VERDONCK KLOOSTER & ASSOCIATES

# EXPERT OPINION PUBLIEKE AUTHENTICATIE

**Advies over implementatiestrategie DigiD Substantieel en Hoog en alternatieven**

VERDONCK KLOOSTER & ASSOCIATES

# EXPERT OPINION PUBLIEKE AUTHENTICATIE

Advies over implementatiestrategie voor DigiD Substantieel en Hoog en alternatieven

**Mark Beermann, Robert Garskamp, Jaap Kuipers, Esther Makaay, Maarten Wegdam en Kick Willemse. René van den Assem (redactie)**


| | |
|---|---|
| DATUM | 23 november 2017 |
| STATUS | Definitief |
| VERSIE | 1.0 |
| PROJECTNUMMER | 20174449 |
| INTERNE TOETS | Johan van den Bosch |

# INHOUDSOPGAVE

# MANAGEMENT SAMENVATTING

In dit rapport buigt een groep authenticatie-experts zich over de huidige implementatiestrategie voor publieke authenticatie op de niveaus eIDAS Substantieel en eIDAS Hoog. Is het een goede strategie of is aanpassing of aanvulling gewens? En wat zijn eventuele alternatieven?

De experts geven aan dat de huidige strategie voor DigiD Substantieel goed is en dat de thans beperkte doelgroep dient te worden verbreed door aanvullende enrollment-methoden voor de DigiD app in te voeren. Daarbij wordt er verwezen naar een Logius-onderzoek dat de experts overigens niet hebben.

Om op het niveau eIDAS Substantieel niet geheel afhankelijk te zijn van DigiD en dan met name de DigiD app, kan de markt worden uitgedaagd om een alternatieve oplossing aan te dragen.

Voor DigiD Hoog wordt de huidige implementatiestrategie in mindere mate onderschreven. Gebruikersvriendelijkheid en tempo worden als minder goed ervaren. Derhalve wordt aangeraden om een geheel mobiele variant van DigiD Hoog te ontwikkelen. De huidige ontwikkelingen voor DigiD Hoog, zoals het opnemen van applets op NIK en rijbewijs, kan ongestoord doorgang vinden. Alleen wordt de variant op basis van een aparte NFC-reader als minder kansrijk gezien vanuit het perspectief van gebruikersvriendelijkheid.

Voor een mobiele versie van DigiD Hoog worden twee oplossingsrichtingen gezien:

- Een SIM-oplossing en een
- Centrale oplossing, waarbij Secure Elements van mobiele toestellen worden nagebootst.

In de centrale oplossing kunnen de bezwaren van het centrale karakter effectief worden ondervangen door *multi-party computing* technieken toe te passen (*split key* en *treshold* systemen). Ook kan van specifieke hardware ondersteuning in mobiele apparaten gebruik worden gemaakt (TrustZone op Android toestellen en Secure Enclave op de iPhone).

We stellen voor om deze oplossingsrichtingen verder te detailleren in een ‘buitenboordmotor’ model, losjes gekoppeld aan de huidige ontwikkeling en ontwikkelaars en onder de regie van het ministerie van BZK. Het produceren van een haalbaarheidsstudie inclusief architectuurschets is dan de scope van de activiteiten, waarbij veel expertise van buitenaf wordt ingebracht op het gebied van mobiele oplossingen, multi party computing technieken en security. Niet alleen de technische haalbaarheid, maar nadrukkelijk ook de haalbaarheid in de markt en de gebruikersvriendelijkheid worden daarbij onderzocht.

Aanvullend bevelen de experts aan dat DigiD van dynamische authenticatie gebruik gaat maken. Dit biedt de mogelijkheid om meerdere authenticatiefactoren in te zetten, op basis van de risico’s bij een authenticatie. Dit biedt de mogelijkheid om in te spelen op de specifieke risico’s die rondom een enkele authenticatie aanwezig zijn. Maar bovendien biedt het de mogelijkheid om

een *lifecycle* benadering toe te passen op de individuele authenticatiefactoren die binnen DigiD voorhanden zijn.

Ten slotte bevelen de experts aan om de verhouding publiek-privaat nader te bezien. Met name de mogelijkheid om op eenvoudige wijze andere (private en publieke) authenticatiemiddelen af te leiden van de DigiD middelen, wordt als wenselijk gezien.

# 1 INLEIDING

## 1.1 Aanleiding

Er is een grote behoefte aan een publiek authenticatiemiddel met een hoger betrouwbaarheidsniveau dan het huidige DigiD Midden, voor toegang tot dienstverleners in het BSN-domein. Zowel DigiD Basis als DigiD Midden vallen binnen eIDAS Laag, terwijl veel transacties bij de overheid het niveau Substantieel vragen. Een korte bestudering van de Handreiking Betrouwbaarheidsniveaus van het Forum Standaardisatie leert ons dit al. Enkele toepassingen, zoals toegang tot medische (of andere zeer gevoelige) gegevens en het direct aanpassen van basisregistraties, vragen zelfs om eIDAS Hoog. Momenteel worden toepassingen die een hoger betrouwbaarheidsniveau vereisen vertraagd vanwege het ontbreken van een breed beschikbaar (publiek) authenticatiemiddel, of wordt tijdelijk volstaan met een lager betrouwbaarheidsniveau dan strikt genomen noodzakelijk. Zo vindt VWS – in lijn met de Handreiking Betrouwbaarheidsniveaus – dat voor medische gegevens authenticatie op eIDAS Hoog nodig is, maar is men bereid tijdelijk eIDAS Substantieel toe te laten.

Naast de behoefte aan publieke authenticatiemiddelen op een hoger betrouwbaarheidsniveau speelt ook de wens om naast DigiD, nog een ander authenticatiemiddel ter beschikking te hebben, zodat ‘niet alle eieren in één mandje’ liggen. Dit is een secondaire reden voor het Ministerie van BZK om te bezien welke alternatieven hiervoor in de markt beschikbaar zijn. Om op dit punt een beeld te verkrijgen heeft het Ministerie met name een marktconsultatie geïnitieerd.

Binnen het Impuls eID programma wordt daarom ook voortvarend gewerkt aan publieke authenticatiemiddelen op het niveau eIDAS Substantieel en eIDAS Hoog. De beide huidige oplossingsrichtingen DigiD Substantieel en DigiD Hoog, kennen echter wel zwakke punten:

- De huidige oplossing voor DigiD Substantieel, Remote Document Authentication, vraagt, ten behoeve van de enrollment, om een smartphone met een geschikte NFC-implementatie en softwarematige ondersteuning. Dit beperkt de doelgroep op dit moment tot ruim 4 miljoen burgers binnen de DigiD gebruikersgroep [VKA2016]. Dit kan weliswaar nog groeien, maar voor de iPhone-gebruikers is er vooralsnog geen oplossing voorhanden. Ook is er geen duidelijkheid of en wanneer die er wèl komt.
- De beoogde oplossing voor DigiD Hoog is gebaseerd op een authenticatie-applet op een rijbewijs op NIK. Deze heeft als aandachtspunt dat er communicatie met die applet dient plaats te vinden bij elke authenticatie. Afgezien van de gebruikersvriendelijkheid hiervan, geldt dat deze communicatie via NFC dient te verlopen. Zodoende is ofwel een bruikbare NFC-implementatie op een smartphone nodig, ofwel een externe NFC-lezer, te koppelen aan bijvoorbeeld de laptop waarop de burger de digitale dienst afneemt.
  Dit introduceert ofwel een beperking van de doelgroep (wederom geen ondersteuning voor de iPhone) ofwel het introduceert de noodzaak van een externe lezer met bijbehorende problemen.

- Daarnaast duurt het zeer lang voordat een grote groep burgers ook daadwerkelijk kan beschikken over DigiD Hoog, omdat eerder is besloten om niet tot grootschalige versnelde vervanging van NIK's en rijbewijzen over te gaan, maar om mee te gaan in het natuurlijke vervangingstempo van deze documenten, die een levensduur van 10 jaar hebben.
- Weliswaar zouden zowel DigiD Substantieel als DigiD Hoog ook met een externe NFC lezer verbonden aan een laptop of smartphone gebruikt kunnen worden, maar dit gaat ten koste van gebruikersgemak en brengt kosten met zich mee. Een eerdere pilot met externe lezers was weinig succesvol omdat burgers dit te ingewikkeld vonden.

Het Ministerie van BZK heeft vanwege bovengenoemde punten besloten om te laten onderzoeken 1) hoe de genoemde zwakheden van de huidige implementatiestrategie voor DigiD Substantieel en DigiD Hoog zijn te ondervangen en 2) welke andere mogelijkheden zich aandienen voor authenticatie op de hogere betrouwbaarheidsniveaus.

Logius heeft voor de verbreding van de doelgroep van DigiD Substantieel eveneens een onderzoek lopen, uitgaande van de huidige architectuur van DigiD. Dit onderzoek richt zich vooral op aanvullende enrollment-methoden voor de DigiD app. Om overlap te vermijden ziet voorliggend advies niet op dat onderwerp.

## 1.2 Vraagstelling

Op basis van de vraagstelling van het ministerie van BZK, zijn voor dit onderzoek de volgende deelvragen geformuleerd.

Vraag 1. In hoeverre voldoen de huidige publieke authenticatieoplossingen voor eIDAS Substantieel en eIDAS Hoog, die zich kenmerken door hun koppeling aan een NFC-chip in reisdocumenten en rijbewijs?

Vraag 2. Welke externe ontwikkelingen zijn er op technologisch gebied? En welke externe ontwikkelingen zijn er in de (internationale) toepassing betrouwbare authenticatie (eIDAS Substantieel of Hoog).

Vraag 3. In hoeverre levert dat alternatieven of aanvullingen op, die kansrijk zijn om op in te zetten in de publieke authenticatie in Nederland?

Vraag 4. Hoe verhouden die alternatieven en ontwikkelingen (die volgen uit de antwoorden op vragen 2 en 3) zich tot de oplossingen DigiD Substantieel en DigiD Hoog in termen van tenminste de volgende criteria:

- Succesvolle toepassing. Wordt de ontwikkeling of het alternatief elders succesvol toegepast?

- Adoptiepotentieel. Omvang van de te ontsluiten doelgroep.
- Gebruikersvriendelijkheid. Hoe eenvoudig is de oplossing om te gebruiken c.q. welke invloed heeft de ontwikkeling op de eenvoud van gebruik?
- Waarschijnlijkheid dat hiermee eIDAS compliance wordt bereikt op niveau Substantieel of Hoog.
- Toekomstvastheid. Hoe waarschijnlijk is het dat de oplossing ook in de toekomst beschikbaar blijft?
- Standaardisatie. Kenmerkt de oplossing c.q. de ontwikkeling zich door een aanwezigheid van algemeen geaccepteerde standaarden.
- Kosten.

## 1.3 Leeswijzer

In hoofdstuk 2 is een verantwoording van het gevolgde proces gegeven. In hoofdstuk 3 zijn externe ontwikkelingen beschreven. Dit betreft technische ontwikkelingen die worden gezien op het gebied van authenticatie maar ook de ontwikkelingen die worden gezien in andere landen op het gebied van publieke toepassingen van authenticatie, gekoppeld aan tussentijdse conclusies en aanbevelingen. In hoofdstuk 4 is analyse van de huidige implementatiestrategie van DigiD Substantieel en Hoog gegeven, gekoppeld aan tussentijdse conclusies en aanbevelingen. Uit deze hoofdstukken komen enkele alternatieven naar voren die in hoofdstuk 5 worden geanalyseerd. In hoofdstuk 6 tenslotte worden de onderzoeksvragen beantwoord en belangrijkste conclusies en aanbevelingen gedaan, waarbij wordt teruggegrepen op de eerdere conclusies in hoofdstukken 4 en 5.

# 2 VERANTWOORDING

De opdrachtgever voor deze adviesopdracht, het ministerie van BZK, heeft de behoefte aan een gezaghebbend en deskundig advies over de thans gevolgde implementatiestrategie voor het publieke authenticatiemiddel op de hogere betrouwbaarheidsniveaus. Concreet betreft dat dus DigiD Substantieel en DigiD Hoog.

Deze behoefte bleek lastig in te vullen omdat in Nederland deskundigen eigenlijk altijd zijn betrokken geweest bij de ontwikkeling van deze authenticatiemiddelen of belangen hebben bij specifieke producten. Om dit probleem te ondervangen heeft Verdonck, Klooster & Associates in samenwerking met MobileMindz gebruik gemaakt van een groep experts voor de formulering van het voorliggende advies. Deze experts zijn geselecteerd op hun deskundigheid. Ze hebben alle een goed overzicht over de stand van zaken van publieke en private authenticatie-initiatieven. De experts zijn bovendien ook experts op specifieke deelgebieden zodat hun expertises elkaar op onderdelen aanvullen. De experts zijn:

- Mark Beermann
- Robert Garskamp
- Jaap Kuipers
- Esther Makaay
- Maarten Wegdam
- Kick Willemse

De formulering van dit advies is steeds op basis van consensus tussen de experts. Waar er op relevante punten geen consensus konden bereiken en wel van mening waren dat hierover een conclusie was te trekken of advies te geven, hebben we een meerderheidsstandpunt geformuleerd als advies. Het minderheidsstandpunt hebben we echter wel steeds vermeld. Om dit proces te doorlopen zijn 1 on-line en 2 face-to-face bijeenkomsten geweest met de experts, aangevuld met 3 schriftelijke commentaarrondes op het advies in wording. De procesbegeleiding hiervoor, alsmede de redactie van het uiteindelijke rapport, lag in handen van René van den Assem.

Naast het advies van de experts dat zodoende is opgetekend, is er bureauonderzoek gedaan en zijn bedrijven bevraagd die oplossingen op relevante onderdelen kunnen bieden. Ook zijn vragen uitgezet aan partijen achter diverse internationale ontwikkelingen. De procesbegeleiding hiervoor lag bij Mark Beermann van MobileMindz. Personen die inhoudelijke bijdragen hebben geleverd zijn Andre Koot (Nixu), Carlos Serratos, Jeroen Slump (AET Europe), Cor de Jonge (Justitiële Informatiedienst), Denis Joannides (OneGini), Jeroen Dijkgraaf (Belastingdienst), Pieter Verhagen (TNO), Chrisjan de Weerd (MobileMindz), Kalev Pihl (SK, Estland).

