cidSafe

een visie voor een betrouwbare en herbruikbare consumenten identiteit

Colofon

Datum :	Dec-2010
Versie :	0.91
Verandering :	Commentaar core team/PMC verwerkt
Toegangsrechten :	Consortium intern (tot final versie, die wordt publiek)
Status :	Ter review aan stuurgroep
Editor :	Maarten Wegdam
Auteurs :	Maarten Wegdam, Bob Hulsebosch
Opdrachtgever :	SI-I, cidSafe consortium
Sleutelwoorden:	cidSafe, consumer identity
Bijdragen van:	APG: Herman Hanssen Rabobank: Ruud Smeulders SIVI: Gerhard Gerritsen, Florus van der Linden DigiNotar: Jaap Kuipers, Marcel Jak Novay: Martijn Oostdijk, Wouter Bokhove
Reviewers:	Novay: Henk Eertink, Janine Swaak cidSafe core team

Synopsis:

Dit document beschrijft de visie voor een betrouwbare en herbruikbare consumenten identiteit. Deze visie is ontwikkeld in het cidSafe project gedurende 2010, en stelt trust frameworks centraal als oplossingsrichting.

Management samenvatting

Dienstverlening via het internet heeft een grote vlucht genomen in Nederland. Voor dienstverleners biedt online dienstverlening veel potentie voor kostenbesparing en nieuwe diensten, en consumenten blijken het in toenemende mate te omarmen. Voor veel diensten is het nodig om met voldoende zekerheid de identiteit van de consument vast te stellen, vooral als het gaat om privacy-gevoelige informatie en bij fraudegevoelige diensten, maar ook wanneer er vanuit wetgeving of bedrijfsbeleid een zorgplicht is.

De huidige situatie op het internet is dat de consument voor elke dienst een ander authenticatiemiddel nodig heeft om zichzelf kenbaar te maken. Meestal is dit een combinatie van gebruikersnaam en wachtwoord. De zogenaamde digitale sleutelbos die hiermee gepaard gaat is erg gebruikersonvriendelijk, onder meer omdat gebruikers de specifieke gebruikersnamen en wachtwoorden vergeten als ze niet frequent gebruikt worden. Het is ook erg duur vanwege de beheerslasten die hiermee gemoeid zijn. Daarnaast brengt dit een groeiend aantal beveiligingsproblemen met zich mee door diefstal van of fraude met digitale identiteiten.

Dit kan opgelost worden met een *betrouwbare* en *herbruikbare* digitale identiteit. Een *betrouwbare* identiteit vereist een veilig authenticatiemiddel, veiliger dan gebruiksnaam/wachtwoord aangezien dit erg phishing gevoelig is, en een goed registratieproces, bijvoorbeeld door voor afgifte van de digitale identiteit fysiek iemands paspoort te controleren. Zowel een veilig authenticatiemiddel als een goed registratieproces zijn duur. *Hergebruik* betekent dat een consument dezelfde identiteit kan gebruiken bij meerdere online dienstenaanbieders. Dit is gebruikersvriendelijk omdat de consument dezelfde authenticatiemiddelen veel vaker kan gebruiken (en dus zijn wachtwoorden beter kent). Ook is het goedkoper omdat de kosten van deze herbruikbare identiteit gedeeld kunnen worden door meerdere dienstenaanbieders.

Voor zowel gebruikersgemak als kosten is het belangrijk dat een herbruikbare identiteit zo breed mogelijk ingezet kan worden. Oplossingen kunnen onderscheiden worden op basis van de aanbieder: de overheid of de markt.

De *Nederlandse overheid* voorziet al haar burgers van een digitale identiteit: DigiD. Echter, het gebruik ervan door dienstenaanbieders is voorbehouden aan partijen die gebruik mogen maken van het BSN. Dit beperkt het gebruik van DigiD tot voornamelijk de overheid. DigiD mag dus niet gebruikt worden voor consumer-2-business dienstverlening behoudens specifieke uitzonderingen. De specifieke uitzonderingen zijn de zorg- en pensioensector. Hoewel er een wetvoorstel ligt voor het gebruik van BSN in de financiële sector, ziet het er niet naar uit dat dit voldoende aanknopingspunten zal bieden voor het gebruik van DigiD als identiteitsoplossing door bijvoorbeeld verzekeraars. Een andere ontwikkeling bij de Nederlandse overheid is de elektronische Nederlandse identiteitskaart (eNIK). Dit speelt al enige jaren, maar het is onzeker of - en zo ja wanneer - en hoe dit vorm zal krijgen. Het zou kunnen dat het mogen gebruiken van de eNIK losgekoppeld wordt van het mogen gebruiken van BSN.

Het cidSafe project heeft zich geconcentreerd op een marktoplossing. Zo'n *marktoplossing* kent diverse grote uitdagingen, met name betrouwbaarheid, schaalbaarheid en marktintroductie. Voor betrouwbaarheid en schaalbaarheid is een trust framework een goede benadering. In een trust framework (ook wel afsprakenstelsel genoemd) worden afspraken gemaakt over betrouwbaarheid (meestal via auditing van identiteitsproviders), het business model, de veiligheidseisen en privacy van de gebruiker van de identiteit. Ook worden in een trust framework afspraken gemaakt over schaalbaarheid, zoals interoperabiliteit en het gemak waarmee dienstenaanbieders kunnen aansluiten. Een belangrijk onderdeel van het trust framework is een governance orgaan waarin belanghebbenden vertegenwoordigd zijn. Dit orgaan controleert de afspraken en beheert het trust framework. Het wordt verder aan de markt overgelaten wie de identiteitsproviders worden, inclusief welke authenticatiemiddelen ze gebruiken zolang deze en het uitgifteproces binnen de regels van het trust framework passen.

