen andere oplossingen vanuit het buitenland de Nederlandse markt betreden, terwijl die niet voldoen aan de nu geformuleerde Nederlandse USvE, maar aan een veel lichter regime. Deze ongelijkheid in Europa is zeer onwenselijk.

4.4 Financiering en verplichtende werking

Artikel 21 van de conceptwet GDI geeft de overheid het recht om zich met de prijsstelling en voorwaarden van private partijen te bemoeien. De Betaalvereniging heeft begrip voor het treffen van een algemene regeling die zorgt voor laagdrempelige toegang tot eID dienstverlening, maar vindt deze concrete invulling ongepast en marktverstorend. Deze marktverstoring zal zich niet beperken tot het overheidsdomein maar zal ook in het private domein gevoeld worden.

In een afsprakenstelsel als iDIN gelden als het gaat om (product-)voorwaarden zogenaamde ketens van verklaringen, ofwel voorwaarden voor een zakelijke afnemer (Dienstverlener) hebben hun weerslag via de verschillende ketenpartijen in de voorwaarden voor de Gebruiker. Het ingrijpen in voorwaarden krachtens een maatregel van bestuur heeft dus potentieel gevolgen voor alle klantvoorwaarden binnen de verschillende oplossingen. Deze mogelijkheid achten we onwenselijk en niet proportioneel.

De financiële bepalingen van de conceptwet GDI maken het mogelijk dat de overheid de kosten voor certificering en erkenning, én een vaste vergoeding aan het Rijk (voor centrale voorzieningen) op de participanten verhaalt. Dit is zeer onwenselijk omdat op deze wijze ook de mogelijke inefficiency in ontwikkeling van centrale overheidsoplossingen wordt afgewenteld op kosten efficiëntere private oplossingen. Omdat de minister ook kan ingrijpen op de tarieven die een private aanbieder mag rekenen is het maar de vraag of al deze kosten doorbelast kunnen worden aan de Dienstverleners in het BSN domein. Het wordt voor private partijen op deze manier nagenoeg onmogelijk gemaakt om een gezonde businesscase te ontwikkelen. Bovendien wordt hiermee ook geen recht gedaan aan de reeds gemaakt kosten voor onderzoek en ontwikkeling bij deze partijen.

Onze indruk bestaat dat de noodzaak voor artikel 21 vanuit de overheid vooral gevoeld wordt vanuit de voorgestelde verplichte werking van acceptatie van erkende middelen door alle Dienstverleners, overheden en private organisaties met een publieke taak. Dit weerspiegelt op nationaal niveau de Europese verplichte acceptatie op een ongewenste manier. Die verplichte acceptatie is op zichzelf al marktverstorend en niet noodzakelijk. Een Publieke Dienstverlener is ons inziens prima in staat om vast te stellen welke oplossingen bijdragen aan de strategie en doelstellingen van de organisatie,

zonder dat daar een verplichting voor nodig is. En een oplossing zou meer moeten kunnen zijn dan alleen de prijs, er kunnen immers ook andere overwegingen een rol spelen in de afweging voor de in gebruik name van een product, zoals aanvullende functionaliteit, gebruiksgemak, bereik, eenvoud in implementaties, etc.

Conform de eIDAS-verordening geldt natuurlijk wel de verplichte acceptatie, maar voor zover wij het begrijpen betekent erkenning op basis van de USvE nog niet automatisch dat een oplossing genotificeerd wordt. Dat zou vanuit de optiek van de aanbieders van iDIN en de Betaalvereniging ook niet wenselijk zijn op dit moment.

4.5 Techniek

Een groot deel van de USvE 1.0 is gewijd aan de uitwerking van de techniek, paragraaf 1.3. Deze paragraaf beschrijft de rollen in enkele pagina's en geeft daarna in de pagina's 39 tot en met 125 de technische invulling van het stelsel.

4.5.1 Meerdere stelsels in plaats van één

De kern van de multimiddelen strategie die de overheid zegt voor te staan is in onze ogen is dat er meerdere stelsels komen, die technologie onafhankelijk zijn en onafhankelijk van elkaar kunnen opereren waardoor er geen wederzijdse verwevenheid of afhankelijkheid ontstaat. De multimiddelen strategie beoogt immers de inherente kwetsbaarheid van de afhankelijkheid van één systeem (DigiD) op te lossen. Die kwetsbaarheid blijft echter bestaan wanneer er de facto één stelsel voorgeschreven wordt. Zelfs het delen van één centraal sleutelbeheer zoals nu wordt voorgesteld, is risicovol vanwege diezelfde kwetsbaarheid, zo heeft de Diginotar affaire ons geleerd.

In het Memorie van Toelichting bij de conceptwet GDI wordt ook aangegeven (bij par. 4.5): "Meerdere middelen van meerdere leveranciers hebben bovendien als voordeel dat meerdere technologieën naast elkaar worden gebruikt." De huidige invulling binnen de USvE 1.0 komt hier niet aan tegemoet en legt een nagenoeg dekkende technologie op aan alle participanten. In die zin lijkt het meer op de uitwerking van de eID 2.0 uitwerking uit 2014, dat inderdaad poogde één landelijk dekkend systeem te creëren. Dit is destijds verlaten vanwege de complexiteit. Nu lijkt het erop dat deze complexiteit opnieuw beoogd wordt, wat onzes inziens nooit de bedoeling van de minister kan zijn geweest.

Tot slot zijn er, zoals gezegd, niet alleen maar zeer beperkt eigen keuzes te maken, er is ook niet of zeer beperkt rekening gehouden met functies die reeds door participanten ingevuld worden. Deze zijn in bijlage 1 per voorgesteld koppelvalk beschreven.

4.5.2 Geen open standaarden

In de MvT valt te lezen dat binnen de USvE het principe van open standaarden gepromoot wordt en zelfs sterker aangezet wordt dan het huidige *pas-toe-of-leg-uit* principe. Wat we echter constateren

bij het bestuderen van de verschillende technische invullingen die nu onderdeel zijn van de USvE, is dat de voorgestelde technische infrastructuur hier maar beperkt aan voldoet. Het meest in het oog springend is het gebruik van de Polymorfe Pseudonimisering, dat duidelijk nog niet de volwassenheid heeft die grootschalige toepassing mogelijk maakt. Met name voor Dienstverleners heeft dit een grote impact. Niet alleen is de techniek complex, maar door het specifieke gebruik van de techniek binnen de USvE, die niet standaard is, zijn er geen open source libraries te gebruiken en zal de Dienstverlener dus veel meer zelf moeten ontwikkelen. Op dit moment kan nog niet worden overzien wat hier de kosten voor zijn, maar naar verwachting zijn deze zeer aanzienlijk (zie ook de volgende paragraaf).

4.5.3 Technologieneutraal

Het uitgangspunt van eIDAS is dat dit technologieneutraal is. Dit om meerdere invullingen te ondersteunen die leiden tot een zelfde betrouwbaarheidsniveau. De nu voorliggende uitwerking is dat bepaald niet, want er wordt juist erg veel techniek voorgeschreven. Wij constateren daarbij een aantal zaken:

- Veel techniek lijkt ontworpen vanuit een Idensys/eHerkenning uitgangspunt, waaraan een aantal centrale voorzieningen is toegevoegd. Onze ervaring is dat deze techniek vrij complex is in de implementatie daarvan. Dit pakt voor alle participanten nadelig uit;
- Nut en wenselijkheid van de centrale systemen staan ter discussie (zie 4.7);
- Door in één stelsel alle mogelijke functies af te willen dekken ontstaan er ongewenste en onnodige onderlinge afhankelijkheden;
- De iDIN-oplossing is gebaseerd op het éénmalig koppelen van ‘accounts’ en daarna inloggen via een voor iedere Dienstverlener specifiek pseudoniem. De Dienstverlener moeten dat pseudoniem weliswaar opslaan, maar onze indruk is dat dit veel minder impact heeft dan de voorgestelde techniek van de USvE, terwijl de werking hetzelfde is;
- Door de Authenticatiediensten toegang te geven, onder condities, tot de BRP, via bestaande BRP koppelingen zou zelfs het BSN koppelregister overbodig zijn.

Onze aanbeveling, als het gaat om techniek, is om veel terughoudender te zijn in het voorschrijven van techniek, de private en publieke oplossingen niet onder te brengen in één technisch stelsel, en de mogelijkheden die vanuit oplossingen, zoals iDIN, geboden kunnen worden een plek te geven in de mogelijke toepassingen bij Dienstverleners, zodat er meer differentiatie mogelijk is om aan te sluiten bij de specifieke wensen en situatie van die Dienstverlener.

4.6 Resultaten Proof of Concept iDIN met Polymorfe encryptie en pseudonimisering

Een belangrijk deel van de gekozen inrichting hangt samen met de technische keuze om encryptie en pseudonimisering toe te passen met een zeer specifieke techniek: Polymorfe encryptie en pseudonimisering. Dit is een uiterst complexe techniek (zie pagina’s 39 tot en met 46 van de USvE voor een hoog-over indruk van deze techniek), die beoogt het BSN op een ‘privacy vriendelijke’ manier bij de Dienstverlener te brengen, door er bij de Authenticatiedienst en ‘onderweg’ een niet op de persoon herleidbaar pseudoniem van te maken, die dan door enkele cryptografische handelingen

door de Dienstverlener teruggebracht kan worden tot een BSN van de burger die op dat moment inlogt.

4.6.1 Onderzoeksvragen bij Proof of Concept

Om te onderzoeken of deze techniek ook vanuit iDIN werkbaar en bruikbaar is heeft de Betaalvereniging (iDIN) samen met Logius geparticipeerd in een zogenaamde Proof of Concept (POC). Hier is in een laboratorium omgeving de techniek geïmplementeerd en zijn er drie hoofdvragen onderzocht:

1. Is deze oplossing bruikbaar, uitvoerbaar en werkbaar voor een Dienstverlener? Immers, zowel grote (bijv. SVB) als kleine partijen (bijvoorbeeld een fysiotherapeut) die werken met BSN's zullen deze oplossing moeten kunnen realiseren en ermee moeten kunnen werken.
2. Dezelfde vraag, maar dan voor het iDIN-stelsel, met name voor de instellingen die het dienen te administreren.
3. De vraag of er daadwerkelijk de beoogde privacy bijdrage aan de burger wordt geleverd bij het gebruik van iDIN in het BSN-domein.

4.6.2 Algemene conclusie Proof of Concept iDIN met Polymorfe encryptie en pseudonimisering

De resultaten van de POC gaven aan dat er op dit moment grote risico's kleven aan het gebruik van deze techniek, en dat deze op dit moment door de bank-experts op het gebied van (informatie-) beveiliging nog onvoldoende volwassen wordt geacht. De belangrijkste bevindingen worden uitgebreider beschreven in Bijlage 2.

Op basis van deze drie hoofdvragen kan het volgende worden geconcludeerd:

1. De complexiteit voor Dienstverleners is erg groot, wat met name gevolgen heeft voor het tempo en de kosten van de realisatie bij alle partijen en de beheerslasten en kosten daarna. Ook verwachten we dat een groot deel van de Dienstverleners niet in staat zal zijn deze technologie foutvrij te implementeren. In de markt is de benodigde kennis om partijen adequaat te ondersteunen bij de invoering niet aanwezig;
2. Ook voor Authenticatiediensten is de complexiteit erg groot, groter nog dan voor Dienstverleners, en bij de Authenticatiediensten zullen de kosten voor invoering en beheer, het risico van een onvolwassen technologie een grote rol spelen. Het is geen open standaard en heeft zich niet bewezen in een high performance architectuur. Ook Authenticatiediensten zullen last hebben van de gebrekkige kennis (en niet of beperkt beschikbare specifieke security hardware) in de markt;
3. Specifiek voor iDIN, en naar we vermoeden ook voor Idensys, is de beoogde privacywinst er niet (iDIN en vermoedelijk DigiD) of maar zeer beperkt (Idensys). Ook dat is dus geen reden voor het introduceren van deze technologie.

De conclusie is dat het op dit moment niet verantwoord is deze techniek in te voeren.