# 3 EXTERNE ONTWIKKELINGEN

## 3.1 Analyse trends

In onze omgeving zien we verschillende trends op het gebied van authenticatie. De belangrijkste achten we de volgende:

- Mobiele authenticatie
- Dynamisering van authenticatie
- Biometrie
- Blockchain
- Sterke authenticatie in PSD2
- Omnichannel identificatie en authenticatie

Deze trends worden hieronder nader geduid.

*Mobiele authenticatie*
De laatste jaren wordt de mobiele telefoon steeds meer als de 'bezitsfactor van keuze' gezien. Waar voorheen hardware tokens van een brede variëteit de markt domineerden, wordt er in authenticatieoplossingen steeds meer gebruik gemaakt van de mobiele telefoon van de gebruiker. Naarmate we meer praten over publieke oplossingen en cloud based oplossingen (Authentication-as-a-Service, AaaS), is de focus op de mobiel nadrukkelijker.

*Dynamisering van authenticatie*
Een trend is waarneembaar om niet meer één of enkele vaste authenticatiefactoren rondom één vast tijdstip te authenticeren, maar om de uitdaging van authenticatie meer als een dynamische opgave te beschouwen. Als we een inlogactie voor een bepaalde dienst zien vanaf een IP-adres en vanaf een device dat we verwachten en eerder gezien hebben, dan is de kans groot dat het een legitieme inlogactie betreft. Zien we echter een afwijking van het recente patroon, dan is het raadzaam om wat extra zekerheid te verkrijgen omtrent de identiteit van de gebruiker. Onder andere Google en banken maken gebruik van zo'n dynamische aanpak. Bij banken maakt het deel uit van een bredere analyse van gebruikspatronen in het kader van fraudebestrijding.

Een beslissing nemen op het moment van inloggen, is een waarneembare trend. Maar na het moment van inloggen liggen ook gevaren op de loer. Een andere gebruiker kan op een open sessie op een laptop of tablet verdergaan en zo onterecht gebruik maken van de rechten. *Continuous authentication* is een trend die hier een antwoord op biedt. Door voortdurend met name biometrische kenmerken te verzamelen van de gebruiker (het patroon van toetsaanslagen bijvoorbeeld), is het mogelijk om – gedurende de sessie – te concluderen dat het niet meer de legitieme gebruiker is die actief is, om vervolgens de sessie te verbreken.

De eIDAS uitvoeringsnorm is nog geheel gebaseerd op statische authenticatie (vast aantal factoren van een vaste sterkte) en formuleert hier eisen aan, waarmee er weinig ruimte lijkt te zijn voor het

faciliteren van dit soort dynamische ontwikkelingen in de publieke authenticatie. Toch is deze conclusie te kortzichtig. De eIDAS uitvoeringsnorm formuleert naast de vaste eisen aan bijvoorbeeld identiteitsverificatie in het aanvraag- en uitgifteproces ook een eis aan de sterkte van het authenticatiemechanisme. Voor eIDAS Substantieel geldt bijvoorbeeld dat dat authenticatiemechanisme bestand dient te zijn tegen aanvallen met een *gematigd aanvalspotentieel*. Voor eIDAS Hoog gelden een aantal aanvullende eisen en een eis dat het authenticatiemechanisme bestand dient te zijn tegen aanvallen met een *hoog aanvalspotentieel*. Juist dit mechanisme van het aanvalspotentieel biedt in de praktijk mogelijkheden om tenminste *de facto* en wellicht zelfs *de jure* (van de eIDAS uitvoeringsnorm, [eIDAS1502]) een hogere betrouwbaarheid van authenticatie te realiseren.

*Biometrie*
Biometrie heeft de laatste paar jaren een grote stap gezet in betrouwbaarheid maar vooral in de gebruikersvriendelijkheid en brede toepasbaarheid. Met name de gebruikersvriendelijke ondersteuning op mobiele devices is opmerkelijk. Achteraf gezien is met name de introductie van TouchID op de iPhone in 2013 als het kantelpunt te beschouwen (https://en.wikipedia.org/wiki/Touch_ID). We zien de ondersteuning van biometrische methoden nu vrij breed in mobiele devices: fingerprint herkenning, irisherkenning en gelaatsherkenning zijn inmiddels gangbaar op de mobiele devices.

Ook zien we inmiddels dat biometrie zijn weg vindt als één van de factoren in een systeem van multi-factor authenticatie in bancaire toepassingen. De ING, de Rabobank en de ABN AMRO ondersteunen dit nu, zij het dat het nog aan de individuele klant is in hoeverre die daar gebruik van wil maken. De meest gangbare benadering is dan dat het biometrische kenmerk is uit te wisselen met een PIN. Dit komt de gebruikersvriendelijkheid ten goede en het doet – mits goed geïmplementeerd – niet onder voor de beveiligingswaarde van een PIN. Naast de bekende methodes zien we in bancaire toepassing soms ook stemherkenning gebruikt. Zie ook de korte signalering van de trend in http://www.m2sys.com/blog/important-biometric-terms-to-know/biometric-technology-replacing-passwords-and-pins-in-banking/

*Blockchain, Self-Sovereign Identity*
Op het gebied van blockchain zien we met name de opkomst van de Self Sovereign Identity (SSI). Het idee hierachter is dat burgers hun eigen digitale identiteit gaan bijhouden, waarbij geverifieerde identiteitsgegevens van verschillende bronnen worden betrokken en op de blockchain geplaatst. Sommige van die gegevens kunnen vervolgens selectief ter beschikking worden gesteld aan dienstverleners die een of meerdere attributen nodig hebben. Doordat hierbij de burger met de identiteit in kwestie noodzakelijk betrokken is, weten de dienstverlener in kwestie wie de betrokken burger is die zich tracht te identificeren en authenticeren.
Er zit in Nederland ook veel energie op dit concept, zie ondermeer https://ercim-news.ercim.eu/en110/special/self-sovereign-identity-framework-and-blockchain.
Ook vanuit de overheid is er interesse en steun voor dit concept van de self-sovereign-identity (ondermeer RvIG).

Op deze wijze is blockchain een technische mechanisme waarmee (identiteits-)gegevens vanuit verschillende bronnen kunnen worden verzameld, opgeslagen en onder de regie van de burger ook weer kunnen worden vrijgegeven. Dit lost diverse problemen met digitale identiteiten op:

- Het ontbreken van één autoriteit, die alles omtrent een identiteit vaststelt. In plaats daarvan kunnen er vele autoriteiten voorkomen, die alle door hun gevalideerde (identiteits-)gegevens op de blockchain kunnen schrijven. Hiermee kan dus een ecosysteem worden gecreëerd waarin vele autoriteiten – publiek en privaat - kunnen bijdragen aan een digitale identiteit, wat veel meer in lijn is met de feitelijke maatschappelijke situatie.
- Het ontbreken van één centrale database van authenticatiegegevens die ook misbruikt zou kunnen worden of één centraal systeem of stelsel waarop ingebroken zou kunnen worden.
- Het feit dat er meerdere contexten zijn waarin een identiteit door meerdere sets identiteitsgegevens kunnen worden beschreven.
- Het volledig user-centrisch maken van het identity systeem, in lijn met de gedachte van Regie op Gegevens, zoals ook als streven benoemd in het regeerakkoord.

Hoewel in Nederland het begrip Self-Sovereign-Identity in één adem wordt genoemd met blockchain, is blockchain slechts één van de mogelijke mechanismes om een self-sovereign-identity te realiseren. Een techniek als IRMA is ook heel bruikbaar om dit voor elkaar te krijgen.

Hoewel blockchain door sommigen als dé oplossing wordt gezien voor identity management, lost de blockchain zelf het probleem van de basale authenticatie niet op. Alles start op de blockchain met een private key, waarmee de burger toegang verkrijgt tot die blockchain. De aanvraag- en registratieprocessen, alsmede de veilige opslag en verwerking van de private key blijven apart op te lossen punten. Hiervoor blijven enrollment processen en de veilige opslag van een private key noodzakelijk. Voor dat laatste wordt overigens wel gespecialiseerde hardware oplossingen aangeboden, de zogenaamde ‘blockchain wallets’.

Daarmee is de blockchain een uiterst relevante technologie voor het bredere onderwerp van de *digitale identiteit* en zeker ook voor het leveren van identificerende attributen, maar het lost het nauwere vraagstuk dat in dit rapport centraal staat niet direct op.

*Sterke authenticatie in PSD2*

Voor de fintech industrie is het een vereiste om klanten sterk te authenticeren vanuit de Payment Services Directive 2. Dat zal ertoe leiden dat nieuwe fintech-bedrijven sterke authenticatiemiddelen voor klanten zullen ontwikkelen en aan die klanten gaan uitgeven. We zien organisaties die zich bezighouden met sterke authenticatie zoals de FIDO Alliance (https://fidoalliance.org/) zich richten op deze nieuwe behoefte. Zie ook https://fidoalliance.org/wp-content/uploads/FIDO-PSD2-whr-FINAL.pdf.

*Omnichannel identificatie en authenticatie*

Gebruikers willen op meerdere platforms zoals desktop, laptop, tablet en mobiele telefoon actief kunnen zijn. Ze willen zich ook kunnen identificeren en authenticeren langs die verschillende kanalen: in apps, voor webservices, in texting applicaties, over de telefoon en ook via de balie. Authenticatiemethodes en de digitale identiteit dienen hier een antwoord op te bieden. Gebruikers willen ook over kunnen schakelen tussen kanalen in hun interactie en hier dienen de authenticatiemethoden ook bruikbaar voor te zijn: de authenticatie maakt het mogelijk de gebruiker steeds eenduidig aan een account te kunnen koppelen.

## 3.2 Internationaal gebruikte authenticatieoplossingen

In de inventarisatie van internationaal gebruikte authenticatieoplossingen wordt gesteund op een rapport dat PwC thans opstelt in opdracht van de Europese Commissie naar de adoptie van eID: *Marketing Plan to stimulate the take-up of eID and trust services for the Digital Single Market.* Wij hebben daarbij het concept gehanteerd zoals dat eind september 2017 voorhanden was.
We geven hier een overzicht van de belangrijkste punten uit dat rapport met de kanttekeningen die de experts bij dit rapport hebben gemaakt. Bovendien hebben we enkele eigen observaties gedaan aangaande internationale oplossingen.

Enkele relevante conclusies die in het conceptrapport worden getrokken zijn:

1. Adoptie wordt bepaald door (a) de ervaren toegevoegde waarde en (b) vertrouwen en veiligheid van de eID oplossing.
2. De ervaren toegevoegde waarde hangt direct samen met de toepassingen die worden ontsloten en het gemak waarmee de eID oplossing is te gebruiken.
3. De meerderheid van de toepassingen van eID liggen in de private sector. Bruikbaarheid van een eID oplossing in de private sector vergroot de adoptie derhalve significant. Het PwC rapport stelt zelfs dat dit de enige manier is om een hoge adoptiegraad te bereiken!
4. Openheid van een eID schema voor private eID operators is nodig om eID enabled toepassingen te verkrijgen in de private sector.
5. Private eID enabled oplossingen worden gehinderd door het feit dat lidstaten elk een eigen beleid kunnen voeren voor de toepassing van eID's in de private sector. Het rapport roept op tot een homogenisatie op dit punt.
6. Mobiele eID oplossingen hebben aanzienlijk betere adoptiegraden dan andere oplossingen, met name de kaartgebaseerde oplossingen.
7. In landen waar (onder voorwaarden) gebruik mag worden gemaakt van de data op de chip in identiteitsbewijzen of geverifieerd mag worden tegen een overheidsregister, ontstaat er een grotere variëteit aan eID's, voornamelijk voor mobiele devices. Een recente ontwikkeling op dit gebied is een aantal 'split-key' solutions. Die maken het mogelijk om mobiele eIDs met grote betrouwbaarheid onafhankelijk van mobiele operators te leveren. (De private key staat deels op het device en deels op een centrale server of in de cloud).

Het expert panel maakt enkele kanttekeningen bij deze conclusies:

1. Het PwC rapport is erg stellig dat een hoge adoptiegraad slechts haalbaar is bij vergaande publiek-private samenwerking. Hoewel het ongetwijfeld waar is dat de meerderheid van de toepassingen voor eID in de private sector ligt, is het PwC rapport al te stellig. Het succes van DigiD alleen al geeft aan dat er wel ruimte is voor een route als in Nederland, waarbij de publieke en de private ruimtes goeddeels gescheiden zijn.
2. Het is op te merken dat sommige EU-lidstaten via hun eID stelsel ook private toepassingen ontsluiten. Zodra er een Nederlands publiek authenticatiemiddel wordt genotificeerd en wordt aangesloten op de eIDAS-infrastructuur, kunnen deze in dat land gebruikt worden voor toegang tot die private toepassingen. Kortom: dan ontstaat de merkwaardige situatie dat een DigiD Substantieel of Hoog wel in het buitenland in de private sector bruikbaar is, maar niet in Nederland!
3. Het punt dat de mobiele eID oplossingen een superieure adoptiegraad kennen, wordt nadrukkelijk onderschreven. Veel landen zijn aanvankelijk begonnen met een smartcard oplossing, om later naar gebruikersvriendelijker oplossingen over te stappen toen succes achterbleef. Samenwerking met banken en mobiele operators zijn daarin steeds weerkerende thema's.
4. Ook het laatste punt, waarbij de mogelijkheid ontstaat om meerdere (mobiele) eID te kunnen baseren op gegevens op de chip van een ID-kaart of op gegevens in een overheidsregister, wordt nadrukkelijk onderschreven.

Hieronder vatten we enkele kenmerken van nationale eID-schema's samen, aan de hand van de volgende punten:

- de algemene aanpak voor identity management
- samenwerkingsmodel tussen privaat en publiek
- karakteristieken van de eID middelen

Tevens bezien we twee aspecten:

- De openheid van eID schema's
- De opkomst van mobile eID-oplossingen

**Algemene aanpak**

Veel EU landen zijn begonnen met een smartcard als eID. In sommige EU landen is er ook een sterke culturele basis voor de smart card: Spanje, België en Duitsland. In enkele landen is de eID card ook een verplichte ID-card voor burgers: België, Estland en Spanje.