Voor een succesvolle marktintroductie is het vooral noodzakelijk dat er al bij de start een hoge penetratie van de digitale identiteiten is onder consumenten. Vanwege de benodigde investeringen die nodig zijn voor een veilige identiteit brengt dit met zich mee dat bestaande identiteiten hergebruikt moeten kunnen worden. Met name banken zijn hier goed voor gepositioneerd, omdat dit vertrouwde partijen zijn die gezamenlijk het overgrote deel van alle volwassen Nederlanders al voorzien hebben van een digitale

identiteit die gebruikt wordt voor online bankieren. Ook bijvoorbeeld mobiele operators zijn goed gepositioneerd.

Hoewel het hierboven geschetste trust framework primair een marktaangelegenheid is, is het om een brede maatschappelijk acceptatie te krijgen, en om het vertrouwen te vergroten, wenselijk zo niet noodzakelijk dat de overheid een rol heeft als toezichthouder. Hierom, en omdat de trust framework benadering goed aansluit op de aanpak van eHerkenning voor bedrijven die het ministerie van EL&I aan het introduceren is, ontstaat er een potentiële win-win situatie als een consumer-2-business trust framework aansluiting vindt bij eHerkenning. Dit biedt ook praktische voordelen voor zowel consumenten als online dienstenaanbieders, waaronder meer hergebruik en schaalvergroting.

Dit rapport beschrijft de visie op een trust framework voor consumenten identiteit, en doet uitspraken over de onderstaande keuzes hierin:

- *Veiligheidsniveaus* - Het trust framework zal om toekomstvast en schaalbaar te zijn, een zekere variëteit aan middelen en processen moeten toestaan. Dit zal vastgelegd worden in zogenaamde veiligheidsniveaus. Gezien de initiële focus van cidSafe op de financiële sector, zijn verzekeraars de grootste groep aan potentiële dienstenaanbieders die gebruik kunnen gaan maken van dit trust framework. Uit een inventarisatie onder drie grote verzekeraars, blijkt dat zij behoefte hebben aan veiligheidsniveaus waaraan bestaande bancaire authenticatiemiddelen en registratieprocessen ruimschoots voldoen[1].
- *Business model* – Uit studies in het buitenland blijkt dat consumenten niet of slechts heel beperkt willen betalen voor een identiteit. Dit zal meer indirect onderdeel moeten zijn van de dienstverlening. In het business model zullen de online dienstenaanbieders daarom degenen moeten zijn die de identiteitsproviders betalen. Om het makkelijk te maken voor online dienstenaanbieders om zich aan te sluiten kan het introduceren van een extra partij in het business model helpen. Deze partij zit tussen de dienstenaanbieder en de identiteitsproviders in, zodat dienstenaanbieders zowel technisch als contractueel de aansluiting niet per identiteitsprovider hoeven te doen. In eHerkenning voor bedrijven heet deze rol de herkenningsmakelaar.
- *Mobiel* – het mobiele kanaal neemt in belangrijkheid toe, en de mobiele telefoon wordt in toenemende mate gezien als het authenticatiemiddel van de toekomst. In het trust framework mogen geen afspraken staan die dit in de weg staan.
- *Privacy* – Een herbruikbare identiteit brengt potentieel privacy nadelen met zich mee. Het trust framework moet state-of-the-art privacy enhancing technologieën, privacy-by-design en informed consent verplichten. Daarnaast moeten algemene eisen gesteld worden met betrekking tot de privacy aan de identiteitsprovider en dienstenaanbieders, op basis waarvan auditing plaats kan vinden.

Belangrijk voor de haalbaarheid van een trust framework aanpak zoals hierboven geschetst, is dat er drie (groepen van) partijen een commitment uitspreken hiervoor, namelijk:

1. *Dienstenaanbieders* – zij moeten duidelijk maken dat ze externe identiteitsproviders gaan gebruiken, en welke eisen ze stellen.
2. *Identiteitsproviders* – hoewel het trust framework open is, en identiteitsproviders die aan de eisen voldoen ook later moeten kunnen toetreden, is het nodig dat een initiële groep van identiteitsproviders met een voldoende grote dekking onder consumenten zich commit.
3. *De overheid* – niet alleen om het vertrouwen in het trust framework te vergroten, maar ook om te voorkomen dat er niet alsnog een overheidsoplossing op de markt wordt gebracht, die de investeringen van de identiteitsproviders teniet zou doen.

Als de noodzaak en urgentie niet bij al deze drie (groepen van) partijen in voldoende mate gevoeld wordt, is haalbaarheid van een trust framework onwaarschijnlijk.

[1] Het gaat hier om STORK Levels of Assurance 2 en 3.

Inhoudsopgave

1. Introductie

Het doel van het cidSafe project is een doorbraak te bewerkstelligen voor een veilige en gemakkelijke digitale sleutel voor algemeen gebruik door consumenten op het internet. Het gaat hier om een betrouwbare oplossing, die zich flexibel aanpast aan toekomstige ontwikkelingen en die breed gebruikt kan worden voor allerlei interacties, vooral als deze privacy- of fraudegevoelig zijn.