Het kan in de toekomst mogelijk zijn dat het als encryptie technologie interessant wordt. Vooral wanneer bestaande sleutellengtes en mechanismen niet meer voldoen. Tegen die tijd verwachten we evenwel dat het veel meer een open standaard is geworden en HSM-leveranciers dergelijke mechanismen ook standaard zullen ondersteunen. De kosten voor invoering zullen dan ook navenant lager zijn, voor alle partijen.

Het lijkt er ook op dat deze technologiekeuze vanuit een heel ander ontwerp is gekozen: het gebruik van polymorfe encryptie en pseudonimisering is bedoeld in een situatie dat eID-smartcards uitgegeven worden waar geen BSN in opgeslagen mag zijn. De Gebruiker kan zich dan alleen met behulp van een smartcard identificeren zonder tussenkomst van een Authenticatiedienst. Wanneer deze laatste wel een rol speelt, zoals nu het geval is, en deze het polymorf pseudoniem opslaat, naast alle andere persoonsgegevens die hij al heeft in het kader van andere dienstverlening, is de 'winst' van deze techniek, zowel functioneel als op het terrein van privacy zeer beperkt. De Pseudoniemen zijn bovendien alleen maar relevant in het private domein, een Overheidsinstelling zal altijd de identiteit (lees: BSN) willen vaststellen van een Gebruiker.

4.7 Centrale voorzieningen

In de uitwerking van de USvE wordt een tweetal extra centrale voorzieningen geïntroduceerd, naast het BSN koppelregister voor validatie op de BRP (Basis Registratie Persoonsgegevens), waarvan we het nut en de wenselijkheid ter discussie stellen.

4.7.1 Het centraal Inzageregister vormt een privacy hotspot en frauderisico

Het nut van het centraal bijhouden van de status van een inlogmiddel zoals die bijvoorbeeld door een bank wordt uitgegeven wordt door ons sterk betwijfeld. De banken houden zelf al de status van de authenticatiemiddelen bij. Bovendien is het niet aannemelijk dat Gebruikers via de overheid hun middelen gaan inzien en/of blokkeren. Het is veel logischer dat de Gebruiker zelf direct contact opneemt met zijn/haar Authenticatiedienst. Bovendien zal er op deze manier een nieuwe rijke gegevensverzameling ontstaan bij de overheid die grote privacy- en veiligheidsrisico's met zich mee brengt.

Concreet voorbeeld:

- Het iDIN-authenticatiemiddel wordt ook voor andere zaken gebruikt, zoals internetbankieren. Wanneer er onterecht een ander middel is aangevraagd op naam van een burger kan gelijk door de fraudeur in het centraal inzageregister gezien worden welke middelen het slachtoffer nog meer heeft, bij welke bank hij of zij bankiert en welke telefoon bijvoorbeeld gebruikt wordt voor authenticatie. Voor phishing is een dergelijk centraal register een zeer aantrekkelijk doelwit.
- Ook ontstaat er een gegevensverzameling buiten de bank, van alle banken bij elkaar, van alle middelen van een bank die gebruikers kunnen gebruiken om in te loggen bij allerlei partijen, inclusief de bank zelf. Daarmee ontstaat er een zeer onwenselijke privacy hotspot.

Voor het afdekken van het risico dat er middelen uitgegeven worden op naam van de Gebruiker zonder dat deze het weet, zal een Inzageregister ook geen soelaas bieden, want wie gaat dat register raadplegen? Het is eigenlijk symptoombestrijding voor een eventueel zwak middelenuitgifteproces. Als het middelenuitgifteproces voldoende veilig is, is een centraal inzageregister onnodig. Bovendien, laten we niet vergeten, binnen eIDAS is er geen voorschrift voor een dergelijk register.

De conclusie is dat het Inzageregister meer risico's creëert dan dat het problemen oplost.

4.7.2 Misbruik register is dubbelop

Er is in het concept van de Wet GDI een verplichting opgenomen om 'opmerkelijke transacties' te melden bij een Misbruik register. Er ontbreekt evenwel een heldere definitie van 'opmerkelijke transactie'. De impact van het bepalen wat opmerkelijke activiteiten zijn en van het besluit om deze, naast de Dienstverlener, ook aan de centrale voorzieningen van de overheid door te geven is erg groot. De toegevoegde waarde ervan lijkt echter nihil of zelfs negatief. De fraudesystemen van de banken zijn gebaseerd op jaren ervaring en fine-tuning. Daarin worden de laatste ontwikkelingen meegenomen om de cyber-crimineel zoveel mogelijk een stap voor te blijven. Wanneer er ook gegevens doorgegeven worden aan het centrale Misbruik register is het de vraag of, en zo ja, op welke termijn, hier ook een zinvolle aanvulling mee gerealiseerd wordt ten opzicht van de bestaande fraudebeheersingssystemen. Tot die tijd kunnen verkeerde signalen uit een centraal systeem leiden tot verwarrende boodschappen aan de Gebruiker.

De werkelijke activiteit (wat gaat de ingelogde Gebruiker doen wanneer hij is ingelogd?) vindt plaats bij de Dienstverlener. Het lijkt zinvoller om een eventuele aanvullende fraudedetectie daar aan te koppelen, daar kan immers veel beter worden afgewogen welke handelingen risicovol zijn en welke niet.

Ook in dit geval ontstaat er weer een gegevensverzameling bij de overheid waarvan het doel en de toegevoegde waarde onduidelijk is.

De conclusie is dat een Misbruik register niet nodig is omdat er al uitgebreide fraude/misbruik detectie systemen actief zijn.

4.8 Dubbel Toezicht

De componenten waar iDIN uit bestaat staan al onder toezicht. Aan de hand van bestaande wettelijke kaders (o.a. Wwft, WFT), regulations (o.a. PSD, AML) en richtlijnen (o.a. SeCuRePay) ziet DNB (en in een aantal gevallen de ECB) toe op de processen voor klant-identificatie en -registratie, informatiebeveiliging, (toegang tot) de betaalinfrastructuur etc. iDIN is in dat opzicht niet nieuw, maar maakt gebruik van wat banken al hebben, zoals de inlogmiddelen, processen en infrastructuur.

En dat geldt ook voor de toezicht kaders. Neem bijvoorbeeld het thema Informatiebeveiliging. De invulling hiervan door een instellingen het toezicht daarop is gebaseerd op de naleving van een combinatie van standaarden (w.o. COBIT, NIST, ISO 27001, Standard of Good Practise (SoGP) van het ISF), op maat gesneden voor de betreffende instelling en bewaakt door de zogenoemde three-lines-of-defence. Het resultaat hiervan in termen van veilige werking geniet reeds een ruim vertrouwen bij klanten en overheden en kan beschouwd worden als state-of-the-art in vergelijking met de ons omringende landen. Naast het bestaande DNB toezicht op de individuele instellingen is er vanuit de producteigenaar ook toezicht op de aan iDIN deelnemende instellingen via hun licentiehouder- of certificaathouderschap voor de product specifieke kenmerken, net als voor iDEAL, Acceptgiro en Incassomachtigen. De informatiebeveiligingseisen vanuit de USvE voorzien voor een deel in deze inrichting (zie 2.4.3, Substantieel punt 1), maar zal de toetsing, toelichting en verantwoording via een nieuwe toezichthouder laten plaatsvinden.

Naast dit onderwerp zijn er ook eisen vanuit de SeCuRePay richtlijn van de ECB en de PSD2 RTS vanuit de EBA, waar ook DNB/ECB toezichthouder op is. Deze verschillende regelingen betreffen eisen aan processen die ook in de USvE beschreven worden. Wanneer dit voor de banken zou leiden tot een tweede toezichthouder op deze processen, dan kunnen er hele complexe situaties kunnen ontstaan rond het voldoen aan al deze eisen, omdat die eisen niet altijd goed op elkaar afgestemd zijn en soms zelfs kunnen conflicteren. Zeker wanneer deze eisen ‘rule-based’ zijn is die kans erg groot. Als de verschillen dan ook nog eens met verschillende toezichthouders besproken moeten worden, met verschillende specialisten en verschillende meningen leidt dat tot onnodig veel conflicten, onduidelijkheden, ‘overhead’, doorlooptijd en compliance-kosten, terwijl de baten vermoedelijk nihil zijn. Dit is niet in het belang van de burger.

Het eerder voorgestelde drie-lagen model, met sectoraal toezicht komt hier aan tegemoet door per oplossing vast te stellen wie de toezichthouder moet zijn.

Daar komt bij dat de banken van mening zijn dat toezicht op de oplossing niet beperkt moet zijn tot de toepassing ervan binnen het publieke domein. De huidige wetsvoorstellen voor de GDI dekken alleen het publieke domein. Ook de toepassing binnen het private domein zou onder toezicht moeten vallen. Door DNB voor de banken, Agentschap Telecom voor Idensys en het Bureau Financieel Toezicht (BFT) voor NotarisID (wanneer die ook erkenning zouden wensen) aan te wijzen als toezichthouder, wordt dubbel toezicht voorkomen en is toezicht voor het gebruik binnen alle sectoren geborgd, dus ook de private. Het toezicht op DigiD kan binnen de overheid ingericht worden, aangezien het gebruik ook beperkt is tot de overheid.

4.9 Definities

In de uitwerking van de USvE is veel gebruik gemaakt van modellen, definities en uitwerkingen van het Idensys stelsel / eHerkenning. Dit is ook begrijpelijk omdat deze stelsels met veel inspanning vanuit de overheid (Logius, EZ en BZK) ontwikkeld zijn en waar ‘leveranciers’ kunnen participeren in een door de overheid strak geregisseerde samenwerking. Bij de totstandkoming van de USvE lijkt het daarom alsof er veel gebruik gemaakt is van de specifieke inrichtingservaring van deze

organisaties en er niet gekeken is naar andere inrichtingen die hetzelfde doel bereiken. Dat betekent dat er op allerlei detailniveaus een vertaalslag nodig is van de USvE voor de inrichting van iDIN..

Eerder is al eens vanuit de beheerorganisaties van Idensys (Logius) en iDIN (de Betaalvereniging) gekeken naar de verschillen en overeenkomsten tussen beide stelsels. De algemene conclusie was toen dat beide stelsels weliswaar een andere invulling en ontstaansgeschiedenis (resp. eHerkenning vs. iDEAL) kennen, maar kwalitatief vergelijkbaar zijn en ook hetzelfde beogen: betrouwbaar en gebruiksvriendelijk inloggen binnen de kaders van de geldende wetgeving zoals voor privacy.

Doordat de USvE op detail niveau is uitgewerkt en daarbij vooral de Idensys inrichting is gevolgd, ontstaan er veel fricties met de opzet van iDIN. Een voorbeeld van de mismatch is:

De definitie van **authenticatiemiddel**. De USvE stelt: *Een middel op grond waarvan Authenticatie van een Gebruiker kan plaatsvinden.*
Binnen iDIN is een authenticatiemiddel eigenlijk de manier waarop je toegang hebt tot iDIN zoals dat door je bank geboden wordt. Dit kan zijn via internetbankieren of bijvoorbeeld via de bank-app, waarbij het middel bestaat uit een geïnstalleerde en binnen internetbankieren geautoriseerde (ge-'bind'-e) app en telefoon of identifier (iets dat je hebt), waarbij de toegang tot bijvoorbeeld de bank-app (via biometrie of pincode) gebeurt door iets wat je bent of iets dat je weet. Met andere woorden, een klant heeft mogelijk bij dezelfde bank meerdere middelen, waarbij ook hetgeen een Gebruiker heeft (een smartphone met werkende bank-app), weet (pincode) en/of is (biometrie) feitelijk hoort bij het middel. De banken gebruiken voor iDIN dezelfde middelen als ook voor internetbankieren en online betalen via bijvoorbeeld iDEAL.

Het effect hiervan is niet triviaal: wanneer een Middelenuitgever (volgens de USvE dus de bank) meerdere middelen uitgeeft (bijvoorbeeld een identifier, bankpas en de bank-app op een smartphone) zal van al deze middelen apart een status moeten worden bijgehouden (zie USvE AUC3, pagina 55) ten behoeve van het Inzageregister. Dus ook wanneer een Gebruiker een nieuwe smartphone gaat gebruiken, j een nieuwe identifier ontvangt en (strikt genomen) wanneer hij of zij een nieuwe pincode gaat gebruiken. Dat is uitermate onwenselijk en creëert een hoop extra berichten, veel extra kosten, zonder enige toegevoegde waarde.