**Samenwerking tussen privaat en publiek**

In alle landen wordt 'samengewerkt' met private leveranciers voor de levering van hardware en softwarecomponenten van eID middelen en het bouwen van de infrastructuur. Dit beschouwen we echter niet als echte samenwerking, het is de gebruikelijke opdrachtgever-opdrachtnemer relatie.

Soms gaat de samenwerking met de private sector echter verder, waarbij er twee niveaus zijn te

onderscheiden:

- de zelfstandige uitgifte van de eID middelen door private operators
- het gebruik van de eID middelen als een authenticatieoplossing voor toegang tot de private sector services.

Sommige landen vertrouwen op private operators voor de uitgifte van het eID middel met een publieke sector mandaat: Oostenrijk, IJsland, Liechtenstein, Luxemburg, Nederland en Zweden. In andere landen worden de eID middelen uitgegeven door publieke organisaties: België, Estland, Finland, Italië, Letland, Portugal en Spanje.

In enkele landen zijn er zowel private als publieke eID middelen: Oostenrijk, Finland en Noorwegen.

**Karakteristieken van de eID middelen**

In onderzoeken (bijvoorbeeld [PBLQ1]) worden de volgende eID types onderscheiden:

- gebruikersnaam-wachtwoord
- gebruikersnaam-wachtwoord met SMS verificatie
- software gebaseerde certificaten
- smartcards met contact of contactloze chips (NFC) waarop een certificaat is geplaatste
- Mobiele ID: mobiele (smart)phone of een combinatie van een mobiele telefoon met een contactloze smartcard.

NB twee opmerkingen:

- In Estland en België wordt e-handtekening functionaliteit toegevoegd om online transacties te beveiligen.
- Met name voor grensoverschrijdend gebruik wordt het betrouwbaarheidsniveau (LoA Level of Assurance) in aanmerking genomen. De LoA is afhankelijk van het enrollment proces uitgifte alsmede de sterkte van het middel en het bijbehorende authenticatiemechanisme.

**Openheid van eID**

De openheid van het eID schema voor private operators wordt in het PwC rapport aangemerkt als een noodzakelijke (doch onvoldoende) voorwaarde voor de ontwikkeling van eID-enabled applicaties in de private sector. Zoals eerder gezegd plaatsen de experts hier kanttekeningen bij. Wel is het zo, dat de openheid van een eID-schema de mogelijkheid biedt dat er meerdere vormen van een eID beschikbaar komen, zodat de gebruiker vaker een eID naar zijn keuze kan vinden. Hergebruik van eID-middelen draagt bovendien altijd bij aan het succes. Zie bijvoorbeeld de mogelijkheid van hergebruik van de social media login (inloggen op basis van het Google of Facebook account op basis van het OAuth protocol).

Er zijn drie modellen van ‘openheid’:

1. eID schema open voor private sector (België, Estland, Duitsland en Letland)
- In de meeste gevallen door een nationale eID smartcard met lage kosten voor gebruik

door de private partijen.

2. Multi-middelen (Oostenrijk)

- eID oplossing is niet afhankelijk van specifieke hardware. De eID oplossing kan worden geïntegreerd op een smartcard van zowel de private als de publieke sector. Daarnaast een mobiele implementatie van met name de digitale handtekening.

3. Uitgifte door de private sector (Zweden, Noorwegen, UK).

- Het derde model, dat het hoogste niveau van gebruik bereikt, is gebaseerd op eID middelen die worden uitgegeven door de private sector en gebruikt kunnen worden voor toegang to online e-overheids diensten.

**Mobiele eID**

Mobiele eID oplossingen lijken een ommekeer in de markt te bewerkstelligen omdat ze significante verbeteringen in gebruiksgemak mogelijk maken.
Landen die een mobiele eID oplossing hebben ontwikkeld, tonen dan ook aanmerkelijk verbeterde adoptie resultaten:

- Oostenrijk: mobiele handtekening in relatie tot de Burgerkaart (sinds 2009 actief, 500.000 gebruikers terwijl de eID kaart nooit voorbij de 100.000 is gekomen)
- Estland (Een tiende vh aantal gebruikers van de eID kaart, maar goed voor een kwart van het aantal transacties.)
- Noorwegen. (Mobiele ID sinds 2014, bij ca. 10% van de bevolking in bezit. Wel inmiddels goed voor een verdubbeling van het transactievolume)

Het succes wordt verklaard door de verschillende voordelen die mobiele eID oplossingen bieden:

- Geen specifieke hardware (readers) of software is nodig
- Burgers hebben in het algemeen hun smartphone altijd bij zich
- Mobiele eID reflecteert lifestyle, het straalt positief af op de gebruiker.

Er zijn twee implementatie modellen in gebruik:

- SIM kaart gebaseerde modellen.
- Centraal authenticatie model, bijv. in Oostenrijk

SIM gebaseerde systemen zijn nu vaak nog gebaseerd op de (relatief oude) mobile PKI-technologie. Hiervan zijn veel meer voorbeelden dan hierboven genoemd. Op de SIM wordt dan een PKI-applet geplaatst, vergelijkbaar met de smartcard (veelal conform de PKCS#15 standaard). Hiervan zijn vele voorbeelden. Mobile PKI heeft echter nooit heel grote vlucht genomen, vanwege de coördinatie met de mobiele operators die er nodig is. Een overheid moet dan onvermijdelijk met alle mobiele operators in een land samenwerken, omdat de SIM in alle opzichten wordt beheerst en beheerd door de mobiele operator. (Pas met de opkomst van de eSIM ontstaat de mogelijkheid om deze nauwe koppeling tussen SIM en mobiele operator te open te breken, zie daarvoor verderop in dit rapport.)

Relatief recent heeft GSMA Mobile Connect ontwikkeld, een raamwerk die deelnemende mobiele operators toestaat een provider van Mobile eID te worden, zie

https://www.gsma.com/identity/mobile-connect. Dit wordt inmiddels door verschillende operators opgepikt.

Ad 1. Een mooi voorbeeld van een modern Mobile ID-systeem, dat dus is gebaseerd op de SIM, is het Belgische itsme. Dit is tevens een mooi voorbeeld van samenwerking tussen banken en mobile operators, wat in Nederland meermalen enkele malen is geprobeerd maar wat tot op heden heeft gefaald.
Een ander modern Mobile ID-systeem wordt rond deze tijd in Duitsland geïntroduceerd.
Dit zijn meer recente voorbeelden dan de eerdergenoemde voorbeelden en het zijn dus ook nog geen voorbeelden waarvan nu al overtuigende gebruikscijfers voorhanden zijn.

Ad 2. Een mooi voorbeeld van een model, waarbij de digitale identiteit feitelijk centraal wordt bewaard en beheerd, is het Oostenrijkse model. Oostenrijk heeft, vanaf het moment dat men hun elektronische overheid planden (2004/2005) een sterke vorm van authenticatie en een gekwalificeerde elektronische handtekening als basisfuncties bedacht, waar elke burger over zou moeten kunnen beschikken. Hiervoor is het ontwerp van een Burgerkaart bedoeld, die oorspronkelijk beschikbaar kwam op een smartcard. Deze Burgerkaart levert bovendien identiteitsgegevens (persoonsnummers) die voor de verschillende sectoren verschillend waren om privacyredenen. Na een aanvankelijk vrij bescheiden adoptie, is besloten om een versie van de Burgerkaart op de smartphone te maken. De smartphone bevat beperkte sleutelgegevens, maar de gebruiker authenticeert zich primair aan een soort gevirtualiseerde smartcard op een centrale host, alwaar bijvoorbeeld een digitale handtekening wordt aangemaakt. Zie ook https://www.a-sit.at/pdfs/Praesentationen%20ab%202016/20160614%20EYou%20DenHaag%20Leitold.pdf en https://www.eema.org/wp-content/uploads/leitold-2.pdf.

Deze techniek lijkt in de verte ook op het model dat Digidentity implementeert om met gekwalificeerde certificaten en de digitale handtekening om te gaan (Digidentity is hiervoor gecertificeerd met dit model). Dit model is behalve voor digitale handtekeningen ook goed bruikbaar voor eID's. De techniek heeft ook overeenkomsten met Host Card Emulation, die met name is ontwikkeld om ook op telefoons zonder Secure Element toch iets van hardwareondersteuning te kunnen bieden. Met name Google en Microsoft hebben dit is samenwerking met banken geïmplementeerd om ook op low-end mobiele telefoons mobiele betalingen te kunnen bieden, zie http://www.tomshardware.com/news/host-card-emulation-secure-element,28804.html
Onmiskenbaar is deze techniek minder veilig en minder privacyvriendelijk dan een techniek waarbij er gebruik wordt gemaakt van de SIM of embedded Secure Element op de mobiel zelf, maar het is wel goed om te onderkennen dat dit een mogelijkheid biedt voor brede ondersteuning.

# 4 ANALYSE HUIDIGE IMPLEMENTATIESTRATEGIE

In dit hoofdstuk analyseren en beoordelen we de huidige implementatiestrategie voor publieke authenticatie op de hogere betrouwbaarheidsniveaus. We geven ook aan hoe nadelen eventueel zijn te ondervangen. Dit leidt tot tussentijdse conclusies en aanbevelingen.

## 4.1 Beschrijving van de huidige implementatiestrategie

De huidige implementatiestrategie is als volgt te beschrijven. Het niveau eIDAS Substantieel wordt ingevuld met een combinatie van de DigiD app en een registratieproces waarin de geschikte identiteitsdocumenten op afstand worden gecontroleerd, waarbij de burger beschikt over een geschikte mobiele telefoon met een geschikte NFC-implementatie om op die manier de identiteit die behoort bij het identiteitsdocument te controleren. Doordat op de mobiele telefoon eerder een gepersonaliseerde DigiD app is aangebracht, is de relatie tussen de mobiele telefoon, het telefoonnummer, het DigiD account en een identiteitsdocument gemaakt. In de gebruiksfase wordt volstaan met een challenge-response interactie met de DigiD app.

Voor het niveau eIDAS Hoog is er wederom een afhankelijkheid van de identiteitsdocumenten, in dit geval de NIK en het rijbewijs. Op de chip van deze documenten wordt een applet bijgeladen, waarmee de DigiD server een challenge-response interactie doet. Er is wederom een afhankelijkheid van het hebben van een NFC-lezer, eventueel kan hiervoor de mobiele telefoon worden gebruikt.

Een tweede onderdeel van de huidige implementatiestrategie is dat de komende releases van DigiD zijn gericht op de realisatie van DigiD Hoog. Pas daarna is er ruimte voor eventuele verbreding van DigiD Substantieel.
Een derde onderdeel van de huidige implementatiestrategie is de mogelijkheid om gebruik te maken van marktmiddelen voor de authenticatie in het BSN-domein. Het voornemen is dit te doen middels een eventuele aanbesteding. Ter voorbereiding hiervan wordt momenteel een marktconsultatie uitgevoerd.

## 4.2 Conclusies en aanbevelingen omtrent de huidige implementatiestrategie

Het expertpanel trekt de volgende conclusies op hoofdlijnen over de huidige implementatiestrategie:

1. De huidige benadering voor DigiD Substantieel en DigiD Hoog om identiteitsdocumenten te gebruiken wordt over het geheel genomen door de experts onderschreven, aangezien hiermee op een goede wijze hergebruik wordt gemaakt van het bestaande, zeer

betrouwbare, aanvraag- en uitgifteproces van identiteitsdocumenten.[1]

2. Ook de techniek van die identiteitsdocumenten is van een hoog niveau, zodat hierop kan worden voortgebouwd. Wel is te concluderen dat 10 jaar een erg lange periode is om technische oplossingen in de markt te hebben staan. De kans is aanzienlijk dat er zich in die periode kwetsbaarheden in die techniek openbaren, die de techniek minder of geheel niet veilig maken.
3. We merken op dat de huidige ontwikkelplannen voorzien in het realiseren van een oplossing voor DigiD Hoog, terwijl de huidige oplossing voor DigiD Substantieel geen heel breed bereik heeft (ca. 4 miljoen burgers). Dit terwijl
   - DigiD Hoog nog zeer lange tijd zal nemen voordat dit beschikbaar is voor grote groepen burgers;
   - De versnellingsmogelijkheden voor DigiD Hoog beperkt zijn, omdat dit leidt tot ongewenste pieken in met name de productieprocessen van identiteitsdocumenten;
   - Er ook geen alternatieven voorhanden zijn, waarmee de publieke authenticatie op niveau eIDAS Hoog op korte termijn is te realiseren zonder zeer hoge kosten te maken;
   - Er een acute behoefte is, met name vanuit de zorg, aan breed beschikbare authenticatiemiddelen op tenminste niveau eIDAS Substantieel en uiteindelijk eIDAS Hoog.
4. Dat maakt dat korte termijn vergroting van de doelgroep voor DigiD Substantieel belangrijk is en vanuit businessperspectief prioriteit zou moeten krijgen boven het implementeren van DigiD Hoog.
5. De gewenste vergroting van de doelgroep voor DigiD Substantieel dient vooral te worden gevonden in een verbreding van de *enrollment*-methoden voor de DigiD app. Naast de enrollment, waarbij het identiteitsdocument met NFC wordt uitgelezen op de eigen telefoon is er nog een variatie aan andere enrollment methoden mogelijk. Hiertoe loopt momenteel een onderzoek bij Logius, de resultaten waarvan echter niet bekend zijn op het moment van schrijven van dit advies. De experts onthouden zich op dit punt van advies.
6. Wel is publieke authenticatie op niveau eIDAS Hoog wenselijk op een snellere termijn dan de ongeveer 10 jaren, die voortkomen uit het natuurlijke vervangingstempo van identiteitsdocumenten. Hierop dient de implementatiestrategie nog te worden aangepast.
7. Vanuit verschillende bronnen, maar zeker ook vanuit internationale ervaringen, is een mobile first benadering aan te raden. Dit blijkt een essentiële stap om een goede gebruikerservaring te bieden. DigiD Substantieel is een voorbeeld van een mobile first strategie. In mindere mate geldt dit ook voor DigiD Hoog.

---

[1] We merken op dat er plannen zijn om te innoveren in het aanvraag- en uitgifteproces van identiteitsdocumenten. Vooralsnog is er echter wel tenminste één face-to-face identificatie voorzien in dat aanvraag- en uitgifteproces (door een hiervoor adequaat opgeleide persoon), zodat ook aan de hoge eisen van eIDAS Hoog zal worden voldaan in de afzienbare toekomst.