De initiële focus van cidSafe ligt op de financiële sector omdat daar de behoefte aan een betrouwbaar authenticatie-oplossing voor consumenten het grootst en urgentst lijkt. Het is nadrukkelijk de bedoeling dat een oplossing zich zal verbreden naar meerdere sectoren. Denk hierbij aan de zorg, energie, telecommunicatie, online retail en beveiligingssector. Deze verbreding zal ertoe leiden dat zo'n oplossing vaker gebruikt wordt en daardoor goedkoper en makkelijker wordt voor de consument.

Dit document beschrijft op een hoog niveau de uitkomsten van het cidSafe project. Dit document is geschreven voor beslissers en beleidsmakers bij bedrijfsleven en overheid die een zekere affiniteit hebben met het gebied, zonder dat ze experts hoeven te zijn. Bijvoorbeeld verantwoordelijken voor identiteitszaken bij verzekeraars, CIOs, information security officers, innovation managers en verantwoordelijken voor het internetkanaal.

Over het cidSafe project

Het cidSafe project (http://cidsafe.novay.nl) is een consortium project met als partners APG (Loyalis), Rabobank, DigiNotar, SIVI en Novay. cidSafe is gestart in begin 2010, en eind 2010 afgesloten. De naam cidSafe is gebaseerd op de *safe consumer identity.* De focus van het project was het bepalen van een oplossingsrichting voor een betrouwbare consumenten identiteit, en de haalbaarheid van het realiseren van deze oplossingsrichting in termen van draagvlak en business cases. De draagvlak activiteiten hebben zich geconcentreerd op de financiële sector en de rijksoverheid. Onderdeel hiervan was een klankbordgroep met Achmea, Aegon, Adfiz, Nationale Nederlanden, OHRA en SNS Reaal. Ook waren de ING en ABN-AMRO betrokken bij het project, via de Rabobank. Het cidSafe project heeft ook twee netwerkevents georganiseerd, waar o.a. vertegenwoordigers van de rijksoverheid, online retail en mobiele telecom aanwezig waren.

2. Situatie in Nederland

De huidige situatie op het internet is dat de consument voor elke dienst een ander authenticatiemiddel nodig heeft, meestal is dit een combinatie van een gebruikersnaam en wachtwoord. Dit leidt tot een 'digitale sleutelbos' met veel verschillende gebruikersnamen/wachtwoorden. Een vuistregel is dat gebruikers wachtwoorden vergeten die ze minder dan één maal per maand gebruiken[2], waardoor er een drempel ontstaat voor gebruik van die dienst. Dat is niet gebruikersvriendelijk voor de klant, en duur qua beheerslasten voor de online dienstenaanbieder. Daarnaast brengt het lage beveiligingsniveau van gebruikersnaam/wachtwoord combinaties een groeiend aantal beveiligingsproblemen met zich mee door diefstal of fraude met de digitale identiteit.

Voor een veilige identiteit is het nodig een veilig authenticatiemiddel te gebruiken. Hierbij is een wachtwoord (of pincode), ook wel aangeduid als een "iets wat de gebruiker weet", niet voldoende. Veiligere authenticatie vereist dat er ook sprake is van een "iets van de gebruiker heeft", zoals een smartcard, one-time-password token of een mobiele telefoon[3]. Naast een veilig authenticatiemiddel is het ook nodig een veilig registratieproces te hebben. In dit proces wordt vastgesteld wie de gebruiker is aan wie het authenticatiemiddel wordt verstrekt, bijvoorbeeld door het sturen van activeringscodes naar een bekend adres, of een face2face controle van de identiteit aan de hand van een paspoort. Zowel een veilig authenticatiemiddel als een veilig registratieproces zijn duur, en vaak ook omslachtig voor de gebruiker. Conclusie is dat een veilige identiteit hergebruik vereist om de kosten niet onnodig op te laten lopen.

[2] Zie bijvoorbeeld Forrester rapport, "Government eID Projects Need Private Sector Initiative And Support For Broader Success", 7 April 2008.

[3] Of een "iets wat de gebruiker is", wat neer komt op een biometrie zoals vingerafdruk of irisscan. Dit is echter weinig in gebruik voor de consumentenmarkt en laten we verder buiten beschouwing.

Bancaire sector

Op het gebied van consumentenidentiteit vormen banken in Nederland een uitzondering, omdat ze een relatief veilige identiteitsoplossing hebben voor hun klanten. Wat het registratieproces betreft is er, ook gedwongen door wetgeving, altijd sprake geweest van controle van de gebruikersidentiteit aan de hand van een formeel identiteitsbewijs. Het authenticatiemiddel dat de banken gebruiken voor online betalen is gebaseerd op een wachtwoord/pincode in combinatie met 'iets wat de gebruiker heeft' zoals een smartcard met bijbehorende reader (bijvoorbeeld Rabobank en ABN-AMRO) of een mobiele telefoon (bijvoorbeeld ING).