Door de regelgeving meer Principle Based op te zetten is er ook minder noodzaak om alles te definiëren op dit detailniveau. Voor de definities die over blijven, wordt aanbevolen die zo op te stellen dat ze minder dwingend slechts één invulling ondersteunen.

4.10 Rollenmodel

Voor een adequate werking van private oplossingen is het noodzakelijk dat:

- Private oplossingen vrij gelaten worden in de opzet van het rollenmodel dat zij wensen te gebruiken, waardoor oplossingen elk hun eigen rollen en distributiemodel kunnen hanteren en de Dienstverlener in staat is te kiezen hoe hij de dienst wenst af te nemen;

- Niet alle use cases en alle mogelijke functies van elkaar afhankelijk gemaakt worden. Daarmee ontstaat er een complexiteit die moeilijk is te overzien en waar doorontwikkeling van de ene participant altijd afhankelijk is van alle andere participanten.

In samenhang met de opmerkingen en zorgen over het bereik pleiten we voor een beperking van de reikwijdte van de wet- en bijbehorende regelgeving tot alleen het burgerdomein voor zover daar waar het BSN gebruikt wordt.

Dat beperkt ook gelijk het aantal rollen dat nodig is. En als er dan een noodzakelijke nieuwe rol ontstaat, stel de regels dan zo op dat de eisen onafhankelijk van elkaar kunnen worden afgesproken. Dat dus een Authenticatiedienst in het burgerdomein geen rekening hoeft te houden met bijvoorbeeld het bedrijvendomein, met machtigingsdiensten, application-to-application of machine-to-machine communicatie, zoals aangekondigd op pagina 59 van de USvE.

4.11 Rol als verantwoordelijke voor BSN

Voor iDIN geldt dat de rol van de Authenticatiedienst in het BSN-domein een vreemde situatie oplevert. Momenteel zijn de banken bewerker voor de verwerkingen in het kader van iDIN in het BSN-stelsel. Deze bewerkersrol geldt alleen jegens BZK en het gebruik van het koppelregister daarvoor. Omdat daar ook andere persoonsgegevens meegestuurd worden (ter validatie) zijn banken voor dezelfde handelingen en zelfs hetzelfde bericht zowel Verantwoordelijke als Bewerker.

Voor de banken is dit een bijzondere rol gezien hun rol als verantwoordelijke ten opzichte van de BSN-verwerkingen buiten het iDIN-stelsel (bijv. renseignering (VIA) bij de Belastingdienst). Gezien de belangen van gebruikers en banken lijkt het in de rede te liggen dat de banken een grotere verantwoordelijkheid krijgen met betrekking tot het verwerken van BSN in het kader van iDIN.

Naar huidig recht bestaat er geen wettelijke grondslag voor de banken om onder eigen verantwoordelijkheid het BSN in het iDIN-stelsel te verwerken. Het verdient aanbeveling dat hier wettelijk ruimte voor wordt gemaakt. Wij stellen een algemene verplichting voor de banken voor om in dit kader het BSN te verwerken zin de Wet Digitale Infrastructuur. In de MvT lezen wij dat dit de bedoeling is, maar dit zien dit niet terug in de tekst van artikel 9 van het wetsvoorstel.

Natuurlijk is validatie van het BSN via het BSN-koppelregister of de BRP wel een voorwaarde. Het moet immers voorkomen worden dat er fouten sluipen in de persoonsgegevens bij het BSN, of dat het BSN bij de verkeerde wordt geadministreerd. Die validatie zal voor meer persoonsgegevens van toegevoegde waarde zijn, in het verhogen van de datakwaliteit en daarmee de betrouwbare toepassing in bijvoorbeeld het opsporen van witwasfraude, uitkeringsfraude of gegevensverwerking bij bijvoorbeeld de VIA. Graag zien we de mogelijkheden daartoe uitgebreid.

4.12 Overlap met andere wet- en regelgeving

Bij de eisen bij aanvraag en registratie (par. 2.1.1, pag. 129 ad 4) wordt voorgeschreven dat Authenticatiediensten het BSN moeten overnemen uit het identiteitsbewijs (IDBW). Dus alleen Nederlandse IDBWs zijn toegestaan. Dit is onwenselijk om vier redenen:

1. Het beperkt de gebruikersgroep behoorlijk. Conform uitvoeringsregeling Wwft staan banken IDBWs zonder Nederlands BSN toe. Dit zijn niet alleen buitenlandse IDBWs, maar ook Nederlandse vreemdelingendocumenten. Behoorlijk wat klanten zijn geïdentificeerd met dit soort IDBWs. Denk aan expats, vluchtelingen, klanten met dubbele nationaliteit. Het BSN kan van andere documenten overgenomen worden.
2. Er is veel impact voor banken en klanten. Bij veel banken is niet centraal vastgelegd met wat voor soort IDBW de klant geïdentificeerd is. De vraag is überhaupt of alle banken dit soort metadata vastleggen bovenop de kopie IDBW. De eis vergt dus systeem- en procesaanpassingen. Klanten zouden zich opnieuw moeten identificeren met een ander IDBW, terwijl er feitelijk geen nieuwe gegevens nodig zijn of onduidelijkheid is over iemands identiteit. Dat kunnen we onze klanten niet goed uitleggen.
3. Beperkt mogelijk Europese concurrentie. Als niet-Nederlander (maar wel ingezetene van Nederland) kun je iDIN dus niet gebruiken bij de overheid. Dit beperkt de concurrentie op Europees-niveau. Zo kunnen Nederlanders en inwoners van andere lidstaten wel bijvoorbeeld in Estland een eID aanvragen. Maar inwoners van Estland en andere lidstaten niet in Nederland. Bovendien kan dit als discriminatie worden beschouwd.
4. Het is tegenstrijdig met bepalingen in USvE waarin staat dat een WID als bedoeld in artikel 1 Wet op de identificatieplicht gebruikt mag worden. In dat artikel staan bijvoorbeeld ook IDs van andere lidstaten (dus zonder BSN).

De USvE maakt geen onderscheid in de identificatie en verificatie van meerderjarige en minderjarige gebruikers. Voor de Wwft is identificatie van minderjarigen via de ouder/voogd voldoende om financiering van terrorisme en witwassen tegen te gaan. Dit zou ook hier gevolgd moeten worden. Bovendien is de ouder/voogd wettelijk vertegenwoordiger voor de minderjarige.

In de USvE wordt gesteld (par 2.4.2, pag. 25) dat informatie bij de Authenticatiedienst minimaal op niveau Substantieel beschermd moet worden. Dit impliceert dat alle (private) Authenticatiediensten ook zelf in de rol van Dienstverlener moeten acteren en (erkende?) middelen accepteren. Terwijl de private Authenticatiedienst zelf middelen uitgeeft, al dan niet binnen de erkenning door de Minister. We zijn van mening dat de private Authenticatiedienst zelf verantwoordelijk is hoe hij zijn gegevens naar zijn klant toe ontsluit. De Wbp verplicht organisaties al om bijvoorbeeld inloghistorie of persoonsgegevens afdoende te beschermen. Deze eis zou in de USvE moeten vervallen.

Bij de bewaartermijnen van de inloghistorie (USvE par 2.4.4, pag. 27) staat dat het alleen op uitdrukkelijk verzoek van de gebruiker inloghistorie langer bewaard mag worden dan 14 maanden. Dit lijkt een te strikte formulering en bovendien een overlap of misschien zelfs in strijd met de Wbp. De Wbp schrijft voor dat er een doel moet zijn om gegevens te bewaren. Zolang er een doel is dat het langer dan 14 maanden bewaren rechtvaardigt, mag dit langer worden bewaard. Dit doel moet uiteraard wel worden gecommuniceerd aan de gebruiker. Hier past een verwijzing naar de Wbp.

De bewaartermijnen van de bij punt 5 (pag. 27) genoemde gegevens zijn niet doelmatig en veel te uitgebreid. Het is moeilijk te verdedigen dat al deze gegevens zo lang bewaard moeten worden. Hierdoor ontstaan er nieuwe privacy hot spots en risico's die vermeden kunnen worden. Ook hier is sprake van strijdigheid met de Wbp.

In paragraaf 2.2.4 op pagina 136 wordt voorgeschreven dat een middelenuitgever eenmaal per vijf jaar de juistheid van de geregistreerde persoonsgegevens moet verifiëren. In de toelichting staat dat initieel (bij uitgifte middel) de juistheid wordt geverifieerd door koppeling in het BSN-koppelregister. Dit suggereert dat de periodieke verificatie niet met het BSN-koppelregister kan. Ook dit is een voorbeeld waarin Wwft en deze concept regels elkaar overlappen. De Wwft stelt eisen aan de betrouwbaarheid van de identiteit van feitelijk elke financiële transactie. Door event driven en periodieke monitoring (een vereiste vanuit de Wwft) van de (transacties van de) klanten (Gebruikers) door de systemen van de bank zal de kwaliteit van de identiteit gewaarborgd blijven en zelfs toenemen. Het is dus volkomen onnodig en bijzonder impactvol de Gebruiker opnieuw volledig te laten identificeren. De vaste gegevens (geboortedatum, geslacht etc.) veranderen in de regel ook niet. En als er wel een relevante verandering is, dan is de kans dat dit al veel eerder bij de bank gemeld en verwerkt is behoorlijk groot.

In de bepalingen voor privacy en informatiebeveiliging (par 2.3.1, pag. 137) staat bij ad 5 (substantieel) en ad 1 (hoog) dat authenticatiediensten in het primaire proces naast de naam van de Dienstverlener ook een eventuele *dienst* (=doel) tonen aan Gebruikers. Het communiceren van het doel van de gegevensverstrekking / inloggen is een verplichting van de Dienstverlener (conform Wbp). De vraag is waarom een Authenticatiedienst ook deze gegevens zou moeten ontvangen, nog los van het feit of die er iets mee doet. Dit wekt de suggestie dat de Authenticatiedienst zicht en/of controle heeft op waar de gegevens / inlog voor gebruikt worden. Dat is natuurlijk niet zo. De Authenticatiedienst levert een authenticatiedienst en heeft in het geheel geen bemoeienis met of oordeel over het gebruik of de dienst van de Dienstverlener. Vanuit het oogpunt van scheiding van bevoegdheden zijn wij van mening dat de dienst (van de Dienstverlener) dan ook niet dient te worden meegegeven aan de Authenticatiedienst.

In de toelichting staat dat de genoemde dienst bij de Dienstverlener de Gebruiker inzicht geeft of een authenticatie mogelijke rechtsgevolgen heeft. Het tonen van je identiteit is echter per definitie geen rechtshandeling, maar een feitelijke handeling. Als Dienstverlener de Gebruiker een rechtshandeling wil laten uitvoeren, moet hij daar een product voor gebruiken dat daarvoor bedoeld is. Bijvoorbeeld een ondertekendienst. Omdat identificeren een feitelijke handeling is, kunnen ook handelingsonbevoegden en handelingsonbekwamen eID-middelen gebruiken (deze groepen zijn door USvE en door iDIN niet uitgesloten), terwijl bepaalde rechtshandelingen niet door hen uitgevoerd mogen worden. Daarom is de aanname van de USvE dat de authenticatie mogelijke rechtsgevolgen heeft niet correct en kan leiden tot misbruik, of tot het gevolg dat handelingsonbevoegden of handelingsonbekwamen moeten worden uitgesloten van de eID dienst, terwijl ze dat niet zijn in de fysieke wereld..

In de MvT staat (p.70) de volgende tekst/; “*De authenticatiedienst controleert deze gegevens aan de hand van het overlegde identificatiemiddel en bewaart geen integrale kopie, maar een kopie waarop de gelaatsfoto en het BSN zijn verwijderd. Hierdoor ontstaat er bij de authenticatiediensten geen verzameling van persoonsgegevens (zogeheten hotspot), waardoor de privacy van de gebruikers wordt beschermd.”*

Inhoudelijk is dat aanvechtbaar, ook zonder BSN zijn er nog tal van identificerende gegevens op een kopie identiteitsbewijs, maar het overlapt ook met al geldende bepalingen voor banken. Banken mogen op grond van de wet een kopie paspoort bewaren. Banken moeten immers kunnen bewijzen dat zij aan de hand van een juist identificatiemiddel de klanten juist hebben geïdentificeerd en het vastleggen van een kopie identiteitsbewijs is daarvoor binnen de Wwft een beproefde invulling, zonder aanvullende eis dat gelaatsfoto en BSN worden verwijderd. De (al bestaande) opslag van deze gegevens voldoet aan de daarvoor geldende eisen voor beveiligde opslag van persoonsgegevens. Er wordt dus geen nieuwe *hotspot* gecreëerd. Deze aanvullende eis zou moeten vervallen.