8. DigiD Hoog kan ook de vorm hebben van een losse kaartlezer gekoppeld aan de PC, laptop of tablet van de burger. Via de losse kaartlezer dient er met NIK of rijbewijs te worden gecommuniceerd. Dit is voor de burger een tamelijk klassieke vorm van kaartgebaseerde authenticatie en deze aanpak is in veel landen minder succesvol geweest. Een meer mobielgericht model verdient de voorkeur, waarbij de DigiD app dan het logische punt is waarop alles bij elkaar komt in de mobiel.
9. DigiD Hoog werkt met een per authenticatie weerkerende interactie nodig met NIK of rijbewijs. Dat heeft een paar forse nadelen:
    - Het duurt nog jaren voordat er voldoende geschikte NIK's en rijbewijzen onder de bevolking aanwezig zijn.
    - Ook hiervoor is een werkende NFC-oplossing nodig. Als we mobiel-centrisch willen werken, betekent dat dus NFC-ondersteuning in de smartphone. En dat brengt weer dezelfde problemen met zich mee van DigiD Substantieel, namelijk dat het aantal burgers dat we daarmee bereiken vooralsnog beperkt is (geen iPhone-ondersteuning, slechts een deel van de Android telefoons). Wel is te verwachten dat met de toename van NFC-toepassing in mobiele telefoons, deze beperking minder burgers zal betreffen.
    - De burger moet steeds zijn NIK of rijbewijs erbij halen als hij een authenticatie wil doen. Dat is weliswaar uit te leggen, maar het kan ook als minder gebruikersvriendelijk worden ervaren.
10. **Vanwege bovenstaande nadelen, is het gewenst om voor het huidige DigiD Hoog alternatieven te ontwikkelen, waarbij een mobile first benadering het meest kansrijk wordt geacht.**
11. Naast alternatieven voor DigiD Hoog, is ook de wens geuit om een alternatief te hebben voor DigiD. Het idee is daarbij dat DigiD geen *single-point-of-failure* zou mogen zijn. De grootste kans op falen is daarbij gelegen is het falen van de techniek van een enkele authenticatiefactor, bijvoorbeeld in het geval van DigiD Substantieel het falen van de DigiD app, of in het geval van DigiD Hoog het falen van de applet op de identiteitsdocumenten.

    Een aanpak is gewenst waarbij het risico van de single-point-of-failure wordt beperkt door
    - Ofwel voor individuele authenticatiefactoren achter de hand te houden die in geval van nood snel zijn te activeren,
    - Ofwel er voor individuele authenticatiefactoren reeds voorhanden en actief zijn.

    Strategische overwegingen kunnen een rol spelen bij de positionering van dergelijke alternatieve authenticatiefactoren. Stelt men bijvoorbeeld een alternatieve methode gelijk aan de 'gedachte hoofdvariant', dan loopt men de kans dat de burger het alternatief blijkt te prefereren. Ook een 'winner-takes-all' situatie zou zich kunnen voordoen, in welk geval er alsnog geen sprake is van de beoogde situatie waarin men snel tussen alternatieve authenticatiefactoren zou kunnen schakelen.
12. Bij het bovenstaande is een dynamische benadering van authenticatie zeer wenselijk. Concreet betekent dit dat DigiD aanvullende authenticatiefactoren inzet, afhankelijk van het risico dat de betreffende authenticatie-situatie met zich meebrengt. In een dergelijke benadering is ook het verminderde vertrouwen in bepaalde authenticatiefactoren goed inpasbaar.

13. De strategie om de beoogde identiteitsdocumenten nu wel reeds van een applet te voorzien waarmee te zijner tijd DigiD Hoog kan worden uitgevoerd, achten de experts zinvol. De meerkosten hiervoor (2-3 euro per document) zijn deels te beschouwen als voorinvestering in DigiD Hoog, maar ook als investering in een voorzorgsmaatregel voor het geval dat er een serieus security-probleem ontstaat met DigiD Substantieel.
14. De strategie om nu vooral eerst DigiD Substantieel breed te verspreiden staat haaks op een alternatieve strategie, waarbij het streven zou zijn om alle burgers te voorzien van een authenticatiemiddel dat technisch vanaf dag 1 geschikt is voor eIDAS Hoog en dat naar behoefte op niveau Substantieel of Hoog kan worden gebracht via een toepasselijke *enrollment*-methode. Gedacht kan dan worden aan een SIM of een smartcard. Zonder bijzondere fysieke beveiligingskenmerken en exclusief het *enrollment*-proces en versturen zou een dergelijk middel circa 5 euro per stuk kosten. Deze strategie geven de experts echter niet de voorkeur aan in verband met de hoge kosten voor een dergelijke benadering en het gegeven dat eIDAS Hoog vooralsnog niet voor alle burgers noodzakelijk is. Dit zou eerder liggen in het gebied van te onderzoeken alternatieven.

In het navolgende hoofdstuk worden alternatieve authenticatiemogelijkheden onderzocht.

# 5 ALTERNATIEVEN

## 5.1 Inleiding

In dit hoofdstuk behandelen we diverse alternatieve authenticatiefactoren en –methoden. Dit hoofdstuk kan niet geheel los worden gelezen van de tussenconclusies van de experts in het vorige hoofdstuk.

Uit het voorgaande spreekt immers een duidelijke voorkeur voor een 'mobile first' benadering. Fallback-mogelijkheden of oplossingen voor kleine specifieke doelgroepen hoeven niet zozeer op de mobiele telefoon te worden gefocust, maar de hoofdvarianten wel. *Concreet betekent dat ook dat alternatieven voor DigiD Hoog primair rondom de mobiel dienen te worden gecentreerd.*

In het navolgende behandelen we enkele soorten alternatieven, die waarbij we de toepasselijkheid van die oplossing in het licht van het bovenstaande duiden. In willekeurige volgorde betreft dit:

- Idensys dienstverlening
- iDIN dienstverlening
- IRMA
- Hardware tokens incl. crypto calculators
- Mobiele oplossingen op basis van de SIM
- Mobiele oplossing op basis van in de mobiel ingebouwde (embedded) Secure Elements
- Mobiele oplossing op basis van de in de mobiele aanwezige Trusted Execution Environment
- Mobiele oplossingen met centrale hardware ondersteuning

## 5.2 Idensys oplossingen

In het kader van eHerkenning en Idensys zijn oplossingen voorhanden en beproefd op het niveau eIDAS Substantieel. Ook zijn er oplossingen op het niveau eHerkenning 4 geregistreerd, waarmee er een aanzienlijke kans is dat die oplossingen ook voldoen aan de eisen voor eIDAS Hoog.

De meeste van deze oplossingen betreffen PKIoverheid certificaten. Wil hiermee het hoogste betrouwbaarheidsniveau worden gerealiseerd, dan zal er ook gebruik moeten worden gemaakt van veilige hardware, een zogenaamd *gekwalificeerd middel*. Waarmee we weer terug zijn op veilige smartcards of vergelijkbare hardware (USB-dongles). Digidentity heeft een complete authenticatie-app met PIN op het niveau eHerkenning 4. Digidentity heeft een face-to-face enrollment proces dat voldoet aan eIDAS Hoog.

Ten behoeve van Idensys pilots zijn er door KPN en Morpho ook apps ontwikkeld op het niveau eIDAS Substantieel. Daarbij zijn er ook enrollment methoden gehanteerd die goed schaalbaar zijn.

Het aanbod in eHerkenning en Idensys is all-in. Het omvat zowel het *enrollment*-proces als het technische authenticatiemechanisme en een makelaarsfunctie, waarop dienstverleners kunnen aansluiten. In het algemeen zijn de prijzen voor alternatieven in eHerkenning te hoog om geschikt te zijn voor brede uitrol onder burgers. In Idensys verband – dat wel gericht was op brede uitrol onder de burgers - zijn er nooit realistische prijsniveaus bepaald. De kosten worden hier dan ook niet verder gespecificeerd.

We kunnen samenvattend stellen dat via eHerkenning en Idensys geschikte technologie is ontwikkeld, die relatief snel is in te zetten. Deels betreft dit ook mobiel-gerichte oplossingen (KPN, Digidentity, Morpho). Voor eIDAS Substantieel zou dit pilotaanbod direct zijn op te schalen. Voor eIDAS Hoog is wellicht de technologie van Digidentity toepasbaar. Over de kosten voor deze technologie, in combinatie met de services van de leveranciers, is in dit stadium weinig zinvols te zeggen.

### 5.3 iDIN

iDIN is een authenticatiedienst van de samenwerkende banken. Gebruik wordt gemaakt van de authenticatiemethodes die banken al hanteren voor internetbankieren. Daarbij wordt er gesteund op het feit dat banken hun klanten kennen en ooit in persoon hebben geïdentificeerd.

Het grote voordeel van iDIN is uiteraard dat in één klap de meeste gebruikers van internetbankieren kunnen worden ontsloten. Bovendien zijn die gebruikers de authenticatiemethode van dat internetbankieren ook al gewend, dus gewenning en gebruikersvriendelijkheid zullen geen grote aandachtspunten zijn. Dit ondanks het feit dat de iDIN nadrukkelijk geen voorbeeld van ‘Mobile First’ is.

Met iDIN zijn er wel de volgende aandachtspunten:

- Prijsmodel en prijsniveau. iDIN hanteert een ‘kosten per tik’ model. De precieze kosten worden bepaald door de bank in kwestie. De eerste indicaties zijn dat een iDIN authenticatie ook wezenlijk duurder is dan een DigiD authenticatie (0,14 euro).
- Het betrouwbaarheidsniveau van iDIN. Onduidelijk is wat het betrouwbaarheidsniveau van iDIN is. Dit is vooral gelegen in de kwaliteit van de geregistreerde identiteiten, die minder transparant is dan wenselijk. Wel is op basis van het wettelijk kader duidelijk dat de identiteit van rekeninghouders ooit in persoon is geverifieerd. De technische authenticatiemethoden verschillen daarnaast per bank en zullen dus ook van bank tot bank beoordeeld moeten worden.
- De authenticatie op basis van SMS (ING) haalt daarbij waarschijnlijk het niveau eIDAS Substantieel niet, gegeven de kwetsbaarheden (afluisterbaarheid netwerk, afluisterbaarheid op smartphones), maar dit zou voor deze specifieke implementatie nader dienen te worden uitgezocht.

Samenvattend is iDIN geen alternatief op eIDAS Hoog en is het twijfelachtig of het integraal aan de eisen van eIDAS Substantieel kan voldoen. Individuele technieken van banken zouden na een formele toelating op eIDAS Substantieel als alternatief voor DigiD Substantieel inzetbaar zijn.

## 5.4 IRMA

IRMA biedt een oplossing om op een privacy-vriendelijke manier in te loggen. Bij dat inloggen onthult de gebruiker enkele relevante eigenschappen (attributen) van zichzelf, via een IRMA app op de eigen mobiele telefoon.

IRMA is wezenlijk verschillend van alle andere identity management systemen, in de zin dat IRMA een decentraal model heeft waar het gaat om de opslag van attributen. De attributen die een gebruiker vrijgeeft zijn alleen op de telefoon van de gebruiker opgeslagen en niet op de computer van een authenticatiedienstverlener of makelaar.

IRMA biedt ook de mogelijkheid om per geval te bepalen welke attributen u beschikbaar stelt aan een dienstverlener (webshop of dergelijke). Op zich is 'user consent' voor de vrijgave van attributen ook in eHerkenning / Idensys verband geregeld, maar IRMA draait er helemaal om, om dit zo veilig en privacycriendelijk mogelijk te doen. In die zin is het dus een invulling van de principes van 'Regie op gegevens'.

De IRMA app kan ook dienst doen als authenticatiemiddel, reden om hem ook hier op te nemen. De app genereert daarvoor zelf het benodigde bewijs en er zijn geen centrale partijen als authenticatiediensten en makelaars nodig om de authenticatie mogelijk te maken. Die centrale partijen kunnen de burger en zijn gedrag dus ook niet in de gaten houden.

Voor de enrollment kan de IRMA app bijvoorbeeld iDIN attributen van de gebruiker ontvangen en later ter beschikking stellen. Uiteraard zou een dergelijke combinatie in de enrollment ook gevonden kunnen worden met DigiD en/of identiteitsdocumenten. IRMA is een open systeem waarbij velerlei attributen in je eigen app verzameld kunnen worden. Nu al worden bijvoorbeeld attributen over beroepen in de zorg vanuit het BIG-register uitgegeven, waarmee je kunt bewijzen dat arts bent.

Zoals ook bij andere mobiele authenticatiemethoden, is er veilige opslag van cryptografische geheimen nodig. Elders in dit hoofdstuk presenteren we daar decentrale methoden (SIM, embedded Secure Elements, Trusted Execution Environment) en een centrale methode (Host Card Emulation of vergelijkbare technieken) voor. De IRMA-implementatie gebruikt hiervoor een methode waarbij zulke cruciale geheime informatie verdeeld wordt tussen de IRMA-app en de MijnIRMA server van de stichting. De app en de server moeten heel precies samenwerken om IRMA te laten werken. Ze hebben daar ieder alleen niet genoeg informatie voor: ze moeten samenwerken en hun eigen geheimen apart gebruiken voor een gezamenlijke berekening. Dit heet een *multi-party computation*. Vergelijkbare technieken worden ook gebruikt bij andere apps, die geen 'eigen' veilige opslag hebben op de mobiel.
In de MobileID van Estland wordt ook een vergelijkbare techniek toegepast.

IRMA is in beheer bij Stichting Privacy by Design en geeft stelt haar software onder een open source model ter beschikking.

Samenvattend is IRMA een interessant concept dat veel verder strekt dan authenticatie, maar wel degelijk ook betrouwbare authenticatie kan bieden. IRMA biedt geen specifieke oplossing voor enrollment, maar kan met verschillende methoden worden gecombineerd. Om IRMA geschikt te maken voor eIDAS Hoog, is combinatie met veilige mobiele 'dragers' nodig. De combinatie met een centrale oplossing (zie paragraaf 5.9) ligt dan het meest voor de hand gegeven de huidige implementatievorm van IRMA, maar andere technieken zouden ook gebruik kunnen worden. De kosten voor de IRMA oplossing zijn laag omdat er de basissoftware volledig vrij is gegeven.