Ondanks de relatieve sterkte van de huidige bankauthenticatiemiddelen zijn banken continu op zoek naar verbeteringen. Banken vormen een aantrekkelijk doelwit voor hackers en de verleiding tot het aangaan van frauduleuze financiële transacties is groot, zoals ook blijkt uit de sterke toename van fraude met internet bankieren[4]. Een robuuste online identiteit met degelijke verificatie via een authenticatiemiddel is van essentieel belang om deze aanvallen en verleidingen te weerstaan. Alleen het hoogste niveau van authenticatie is hierbij gewenst.

Verzekeringsbranche

Verzekeraars bieden steeds meer online dienstverlening aan, wat in de meeste gevallen met zich mee brengt dat consumenten zich online moeten identificeren. Direct writers doen dit vaak al langer, maar ook intermediairs gaan steeds vaker via het internetkanaal met consumenten communiceren, bijvoorbeeld voor self-service. De recent goed-gekeurde wetgeving rondom de Digitale Polis[5] zorgt er ook voor dat het aantrekkelijker is geworden voor verzekeraars om meer het online kanaal te gebruiken voor hun dienstverlening. Naar verwachting zal dit ook een drive zijn voor nog veiligere en meer gebruikers-vriendelijke identiteitsoplossingen.

Binnen het cidSafe project is een inventarisatie uitgevoerd bij drie grote Nederlandse verzekeraars naar de behoefte aan veilige identiteiten. Hierbij werd gebruikt gemaakt van de Levels of Assurance (LoA, zie kader hiernaast) om discrete veiligheidsniveaus aan te kunnen duiden. Uit deze inventarisatie blijkt

Betrouwbaarheidsniveaus: Levels of Assurance

Verschillende diensten hebben verschillende risico profielen, bijvoorbeeld qua fraude of privacy risico, en vereisen daarom ook verschillende niveaus van zekerheid/betrouwbaarheid. Gebaseerd op het concept van Levels of Assurance (niveaus van zekerheid/betrouwbaarheid, LoA) zoals dit ook gebruikt wordt in nationale en internationale standaardisatie kan een inventarisatie gemaakt worden van de noodzakelijke LoAs voor online diensten in de verzekeringsector in Nederland.

Een voordeel van de LoA-aanpak is dat dienstenaanbieders, op basis van een risico-analyse, een bepaald LoA kunnen toekennen aan hun diensten zonder dat ze hiervoor een specifieke authenticatie-oplossing hoeven te benoemen. In gefedereerde of trust framework omgevingen komt dit de interoperabiliteit, herbruikbaarheid en schaalbaarheid van (bestaande) authenticatie-oplossingen ten goede.

In het Europese STORK project voor eID interoperabiliteit zijn vier niveaus voor de betrouwbaarheid van authenticatie gedefinieerd:

1. Geen of minimale zekerheid over de identiteit (bijvoorbeeld gebruikersnaam/wachtwoord);
2. Beperkte zekerheid (bijvoorbeeld DigiD, SMS-authenticatie via online registratie);
3. Redelijke zekerheid (bijvoorbeeld SMS-authenticatie met fysieke aanwezigheid, bankauthenticatie);
4. Hoge zekerheid (bijvoorbeeld PKI Overheid certificaat).

STORK definieert een compleet raamwerk voor het toekennen van deze LoA aan authenticatie-oplossingen. Hierbij wordt niet alleen gekeken naar de technische aspecten van de oplossing, zoals de sterkte van de encryptie en het type middel, maar ook naar de procesmatige aspecten zoals de registratie en uitgifte van het middel. Soortgelijke LoA zijn ook door het Amerikaanse NIST en eHerkenning gespecificeerd. Beide alternatieve raamwerken kennen ook 4 niveaus en vertonen veel overlap met de in STORK gedefinieerde niveaus.

[4] Uit NVB persbericht, "Samen houden we bankieren veilig", 13 oktober 2010, blijkt een toename van internetbankieren fraude in 2010 t.o.v. 2009 van meer een factor 4. Zie http://www.nvb.nl/scrivo/asset.php?id=535052..

[5] Zie Staatsblad 222 van 30 juni 2010, http://www.eerstekamer.nl/behandeling/20100630/publicatie_wet/f=/vij1akmaojzf.pdf.

dat er geen behoefte is aan het hoogste betrouwbaarheidsniveau (LoA 4) bij de verzekeraars. Het risicoprofiel van de online diensten is dusdanig dat maximaal LoA 3 nodig is. Er zijn daarnaast voldoende maatregelen in het offline dienstverleningsproces die ervoor zorgen dat eventuele restrisico's, die met LoA 3 gepaard gaan, weggenomen kunnen worden. LoA 3 wordt vooral toegekend aan transacties die het wijzigen of royeren van polissen met zich meebrengen. Maar dit geldt niet voor alle aan deze inventarisatie meewerkende verzekeraars. Eén verzekeraar geeft aan dat voor dit soort diensten ook LoA 2 voldoende is op dit moment. Deze verzekeraar is nog aan het overwegen of in de toekomst hogere niveaus gewenst zijn. Andere mogelijke overwegingen om te opteren voor een lager LoA zijn een strategische, om ten gunste van lagere kosten en hogere gebruiksvriendelijkheid een hoger risicoprofiel te accepteren, en tactische, door extra maatregelen te treffen in back-office systemen. Voor het inzien van polissen wordt LoA 2 voldoende geacht. Hetzelfde geldt voor het verstrekken van een offerte met privacygevoelige gegevens. Algemene dienstverlening rondom informatieverstrekking van producten en offertes zonder persoonsgegevens vereisen LoA 1.