5. Artikelsgewijze reactie op de wet GDI

Onverminderd onze principiële bezwaren bij het wetsvoorstel en de bijhorende USvE hebben wij de volgende commentaren.

5.1 Artikel 2. Standaarden

Ad lid 2a)

De Betaalvereniging en de instellingen die iDIN aanbieden zijn voorstander van het gebruik van standaarden en zien dit als voorwaardelijk voor een brede marktintroductie. Bij de ontwikkeling van iDIN hebben we hier ook gebruik van gemaakt.

In de praktijk zijn er voor een toepassingsgebied meerdere standaarden in de markt. Voor authenticatie is bijvoorbeeld nu *SAML* in de lijst opgenomen terwijl *oauth* en *openid connect* internationaal ook zeer gangbaar zijn.

Het eID stelsel biedt de mogelijkheid dat private aanbieders hun oplossing aanbieden aan de overheid. Doordat deze een verschillende ontstaansgeschiedenis of innovatiekalender kennen is het mogelijk dat deze oplossingen niet op een voor de overheid geldende *pas-toe-of-leg-uit* lijst voorkomen. Strikt genomen hoeft dat ook niet omdat het niet gaat om een ICT-dienst of -product, maar om een identificatie- of Authenticatiedienst die wordt afgenomen. Om private partijen ook niet te dwingen hun oplossing hieraan aan te passen, en hen daardoor te remmen in efficiency en innovatie, stellen wij voor de toepassing van dit artikel te beperken tot het overheidsdomein waarbij beide kanten van de elektronische communicatie overheidspartijen zijn, zoals de lijst ook bedoeld is (zie bijvoorbeeld de MvT, paragraaf 3.3). Dit zou tevens voorkomen dat ook de private partijen een rol moeten spelen in de besluitvorming over de *pas-toe-of-leg-uit* lijst. Naar onze mening zou dat wel moeten wanneer de lijst ook voor private partijen een verplichtend karakter zou krijgen.

Daarnaast staan verschillende oplossingen die nu in de USvE aangedragen worden erg ver af van plaatsing op een open standaarden lijst. Met name polymorfe pseudoniemen, als voorgeschreven encryptie-technologie, is beslist geen volwassen open standaard die nu voorgeschreven zou moeten worden. Ook hiervoor geldt dat private partijen geen rol hebben gehad in de besluitvorming en deze techniek ook om die reden nu niet verplichtend opgelegd kan worden, los van alle overige geconstateerde tekortkomingen.

Aanbeveling: beperk de reikwijdte van dit artikel tot elektronische communicatie binnen het overheidsdomein.

5.2 Artikel 3. Reikwijdte

Ad lid 2-4)

In een groot deel van de wet GDI, MvT en USvE wordt ingegaan op het burgerdomein en het gebruik van het BSN ten behoeve van authenticatie van burgers bij bestuursorganen en aangewezen organisaties. Op een aantal plaatsen echter wordt gesteld dat het bereik breder is dan het gebruik van het BSN en breder is dan het burgerdomein, namelijk ook geldend voor bedrijven (bijvoorbeeld

MvT, pag. 32)Volstrekte duidelijkheid over het bereik is nu vereist, omdat dit noodzakelijk en randvoorwaardelijk is voor de verdere ontwikkeling van eID-oplossingen in de markt.

Onze aanbeveling is om de huidige set van Wet GDI, MvT en USvE te beperken tot het burgerdomein en dan alleen waar dit ziet op het gebruik van het BSN. Voor het bedrijvendomein zijn de eID uitdagingen anders en is sinds 2009 al een oplossing in de markt: eHerkenning. Als er al bepalingen voor het bedrijvendomein zouden moeten gelden, dan zouden deze duidelijk gescheiden moeten worden van het burgerdomein, zonder verwevenheid daarmee. De onnodige complexiteit en onderlinge afhankelijkheid die daarmee samenhangt kan daarmee worden vermeden.

Aanbeveling: beperk de wet GDI en USvE tot het burgerdomein en dan alleen waar dit ziet op het gebruik van het BSN.

5.3 Artikel 4. Taken en verantwoordelijkheden

Ad lid 1b)

De overheid reguleert machtigingen die gebruikt worden binnen de context van de overheid zelf. Het is niet de bedoeling dat het gebruik van private machtigingsdiensten in de private sector geregeld worden binnen de context van deze wet. In de MvT wordt benadrukt (pag. 59) dat dit wel noodzakelijk is en deze dient hierop aangepast te worden. Machtigingen die mogelijk in de private sector gebruikt kunnen worden, dienen expliciet buiten de scope van dit wetsvoorstel te vallen. Dat zou een private machtigingsdienst kunnen worden, maar die hoort niet te vallen onder de hier bedoelde erkenning. Private Machtigingsdiensten die bedoeld zijn om (ook) binnen de overheid gebruikt te worden, zullen, wanneer deze ook het BSN voor de burger gaan verwerken, wel horen te vallen onder het bereik van de wet.

Wij verwachten en wensen overigens dat een machtigingsdienst niet zo wordt opgezet dat er voor gebruik ervan binnen de context van de Overheid zowel een publieke als een private machtigingsdienst nodig is. Het vastleggen van een machtiging zou moeten kunnen met zowel publieke als private (erkende) eID-middelen. Op voorhand valt immers niet te sturen welk middel een burger heeft of wil gebruiken in relatie tot het vastleggen van de machtiging. Wij denken dat de publieke machtigingsdienst zo opgezet kan en moet worden dat deze onafhankelijk is van het gebruikte eID-middel en dat het raadplegen ervan zonder eID-middel door elke publieke instelling kan gebeuren, na inlog van een Gebruiker (zoiets als: “wilt u gebruik maken van een machtiging, klik dan hier”).

In de MvT, pag. 60, laatste twee zinnen staat nu:
"Informatie over verrichte elektronische dienstverlening is verkrijgbaar bij de desbetreffende authenticatiedienst. Ingevolge de EU verordening gegevensbescherming (AVG) is de authenticatiedienst gehouden deze informatie aan de gebruiker te verstrekken."

De informatieverplichting die uit de AVG voortvloeit is niet zo concreet en vergaand zoals de zin "Ingevolge.." suggereert. Er bestaat geen expliciete verplichting tot het verstrekken van informatie over "verrichte elektronische dienstverlening". Wel bestaat de plicht onder meer om duidelijk en transparant te informeren over de verwerking van persoonsgegevens. Dit vloeit voort uit artikelen 12-14 van de AVG waarin een opsomming wordt gegeven over de aspecten waarover de betrokkene door de verwerkingsverantwoordelijke dient te worden geïnformeerd. Gelet op de onjuistheid van de laatste zin van p. 60, stellen we voor om deze zin te schrappen.

Ad lid 1c)

We begrijpen dat vanuit het risico dat er middelen uitgegeven worden waar de burger geen weet van heeft er een passende maatregel genomen moet worden om de burger hiervan in kennis te stellen. Echter vanuit privacy, veiligheid en verwacht gebruik van dat register stellen wij dat een centraal inzageregister niet proportioneel is ten opzichte van dit risico en juist nieuwe veiligheids- en privacy (hot-spot) risico's introduceert. Daar komt nog bij dat de complexiteit van het bijhouden van een dergelijk register aanzienlijk is.

We stellen vast dat de introductie van een statusweergave vanuit een private Authenticatiedienst onnodig complex is, vanuit privacy- en veiligheidsoverwegingen ongewenst (privacy hotspots) en mogelijk in strijd is met privacy regelgeving. We denken dat hiermee te veel nieuwe risico's worden gecreëerd en dat deze maatregel niet proportioneel is. We stellen daarom voor dit register en alle bijkomende complexiteit te schrappen.

Aanbeveling: scherp de MvT aan op de genoemde punten, beperk de onderlinge afhankelijkheden, en schrap het deel in artikel 1c dat inzageregister betreft.

5.4 Artikel 5. Acceptatieplicht

Ad lid 1 en 2)

Wij stellen voor om de verplichte acceptatie geheel te schrappen. Verplichte acceptatie van alle erkende middelen brengt met zich mee dat de marktwerking onder private middelen/oplossingen ernstig wordt belemmerd, temeer omdat prijzen eenzijdig door de minister opgelegd kunnen worden. Deze combinatie van eisen staat een normale, gezonde marktwerking in de weg (zie ook commentaar bij art. 21). Wel wordt aanbevolen de Dienstverleners in het overheidsdomein te adviseren erkende en algemeen geaccepteerde inlogmiddelen te ondersteunen om het gewenste betrouwbaarheidsniveau te kunnen garanderen en de afhankelijkheid van één centraal inlogsysteem te mitigeren.

Ad lid 3)

De huidige invulling van de USvE en erkenning door de minister in Nederland is veel zwaarder dan de notificering zoals de eIDAS-verordening voorschrijft. Hierdoor ontstaat er geen level playing field binnen Europa. Andersoortige oplossingen (niet –NL) kunnen hierdoor wel gebruikt worden binnen Nederland, terwijl NL oplossingen door relatief hoge implementatie- en beheerskosten niet kunnen concurreren met niet-NL oplossingen. Dit zet Nederlandse oplossingen die wel voldoen binnen Europa op achterstand. Van gelijkstelling is om die reden geen sprake. Wij pleiten voor een Europees level playing field, waarbij de Nederlandse voorschriften in de wet GDI en USvE gelijk getrokken worden met de uitwerking van de Uitvoeringsverordening (EU) 2015/1502 van de Commissie, van 8 september 2015.

Ad lid 4)

De beschreven relatie tussen het eID-middel en de elektronische handtekening is onduidelijk, het nut en de noodzaak van lid 4 is eveneens onduidelijk. Voor zover wij begrijpen is e.e.a. al geregeld in andere wetgeving, met name vanuit eIDAS. Onze verwachting is dat niet bedoeld wordt dat eID-middelen ook verplicht worden tot het bieden van (mogelijkheden voor) elektronische handtekeningen, maar wij zien dat graag explicieter in een aangepaste tekst.

Aanbeveling: schrap de verplichte acceptatie van erkende middelen, ontkoppel deze van de notificatie in Europa, breng de zwaarte van de NL-eisen terug op het EU niveau

5.5 Artikel 6 Erkenning

Voor een adequate werking van private oplossingen is het noodzakelijk dat private oplossingen vrij gelaten worden in het rollenmodel dat zij wensen te gebruiken. Wij stellen dan ook voor de formulering hierop aan te passen, waardoor oplossingen hun eigen rollen en distributiemodel kunnen hanteren en de Dienstverlener in staat is te kiezen hoe hij de dienst wenst af te nemen. Of een ontsluitende dienst daarin een rol zou moeten spelen voor een Dienstverlener zou optioneel moeten zijn.

Erkenning kan daarmee beter plaatsvinden op het stelsel-niveau, in navolging op het drie-lagen principe zoals elders aangegeven. Als het toch noodzakelijk is individuele partijen te erkennen dan zou dat alleen moeten gelden voor de Authenticatiedienst, of liever de partij die de verklaringen afgeeft. De overige partijen zijn immers alleen maar nodig voor het distribueren daarvan.