## 5.5 Hardware tokens

In beginsel kunnen vele hardware tokens worden ingezet als bezitsfactor in een multi-factor authenticatie. In het mobile first scenario wordt daarvoor vooral de mobiel zelf ingezet. Er zijn vele hardware tokens beschikbaar. Deze zijn met name in de zakelijke markt lang de leidende methode geweest om 2-factor authenticatie te realiseren.

Populaire soorten hardware tokens zijn:

- USB-tokens. Vergelijkbaar met een smartcard, maar geen kaartlezer nodig, slechts een USB-poort.
- Keyfobs, die een One-Time-Password genereren. De gebruiker kan dit One Time Password invullen. Vaak te gebruiken in combinatie met een PIN.
- Cryptocalculatoren, waarmee een challenge-response interactie kan worden uitgevoerd. Deze worden bij veel banken gezien. Soms in een variant waarin het token is gepersonaliseerd, soms in een variant waarin een niet-gepersonaliseerd token samenwerkt met een gepersonaliseerde bankkaart.

Met hardware tokens, waarvan het gebruik beveiligd is met een PIN, zou in beginsel eIDAS Hoog haalbaar kunnen zijn. Om in te kunnen zetten op eIDAS Hoog zouden de tokens zelf of de authenticatiemethode waarin ze gebruikt worden, ook bestand moeten zijn tegen 'man-in-the-browser' aanvallen, hetgeen voor sommige modellen het geval is. De methode die de Rabobank met haar Raboscanner gebruikt lijkt hier bijvoorbeeld aan te voldoen.

Hardware tokens zijn dus vaak ingezet als bezitsfactor in 2-factor authenticatie (of multi-factor authenticatie). Traditioneel heeft elk product daarbij zijn eigen technische interface. Met de komst van FIDO U2F (Universal 2nd Factor) is hier echter ook een standaard voor.

Hardware tokens zijn niet heel goedkoop. In grote aantallen tussen de 5-10 euro voor de meest basale modellen USB tokens conform de FIDO U2F standaard (enkelstuksprijzen vanaf 15 euro). Vergelijkbare prijzen zijn haalbaar voor keyfobs met een display en zonder toetsen. Voor cryptocalculators zijn prijzen vanaf 15 euro voor een calculator met display en toetsen te verwachten, in grote aantallen. Ingewikkelder modellen zoals de Raboscanner zijn slechts goedkoop (ordegrootte 15-20 euro) te houden bij aanschaf van zeer grote aantallen.

De grootste nadelen zijn echter de wisselende vormfactoren, variatie in de werking van de verschillende modellen en de logistiek voor de verstrekking van tokens die bovendien gepersonaliseerd moeten worden door ze aan personen te koppelen.
Wisselende werking en protocollen zijn overigens met de FIDO-standaard te ondervangen, de overige punten niet.

Samenvattend zijn hardware tokens geen aantrekkelijk alternatief voor eIDAS Hoog, met name vanwege de kosten en het feit dat ze niet passen in een mobiel-centrische filosofie. Voor specifieke doelgroepen die geen gebruik kunnen maken van smartphones zou het eventueel nog wel overwogen kunnen worden.

### 5.6 Mobiele oplossingen op basis van de SIM

Zoals aangegeven hebben tenminste de oplossingen op eIDAS Hoog, maar bij voorkeur ook de oplossingen op eIDAS Substantieel hardware ondersteuning nodig in het veilig bewaren van cryptografische sleutels en het beheersen van bepaalde cryptografische operaties (authenticeren, ondertekenen), alsmede het veilig hosten van kritische toepassingen.

De allerveiligste oplossingen bestaan uit geheel gescheiden hardware, die qua security state-of-the-art is en gecertificeerd op een hoog niveau. Dergelijke hardware kennen we traditioneel als smartcard. In de mobiele omgeving spreken van een Secure Element, dat is gestandaardiseerd door GlobalPlatform. Daarbij heeft Global Platform 3 vormfactoren gespecificeerd:

- De SIM;
- De embedded Secure Element, die vast in het mobiele toestel is ingebouwd. Als alleen over ‘Secure Element op de mobiel’ wordt gesproken, wordt veelal dit embedded Secure Element bedoeld;
- De micro SD Secure Element.

Het Secure Element is van essentieel belang voor kritische *Value Added Services* zoals mobiel betalen, vervoer en digitale identiteit, waarbij de sleutels maar ook (delen van) de applicatie op het Secure Element zijn ondergebracht. De SIM en de embedded Secure Element zijn relevant als alternatieven voor DigiD Hoog. De micro SD vormfactor is nooit aangeslagen en hoewel deze interessant zou zijn voor die mobiele toestellen die een micro SD-slot hebben, moet dit toch als een theoretische mogelijkheid worden beschouwd. Bovendien zou die voor de iPhone ook geen soelaas bieden.

GlobalPlatform specificeert alle relevante standaarden om deze chips en hun capaciteiten te gebruiken en te beheren. Technisch is er – buiten het verwijderbare karakter van de SIM en de microSD – geen fundamenteel onderscheid tussen de behandeling van deze 3 vormen van Secure Element. In hun business gebruik zijn er echter wel degelijk grote verschillen.

SIM's staan traditioneel en in de praktijk nog steeds onder de controle van de mobiele operators. Dat betekent dat indien met een mobile ID-toepassing op de SIM van een operator wil plaatsen, men hiervoor de medewerking van de operator nodig heeft. De SIM zou in theorie ook door een derde partij kunnen worden beheerd in een multi-tenant model, maar dit model wordt in de praktijk weinig gezien. Dat heeft een praktische reden: wie zou er dan opstaan voor het beheer van de SIM? Maar het heeft vooral een business reden. Waarom de sleutel voor mobiele *value added services* als mobiele betalingen, transport en mobile ID bij voorbaat weggeven, als dat ook een potentiele inkomstenbron is? Is het voor een mobiele operator niet veel aantrekkelijker om die macht aan zichzelf te houden?

Een van de gevolgen is echter dat *value added services* altijd weer opnieuw dienen te worden geconfigureerd en gepersonaliseerd als men van SIM verandert. Stapt men over naar een andere mobiele operator, dan is dat tot op heden altijd het geval. In de praktijk wordt een SIM overigens beduidend langer gebruikt dan een mobiel toestel, dus dit biedt al een voordeel boven een implementatie op basis van een embedded Secure Element.

De basistechnologie voor een SIM-gebaseerde mobile ID is al geruime tijd voorhanden met leveranciers als Gemalto en G&D. Zoals gezegd is er voor een mobile ID op SIM basis altijd wel een sterke samenwerking nodig tussen de overheid en mobiele operators om dit te laten werken. Of dit lukt is cultureel en situationeel bepaald.  Daar komt bij dat meestal ook mobiele betalingen in beeld zijn als het om het vormen van een dergelijke samenwerking gaat. Dergelijke samenwerkingsverbanden zijn moeilijk tot stand te brengen en stabiel te houden. Niettemin is het in het verleden al geregeld gelukt met een mobile ID als resultaat. In het verleden ging het vaak om Mobile PKI. Voorbeelden zijn implementaties in Estland, Finland, Litouwen, Turkije maar ook bijvoorbeeld Oman. Zie ook https://en.wikipedia.org/wiki/Mobile_signature en http://www.gemalto.com/govt/customer-cases/oman-new-infrastructure.

Het Belgische *itsme®* is een moderne vorm van mobile ID op basis van de SIM, die een interessant voorbeeld kan vormen ook voor de Nederlandse situatie. Daarbij is er ook sprake van een uitgebreid samenwerkingsverband, waarbij operators en banken de kern vormen. Een functioneel interessant aspect van itsme® is ook de regie die de burger/consument heeft over het ter beschikking stellen van gegevens, waarbij uit een bredere set identiteitsgegevens kan worden gekozen. Zie voor een uitgebreidere beschrijving https://www.belgianmobileid.be/nl. Duitsland heeft met *Verimi* een vergelijkbaar initiatief. Zie https://www.db.com/newsroom_news/2017/verimi-new-registration-identification-and-data-platform-to-launch-at-the-turn-of-the-year-2017-2018-with-new-pa-en-11645.htm.

We verwachten echter dat de ontwikkelingen rondom de SIM, vooral gedreven vanuit embedded toepassingen en Remote SIM Provisioning, de traditionele verhoudingen rondom de SIM zullen veranderen. Allerhande apparaten worden uitgerust met mobiele connectiviteit en die bevatten om die reden een embedded SIM oftewel eSIM. Dit is een SIM die vast in de elektronica van het apparaat is opgenomen in tegenstelling tot de klassieke verwisselbare SIM. Om de gegevens en

toepassingen van een operator in die SIM op te nemen is een procedure nodig, genaamd Remote SIM Provisioning. De GSMA levert hiervoor de standaarden en specificaties. Mobiele operators in Nederland doen proeven met deze eSIM en Remote SIM Provisioning.

Er bestaan binnen de GSMA 2 verschillende productlijnen te weten:

1. M2M specificaties

Deze specificaties zijn bedoeld voor IoT devices/sensors en andere apparatuur waar geen menselijke interactie mogelijk is. Zie GSMA website: https://www.gsma.com/iot/embedded-sim/

2. Consumer specificaties

Deze specificaties zijn bedoeld om bijvoorbeeld een consument van een 2e SIM voorzien te behoeve van: wearables, navigatie apparatuur dus waarbij menselijke interactie mogelijk is. Zie GSMA website: https://www.gsma.com/rsp/

Meestal wordt en voor M2M of IoT van een eSIM uitgegaan die op een printplaat gesoldeerd kan worden, een zogenaamde MFF2 versie. Dit is nog maar in een enkele mobile telefoon het geval. Een interessante ontwikkeling is echter dat SIM-fabrikanten nu ook eSIM-functionaliteit in de traditionele SIM stoppen, een zogenaamde 2FF/3FF/4FF vorm factor. Deze eSIM kan gewoon gebruikt worden in de huidige verkrijgbare mobiele telefoons.

De relevantie van dit alles is niet zozeer het aantal mobiele telefoons die een eSIM ingesoldeerd hebben, wat minimaal is, maar de feiten dat:

- eSIM technologie nu breed wordt geadopteerd door operators en dat
- Remote SIM provisioning vanuit operators standaard aangeboden gaat worden

Beide trends zijn duidelijk waarneembaar.

Dit opent de mogelijkheid voor de overheid om – anders dan hiervoor – zelf actief deel te gaan uitmaken van het mobiele landschap en bijvoorbeeld een eSIM in klassiek SIM-formaat uit te gaan geven, in welk samenwerkingsverband dan ook, waarop:

- De SIM van de operator wordt geladen middels RSP
- De overheid haar eigen toepassingen inbrengt zoals een digitale identiteit, een digitaal rijbewijs etc
- Banken hun mobiel betalen toepassingen laden
- etc

Dit is een interessant perspectief omdat hiermee de afhankelijkheid van de operators drastisch gereduceerd is. Uiteraard dient de haalbaarheid van het bovenstaande idee nog wel nader te worden getoetst. Enkele gesprekken die we met opstellers van de GSMA-specificaties en leveranciers van SIM's hebben gevoerd ondersteunen deze gedachtenlijn vooralsnog.

Het evidente nadeel van een dergelijke route is nog wel dat een nieuwe SIM moet worden uitgegeven. Dit zou bijvoorbeeld gewoon per post bezorgd kunnen worden, waarna personalisatie zou kunnen plaatsvinden langs een van de twee volgende routes:

- Een afleiding van een WID-document met de DigiD Hoog applet, die dus geheel zonder menselijke tussenkomst kan worden vormgegeven. De regels van eIDAS laten een dergelijke afleiding toe, alsmede verlenging.
- Als de burger in kwestie zo'n WID-document met DigiD Hoog applet nog niet heeft: een personalisatie aan een balie bij bijvoorbeeld een gemeente.

Samengevat gaat het hier om een zeer interessante mogelijkheid, waarbij met name de eSIM-opkomst de mogelijkheid biedt om de sterke afhankelijkheid van de mobiele operators te reduceren. Hiervoor zijn diverse wegen denkbaar, waaronder het uitgeven van een eSIM in klassiek SIM-formaat, als alternatief voor de SIM van de mobiele operator.

## 5.7 Mobiele oplossingen op basis van een embedded Secure Element

Technisch lijken de embedded Secure Elements in hoge mate op SIM's. De beveiliging staat dus op een zeer hoog niveau. Ook in deze markt domineren de GlobalPlatform specificaties. De technieken om gebruik te maken van een Secure Element zijn vergelijkbaar met die door de SIM (dezelfde GlobalPlatform specs zijn van toepassing).

In tegenstelling tot de SIM, wordt de ruimte rondom de eSE bepaald door de leveranciers van mobiele hardware en de leveranciers van de operating systems, de facto dus Google en Apple. De eSE is vaak ook gekoppeld aan de NFC-functies in de mobiele telefoon. In onze verkenning is niet duidelijk geworden of het eSE in de iPhone kan worden gebruikt, buiten de aansturing van de NFC-functies om, dit lijkt niet het geval te zijn.

Veel mobiele toestellen zijn al uitgerust met een eSE, huidige cijfers geven een penetratie van meer dan 40% aan. Hoewel embedded Secure Elements op termijn wel interessant kunnen worden, nemen we ze in de beschouwing hier verder niet mee.

## 5.8 Mobiele oplossingen op basis van een Trusted Execution Environment

De behoefte aan hardware ondersteuning voor de beveiliging van bepaalde gegevens is evident uit het voorgaande. Zoals ook duidelijk is, bieden de SIM en de embedded Secure Element (eSE) hiervoor zeer sterke kwaliteiten: state-of-the-art security, aparte hardware, gecertificeerd tot op hoog niveau.

Uit deze verkenning is echter ook duidelijk dat:

- De SIM weliswaar in elke mobiele telefoon zit, maar daarmee nog niet in elk mobiel apparaat met genoemde security behoefte.
- Het gebruik van de SIM tot op heden gedomineerd is door de mobiele operators.
- De eSE nog in lang niet alle mobiele apparaten aanwezig is.
- Het gebruik van de eSE nog weinig vlucht heeft genomen.
- De bruikbaarheid van de eSE wordt (mede) bepaald door de leverancier van het operating system op het mobiele apparaat.