De authenticatiemiddelen die momenteel ingezet worden door verzekeraars zijn de gebruikersnaam en wachtwoord combinatie en in mindere mate SMS-authenticatie. Het registratieproces hierbij is van verschillend niveau, zoals: geen verificatie, verificatie via een e-mail activering, of op grond van een kopie van het paspoort. Zonder in detail naar deze SMS-authenticatie oplossingen te hebben gekeken, lijken dit eerder LoA 2 oplossingen te zijn dan LoA 3. SMS-authenticatie staat momenteel erg onder druk omdat het encryptie-algoritme ervan gekraakt is en er geen end-to-end beveiliging is. Een betere, LoA 3, oplossing gebaseerd op 2-factor authenticatie met goed registratieproces lijkt dan ook gewenst. Er zijn verzekeraars die dit al toepassen voor een deel van hun gebruikers. Zij hebben geïnvesteerd in meer veiligheid, omdat ze banksparen of andere risicovollere producten online ontsluiten.

Nederlandse overheid

De Nederlandse overheid voorziet al haar burgers van een digitale identiteit, namelijk DigiD. Met DigiD is het mogelijk een Nederlandse burger te authenticeren, waarbij het DigiD systeem zijn of haar BSN nummer ter identificatie gebruikt. DigiD biedt twee veiligheidsniveaus: niveau 1 met gebruikersnaam/wachtwoord, en niveau 2 met one-time-password over SMS. Registratie gaat aan de hand van het huisadres. DigiD biedt geen toegang tot attributen, zoals bijvoorbeeld adres; hiervoor zijn andere systemen zoals de GBA. Het gebruik van DigiD binnen de private sector is voorbehouden aan partijen die gebruik mogen maken van het Burger Service Nummer (BSN). Hierdoor is het niet mogelijk DigiD te gebruiken voor consumer-2-business dienstverlening, met als specifieke uitzonderingen zorg en pensioenen. Hoewel er een wetvoorstel ligt rondom gebruik van BSN is de financiële sector, ziet het er niet naar uit dat dit voldoende aanknopingspunten zal bieden voor het gebruik van DigiD als identiteitsoplossing door bijvoorbeeld schadeverzekeraars[6].

Een andere ontwikkeling bij de Nederlandse overheid is de elektronische Nederlandse identiteitskaart (eNIK). De eNIK is een extra online authenticatiefunctionaliteit op de Nederlandse identiteitskaart, en zal met name DigiD veiliger kunnen maken. De overheid kan ervoor kiezen de eNIK ook beschikbaar te stellen als een consumenten identiteitsoplossing. De discussie rondom eNIK speelt al enige jaren, en het is onzeker of en zo ja wanneer en hoe dit vorm zal krijgen. Om een schatting te maken qua tijdslijn: het is mogelijk dat de Nederlandse regering hier in de eerste helft van 2011 een beslissing over neemt. Bij een positieve beslissing zal het wetgevingstraject mogelijk nog twee jaar duren. Pas dan kunnen de eerste burgers een eNIK krijgen. Vanaf ongeveer de tweede helft van 2018 zou dan elke Nederlander een eNIK functionaliteit hebben op hun identiteitskaart.

Een andere relevante ontwikkeling bij de Nederlandse overheid is het vanuit het ministerie van EL&I geïnitieerde *eHerkenning voor bedrijven* programma[7]. Het eHerkenning programma werkt aan het herkennen van bedrijven en de personen die namens deze bedrijven handelen in de communicatie met de overheid, business-2-government dus. eHerkenning is een afsprakenstelsel waarin marktpartijen concurreren om de eHerkenningsdiensten aan te bieden in plaats van dat de overheid dit doet. Zulke

[6] Zie ook " Geen gebruik DigiD in de financiële sector, De implicaties van de nieuwe sectorwet", cidSafe project, 30 september 2010, Bob Hulsebosch, te downloaden via http://cidsafe.novay.nl.