In artikel 6 lid 1-3 worden rollen geïntroduceerd die in de praktijk niet altijd duidelijk te onderscheiden zijn. Hier zijn een aantal voorbeelden van te geven:

- De authenticatie is de stap die uitsluitend in het Gebruiker – Authenticatiedienst (bank) domein plaatsvindt. De Authenticatiedienst kan dan op basis van de gebruikte middelen vaststellen wie de Gebruiker is. Na instemming van de Gebruiker kan de bank een ‘identiteitsbericht’ opstellen met de gegevens en/of het pseudoniem van de Gebruiker. Deze wordt verzonden aan de Dienstverlener. Hiermee kan de Dienstverlener immers vaststellen wie inlogt. Het delen van deze gegevens (via het afgeven van een “verklaring”) gebeurt dan dus in het kader van identificatie (rol van de authenticatiedienst) en niet voor het verstrekken van gegevens (nu beschreven bij attributendienst).
- Bij de toelichting van ontsluitende dienst (MvT 4.3, pag. 14) staat iDEAL als voorbeeld van een ontsluitende dienst. iDEAL is echter afsprakenstelsel, dat zelf geen operationele rol heeft in een online betaling. De partijen die die rol wel hebben zijn betaaldienstverleners die tot het afsprakenstelsel zijn toegetreden en het merk iDEAL voeren, onder licentie van de producteigenaar. Zij hebben de operationele systemen voor het laten functioneren van het product. Dit geldt ook zo voor iDIN. In de MvT wordt daarmee een verkeerde indruk gewekt, namelijk die van ontsluitende dienst.

Toelichting:
Voor de bancaire oplossing iDIN zijn er maar twee rollen relevant: de rol met de relatie tot de Gebruiker (een gebruiker-eID dienstverlener, de Issuer) en een aanbieder van de dienst (zakelijke eID dienstverlener, de Acquirer). Deze Acquirer valt binnen de iDIN-oplossing en zal alle Issuers, en daarmee alle Gebruikers ontsluiten. Deze Acquirer kan ook leveren aan een ‘tussenpartij’, een service provider in dienst van de Dienstverlener, maar dat hoeft niet. Een service provider kan naast iDIN ook andere diensten aanbieden, waaronder ook andere eID oplossingen, een Acquirer van iDIN levert geen andere eID oplossing. De service provider rol komt het meest overeen met de beschreven ontsluitende dienst. Een Dienstverlener zou echter wel de vrijheid moeten hebben om rechtstreeks op een Acquirer aan te sluiten. Het verplichten van een ontsluitende dienst introduceert een extra schakel in de keten die niet altijd noodzakelijk is.

Dit werkt ook door in andere artikelen.

Ad Lid 4)

Voor de toelatingsprocedure zou in de uitwerking van het drie-lagen model aandacht moeten zijn voor de effectiviteit en zwaarte van de toetsingsprocedure. In navolging van hetgeen gebruikelijk is in veel sectoren, zou een Control Self Assessment (CSA procedure), beoordeeld en getoetst door de onafhankelijke beheerorganisatie van een erkende oplossing onzes inziens goed passend zijn voor de toelating.
Deze procedure is (inter-)nationaal veel gebruikt in allerlei sectoren en ook toezichthouders hebben er veel ervaring mee. Hiermee wordt de zwaarte van het erkenning- en toetsingsproces meer in overeenstemming gebracht met andere, vergelijkbare compliance regimes.

Aanbeveling: beperk de rollen tot alleen die essentieel zijn voor het gebruik van BSN in het publieke domein. Erken oplossingen en maak gebruik van de toelatingsprocedures die daarbinnen al gelden.

5.6 Artikel 7. Eisen aan erkende diensten, erkende middelen en publieke voorziening

Ad lid 1-2)

In de MvT wordt veel verwezen naar uitvoeringsregelgeving, de USvE. De regels die hier gesteld worden over werking, beveiliging en betrouwbaarheid van diensten en de uitgifte van middelen hebben veel impact op de werkprocessen van de bank. Wij zien graag dat de vertegenwoordigers van de private oplossingen van eID-diensten op alle relevante uitvoeringsregelgeving geconsulteerd worden en dat gewenste wijzigingen minimaal een jaar van te voren aangekondigd worden.

Ad lid 5)

In artikel 7 lid 5 staat de kwalificatie *aanzienlijke gevolgen* voor de veilige en betrouwbare toegang tot elektronische dienstverlening. Onduidelijk is wanneer sprake is van aanzienlijke gevolgen en hoe zich dit verhoudt tot ‘ernstige, nadelige gevolgen’ uit de Wet meldplicht datalekken. In lid 6 wordt gesproken over negatieve gevolgen voor een natuurlijke persoon of een rechtspersoon. Dit verdient ook een nadere uitleg. Bijvoorbeeld, is het (tijdelijk) niet kunnen inloggen een meldenswaardig negatief gevolg. Wij stellen voor de meldplicht datalekken hier te volgen, die onzes inziens voldoende de belangen afdekt die spelen bij een eventueel integriteitsverlies.

Ad lid 7)

Op p. 42 van de MvT. wordt ook naar de eIDAS-verordening (nr. 910/2014) en meldplicht verwezen. Wij onderschrijven het uitgangspunt om administratieve lasten te beperken - zo ook de lasten die gepaard gaan met deze meldplicht - en willen dubbele meldplichten voorkomen. Onduidelijk is hoe deze meldplicht zich tot de vele meldplichten uit overige Europese en Nederlandse wetgeving (i.c. de Europese richtlijn Netwerk en Informatiebeveiliging, NIB-richtlijn, Betaaldienstenrichtlijn (PSD2), de Wet gegevensverwerking en meldplicht cybersecurity en de Wet meldplicht datalekken) verhoudt.

Aanbevelingen: richt een governance in met vertegenwoordigers van de verschillende oplossingen en stakeholders. Bespreek daarin de gewenste werking van de eID middelen en eventuele uitvoeringsregelingen die daarvoor nodig zijn. Hergebruik de bestaande meldplichten.

5.7 Artikel 8. Eisen aan bestuursorganen en aangewezen organisaties

Ad lid 1 en 2)

In de MvT lezen wij over eisen aan elektronische dienstverlening van publieke dienstverleners. Voor het stellen van veiligheidseisen voor de ICT-systemen en de verplichting tot onafhankelijke audits wordt verwezen naar een regeling bij en krachtens de wet aangewezen. Voor het allergrootste deel hebben de hier gestelde eisen echter niets te maken met eID dienstverlening en de multimiddelen strategie, maar veeleer met de processen, gegevensverzamelingen en systemen die gebruikt worden nadat een burger zich heeft geauthentiseerd. In tegenstelling tot wat gesteld wordt in de MvT staat dit los van eID-dienstverlening. De elektronische dienstverlening an sich staat immers los van het toegangsmiddel van de Gebruiker, dat dankzij de erkenning al betrouwbaar geacht mag worden.

Aanbeveling: We stellen dan ook voor de verplichte audits voor Dienstverleners uit de wet GDI te schrappen en op te nemen in andere regelgeving, voor zover dat al niet gebeurd is.

5.8 Artikel 9 Verwerking van persoonsgegevens

Ad lid 1)

Zoals nu geformuleerd, lijkt art. 9 lid 1 van het wetsvoorstel te suggereren dat private authenticatiediensten slechts gegevens mogen verwerken voor de "goede werking van de voorziening" zoals bedoeld in deze wet en niet voor andere doeleinden. Dit strookt niet met het feit dat private partijen, die private authenticatiediensten leveren, persoonsgegevens verwerken voor andere doeleinden conform het bepaalde in wet- en regelgeving, waaronder de Wbp. Erkende en niet erkende authenticatiediensten verwerken ook persoonsgegevens om bijvoorbeeld extra attributen mee te geven aan de publieke partijen die de private authenticatiediensten accepteren. Ook verwerken private partijen persoonsgegevens om deze dienstverlening binnen de kaders van de wet aan andere dienstverleners te mogen verlenen. Tot slot verwerken deze partijen persoonsgegevens voor eigen doeleinden los van het verlenen van authenticatiediensten.

Wij stellen voor deze bepaling als volgt aan te passen:

Erkende private authenticatiediensten en erkende private machtigingsdiensten, verwerken ~~slechts~~ persoonsgegevens, waaronder het burgerservicenummer, ~~voor zover dit noodzakelijk is~~ voor zover toegestaan onder meer voor de goede werking van de voorziening, bedoeld in artikel 4, eerste lid, onderdeel c. Bij het gebruik van de voorziening bedoeld in artikel 4, eerste lid, onderdeel c worden niet meer persoonsgegevens, waaronder het burgerservicenummer, verwerkt dan noodzakelijk.

Ad MvT p. 70)

In de MvT bij artikel 9 (p. 70) staat: *"Dit artikel verankert de wettelijke grondslag voor specifiek genoemde bij authenticatie betrokken erkende private diensten om persoonsgegevens, waaronder het BSN, te verwerken voor zover dit noodzakelijk is voor de goede vervulling van hun respectievelijke taken (doelbinding)."*

Opmerking 1

Volgens het huidige Wbp-regime, is een wettelijke grondslag vereist voor de verwerking van het BSN door de private partijen die private authenticatiediensten verlenen. Met inwerkingtreding van de AVG zal dit waarschijnlijk niet veranderen. De Betaalvereniging verwelkomt artikel 9, lid 1 voor zover dit ziet op de wettelijke basis die de verwerking van het BSN mogelijk maakt. Echter, een aparte wettelijke grondslag voor de verwerking van andere persoonsgegevens dan het BSN is niet nodig. De grondslag voor de verwerking van andere persoonsgegevens dan het BSN zal "noodzakelijk voor de overeenkomst" of "toestemming" zijn, beide opgenomen in art. 8 van de Wbp.

Daarnaast merken we op dat het woord "doelbinding" dat tussen haakjes staat aan het eind van de eerste paragraaf (MvT. p. 70) geschrapt zou moeten worden. Deze paragraaf gaat over de grondslagen van verwerking van persoonsgegevens, in het bijzonder gaat deze paragraaf over de grondslag voor de verwerking van het BSN, en niet over "doelbinding". De grondslagen voor de verwerking van persoonsgegevens zijn opgenomen in art. 8 van de Wbp, de specifieke vereisten voor de verwerking van het BSN zijn opgenomen in artikel 24 van de Wbp en de bepaling over doelbinding is artikel 7 en 9 van de Wbp.

Gelet op het voorstaande, stellen we voor om deze paragraaf als volgt aan te passen:

"Dit artikel verankert de wettelijke grondslag voor specifiek genoemde bij authenticatie betrokken erkende private diensten om ~~persoonsgegevens, waaronder~~ het BSN~~,~~ te verwerken voor zover dit noodzakelijk is voor de goede vervulling van hun respectievelijke taken ~~(doelbinding)~~." Optioneel kan de volgende zin hierna worden toegevoegd: “De verwerking van andere persoonsgegevens in dit kader kan worden gebaseerd op een van de grondslagen opgesomd in artikel 8 van de Wet bescherming persoonsgegevens.”

Opmerking 2:
Daarnaast geldt specifiek voor iDIN dat dit voor de rol van de bank van de Gebruiker in het BSN-domein een vreemde situatie oplevert. Momenteel zijn de banken bewerker voor de verwerkingen in het kader van iDIN in het BSN-stelsel. Voor de banken is dit een bijzondere rol gezien hun rol als verantwoordelijke ten opzichte van de BSN-verwerkingen buiten het iDIN-stelsel (bijv. renseignering bij de Belastingdienst). Gezien de belangen van gebruikers en banken lijkt het in de rede te liggen dat de banken een grotere verantwoordelijkheid krijgen met betrekking tot het verwerken van BSN in het kader van iDIN. Naar huidig recht bestaat er geen wettelijke grondslag voor de banken om onder eigen verantwoordelijkheid het BSN in het iDIN-stelsel te verwerken. Het verdient aanbeveling dat hier wettelijk ruimte voor wordt gemaakt. Wij stellen een algemene verplichting voor de banken voor om in dit kader het BSN te verwerken in de Wet Generieke Digitale Infrastructuur.

Ad lid 2)

Artikel 9 lid 2 van dit artikel moet ook conform het voorgaande (zie commentaar bij art. 9 lid 1) worden aangepast.

Ad lid 3)

De reikwijdte van lid 3 is te breed. De in dit lid bedoelde maatregel van bestuur zou slechts moeten toezien op de verwerking van het BSN. Dit lid moet worden aangepast (dit geldt ook voor de tekst uit p. 71 van de Memorie van toelichting). Zie ook de opmerkingen bij lid 1 van dit artikel.