Dit maakt dat er nog steeds sprake is van een ongedekte behoefte. In deze behoefte wordt voorzien door de Trusted Execution Environment. Dit is een concept dat is gestandaardiseerd door GlobalPlatform, de standaardisatieorganisatie die ook SIM's en Secure Elements met succes heeft gestandaardiseerd. Hiermee wordt een apart compartiment in de processor en het hoofdgeheugen gecreëerd. Denk aan de TEE als een soort 'poor man's Secure Element' en/of als buffer tussen de algemene operating system omgeving op de mobiel en de veilige doch beperkt aanwezige Secure Elements.

In de praktijk is de invulling van het TEE-concept met behulp van de TrustZone-techniek in ARM-processoren relevant. De ARM-processoren domineren namelijk de mobiele markt: meer dan 90% van de smartphones bevat een ARM-processor.[2] Apple gaat in haar iPhone nog een stap verder en biedt daar de nog sterker beveiligde techniek van de Secure Enclave. (Sterker dan de standaard TrustZone feature van de ARM-processoren. Men heeft een aparte processorkern gerealiseerd voor security operaties, zoals opslag en behandeling van biometrische gegevens).

Een sterk punt is dat een moderne versie van de ARM-processoren in een zeer groot deel van de mobiele toestellen zitten en dat er een soort TEE op die processoren zit, de zogenaamde TrustZone-functie. Hiermee is het mogelijk om apps met security-kritische functies met veilige hardware te ondersteunen op alle moderne Android telefoons.

Helaas is de TrustZone echter niet bruikbaar op iPhones wegens beperkingen in iOS.
Apple heeft de Secure Enclave, een aparte security subprocessor, geïntroduceerd. TrustZone en Secure Enclave zijn technisch echter niet compatibel.

In de praktijk zijn er aanvullende producten nodig om deze speciale hardware eigenschappen te kunnen gebruiken. Trustonic is een partij die software levert die gebruik maakt van de TrustZone op ARM-processoren. Voor iPhones is een aparte software stack nodig indien de Secure Enclave wordt toegepast. Een vergelijking van de features en de licentiekosten van beschikbare producten is echter niet gemaakt in het kader van deze verkenning.

Al met al lijkt de TEE een breed beschikbare en bruikbare technologie waarmee het eenvoudiger wordt om kritische gegevens op de mobiele telefoon te beschermen. Vooralsnog lijkt TEE – op zichzelf toegepast - onvoldoende om aan de eisen van eIDAS Hoog te voldoen. In ieder geval zijn de oplossingen op basis van SIM en (embedded) Secure Element gecertificeerd of certificeerbaar op een beduidend hoger niveau.

---

[2] Opgemerkt wordt dat ARM niet zelf processoren maakt, maar uitsluitend de architectuur en specificaties van de processoren. In de mobiele markt zijn het dan leveranciers als Qualcomm die de feitelijke chips maken. Er is beperkte concurrentie van alternatieve chip-architecturen. Intel heeft met name getracht x86 chips in de mobiele markt te introduceren, maar met weinig succes.

Zie ook: https://www.globalplatform.org/mediaguidetee.asp, http://sec.cs.ucl.ac.uk/users/smurdoch/talks/rhul14tee.pdf, https://www.trustonic.com/solutions/, https://www.blackhat.com/docs/us-16/materials/us-16-Mandt-Demystifying-The-Secure-Enclave-Processor.pdf en https://en.wikipedia.org/wiki/ARM_architecture#TrustZone.

### 5.9 Mobiele oplossingen met centrale hardware ondersteuning

Zoals we ook hebben gezien met IRMA en eerder de Oostenrijkse mobiele onderteken oplossing, zijn er ook methoden om te steunen op centrale hardware om de security eigenschappen van de mobiel te ondersteunen. Vaak wordt hiervoor een Hardware Security Module (HSM) gebruikt.

Eén zo'n dergelijke techniek is Host Card Emulation (HCE), waarbij met behulp van de centrale server een Secure Element op de mobiel wordt nagebootst. Deze techniek wordt bijvoorbeeld door Google gebruikt om veilige betalingen te faciliteren, waarbij het vanaf Android 4.4 op de mobile is ondersteund. Mastercard ondersteunt deze werkwijze. Zie ook http://www.tomshardware.com/news/host-card-emulation-secure-element,28804.html, https://newsroom.mastercard.com/press-releases/mastercard-to-use-host-card-emulation-hce-for-nfc-based-mobile-payments/ en https://www.emerce.nl/achtergrond/ingpilot-opmaat-grootschalige-introductie-mobiel-betalen.

Het grote voordeel van een dergelijke aanpak is dat die mogelijk is voor alle smartphones. Overigens heeft de HCE-techniek zelf dit bereik niet, deze is uitsluitend geschikt voor alle Android toestellen en dus niet voor iPhones. Maar een gecentraliseerd concept in het algemeen is wel toepasbaar voor zowel Android als iPhone toestellen. Naast een groot bereik kent een dergelijke aanpak vrij lage kosten vergeleken met aanpakken waarbij we de gebruiker voorzien van hardware (SIM, hardware token).

Een nadeel van een dergelijke techniek is het centrale karakter, waardoor de uiteindelijk bereikte security en privacy minder zijn dan in het geval van het gebruik van een SIM of Secure Element hardware op de mobiel. Dit kan ondervangen worden door een vorm van *multi-party computing* tussen de centrale omgeving en de mobiel toe te passen, zoals we al zagen bij de behandeling van IRMA. Wordt dit goed uitgevoerd, dan kan de server niet zomaar optreden namens de gebruiker en kan ook een dief van een mobiel zich niet succesvol uitgeven namens de gebruiker. Inhoudelijk kan multi-party computing op meerdere wijzen worden geïmplementeerd, onder meer door *split key* systemen of zogenaamde *treshold* systemen. Hiermee zijn de bezwaren van het deels centrale karakter van de oplossing te ondervangen.

Als we de bovenstaande route met *multi-party computing* volgen, blijven er nog steeds te beveiligen cryptografische geheimen en operaties in de mobiel over. Hoewel minder kritisch dan in een aanpak die geheel op decentrale basis is opgezet, is het toch prettig als die beveiligd kunnen worden. Technieken als de TEE uit de vorige paragraaf (TrustZone en Secure Enclave) zouden kunnen worden gebruikt. Maar ook technieken als *device fingerprinting* zouden bruikbaar zijn, zodat ook de mobiel zelf wordt geauthenticeerd. Technieken voor *device fingerprinting* bestaan

wel, bijvoorbeeld met toevoegingen van Intrinsic ID. Deze technieken zijn inhoudelijk interessant maar vooralsnog niet breed ondersteund.

Al met al is een centrale oplossing die een Secure Element nabootst een interessant alternatief dat waarschijnlijk ook aan de eisen voor eIDAS Hoog zal kunnen voldoen. Er zijn ook diverse oplossingen voor, die in het domein van de elektronische handtekeningen eerder de status 'gekwalificeerd' hebben gekregen. De kans dat daarmee ook aan de eisen voor eIDAS Hoog wordt voldaan, is aanzienlijk. Versterking met een multi-party computing architectuur en gebruik van hardware beveiliging op de lokale mobiel worden echter wel als wenselijk gezien door de experts.

### 5.10 Positionering van de alternatieven

Alles overziend is het volgende te zeggen over de positionering van bovenstaande alternatieven:

1. Idensys varianten zoals ontwikkeld door Digidentity, KPN en Morpho zijn bruikbaar als alternatieven voor DigiD Substantieel, waarbij in het enrollment proces gebruik wordt gemaakt van videoregistratie en een of meer selfies, naast de gegevens van een identiteitsdocument.
2. Bij het *enrollment*-proces met videoregistraties en selfie kan de kanttekening worden gemaakt dat technieken als *morphing* en *real-time video re-enactment* een bedreiging vormen voor deze techniek, wat deze minder toekomstvast maakt.
3. iDIN zou in beginsel ook geschikt kunnen zijn als alternatief voor DigiD Substantieel, met dien verstande dat er veel onduidelijkheid is over het met iDIN gerealiseerde betrouwbaarheidsniveau. Het lijkt daarom thans meer geschikt als fallback-variant dan als volwaardig alternatief, in ieder geval tot het moment dat een formele toets aan de eIDAS eisen voor niveau Substantieel heeft plaatsgevonden.
4. Binnen de Mobile First benadering zijn volwaardige alternatieven voor DigiD Hoog te ontwikkelen, op basis van SIM en embedded Secure Element.
5. Met name SIM-oplossingen bereiken een hoog niveau van security en certificatie dat vergelijkbaar is met de traditionele smartcard oplossingen, in combinatie met een brede doelgroep (alle smartphone bezitters). Het grootste nadeel is dat er een grote afhankelijkheid is van de medewerking van mobiele operators. De eSIM ontwikkeling biedt evenwel aangrijpingspunten om een ander model te realiseren, echter ten koste van de uitgifte van een nieuwe (e)SIM.
6. De embedded Secure Elements bieden hetzelfde hoge niveau van security en certificatie als SIM's, maar zijn thans slechts in circa 40% van alle smartphone aanwezig. Dit staat vooralsnog brede adoptie in de weg.
7. Een hoog niveau van security en privacy is ook te bereiken met gecentraliseerde oplossingen, waarbij feitelijke Secure Elements worden nagebootst. Deze techniek is in combinatie met alle mobiele telefoons op de een of andere wijze te realiseren. Aanvulling met securitymaatregelen die wèl specifiek zijn voor de telefoon is daarbij wel aan te bevelen, alsmede de toepassing van *multi party computing* technieken (split key en treshold systemen).
   Oplossingen die uitsluitend zijn gebaseerd op de Trusted Execution Environment zijn interessant om veilige opslag van sleutels te realiseren, maar halen niet het security niveau van een SIM of embedded Secure Element. In dat verband zijn deze tweede keuze,

maar wel heel interessant als ondersteuning voor met name de centrale mobiele oplossingen.
NB Hier zien we een scheiding in de techniek voor Android enerzijds (ARM TrustZone met bijbehorende bibliotheken als Trustonic TSP/TAP) en iOS anderzijds (Secure Enclave).

8. Voorgaande betreft dan vooral de 'technische dragers'. Laat open wat voor authenticatiemechanisme wordt geïmplementeerd hierop. Dat zou een bekende techniek als een PKI applet kunnen zijn, een kopie van de eIDAS Token Specificatie applet (de specificatie die model staat voor de DigiD Hoog applet), of een geheel alternatieve techniek als IRMA.
9. Waar PKI en de eIDAS Token Specificatie zijn gericht op authenticatie, is IRMA niet uitsluitend gericht op authenticatie maar daarnaast ook op attribuutverstrekking op een privacyvriendelijke methode. Inpasbaarheid in de overall eID architectuur is gegeven het decentrale karakter van IRMA wel een aandachtspunt, maar dit lijkt zeker niet onmogelijk.
10. Naast authenticatie en attribuutverstrekking is er nog de optie van ondertekening. Eerder besloten de ondertekenmogelijkheid los te koppelen van DigiD Hoog als zodanig. Zowel PKI, de eIDAS Token Specificatie en IRMA bieden echter desgewenst de mogelijkheid om te ondertekenen. IRMA biedt daarin de mogelijkheid om attribuut-gebaseerde handtekeningen te leveren, waarmee de privacy ook in ondertekensituaties op maat kan worden gesneden.
11. Omdat het de wens is om richting de burger voor de DigiD app te positioneren als dé relevante *user interface*, zou van apps de source code beschikbaar moeten komen. Van IRMA is het duidelijk dat hieraan voldaan wordt, van een eventuele Digidentity app zou dat nog onderzocht moeten worden.
12. Hardware tokens zijn weliswaar bruikbaar als alternatief authenticatiemiddel, maar genieten niet de voorkeur omdat ze niet passen in een Mobile First benadering. Ze zijn dus meer te positioneren als oplossingen voor restgroepen, die niet met de Mobile First benadering zijn te bedienen. Ook zijn de kosten en de logistieke processen voor dergelijke hardware oplossingen belangrijke aandachtspunten.

Een schematisch overzicht van de verschillende alternatieven:

| | **Positionering** | **Vorm** | **Kosten** | **Security** | **Adoptie-potentieel** | **Toekomst vast** |
|---|---|---|---|---|---|---|
| Idensys / eHerkenning dienstverlening | Alternatief DigiD Substantieel.<br><br>Digidentity app alternatief voor DigiD Hoog (vergelijkbaar met centrale | Apps<br><br>Digidentity: app | ?<br>Moet markt-consultatie Uitwijzen. | +<br>NB Video enrollment Proces.<br>++ | ++ | ? (Markt, video enrollment proces) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | HSM-oplossing) | | | | | |
| iDIN dienstverlening | Alternatief DigiD Substantieel | Diverse | 0,35 per transactie? | +/- | ++ | + |
| IRMA | Alternatief DigiD Substantieel Of<br><br>DigiD Hoog (mits combi met veilige mobiele hardware) | App<br><br>App | Basis software gratis. Enrollment kosten, zie SIM.<br>Kosten mobiele drager oplossing. Enrollment kosten. | +<br><br>++ icm SIM, eSE, centrale HSM | ++<br><br>++ | ? (Markt) |
| Hardware tokens incl. crypto calculators | Alternatief voor DigiD Hoog, uitsluitend voor specifieke doelgroep zonder smartphone | Diverse hardware | Kosten 10-20 euro voor token.<br><br>Enrollment kosten. Tenminste gelijk aan kosten SIM-scenario. | ++ (mits variant bestand tegen man-in-the-browser aanvallen) | - | + (maar per oplossing afhankelijk van markt) |
| Mobiele oplossingen op basis van SIM | Drager voor alternatieven voor DigiD Hoog | Icm app | Kosten 5 euro per SIM Enrollment kosten 12 euro voor balie. Niets bij afleiding NIK/rijbewijs. | ++ | ++ | ++ |
| Mobiele oplossing met Secure Elements | Drager voor alternatieven voor DigiD Hoog | Icm app | Geen kosten eSE Wel enrollment kosten. Zie SIM | ++ | -- | ++ |
| Mobiele oplossing met | Ondersteuning voor met | Icm app | Licentiekosten libraries | Voldoende als ondersteuning | ++ | ++ |

| | | | | | | |
|---|---|---|---|---|---|---|
| TEE | name centrale HSM oplossing. Versterking DigiD Substantieel | | onbekend.<br><br>Enrollment kosten, zie SIM. | | | |
| Mobiele oplossingen met centrale HSM | Drager voor alternatieven voor DigiD Hoog | Icm app | Kosten centrale omgeving.<br><br>Enrollment kosten, zie SIM. | + | ++ | +/++ (afhankelijk van specifieke oplossing) |

# 6 ANTWOORD OP DE ONDERZOEKSVRAGEN EN AANBEVELINGEN

## 6.1 Antwoord op de onderzoeksvragen

*Vraag 1. In hoeverre voldoen de huidige publieke authenticatieoplossingen voor eIDAS Substantieel en eIDAS Hoog, die zich kenmerken door hun koppeling aan een NFC-chip in reisdocumenten en rijbewijs?*

De oplossing voor DigiD Substantieel voldoet goed. Wel zijn meer enrollment-methoden gewenst om zoveel mogelijk burgers te bedienen. Logius doet momenteel onderzoek naar die verbreding in enrollment-methoden. De resultaten van dit onderzoek zijn ons experts niet bekend en we hebben er voor gekozen om op het punt van deze enrollment-methoden verder geen advies te formuleren. De huidige DigiD app en bijbehorende opwaardeermethode naar eIDAS Substantieel kent nog wel wat aandachtspunten op het gebied van gebruikersvriendelijkheid, maar in de basis voldoet de DigiD app. Gegeven het feit dat de het een eenvoudig bedienbare authenticatieapp is, achten we de kans op een brede adoptie groot.