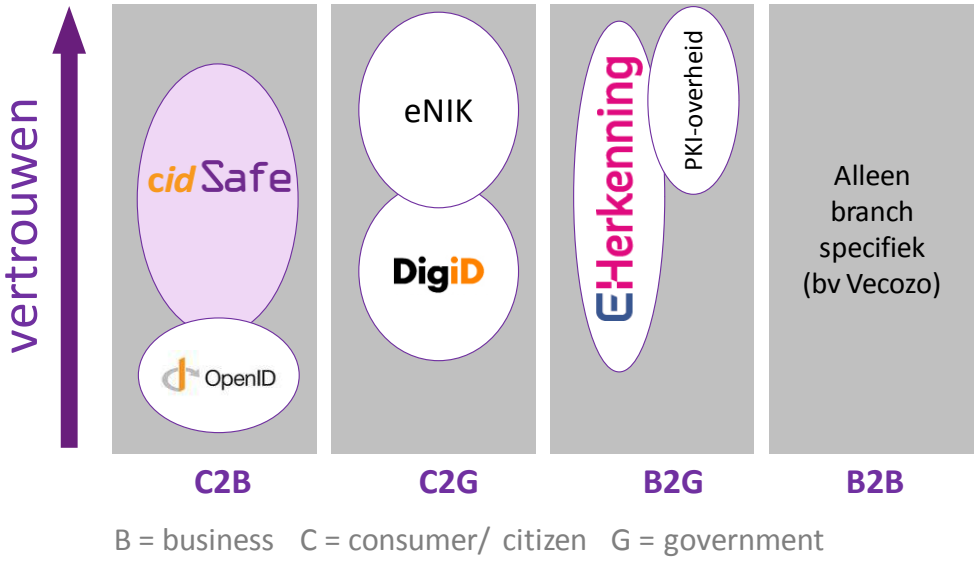
[7] Zie http://www.eherkenning.nl/

diensten betreffen het authenticeren van medewerkers van een bedrijf en het kunnen aantonen dat deze medewerkers gemachtigd zijn om namens het bedrijf met de overheid te mogen communiceren.

eHerkenning ondersteunt verschillende veiligheidsniveaus, waarbij het hoogste niveau door de bestaande PKI Overheid wordt ingevuld. Sinds kort is eHerkenning in beperkte mate operationeel en met het beëindigen van DigiD voor bedrijven wordt een verdere opschaling verwacht in 2011. Ook heeft eHerkenning plannen om business-2-business transacties te ondersteunen; consumer-2-business staat daarentegen (nog) niet op de agenda.

Positionering verschillende oplossingen en initiatieven

Figuur 1 visualiseert op een informele manier de verschillende authenticatie-oplossingen in Nederland t.o.v. elkaar en cidSafe voor verschillende transactiecontexten. Op de horizontale as staan de verschillende domeinen, verticaal is het een stijgend trust niveau. Nog niet eerder genoemd, maar wel vermeld in Figuur 1, is OpenID, een technische standaard die ondersteund wordt door vele grote internetpartijen zoals Google, Yahoo en Hyves, en consumenten in staat stelt in te loggen bij dienstenaanbieders met behulp van hun, bijvoorbeeld, Hyves account. Het gaat hierbij typisch om laagdrempelige toepassingen met lage eisen qua veiligheid. Er zijn wel initiatieven om op basis van de OpenID standaard een hoger betrouwbaarheidsniveau aan te bieden, zoals het OpenIDplus.nl initiatief. cidSafe steekt dus in op de hogere trust lacune in het consumer-2-business transactiedomein.



Figuur 1 Informele positionering van de verschillende NLse oplossingen en ontwikkelingen

3. Consumenten identiteit in het buitenland

Ook in het buitenland is of wordt gewerkt aan oplossingen voor een betrouwbare en algemeen bruikbare online identiteit voor consumenten. Ondanks verschillen in cultuur en wetgeving valt er veel te leren van de consumenten identiteitsaanpak in andere landen. In het cidSafe project is een studie[8] gedaan naar de aanpak in Zweden, Noorwegen, Denemarken, België, Estland, Duitsland en de VS. De identiteitsoplossingen van deze landen halen regelmatig (overwegend) goede publiciteit, worden vaak aangehaald door onderzoeksbureaus als IDABC/ISA en Forrester, en worden vaak gepresenteerd tijdens identity conferenties.

[8] Zie “Consumenten identiteiten: analyse van buitenlandse cases”, cidSafe project, 30 september 2010, Bob Hulsebosch. Te downloaden van http://cidsafe.novay.nl.

De studie richt zich vooral op het onderliggende business model, de business case, de gebruikte technologie en de rol van de overheid. Stuk voor stuk essentiële aspecten voor een gezonde consumenten identiteitsoplossing. Een samenvattend overzicht van deze aspecten per aanpak in het buitenland staat in de onderstaande tabel. Let wel, dit is een momentopname omdat veel oplossingen onlangs zijn uitgerold of nog volop in ontwikkeling zijn. Het overzicht is tot stand gekomen op basis van publiekelijk toegankelijke informatie (desktop research).