5.9 Artikel 10. Toezicht op publieke en private diensten

Ad MvT pag. 72)

In de MvT valt te lezen dat Agentschap Telecom de beoogd toezichthouder is op de banken voor het leveren van deze dienst, “in afstemming” met De Nederlandsche Bank, de bestaande toezichthouder op dit gebied. Ook staat er dat dubbel toezicht zal worden voorkomen.
Dat is in tegenstelling tot elkaar en dubbel toezicht leidt bovendien tot onwenselijke situaties.

Voor het leveren van de bancaire authenticatiedienst wordt teruggevallen op bestaande wettelijke kaders, infrastructuur en middelen. Daarmee staan de onderdelen waar iDIN uit bestaat al onder Toezicht. Op basis van wetten (o.a. Wwft, WFT), regulations (o.a. PSD, AML) en richtlijnen (o.a. SeCuRePay) ziet DNB (en in een aantal gevallen de ECB) toe op de processen voor klant identificatie en registratie, informatiebeveiliging, (toegang tot) de betaalinfrastructuur etc. iDIN is in dat opzicht niet nieuw, maar maakt zij gebruik van wat banken al hebben, zoals de inlogmiddelen, processen en infrastructuur. En dat geldt ook voor de toezichtskaders. Gelet op het belang van deze infrastructuur in de financiële dienstverlening en het strakke toezicht van DNB hierop is een additionele Toezichthouder ongewenst. Het moeten incorporeren van de diverse wet- en regelgeving binnen hetzelfde domein is al lastig genoeg, wanneer over hetzelfde onderwerp ook naar meerdere toezichthouders gerapporteerd moet worden, wordt het ondoenlijk.

DNB houdt via de genoemde kaders ook al toezicht op het gebruik van de bancaire eID middelen in de private sector (bij private Dienstverleners), een domein dat niet gereguleerd wordt in de wet GDI. Wanneer Agentschap Telecom (of een ander) voor het gebruik van iDIN in het overheidsdomein als toezichthouder wordt aangewezen zal dat onherroepelijk tot de situatie leiden waarbij dezelfde middelen, dezelfde infrastructuur, dezelfde processen en procedures en dezelfde partijen die ze leveren onder twee toezichthouders vallen.

Een laatste zorg bij dit artikel is dat in het voorstel het beleid voor authenticatie en toezicht bij hetzelfde ministerie terechtkomen. Ongeacht de beschreven rol van de toezichthouder, AT of DNB, de Minister (van BZK) houdt de regie over toezicht, besluit over het (intrekken van) erkenning, etc. Terwijl de minister aan de andere kant tevens verantwoordelijk is voor het publieke middel. Dit is een ongewenste vermenging van rollen. Toezicht en beleid zouden 100% gescheiden moeten zijn.

Aanbeveling: voorkom overlap in toezichthouders, stel vast dat DNB deze taak vervult voor de instellingen die iDIN aanbieden. Splits beleid en toezicht volledigen dan in het huidig voorstel.

5.10 Artikel 11. Bestuursdwang en dwangsom & Artikel 12. Bestuurlijke boete

In de rede ligt dat naast erkenning en het toezicht kunnen houden op en handhaven van de afspraken die gelden voor erkende partijen, deze partijen ook moeten kunnen stoppen met de dienstverlening om welke reden dan ook, en op zijn minst als gevolg van gewijzigde regelgeving. De in dit artikel genoemde handhavingsmaatregelen zouden a priori ook enige proportionaliteit moeten laten zien ten opzichte van het geconstateerde probleem en de ruimte moeten laten voor het beëindigen van de dienstverlening.

5.11 Artikel 15. Bijzondere bevoegdheden

De tekst van lid 3 is dusdanig geformuleerd dat ieder oneigenlijk gebruik voldoende reden is om de werkzaamheden van een erkende dienst te onderbreken. Deze bepaling is onvoldoende in balans. De inbreuk moet de onderbreking wel rechtvaardigen.

5.12 Artikel 16. Informatieverstrekking

In het kader van onder meer cybersecurity zijn er sectoraal en nationaal al diverse samenwerkingsverbanden en gremia die gebruikt worden voor de in dit artikel beschreven gegevensuitwisseling. In dit kader kan onder meer gedacht worden aan het Nationaal Cyber Security Centrum (NCSC), als onderdeel van het ministerie van Veiligheid en Justitie. Wij stellen daarom voor deze gremia te gebruiken en niet een nieuw ministerie en bijbehorende informatieverplichting te betrekken bij security gerelateerde onderwerpen. Binnen de bestaande gremia en meldplichten bij toezichthouders is de benodigde expertise georganiseerd om de juiste actie uit te zetten.

5.13 Artikel 19. Leges voor publieke authenticatiedienst en publieke machtigingsdienst

Wij zijn van mening dat de leges voor publieke authenticatiediensten en publieke machtigingsdiensten in principe voor rekening dienen te komen van een Dienstverlener. Alleen indien deze gebruik wenst te maken van een ontsluitende dienst zal deze de kosten dragen en een eigen (totaal-)rekening sturen voor de geleverde diensten richting de Dienstverlener. Zie ook de eerdere opmerkingen over het rollenmodel.

5.14 Artikel 20. Doorberekening kosten publieke voorziening en toezicht

Wij maken bezwaar tegen de doorbelasting van de kosten van de centrale voorzieningen aan de erkende partijen.

Dit doorbelastingsmechanisme brengt een onnodige facturenstroom met zich mee, want de kosten zullen toch bij de Dienstverlener terechtkomen. In combinatie met artikel 21 kan de minister een

erkende partij in theorie zelfs failliet laten gaan, door te hoge kosten door te belasten en een te laag tarief daarvoor te vergoeden. Een dergelijke wettelijke ruimte is niet nodig en ook niet acceptabel.

5.15 Artikel 21. Tarifering

Wij maken bezwaar tegen de grondslag voor het vaststellen van een tarief en voorwaarden voor iDIN.

Deze bepaling geeft de minister het recht om de prijsstelling en de voorwaarden van private partijen in het publieke domein eenzijdig te bepalen. Dat is onacceptabel en past niet in een situatie waarbij private diensten geleverd worden om de overheid te ondersteunen in het realiseren van haar digitale agenda.
Het eenzijdig vaststellen van prijzen en voorwaarden door de minister heeft daarenboven ongewenste marktverstorende effecten over het gebruik van private middelen in het private domein. Daar zal immers gekeken worden naar de voorwaarden, de prijs en het gebruik in het publieke domein, waarmee deze laatste onbedoeld bepalend wordt voor het private domein.

We hebben begrip voor het treffen van algemene maatregelen die zorgen voor toegankelijkheid en laagdrempeligheid maar vindt deze concrete invulling ongepast en marktverstorend.

6. Literatuur

1. Regels inzake de generieke digitale infrastructuur (Wet generieke digitale infrastructuur) (22-12-2016)
2. Uniforme Set van Eisen Versie 1.0 (15-12-2016)
3. Uitvoeringsverordening (EU) 2015/1502 van de Commissie, van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.
4. Voortgang programma eID, brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties, van 21 december 2016.
5. Wet bescherming persoonsgegevens (1 september 2001).
6. Verordening (EU) 2016/679 van het Europees parlement en de raad, van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

7. Bijlage 1: Nieuwe technische koppelvlakken en centrale voorzieningen

7.1 Beschrijving koppelvlakken

Om uiteindelijk de polymorfie identiteit en/of het polymorf pseudoniem bij de Dienstverlener te krijgen dienen gegevens te worden uitgewisseld tussen de Authenticatiedienst en het BSN-koppelregister, en de Authenticatiedienst en de Dienstverlener. De uitwisseling van deze gegevens wordt beschreven in zogenoemde koppelvlakken. Een koppelvlak geeft de beschrijving van de technische verbinding tussen twee rollen. Ook voor het 'vullen' van de centrale voorzieningen worden deze gedefinieerd. De USvE stelt eisen aan de volgende koppelvlakken:

Koppelvlak Authenticatiedienst (Authenticatiedienst) – BSN-koppelregister:

1. Activeren van BSN gebruikers en ophalen polymorfe Identiteit en pseudoniem
2. Ophalen van versleutelde identiteit en versleuteld pseudoniem
3. Melden/ophalen van status authenticatiemiddelen
4. Melden 'remarkable activities'

Koppelvlak Dienstverlener – Toegangsdienst (iDIN).

5. Dit is het koppelvlak tussen Dienstverlener en het stelsel iDIN. Hiervoor is in het rollenmodel in de USvE de Toegangsdienst ontstaan.

Elk van de koppelvlakken wordt in meer detail toegelicht in de volgende paragrafen.

7.1.1 Activeren van BSN gebruikers en ophalen polymorfe identiteit en pseudoniem

Authenticatiediensten dienen dit koppelvlak te gebruiken voor het activeren van gebruikers. Gebruikers zullen worden geactiveerd op basis van naam, adres, BSN en geboortedatum. Na activatie wordt een polymorfe identiteit (PI) en polymorf pseudoniem (PP) teruggestuurd naar de Authenticatiedienst. Deze is nodig om BSN uiteindelijk bij de Dienstverlener te krijgen. Dit koppelvlak dient voor elke Gebruiker eenmalig te worden gebruikt.

7.1.2 Ophalen van versleutelde identiteit en versleuteld pseudoniem

Dit is een hulp service van het BSN-koppelregister als de Authenticatiedienst niet in staat is om zelf de polymorfe identiteit of polymorfe pseudoniem voor de Dienstverlener te versleutelen. Indien hiervan gebruik wordt gemaakt moet voor elke BSN-inlog deze service worden geraadpleegd.

7.1.3 Melden/ophalen status authenticatiemiddelen

De Authenticatiediensten dienen de gebruikte authenticatiemiddelen te registreren bij het BSN-koppelregister, indien dit middel nieuw is, of status wijzigt (active, suspended, revoked) e.g. als er een app geactiveerd wordt die ook voor iDIN gebruikt kan worden, of er een bankpas (die gebruikt kan worden voor iDIN) vervangen wordt. De Gebruiker kan dan op een overheidswebsite de status van al zijn/haar middelen zien. Vanuit deze omgeving moet de Gebruiker ook in staat zijn een middel in te trekken.

7.1.4 Melden ‘remarkable activities’

In het kader van fraudepreventie dienen Authenticatiediensten opmerkelijke activiteiten te melden aan een centraal fraude register. Geregistreerde activiteiten kunnen dan door dit register worden gescand voor fraude patronen.

7.1.5 Koppelvlak Dienstverlener – ontsluitende dienst

Hierbij wordt op een bepaald abstractieniveau de technische standaard gedefinieerd waar de dienst aan de Dienstverlener geleverd moet worden:

- Technische specificaties zijn SAML AuthnRequest en SAML Response (inclusief Assertion)
- Het Authenticatieverzoek/Respone mag in een container element worden verpakt (voor iDIN is dit iDx)

Dit koppelvlak blijft een (niet standaard) SAML implementatie, al is er enige implementatievrijheid in het gebruik van de standaard.

7.2 Impact ondersteuning koppelvlakken

7.2.1 Activeren van BSN Gebruikers en ophalen Polymorfe Identiteit

Het moeten kunnen controleren op de ‘betrouwbare bron’ van de BRP of de gegevens van de burger zoals die als Gebruiker bij de bank is geregistreerd, voorafgaand aan het gebruik van iDIN bij de overheid wordt onderkend. Er kunnen immers (vice versa) onbedoelde verschillen in de administratie zijn ontstaan of er kan iets aan de hand zijn met de status van de burger. Dit activatieproces is dus een proces waar banken achter staan en dat moet gebeuren. Dit activatieproces kan op verschillende manieren. Zo kunnen veel (publieke en private) partijen gebruik maken van een BRP-koppeling, waarmee op de BRP gevalideerde gegevens verkregen worden. Authenticatiediensten mogen dit op dit moment nog niet. Het BSN-koppelregister ondersteund daarom ook een zeer rudimentair activatieproces. De overwegingen aangaande het gebruik van Polymorfe identiteit staan elders beschreven.

Impact: Opslaan extra velden

Omdat er maar één PI en PP per Gebruiker is, en het BSN-koppelregister niet bij elke inlog mag worden geraadpleegd, dienen deze velden te worden opgeslagen (beide velden hebben een lengte van ~500 karakters in formaat base64). Hierbij kan worden overwogen om dit in een aparte database op te slaan zodat de impact op bijvoorbeeld het CRM kan worden geminimaliseerd.