Gegeven de behoefte, ondermeer in de zorg, aan authenticatiemiddelen met een verhoogd betrouwbaarheidsniveau, wordt een snelle verbreding van DigiD Substantieel op basis van de DigiD app (dus met meer enrollment-methoden) als topprioriteit gezien.

Voor DigiD Hoog zijn er wel wat kanttekeningen te plaatsen bij de oplossingsrichting. De kansen dat DigiD Hoog in een combinatie met een externe NFC-lezer door de burger geadopteerd zal worden, achten we klein op basis van de eerdere ervaringen met eID kaarten in andere EU-landen. Derhalve ontraden we in te zetten op een variant met een externe NFC-lezer. De vanuit de gebruikerservaring meest wenselijke uitvoering - binnen het huidige DigiD Hoog concept - achten we een variant waarbij de smartphone met daarop de DigiD app als lezer van de NIK of rijbewijs fungeert. Deze variant heeft echter een aantal nadelen:

- Het aantal burgers dat hier gebruik van kan maken, is beperkt: momenteel ruim 4 miljoen burgers. Dit aantal neemt pas significant toe als mobiele telefoons nog breder worden uitgerust met NFC en als de NFC-implementatie op de iPhone geheel open wordt gezet.
- De burger dient nog steeds bij elke authenticatie zijn NIK of rijbewijs aan te bieden.

Bovengenoemde nadelen, gecombineerd met het feit dat het zeer lang duurt voordat DigiD Hoog is uitgerold, maken dat we adviseren om alternatieven voor DigiD Hoog te ontwikkelen. Het leidende principe dient daarbij Mobile First te zijn, gegeven het feit dat we zien dat mobiele oplossingen een wezenlijk hogere adoptiegraad bij de burger bereiken dan oplossingen op basis van eID-kaarten. *Een geheel mobiel authenticatiemiddel op eIDAS Hoog is dus gewenst.*
Die keuze voor een geheel mobiele variant van DigiD Hoog wordt ondersteund door diverse internationale voorbeelden, die aantonen dat mobiele oplossingen beduidend succesvoller zijn dan de traditionele implementaties op basis van eID kaarten. Een sprekend voorbeeld is de casus

van de mobiele handtekening in Oostenrijk, andere succesvolle voorbeelden zijn Estland en Noorwegen. ([PWC1], paragraaf 3.3.6). Maar mobile PKI-oplossingen zijn veel breder in gebruik en een mobiele eID maakt nu in veel landen een belangrijk deel van de mix aan authenticatieoplossingen. Een voorbeeld hiervan is Oman.

De DigiD Hoog applet op de NIK en rijbewijs – waarvan we aanraden om de plannen gewoon door te zetten - zou in zo'n Mobile First benadering meer het karakter van een 'moederkaart' krijgen, waarmee het mobiele authenticatiemiddel kan worden gepersonaliseerd, naast de mogelijkheid om dit te doen via een balieproces. De personalisatie via de afleiding van een 'moederkaart' voldoet aan de eIDAS eisen voor eIDAS Hoog ([eIDAS 1502] Eis 2.1.2 Hoog 1, variant c).

*Vraag 2. Welke externe ontwikkelingen zijn er op technologisch gebied? En welke externe ontwikkelingen zijn er in de (internationale) toepassing betrouwbare authenticatie (eIDAS Substantieel of Hoog)?*

De meest relevante ontwikkelingen in de technologie (in relatie tot de vraagstelling):

- Mobiele authenticatie
- Dynamisering van authenticatie.
- Biometrie.

De opkomst van *mobiele authenticatie* is dusdanig en de ervaringen internationaal zijn dusdanig dat er reden is om de mobiele authenticatie leidend te maken: *mobile first*.

*Dynamisering* van authenticatie is duidelijk in opkomst: het dynamisch inzetten van authenticatiefactoren, afhankelijk van het risico van dat moment. We bevelen aan dit idee te adopteren binnen DigiD, zodat er meerdere authenticatiefactoren ter beschikking staan waar dynamisch gebruik van gemaakt zou kunnen worden. Dit biedt namelijk twee belangrijke business voordelen voor DigiD:

- Als een bepaalde authenticatiefactor minder betrouwbaar wordt door technologische ontwikkelingen, kan soepel worden overgeschakeld op nieuwe of aanvullende authenticatiefactoren. DigiD hanteert daarmee een lifecycle-benadering voor authenticatiefactoren.
- Door bovenop DigiD Substantieel aanvullende zekerheid te verkrijgen door dynamisch gebruik van aanvullende authenticatiefactoren, kan het feitelijke betrouwbaarheidsniveau van DigiD Substantieel worden verhoogd en de praktische levensduur van DigiD Substantieel worden verlengd. Hiermee kan 'tijd worden gekocht' voor een goede *mobiele* implementatie van DigiD Hoog.

*Biometrie* wordt steeds meer gezien op mobiele apparatuur. De technologie is in de recente jaren betrouwbaarder geworden en geschikt gebleken voor massale toepassing. In de bancaire toepassingen zien we biometrie steeds vaker als alternatief voor de PIN. Wij adviseren biometrische verificatie op te nemen als een van de authenticatiefactoren binnen DigiD. Dit kan

dan worden ingezet als alternatief voor de PIN op de DigiD app of als (dynamisch in te zetten) aanvullende authenticatiefactor.

Daarnaast achten we aansluiting op blockchain en digitale identiteit van belang voor DigiD, alsmede het bieden van een bredere ondersteunen over kanalen (Omnichannel benadering). De uitdieping van deze onderwerpen is echter buiten scope voor dit rapport. Deze onderwerpen behandelen we in 3.1Analyse trends.

In de internationale toepassingen achten we met name de verschillende mobiele initiatieven voor DigiD / publieke authenticatie relevant. Als voorbeelden beschouwen we dan de mobiele toepassingen in:

- Belgie: itsme (Sinds medio 2017 van start, nog geen accuraat beeld van de adoptie mogelijk.)
- Duitsland: Verimi (Gaat binnenkort van start.)
- Oostenrijk: mobiele handtekening in relatie tot de Burgerkaart (sinds 2009 actief, 500.000 gebruikers terwijl de eID kaart nooit voorbij de 100.000 is gekomen)
- Estland (Een tiende vh aantal gebruikers van de eID kaart, maar goed voor een kwart van het aantal transacties.)
- Noorwegen. (Mobiele ID sinds 2014, bij ca. 10% van de bevolking in bezit. Wel inmiddels goed voor een verdubbeling van het transactievolume)

Het Belgische itsme is een interessant voorbeeld omdat het daar mogelijk is om de enrollment op verschillende manieren te doen, zowel via de bank als via de eID-kaart.

*Vraag 3. In hoeverre levert dat alternatieven of aanvullingen op, die kansrijk zijn om op in te zetten in de publieke authenticatie in Nederland?*

Alternatieven voor DigiD Substantieel zijn vrij breed beschikbaar. Op dit punt adviseren we de markt zijn werk te laten doen en uit te dagen tot een aantrekkelijk aanbod te komen. In de positionering van alternatieve authenticatiemethoden achter we het wel aan te raden om maatregelen te nemen die een ‘winner-takes-all’ scenario vermijden. Dit zou er immers alsnog toe leiden dat ‘alle eieren in één mandje’ komen te liggen. Vermijden we een single-point-of-failure bij DigiD, krijgen we er vervolgens een bij een marktpartij.

Alternatieven voor DigiD Hoog zijn niet zomaar kant-en-klaar voorhanden als een in te kopen product. Weliswaar zijn er enkele producten beschikbaar, maar een ontwikkeltraject ligt meer voor de hand. Zie hoofdstuk 5 voor de analyse van de verschillende alternatieve technieken. Allereerst dient daarvoor de technische basis, de ‘dragertechnologie’ te worden ontwikkeld. Deze ‘dragertechnologie’ verzorgt dan de veilige opslag van kritische programmacode en cryptografische geheimen, in ondersteuning van de DigiD app. Hiervoor dienen zich de volgende mogelijkheden aan als meest waarschijnlijke kandidaten:

- Centrale hardware, in de vorm van nagebootste Secure Elements of anderszins.
  Deze centrale hardware dient samen te werken met de oplossing op de mobiel in een

uitgekiend ontwerp, zodat er bescherming is tegen zowel de diefstal van de mobiel als misbruik van de gegevens op de server. Zo mogelijk dient deze oplossing te worden gecombineerd met het gebruik van de Trusted Execution Environment op de mobiel (of eventuele andere hardware mechanismen). Zie hiervoor hoofdstuk 5. (De Trusted Execution Environment op zich achten we onvoldoende veilig om eIDAS Hoog te kunnen bieden, in de mobiele omgeving is hiervoor een SIM of embedded Secure Element nodig.)

- Implementatie op de SIM. Eventueel dient de overheid, al dan niet in samenwerking met andere partijen, hiervoor een specifieke SIM uit te geven. De authenticatietoepassing van de burger kan hierop worden geplaatst, eventueel naast andere value added services zoals vervoer, ticketing et cetera.

Wij adviseren bovenstaande mobiele dragertechnologieën parallel te ontwikkelen en te beproeven. We merken voorts op dat het opdoen en borgen van kennis en ervaring met security-kritische toepassingen (identity, zorg, vervoer, ticketing, betalen enzovoorts) in de mobiele omgeving van strategisch belang is voor de overheid en raden aan hiervoor passende stappen te zetten. Het doel hiervan is dat deze kennis – zo mogelijk op meerdere plaatsen – wordt ontwikkeld, geborgd en verspreid zodat die voor een meerdere security-kritische toepassingen in de overheid beschikbaar komt.

Bovenop de te ontwikkelen mobiele dragertechnologie dient dan een toepassing te worden ontwikkeld. We bevelen hiervoor aan de DigiD app verder uit te breiden. Naast eigen ontwikkeling zou gebruik kunnen worden gemaakt van bestaande apps van leveranciers in binnen- en buitenland. In Nederland kan dan bijvoorbeeld worden gedacht aan de app-oplossing van Digidentity of de IRMA oplossing. De voorkeur geniet het om een oplossing te realiseren die een architectuur heeft, waarbij de geheimen verdeeld worden over meerdere componenten. Een voorbeeld hiervan zijn *split key* oplossingen waarbij een component in een zeer veilige omgeving (SIM of nagebootste SE) samenwerkt met een minder zwaar beveiligde component (een ‘gewone’ app op de mobiel). IRMA, maar ook de mobiele ID van Estland zijn hier voorbeelden van.

*Vraag 4. Hoe verhouden die alternatieven en ontwikkelingen (die volgen uit de antwoorden op vragen 2 en 3) zich tot de oplossingen DigiD Substantieel en DigiD Hoog in termen van tenminste de volgende criteria: succesvolle toepassing, adoptiepotentieel, gebruikersvriendelijkheid, waarschijnlijkheid dat eIDAS compliance wordt gerealiseerd, toekomstvastheid, standaardisatie en kosten.*

Zoals bij vraag 3 is aangegeven zijn er voor DigiD Hoog wel alternatieven die ook elders met succes worden toegepast, zie hiervoor bijvoorbeeld de Oostenrijkse ervaringen. Door voor een mobiele oplossing te kiezen worden de gebruikersvriendelijkheid en de adoptie door de burgers naar verwachting sterk verhoogd. Het is echter niet te verwachten dat de elders gebruikte oplossingen één-op-één herbruikbaar zijn voor de Nederlandse situatie, zodat hiervoor een ontwikkeltraject dient te worden gestart. In de beweging naar een mobiele vorm van DigiD Hoog, liggen de alternatieven primair op het gebied van de ‘mobiele dragertechnologie’ als alternatief voor de applet op de chip van NIK en rijbewijs.

De in vraag 3 benoemde 'meest kansrijke' varianten, te weten

- de SIM-gebaseerde oplossing en de
- centrale oplossing om het Secure Element op de mobiel na te bootsen

bieden beide een *zeer hoog adoptiepotentieel*. Een SIM zit in elk mobiel toestel en de centrale HSM-oplossing is voor elke mobiel te bieden. Vrijwel alle moderne Android smartphones en iPhones kennen een vorm van een Trusted Execution Environment (TrustZone versus Secure Enclave), waarmee de veiligheid van de centrale HSM-oplossing verder kan worden versterkt. De gebruikte cryptografische en software-architectuur kunnen eraan bijdragen dat in de centrale oplossing de beheerder van die centrale oplossing niet kan werken zonder inbreng van de gebruiker en zijn mobiel. En omgekeerd dat een gestolen mobiel, waarvan alle gegevens zijn geanalyseerd, niet voldoende is om de identiteit van de gebruiker over te nemen. Zie het antwoord op vraag 3 (*split key* of *treshold* oplossingen).