		Denemarken -nemID	Belgie - beID	Duitsland - eID	Noorwegen – BankID	Zweden - BankID	Estland – ID card	VS –ICAM
Techno-logie	Type Authenticatie	OTP kaart. Authenticatie ge-baseerd op unieke ID.	Smartcard met unieke ID.	Contactloze smartcard zonder unieke ID.	Smartcard of token (OTP generator).	Smartcard of soft-certificate. Beiden hebben een unieke ID.	Smartcard met unieke ID.	Meerdere manieren van authenticatie mogelijk.
	Attributen	Geen uitwisseling van attributen.	Uitwisseling van een kleine set van attributen vanaf de smartcard mogelijk.	Uitwisseling van een kleine set van attributen vanaf de smartcard mogelijk.	Uitwisseling van een kleine set van attributen vanaf de smartcard mogelijk.	Uitwisseling van een kleine set van attributen vanaf de smart card of via het certificaat mogelijk.	Uitwisseling van een kleine set van attributen vanaf de smartcard mogelijk.	Mogelijk om attributen uit te wisselen via bv OpenID.
	Digitale handtekening	Niet mogelijk.	Mogelijk.	Mogelijk (na opt-in).	Mogelijk.	Mogelijk	Mogelijk.	Niet mogelijk.
	Binding	Op basis van fysieke presence en identifica-tie, online na identifi-catie of via de bank.	Op basis van fysieke presence en identificatie.	Op basis van fysieke presence en identificatie.	Op basis van fysieke presence en identificatie.	Op basis van fysieke presence en identificatie.	Op basis van fysieke presence en identificatie.	Variabel, afhankelijk van het LoA.
Business model	Trust	Federatie met overheid als IdP.	PKI met overheid als IdP. Groot-banken doen niet mee.	PKI met overheid als IdP.	PKI met banken als IdP.	PKI met banken als IdP.	PKI met overheid als IdP.	Federatief model met bestaande publieke en private IdPs.
	# corners	3-corner model	3-corner model	3-corner model	3-corner model	4-corner model	3-corner model	4-corner model.
	Market entry	Via publieke en private diensten; C2B, C2G, B2B en B2G.	Via publieke diensten.	Via publieke en private diensten.	Via publieke en private diensten.	Via publieke en private diensten.	Via publieke en private diensten; C2B en C2G.	Via publieke en private diensten.
Business case	Consument	Gratis.	Gratis voor diensten; moet wel smartcard en reader aanschaffen.	Gratis voor diensten; moet wel smartcard en reader aanschaffen.	De kosten voor de consument worden verrekend in het bank totaal-pakket.	Gratis voor consument bij gebruik van soft-certificate; smart cards kosten geld.	Een ID-card kost zo'n 15 Euro. Een zakelijke ID-card kost ongeveer 300 Euro.	?
	RPs	Betalen per login of voor een heel jaar per gebruiker of een vast bedrag.	Gratis.	?	Worden dmv verschillende modellen belast door BankID.	Kosten voor RP per transactie. Verschilt per bank en applicatie.	RPs betalen een vaste prijs per transactie of in bundels.	?
Gover-nance	Toezicht	DanID beheert nemID. Overheid is toezichthouder.	Overheid.	Overheid.	Banken.	Banken.	Overheid en banken.	Overheid.
	LoA	3	4	4	3 en 4	4	4	Alle niveaus.
Succes		Moet nog blijken.	Nog niet.	Moet nog blijken.	Ja, veel Noren hebben een BankID en gebruiken hem ook regelmatig.	Ja, veel Zweden hebben een BankID en gebruiken hem ook regelmatig.	Nu banken en telecom operators ook meedoen is er sprake van succes.	Moet nog blijken; zit nog in een pilot-fase.

Een opvallende observatie is dat initiatieven waarbij banken betrokken zijn vaak beter lopen dan degene die voornamelijk door de overheid geïnitieerd worden. Een oorzaak hiervoor kan zijn dat het belangrijk is dat de consumenten identiteit regelmatig gebruikt wordt en dat lukt niet alleen met overheidsdiensten; private dienstenaanbieders zijn hiervoor essentieel. Online bankieren is één van de diensten die voor een brede uitrol van sterke identiteiten kan zorgen. Initiatieven zonder betrokkenheid van de overheid en van de banken komen niet voor bij de onderzochte landen.

Echt gebruik van een consumenten identiteit begint pas als bijna iedereen er één heeft. De banken zijn, naast de overheid, vaak degenen die de consumenten identiteiten uitdelen. Zij bedienen een groot deel van de consumenten en hebben de middelen om een goede registratie van identiteiten te doen. De infrastructuur voor authenticatie van een consument wordt vaak door een derde partij verzorgd. Deze partij wordt door de banken en door de overheid gecontroleerd. Het bijbehorende business model is daarmee over het algemeen te karakteriseren als een zogenaamd 3-corner model.

Een andere voorwaarde voor succes is dat dienstenaanbieders eenvoudig moeten kunnen instappen in een dergelijk 3-corner model. Een consumenten identiteit mag technisch niet te complex zijn voor de dienstenaanbieders en de risico's moeten te overzien zijn. Dit is onder andere te realiseren door het gebruik van open standaarden waardoor interoperabiliteit tevens gegarandeerd is en het verschaffen van goed geteste software en/of test suites.

De technologische invulling van een consumenten identiteit varieert: een Public Key Infrastructure met smartcards is mogelijk, maar ook zogenaamde one-time-password[9] gebaseerde oplossingen lijken levensvatbaar (Denemarken, Noorwegen). Oplossingen moeten geschikt zijn voor single sign-on (SSO). Digitale handtekeningen functionaliteit wordt nog spaarzaam gebruikt maar lijkt groeiende.

Toezicht van de overheid is vooral bij een federatief model gewenst om ervoor te zorgen dat identiteitsproviders en dienstenaanbieders voldoen aan alle eisen die voor dit model gelden, en daarmee het vertrouwen naar alle partijen toe te vergroten.

Ook voor de consument mag de drempel voor gebruik van een digitale identiteit niet te hoog zijn. Consumenten moeten begrijpen waartoe de betrouwbare digitale identiteit dient en wat de voordelen ervan zijn. Gebruiksgemak valt hier ook onder; de oplossing moet eenvoudig te verkrijgen, te gebruiken en te hergebruiken zijn. In het buitenland wordt dit opgelost door bijvoorbeeld e-functionaliteit op een bestaande identiteitskaart toe te voegen zodat deze ook online gebruikt kan worden (België), of doordat overheid en bedrijfsleven afspraken maken over een gezamenlijke, herbruikbare bestaande oplossing zoals in Estland het geval is.