Impact: **Mogelijk bijhouden extra consent van Gebruiker**

Indien juridisch vereist wordt dat een extra consent moet worden opgeslagen voor het activeren (associëren) in het BSN-koppelregister, moet dit consent worden opgeslagen. Dit dient nog verder te worden onderzocht.

Conclusie: Authenticatiedienst moet dit gebruiken om BSN te valideren. PI/PP ophalen is afhankelijk van de uitkomst van de Proof of Concept.

7.2.2 Ophalen van versleutelde identiteit en versleuteld pseudoniem

Indien de Authenticatiedienst ervoor kiest de hulpservice te gebruiken ontstaat er afhankelijkheid naar het BSN-koppelregister voor elke inlog. Daarnaast, als meerdere Authenticatiediensten ervoor kiezen de hulpservice te gebruiken, ontstaat er een single-point-of-failure. Deze afhankelijkheid en single-point-of-failure is vanuit de banken gezien ongewenst. Impact van dit koppelvlak is alleen relevant als Authenticatiedienst dit gaat gebruiken.

Conclusie: iDIN Authenticatiediensten gaan dit koppelvlak niet gebruiken.

7.2.3 Melden/ophalen status authenticatiemiddelen

Impact: melden status middel bij de overheid

Vereist is dat de Gebruiker zijn/haar authenticatiemiddel via een systeem van BZK kan activeren of deactiveren. De bank dient dit dus aan zijn/haar Gebruikers te ondersteunen. Hiervoor moet de Gebruiker een associatie of de-associatieverzoek kunnen starten bij de bank.

Het doormelden van elk door de burger te gebruiken middel, op het niveau dat de overheid dat lijkt te wensen is echter zeer onwenselijk. Eenmaal ‘geassocieerd’ betekent immers dat elk middel dat vanaf dat moment aan de burger wordt uitgereikt onder het geregistreerde betrouwbaarheidsniveau bruikbaar zou moeten zijn binnen de overheid, onafhankelijk van de gebruikte technische invulling (mits toegelaten), de nieuwe bankpas, of de installatie van de bank-app op een nieuwe telefoon. Als de burger wil weten welke middelen hij kan gebruiken binnen de overheid kan hij dat simpelweg aan de eigen Authenticatiedienst vragen. Onze verwachting is dat een centraal register door de burger ook niet geraadpleegd zal worden. Ook niet als er sprake zou zijn van een gecompromitteerd middel of frauduleus uitgegeven middel op naam van de Gebruiker. Bovendien ontstaat er zo weer een register waar erg veel informatie over een Gebruiker is terug te vinden binnen de Overheid, een aantrekkelijk doelwit voor hackers en phishing fraudeurs.

Conclusie: Een centraal register is ongewenst, banken houden zelf al de status van de authenticatiemiddelen bij. De nut- en noodzaak van dit register is niet duidelijk. Daarnaast is het niet aannemelijk dat Gebruikers via de overheid middelen gaan inzien en/of blokkeren of fraude gaan detecteren, het is veel logischer dat de Gebruiker direct contact opneemt met zijn/haar Authenticatiedienst. Bovendien zal er op deze manier een nieuwe rijke gegevensverzameling ontstaan bij de overheid die grote privacy en veiligheidsrisico’s met zich mee brengt.

7.2.4 Melden ‘remarkable activities’

Wat precies ‘remarkable activities’ is wordt niet in detail beschreven. Een extra transactie naar een centraal frauderegister lijkt de bedoeling, maar dat is een zware implementatie. Gebruikers hebben hier ook geen goedkeuring voor gegeven, die stemmen in met het inloggen bij de Dienstverlener, niet met het melden aan een Centraal systeem. Daarnaast hebben Authenticatiediensten zelf al uitvoerige fraudemaatregelen in plaatst.

Impact: Melden van ‘remarkable activities’

De impact van het bepalen wat opmerkelijke activiteiten zijn en het besluiten om deze, naast aan de Dienstverlener, ook aan de centrale voorzieningen van de overheid door te melden is erg groot. De toegevoegde waarde ervan lijkt nihil of zelfs negatief. De fraudesystemen van de banken zijn gebaseerd op jaren ervaring en fine-tuning. Daarin worden de laatste ontwikkelingen meegenomen om de cyber crimineel zoveel mogelijk een stap voor te blijven.
De werkelijke activiteit (wat gaat de ingelogde Gebruiker doen, wanneer hij is ingelogd?) vind plaats bij de Dienstverlener. Wanneer er een centraal beeld van Gebruikers nodig is kan beter gezocht worden naar de informatie die Dienstverleners hierin kunnen geven.

Conclusie: Er is niet duidelijk beschreven wat een 'remarkable activity' is, waarom wordt dit dan in de USvE meegenomen? Het enige extra voordeel ten opzichte van de fraudemaatregelen die banken nu al uitvoeren, is dat mogelijke inter-authenticatiedienst fraude kan worden gedetecteerd. We denken dat fraude weliswaar voorkomt, maar dat er nu andere manieren van detecteren en handelen zijn dan dat een centrale voorziening daarin kan bijdragen, Bovendien vergroot het de complexiteit en kosten, zitten er implementatie en privacy risico's aan vast en is de maatregel daardoor niet proportioneel.

7.2.5 Koppelvlak Service Provider (Dienstverlener) – Toegangsdienst

Een Dienstverlener koppelt met de technische standaard van iDIN, ook als deze in het BSN domein zit. Het vastleggen van technische uitgangspunten zoals de eisen aan het koppelvlak tussen Dienstverlener en ontsluitende dienst lijken misschien vandaag passend, maar zijn gelijk beperkend in toekomstige ontwikkeling en innovatie. Voor de banken is dat ook heel belangrijk in verband met het in de toekomst kunnen migreren naar andere/ betere standaarden, en het leveren van eventueel gewenste aanvullende diensten of combinaties van diensten.

Het toch willen opleggen van een standaard lijkt ingegeven door een wens de impact voor een Dienstverlener beperkt te houden, maar dat kan ook op andere manieren:

- iDIN wordt geleverd met ondersteuning bij implementatie in de vorm van software libraries in meerdere ontwikkeltalen en later mogelijk ook plug-ins;
- Softwarepartijen worden apart voorbereid waardoor bij de standaard leveranciers de benodigde componenten al aanwezig zijn;
- Juist in de verdere doorontwikkeling zullen stappen naar eenvoudiger talen en protocollen gezet worden, waardoor het ingewikkelde SAML verlaten zou kunnen worden.

Conclusie: Beperkingen leggen op het koppelvlak tussen de Dienstverlener en ontsluitende dienst remt innovatie en doorontwikkeling. Daarom is dit zeer ongewenst.

8. Bijlage 2: bevindingen Proof Of Concept Polymorfe Pseudoniemen

8.1 Algemeen: complex en gebruik van niet bewezen standaard

Om uiteindelijk een pseudoniem of BSN bij de Dienstverlener te krijgen dienen cryptografische handelingen te worden uitgevoerd die een hoge mate van complexiteit hebben en nog niet op grote schaal in de markt worden toegepast. Dit geeft de volgende bevindingen:

- De cryptografie heeft zich nog niet op grote schaal bewezen. Er zijn erg weinig implementaties van deze techniek, en al helemaal geen in high-speed high-volume transactie omgevingen zoals die voor eID gebruikt moeten worden. De vraag is of partijen op dit moment wel het risico durven te lopen met deze technologie te willen werken. De fouten zullen niet zozeer in de theorie zitten, maar in software implementaties. Hier zijn (nog) geen standaard implementaties voor. Het bezwaar hierbij is dat er nog kinderziektes in software implementaties zullen zitten wat de nodige extra implementatie last met zich meebrengt voor alle partijen. De werking in high performance architecturen dient ook nog te worden aangetoond.
- Er zijn geen standaard software bibliotheken beschikbaar die de handelingen kunnen uitvoeren omtrent versleutelen en ontsleutelen van de polymorfe identiteiten en pseudoniemen. Een standaard ontwikkel-werkwijze is daarmee onmogelijk en hiervoor dienen partijen (zowel afnemers als aanbieders van eID diensten) zelf cryptografische software te schrijven. Dit is zeer onwenselijk gezien de beperkte kennis en expertise bij partijen op dit heel specifieke technische terrein. De inspanning om dit te realiseren is daardoor veel groter dan gebruikelijk, zoals bijvoorbeeld in de huidige eID pilots.
- Ook de kennis (in de markt) op het gebied van de nieuwe complexe cryptografie is zeer schaars. Dit betekent dat slechts een zeer beperkt aantal individuen (in Nederland) weten hoe het echt werkt, en waar mogelijk beveiligingsrisico's zitten. Ook hoogopgeleide en ervaren softwareontwikkelaars en security experts hebben veel moeite om de werking hiervan te begrijpen. Dit heeft tot gevolg dat in de realisatie van deze techniek alle partijen geconfronteerd zullen worden met dure inhuurkrachten en vermoedelijk ook nog moeten wachten tot de schaarse resources weer beschikbaar komen. Deze kosten zullen uiteindelijk ook doorbelast worden in de kosten van de dienstverlening.

8.2 Impact Dienstverlener

Voor het ontsleutelen van een EI/EP naar een BSN of Pseudoniem wordt gebruikt gemaakt van OAEP-padding. Deze padding wordt ook gebruikt binnen iDIN in combinatie met RSA sleutelmechanisme. Het probleem is echter dat er geen library beschikbaar is die los deze padding ondersteunt. Deze zal dus speciaal voor dit gebruik moeten worden ontwikkeld. Voor de POC heeft Eric Verheul deze padding software geschreven in Java. Naast de OAEP-padding moet de Dienstverlener ook gebruik maken van Elliptische Curve Cryptografie (ECC). Voor generiek ECC zijn wel libraries beschikbaar, echter de manier waarop het binnen de USvE wordt toegepast niet.

Impact: geen standaard software, extra sleutel beheer koppelingen, meer eigen ontwikkeling en integratie. Grotere afhankelijkheid van consultancy / marktpartijen.

Conclusie:

- Het wordt zeer lastig voor de Dienstverlener om zonder gebruik te maken van de iDIN software libraries een Pseudoniem of BSN te bemachtigen;
- De bestaande iDIN software libraries worden aanzienlijk verzwaard en complex;
- Omdat het geen open standaard is zal het aansluiten van Dienstverleners veel extra (doorloop-)tijd en inspanning kosten, wat zonder ondersteuning van marktpartijen / consultancy eigenlijk niet meer zelfstandig kan.
- Ook voor Dienstverleners wordt het Europese level playing field verlaten door het stellen van specifieke detail invulling.

8.3 Impact voor banken in de rol van Authenticatiedienst

De Authenticatiedienst zal een aantal dingen moeten doen die rechtstreeks gerelateerd zijn aan de Polymorfe encryptie en pseudonimisering. Daarnaast hebben andere punten van de USvE natuurlijk nog impact, maar die worden hier niet meegenomen.

Voor het ophalen van het PP/PI dient een nieuw koppelvlak ondersteund te worden. Omdat dit proces uiteraard alleen met instemming van de gebruiker mag gebeuren zal er een proces ontworpen moeten waarin de Gebruiker dit kan initiëren. Dit kan het beste door een iDIN transactie te starten vanaf een speciaal daarvoor ingerichte Overheidswebsite, analoog aan het activatieproces in de pilot, maar onduidelijk is of dat kan. Anders dan bij de pilot zal er ook een tweetal gegevens teruggegeven worden aan de bank in de rol van AD. Deze gegevens zijn samen met een zestal (stelsel-) encryptiesleutels nodig om het BSN of pseudoniem voor Dienstaanbieders te kunnen leveren.

8.3.1 Gecompromitteerde sleutels en het gebruik van een HSM

Het sleutelmechanisme dat voorgesteld wordt behorende bij het gebruik van de polymorfe identiteiten en pseudoniemen is zeer complex. Voor een Authenticatiedienst zijn er maar liefst zes sleutels van toepassing waarvan enkele met het gehele stelsel zijn gedeeld. Verlies hiervan betekent dan ook dat daarmee het gehele stelsel (alle eID oplossingen, op dit moment DigiD, Idensys en iDIN) gecompromitteerd kan raken. Dat betekent potentieel een veiligheidsrisico voor alle authenticaties bij de overheid (met identiteiten (BSNs) en pseudoniemen).