De kans dat hiermee eIDAS Hoog is te realiseren is in beide varianten groot. De SIM-variant biedt wat dat betreft de meeste zekerheden. Ook zal het feit dat de SIM-variant geheel decentraal is gerealiseerd een geruststelling zijn voor verontruste burgers en actiegroepen.

De SIM-oplossing en de Trusted Execution Environment zijn gestandardiseerd door GlobalPlatform, de standaardisatieorganisatie achter de meeste smartcards, SIM's enzovoorts, die over sectoren heen dus dezelfde technische basis heeft gerealiseerd.
TrustZone en Secure Enclave als onderliggende TEE technieken zijn echter leveranciersspecifiek van ARM en Apple respectievelijk. De nabootsing van Secure Elements is een industriepraktijk, waarvan zal moeten blijken hoe toekomstvast deze is. Grote partijen als Google, Microsoft en bancaire partijen als Mastercard hebben zich er echter al aan verbonden voor de specifieke toepassing van mobiel betalen. Al met al is de SIM-oplossing het best gestandaardiseerd en komt men met de gecentraliseerde oplossing in een veld dat slechts gedeeltelijk is gestandaardiseerd, maar waar wel veel grote partijen actief in zijn. Een vorm van gecentraliseerde oplossing is daarmee zeker toekomstvast, maar de precieze vorm kan door de tijd veranderen naarmate er andere specificaties of standaarden opkomen.

In beide bovenstaande mobiele oplossingen dient er te worden gepersonaliseerd. Dit kan langs twee routes:

- Een balieproces bij bijvoorbeeld gemeentes of een ander face-to-faceproces.
- Afleiding via de DigiD Hoog applet op een WID-document.

De eerste handeling kost circa 12-15 euro per personalisatie. De tweede handeling kan als self-servicehandeling door de burger gebeuren en hier zijn derhalve slechts helpdeskkosten aan verbonden.

Een SIM-oplossing kent hogere hardware kosten. Dit betreft al snel 5 euro per burger. Een SIM-kaart gaat in de praktijk echter wel bijna 5 jaar mee. In deze periode is dus geen nieuwe personalisatie aan de orde. In een gecentraliseerd model zijn er niet direct kosten voor hardware

per burger, maar de personalisatie komt wel te vervallen zodra een nieuwe telefoon in gebruik wordt genomen. Dit gebeurt circa eens per 2,5 jaar, in welk geval een nieuwe personalisatie noodzakelijk is. Precieze kostenscenario's kunnen worden doorgerekend, op basis van realistische behoeftestellingen.

## 6.2 Overige conclusies

1. Er is een aanzienlijke ongedekte behoefte om authenticatiemiddelen uit te breiden naar een digitale identiteit, waarmee het ook mogelijk is om aan de wettelijke identificatieplicht in diverse sectoren te kunnen voldoen. Dit achten we een maatschappelijk relevant onderwerp en voldoende interessant om mee te nemen in de uitbreiding van DigiD Hoog of in verkenningen omtrent de digitale identiteit. Hierbij zijn er tevens raakvlakken met Regie op gegevens te onderkennen vanwege het *user centric* model dat gewenst is voor zowel digitale identiteit als het smallere onderwerp van authenticatie.
2. Het afleiden van identiteiten en authenticatiemiddelen in andere sectoren is een belangrijke toepassing voor DigiD Hoog en de documenten waarop de DigiD Hoog applet is opgenomen. Dit onderwerp hangt nauw samen met het al dan niet gebruiken van het BSN of juist alternatieve nummer. Hierbij is zorgvuldigheid geboden om de single-point-of-failure van DigiD niet te verplaatsen naar een register of een voorziening als het BSN-koppelregister.

## 6.3 Aanbevelingen

Dit alles leidt tot de volgende aanbevelingen:

1. Voer een strategie in om DigiD Substantieel eerst breed geadopteerd te krijgen door de burgers. Doe dit door het verbreden van de enrollment-mogelijkheden. We geven hierover geen gedetailleerd advies, aangezien dit het onderwerp is van een lopend Logius onderzoek. Brede adoptie van DigiD Hoog kan later volgen.
2. Voer onverminderd de plannen door om NIK en rijbewijs van gepersonaliseerde applets voor authenticatie te voorzien zoals thans in de plannen voor DigiD Hoog. Deels om een maatregel te hebben als in de komende jaren een hoger betrouwbaarheidsniveau acuut nodig blijkt, een verzekeringspremie als het ware. Maar de belangrijkste toepassing is waarschijnlijk gelegen in de functie als 'moederkaart', waarmee bijvoorbeeld mobiele authenticatieoplossingen kunnen worden gepersonaliseerd.
3. De bovengenoemde moederkaart-functie dient tevens geschikt te worden gemaakt om authenticatiemiddelen in andere domeinen af te leiden. Denk aan toepassingen binnen publieke en private organisaties. Men dient daarbij dergelijke afleidingen te kunnen traceren om identiteitsfraude te kunnen tegengaan.
4. Ontwikkel functies binnen DigiD om gebruik te maken van een dynamische risicoschatting voor een authenticatie en een dynamische keuze voor (aanvullende) authenticatiefactoren ten tijde van de authenticatie. Hiermee kan het niveau DigiD Substantieel verder versterkt worden, wat 'tijd koopt' om DigiD Hoog goed in te voeren.
5. Hanteer de DigiD app als het middel van eerste keuze voor eIDAS Laag, Substantieel en Hoog.

6. Overweeg een biometrie mogelijkheid in te bouwen in de DigiD app, als alternatief voor de PIN, zulks op basis van voorkeur van de individuele gebruiker. Dit is analoog aan wat veel banken nu doen (o.m. ING, Rabobank en ABN AMRO).
7. Bouw SMS als authenticatiemethode actief af. Overweeg SMS uitsluitend te handhaven voor personen die aangeven niet over een smartphone te beschikken en dan zulks ook nog uitsluitend op tijdelijke basis.
8. Zorg voor één of meer alternatieve middelen voor DigiD Substantieel om niet volledig afhankelijk te zijn van uitsluitend de DigiD middelen. Laat het aanbieden van dergelijke alternatieve middelen aan de markt over. Als experts kunnen we geen unaniem advies geven over de positionering van dit alternatieve middel: als volwaardig alternatief of als backup.
   Voor een aanvankelijke positionering als backup pleit dat er werkelijk meerdere middelen beschikbaar zijn en er geen 'winner-takes-all' situatie ontstaat. Ook is het makkelijker om in deze situatie een eenduidige gebruikerservaring te verzorgen. Voor een positionering als volwaardig alternatief pleit dat de burger zelf kan kiezen, dat is werkelijk user-centrisch. Beide standpunten zijn aan bod gekomen in het expertpanel en op dit punt was geen overeenstemming.
9. Naast de smartcard met een applet die op de NIK en rijbewijs is opgenomen, raden we aan om een mobiel alternatief voor DigiD Hoog te ontwikkelen, naast de DigiD Hoor variant die thans wordt ontwikkeld. Wij raden aan om tenminste de beide voorkeursvarianten te ontwikkelen zoals beschreven onder onderzoeksvraag 3 (SIM en nagebootste Secure Element oplossing) in parallel te ontwikkelen en hiervoor *demonstrators* te realiseren.
10. Een eerste stap voor bovengenoemde ontwikkeling is om in de komende maanden met bij voorkeur externe kennishebbers van authenticatieoplossingen, SIMs en nabootsing van Secure Elements de architectuur van deze oplossingen verder uit te werken. Naast de kennis van de mobiele dragertechnologie als SIMs en nagebootste Secure Elements er is ook daarbij ook kennis van de cryptografische architectuur en toepasselijke software relevant. In dat verband is kennis van cryptografische authenticatie-oplossingen, die een uitgekiende combinatie vormen tussen een centrale component en de mobiel van belang (ondermeer *split key* en *treshold* oplossingen). IRMA en de mobiele ID van Estland zijn systemen in deze categorie.
11. Voor de personalisatie van bovengenoemde alternatieven voor DigiD Hoog raden we aan twee modellen mogelijk te maken, te weten a) een afleiding van de uitgerolde DigiD Hoog middelen (NIK en rijbewijs), uit te voeren door de gebruiker thuis of op servicepunten zonder face-to-face identiteitsverificatie en b) een balieproces. Ontwikkel een veilige en gebruikersvriendelijke methode om de genoemde afleiding mogelijk te maken. Zie ook punt 3 aangaande het gebruik als moederkaart.
12. Omdat niet iedereen zal beschikken over een smartphone is het een keuze of die doelgroep voor de hogere betrouwbaarheid geheel wordt verwezen naar machtigingsconstructies en het sociaal vangnet, of dat voor deze doelgroep toch nog alternatieve technische mogelijkheden worden ontwikkeld. Als experts zijn we van mening dat het verantwoord is om voor deze doelgroep géén technische authenticatiemogelijkheid meer te ontwikkelen. Mocht het politiek-maatschappelijk alsnog wenselijk worden geacht, dan is het te overwegen om hiervoor een geschikte

cryptocalculator te ontwikkelen of in te kopen.

# A Bronnen


[ARM1] *Securing the future of authentication with ARM TrustZone-based Trusted Execution Environment and Fast Identity Online (FIDO),* Rob Coomes, Mei 2015.

[Apple1] *iOS-beveiliging, iOS 10.* Whitepaper. Apple. Maart 2017. https://images.apple.com/nl/business/docs/iOS_Security_Guide.pdf

[Bio1] *Biometric Technology: Replacing Passwords and PINs in banking*, M2SYS Blog, Maart 2016, http://www.m2sys.com/blog/important-biometric-terms-to-know/biometric-technology-replacing-passwords-and-pins-in-banking/

[Block1] *Self-Sovereign-Identity Framework and Blockchain*, Rieks Joosten (TNO), ERCIM News, Juli 2017, https://ercim-news.ercim.eu/en110/special/self-sovereign-identity-framework-and-blockchain

[eIDAS1502] *UITVOERINGSVERORDENING (EU) 2015/1502 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen etc*, Europese Commissie, 8 september 2015.

[eSIM1] Embedded SIM pagina, GSMA Website, geraadpleegd oktober 2017, https://www.gsma.com/iot/embedded-sim/

[eSIM2] Embedded SIM pagina, GSMA Website, geraadpleegd oktober 2017, https://www.gsma.com/rsp/

[FIDO1] Website Fido Alliance, https://fidoalliance.org/

[FIDOPDS2] *FIDO & PSD2, Meeting the needs for strong customer authentication*, FIDO alliance, 2017, https://fidoalliance.org/wp-content/uploads/FIDO-PSD2-white-paper-FINAL.pdf

[GSMA1] Webpagina Mobile Connect, GSMA, https://www.gsma.com/identity/mobile-connect

[HCE1] *Host Card Emulation versus Secure Element: which is more secure?*, Lucian Armasu, Tom's hardware, maart 2015, http://www.tomshardware.com/news/host-card-emulation-secure-element,28804.html

[HCE2] *Mastercard to use Host Card Emulation for NFC-based mobile payments*, persbericht, februari 2014, https://newsroom.mastercard.com/press-releases/mastercard-to-use-host-card-emulation-hce-for-nfc-based-mobile-payments/

[HCE3] *ING-pilot: opmaat naar grootschalige introductie van mobiele betalen*, Emerce, september 2015, https://www.emerce.nl/achtergrond/ingpilot-opmaat-grootschalige-introductie-mobiel-betalen

[Itsme1] Website Belgische Mobile ID en itsme, https://www.belgianmobileid.be/nl

[Leithold1] *Austrian eiD and its road to eIDAS*, Herbert Leihold, 2016, https://www.a-sit.at/pdfs/Praesentationen%20ab%202016/20160614%20EYou%20DenHaag%20Leitold.pdf

[Leithold2] *Austrian experience with Mobile ID versus Smart Card ID*, Herbert Leithold, presentative ISSE, November 2016, https://www.eema.org/wp-content/uploads/leitold-2.pdf

[Mobsig1] Wikipedia lemma Mobile Signature, https://en.wikipedia.org/wiki/Mobile_signature

[MobPKI1] *New Mobile ID in Oman for stronger authentication*, Gemalto website, oktober 2017, http://www.gemalto.com/govt/customer-cases/oman-new-infrastructure

[PBLQ1] *Internationale vergelijking eID middelen*, PBLQ, oktober 2014, https://kennisopenbaarbestuur.nl/media/128873/internationale-vergelijking-eid-middelen.pdf

[PWC1] *Study on a marketing Plan to stimulate the take-up of eID and trust services for the Digital Single Market.* PwC. Concept van eind September 2017.

[Secenclave1] *Start using the secure enclave crypto api*, Trail of bits, juni 2016. https://blog.trailofbits.com/2016/06/28/start-using-the-secure-enclave-crypto-api/

[Secenclave2] *Demystifying the Secure Enclave Processor*, presentatie Mandt, Solnik, Wang, Azimuth Security, OffCell Research, geraadpleegd oktober 2017, https://www.blackhat.com/docs/us-16/materials/us-16-Mandt-Demystifying-The-Secure-Enclave-Processor.pdf

[TEE1] *Trusted Execution Environment Guide*, GlobalPlatform website, geraadpleegd oktober 2017, https://www.globalplatform.org/mediaguidetee.asp

[TEE2] *Introduction to Trusted Execution Environments*, presentatie Steven Murdoch, University of Cambridge, http://sec.cs.ucl.ac.uk/users/smurdoch/talks/rhul14tee.pdf

[TEE3] Trustonic webpagina oplossingen op basis van TEE TrustZone hardware, geraadpleegd oktober 2017, https://www.trustonic.com/solutions/

[TEE4] Wikipedia lemma TrustZone, geraadpleegd oktober 2017, https://en.wikipedia.org/wiki/ARM_architecture#TrustZone

[TouchID] TouchID, Wikipedia (geraadpleegd oktober 2017), https://en.wikipedia.org/wiki/Touch_ID.

[Verimi1] Aankondiging Verimi voor jaarwisseling 2017/2018, https://www.db.com/newsroom_news/2017/verimi-new-registration-identification-and-data-platform-to-launch-at-the-turn-of-the-year-2017-2018-with-new-pa-en-11645.htm