Een manier om dit tegen te gaan is de voorgeschreven Hardware Security Module (HSM). Deze wordt nu voorgeschreven voor Authenticatiediensten. Voor het afdekken van het risico van gecompromitteerde sleutels wordt dit ook onderschreven, al blijft het risico wel aanwezig. Het voorschrijven van HSM brengt echter wel zeer hoge instapkosten met zich mee. Afhankelijk van de high volume high speed infrastructuur en de capaciteit van de HSM's zullen er mogelijk meerdere

HSM's voor een bank ingezet moeten worden, waarbij een bank doorgaans drie rekencentra heeft voor iDIN, dus maal drie. Een HSM is in aanschaf en implementatie erg duur, net als in beheer. Door het specifieke karakter van deze techniek is het onduidelijk welke HSM leveranciers al een werkende oplossing kunnen bieden.
Dit bij het polymorfe identiteiten en pseudoniemen behorende sleutelmechanisme is daarom zeer kostenverhogend, wat zeker voor wat kleinere partijen economisch onverantwoord is. Gebruik blijven maken van het BSN koppelregister voor deze functie lijkt zeer onwenselijk omdat daarmee het single point of failure en de privacy hotspot (alle inlogberichten via het BSN koppelregister) blijven bestaan.

Ook een Dienstverlener krijgt te maken met een ingewikkeld sleutelregime met meerdere sleutels die op de juiste manier gebruikt moeten worden en ververst. Verlies hiervan betekent echter niet direct een risico voor het hele stelsel, een HSM is dus niet direct noodzakelijk.

Het mechanisme is inhoudelijk beoordeeld door de specialisten van de verschillende banken en daaruit zijn de bezwaren geformuleerd. Het belangrijkste is dat het geen open standaard is, dat de techniek zich nog niet heeft bewezen in een high performance architectuur en dat de kennis in de markt over deze complexe techniek nu te beperkt is. Ook blijft er een afhankelijkheid van een "Master Key" bij BZK en van sleutelrisico's bij andere aanbieders, wat doet denken aan Diginotar-achtige risico's. Dat is onacceptabel.

De impact in dit geval is dus een nieuw koppelvlak, 2 opgeslagen gegevens per gebruiker, software die dit verwerkt voor de Dienstverlener, een werkend sleutelmechanisme, met een afhankelijkheid extern en een zestal sleutels in een HSM infrastructuur.

Conclusie: het is geen open standaard, de impact is erg groot, onduidelijk is of de benodigde HSM's wel beschikbaar zijn, en er zitten cruciale risico's inherent in het systeem. Dit werkt niet alleen kostenverhogend maar brengt door haar onvolwassenheid allerlei implementatierisico's met zich mee. Dit is nu niet in te voeren.

8.4 Geen privacy winst ten opzichte van iDIN

Om te beoordelen welke privacy winst er mogelijk behaald kan worden voor iDIN in het BSN domein met polymorfe identiteiten en pseudoniemen is het noodzakelijk om goed te begrijpen welke privacy winstpunten hiermee beoogd zijn. Omdat het gebruik van polymorfe identiteiten en pseudoniemen als idee ontstaan is binnen de Idensys oplossing kan de uitgangsituatie voor iDIN dermate anders zijn dat de beoogde winstpunten voor iDIN anders uitpakken of niet van toepassing zijn.

Voor zover valt te achterhalen zijn binnen Idensys de volgende redenen geweest voor het gebruik van de polymorfe cryptografie:

- Versleuteling / Encryptie van het BSN ten behoeve van de Dienstverlener;
- Het voorkomen van een 'hotspot' in de inloghistorie van burgers;
- Het voor de Authenticatiedienst "anoniem" kunnen inloggen;

- Het niet hoeven opslaan van BSN bij de Authenticatiedienst;
    - Authenticatiedienst hoeft niet te beschikken over het BSN om deze te leveren aan de Dienstverlener. Namelijk de polymorfe identiteit wordt door de Authenticatiedienst opgeslagen en deze is door de Authenticatiedienst niet herleidbaar tot het BSN. Daarnaast is de polymorfe identiteit verschillend voor elke Authenticatiedienst bij dezelfde Gebruiker.
- Ten behoeve van generieke voorzieningen zoals:
    - Centraal systeem voor fraudemonitoring
    - Centraal systeem voor inzage transacties
    - Centraal systeem voor aangemelde middelen

Het gebruik van polymorfe pseudoniemen biedt de volgende voordelen:

- inloggen, op zelfde account, ongeacht de Authenticatiedienst
    - Omdat het pseudoniem dat in USvE gebruikt wordt technische gebaseerd is op het BSN is deze onafhankelijk van Authenticatiedienst.

8.4.1 Versleuteling met standaard technieken

Op het gebied van technische encryptie is het nu al heel goed mogelijk om het BSN zo te versleutelen dat alleen de Dienstverlener deze kan ontsleutelen. In iDIN wordt een twee-laags versleuteling (op attribuut en verbinding) toegepast waardoor veiligheid en betrouwbaarheid geborgd zijn in de oplossing. Hiervoor wordt een ‘standaard’ public-private key versleuteling gebruikt, waardoor je zeker stelt dat alleen de Dienstverlener (houder van de private key) bij de gegevens kan.

De encryptie technologie die in de huidige USvE voorgesteld wordt is op dit moment nog niet volwassen genoeg en niet of nauwelijks in de markt verkrijgbaar. Bovendien worden er hardware componenten vereist (één of meer specifieke HSM boxen; hardware security module), die op dit moment nog niet beschikbaar zijn. Hierbij zijn kosten voor aanschaf en invoering en gebruik nog onduidelijk.

Conclusie: er kan worden gesteld dat vanuit het oogpunt van beveiliging de polymorfe identiteit of pseudoniem niet noodzakelijk is en alleen maar risico’s, kosten en vraagstukken meebrengt.

8.4.2 Het voorkomen van een ‘hotspot’ in de inloghistorie van burgers

De hotspot voor inloghistorie is als PIA issue binnen de Idensys/ETD beoordeling naar boven gekomen als knelpunt. Omdat in de huidige oplossing de authenticatie via elke AD door het BSN koppelregister vertaald wordt naar het BSN ten behoeve van het inloggen bij een Dienstverlener ontstaat daar een punt waar inderdaad alle inlogtransacties van alle burgers in het BSN domein op BSN niveau beschikbaar is. Dat geeft risico’s als een overheids-‘big brother’, datalekken, gevoeligheid voor hacking, etc, naast het technische risico van een single point of failure. In de nieuwe opzet (USvE 1.0) is dit niet langer noodzakelijk omdat (in principe) slechts éénmalig het BSN-koppelregister een rol speelt, bij de activatie en uitgifte van de PI en PP (tenzij Authenticatiediensten de omzetting nog steeds door het BSN-koppelregister laten uitvoeren).

Voor iDIN was het gebruik van een centrale voorziening voor het leveren van BSN's bij inloggen überhaupt niet noodzakelijk, banken kennen het BSN van de burger al omdat zij dat moeten registreren in het kader van de fiscale wetgeving (AWR) en kunnen (na succesvolle activatie) dat versleuteld voor alleen de Dienstverlener, uitleveren. Het is dus niet noodzakelijk en zelfs niet gewenst dat de inlog transacties alleen via het BSN koppelregister gaan. Dienstverleners die dat willen kunnen daardoor ook een rijkere gegevens-set ontvangen (bijvoorbeeld ook contactgegevens zoals email en telefoonnummer, als de burger daarmee instemt) en kunnen ook éénmalig het BSN ontvangen en daarna inloggen met een pseudoniem dat binnen iDIN wordt gebruikt, ten behoeve van dataminimalisatie.

Conclusie: een noodzaak voor het gebruik van een centrale BSN voorziening bestaat niet binnen iDIN, waardoor de hotspot niet bestaat. Een PI en PP is hierom niet noodzakelijk.

8.4.3 Het voor de AD "anoniem" kunnen inloggen

Dit is de situatie dat de Gebruiker zich online bekend wil maken, maar het moet anoniem blijven voor de Authenticatiedienst (de bank) die die dienst levert. Dat kan, maar levert bijvoorbeeld wanneer er navraag of fraude is of gewoon om verantwoording naar de Gebruiker gevraagd wordt de nodige uitdagingen. Vanuit financiële dienstverlening (zoals geborgd in de Wwft) mag een bank geen anonieme (betaal-)diensten leveren. Bij navraag (een gebruiker die belt met een vraag over een (inlog-)transactie) zal de service centre medewerker de vraag niet kunnen afhandelen wanneer er geen gegevens beschikbaar zijn. Aan de Gebruiker is dat niet uit te leggen. USvE 2.4.2 vereist ook dat de Authenticatiedienst inzage moet geven aan de Gebruiker op alle transacties die zijn uitgevoerd met het middel, o.a. ten behoeve van zelfcontrole. Dit onderschrijven we ook, maar wijzen op het conflict om de Gebruiker voor de AD anoniem te laten inloggen, wat niet onderschreven wordt.

Als het gaat om gevoeligheid van de (inlog-)informatie zoals in de zorg kan voorkomen zijn er ook andere manieren die zorgvuldigheid bevorderen. Hieronder vallen onder meer het verbod (in de licentievoorwaarden) om dergelijke informatie te gebruiken voor andere doeleinden dan die met de dienst iDIN verbonden zijn.

Banken hebben al zeer veel privacygevoelige informatie zoals op basis van het betalingsverkeer waar zeer zorgvuldig mee om wordt gegaan.

In de inlogverzoeken die de bank ontvangt (en dus kan registeren) staat alleen maar bij welke partij er ingelogd wordt, niet met welk doel of voor welke dienst. Vanuit Privacy by Design is het kennen daarvan ook voor een authenticatie niet noodzakelijk, en daarom onwenselijk. Daardoor is er maar heel beperkt informatie beschikbaar.

Conclusie: het voor de bank anoniem inloggen klinkt vanuit de privacy van de burger misschien mooi, maar is uitermate onpraktisch bij de secundaire processen van navraag en fraudebestrijding. Het zal dan ook niet op die manier geboden worden en niet de aanleiding zijn voor het introduceren van de PI en PP.

8.4.4 Het niet hoeven opslaan van naamsgegevens en BSN bij de Authenticatiedienst

Voor de Idensys partijen geldt dat deze niet zonder meer een BSN mogen opslaan. Daar lijkt een ‘wisseltruck’ met een PI en PP op zijn plaats om onder de eisen die daarmee gepaard gaan uit te komen. Banken echter moeten vanwege de Algemene Wet Rijksbelasting (AWR) al jarenlang het BSN opslaan. In de klantadministratie van de banken komt dit nummer dus gewoon voor, naast de andere identificerende klantgegevens. Dit argument voor het gebruik van het PI en PP geldt dus niet.

Conclusie: banken slaan het BSN al op en het gebruik van PPI zal dat niet veranderen. Omdat banken dan beide hebben is er geen privacy winst met het gebruik van PPI.

8.4.5 Ten behoeve van generieke voorzieningen

Hiervoor wordt verwezen naar de bijlage die de koppelvlakken beschrijft die nodig zijn voor de nieuwe publieke centrale voorzieningen. Hierin wordt aangegeven dat deze centrale voorzieningen vanuit privacy optiek en vanuit het dubbel voorkomen van functies in de infrastructuur niet gewenst zijn. Daarvoor zal het PI en PP dus ook niet hoeven te worden geïntroduceerd.

Algemene conclusie aangaande privacy, Polymorfe Pseudoniemen en iDIN: Er kan dus worden gesteld dat voor alle beoogde winstpunten voor het gebruik van de polymorfe identiteiten en polymorfe pseudoniemen voor iDIN geen privacy winst oplevert. iDIN is in zichzelf al zodanig privacy vriendelijk ontworpen dat er geen extra maatregelen noodzakelijk zijn, en zeker niet dergelijke ingrijpende. Dit is ook niet vreemd, want zoals al eerder gesteld is het een aanbeveling op basis van de PIA van Idensys, niet van iDIN. De PIA’s en privacy analyses van iDIN hebben nooit aanleiding gegeven voor een dergelijke oplossing.