Een klein bedrag (van enkele Eurocenten) voor elke geauthenticeerde transactie of een jaarlijks bedrag is gebruikelijk, waarbij de dienstenaanbieder en soms ook de consument betaalt. De dienstenaanbieder betaalt in het algemeen de identiteitsprovider voor de geleverde authenticatie- en handtekeningendienst. In landen met een smartcard oplossing moet de consument vaak zelf zijn smartcard en bijbehorende lezer aanschaffen (van ongeveer 15 Euro). De hoogte van de kosten en de manier van innen varieert per land en soms ook per toepassing.

Vertrouwen is essentieel, en daarmee is voorzichtigheid troef bij alle oplossingen. Eenmaal verloren vertrouwen door fouten, of de perceptie hiervan, is moeilijk zo niet onmogelijk te herstellen waarmee de oplossing gedoemd is te falen. Veel landen hanteren daarom een behoedzame strategie voor het introduceren van hun consumenten identiteitsoplossing. Uit de verschillende buitenlandse cases komt niet naar voren dat de rol van de banken nodig is voor het creëren van vertrouwen. Wel speelt de overheid een belangrijke rol als toezichthouder op de aangeboden identiteitsoplossing. Blijkbaar is de rol van de overheid als ‘trusted party’ gewenst.

4. Eisen aan een identiteitsoplossing

Hieronder staan op hoog niveau de eisen geformuleerd waaraan een betrouwbare consumenten identiteitsoplossing moet voldoen. De eisen zijn gebaseerd op gesprekken met experts uit het cidSafe consortium en klankbordgroep, op discussies tijdens de netwerkbijeenkomsten en op de analyse van de buitenlandse cases.

Algemeen bruikbaar – een consument moet één digitale identiteit kunnen gebruiken bij meerdere online dienstenaanbieders. Dit voorkomt de spreekwoordelijke digitale sleutelbos, verhoogt conversie en gebruikersgemak en leidt tot aanzienlijke kostenbesparingen.

Betrouwbaar – de identiteit moet betrouwbaar zijn, zowel voor de online dienstenaanbieder die zijn business ervan afhankelijk maakt, als voor de gebruiker die kwetsbaar is voor bijvoorbeeld diefstal van zijn identiteit. Voor de verzekeringsector gaat het qua veiligheid, in technische termen, om een Level of Assurance 2 en 3 (zie hierboven). Betrouwbaar gaat echter verder dan veiligheid en vereist een vertrouwen in de verstrekkers van de identiteiten, bijvoorbeeld als het gaat om beschikbaarheid, continuïteit en de bescherming van de privacy. Onafhankelijk toezicht en een rol van de overheid kan hierbij helpen.

Hergebruik van bestaande middelen – hergebruik van bestaande identiteiten die mensen al hebben, zoals bancaire identiteiten, is nodig om de business case voor uitdelen van nieuwe identiteiten op de schaal die nodig is voor een consumenten identiteitsoplossing realistisch te houden. Daarnaast is het nodig al bij introductie een hoge penetratiegraad te hebben onder consumenten, anders is de oplossing voor online dienstenaanbieders niet interessant.

[9] Zie http://nl.wikipedia.org/wiki/Eenmalig_wachtwoord.

Toekomstvast – eisen aan identiteitsoplossingen, inclusief de veiligheid van authenticatiemiddelen, zullen veranderen. Een oplossing moet de online dienstenaanbieders hiervan isoleren, en een continue evolutie naar veiligere, gebruikersvriendelijkere of anderszins betere authenticatiemiddelen, registratieprocessen en identiteitsproviders mogelijk maken.

Schaalbaarheid & interoperabiliteit – het moet makkelijk zijn voor, met name, dienstenaanbieders om gebruik te maken van de oplossing. Dit vereist een goede interoperabiliteit, maar ook een simpele manier om contractueel toegang te krijgen. Alleen op deze manier schaalt de oplossing naar veel dienstenaanbieders.

Frequent gebruik – als gebruikers niet vaak genoeg de identiteit gebruiken, vergeten ze het wachtwoord. Daarnaast is volume nodig voor een gezonde business case (lage kosten voor de online dienstenaanbieders). Bancaire middelen hebben het voordeel dat deze in de regel al vaak gebruikt worden, net zoals de, minder betrouwbare, sociale netwerk identiteiten.

Privacy – is belangrijk vanuit het perspectief van de consument, maar ook vanuit de online dienstenaanbieder. De consument wil inzicht en controle over wat er met zijn privacy gevoelige gegevens gebeurt. De online dienstenaanbieder wil voorkomen dat anderen, en met name concurrenten, inzicht krijgen in hoeveel en welke consumenten online haar diensten afnemen.

5. Visie: een trust framework

Omdat een overheidsoplossing niet aannemelijk lijkt in Nederland heeft het cidSafe project de kansen voor een betrouwbare marktoplossing geanalyseerd. Een marktoplossing kent grote uitdagingen, met name voor betrouwbaarheid, schaalbaarheid en kosten van marktintroductie. Voor betrouwbaarheid en schaalbaarheid is een goed trust framework essentieel. In een trust framework (ook wel afsprakenstelsel genoemd) worden afspraken gemaakt rondom betrouwbaarheid, zoals auditing van identiteitsproviders, business model, veiligheidseisen en privacy. Ook wordt in een trust framework afspraken gemaakt over schaalbaarheid, zoals interoperabiliteit en makkelijk contractueel aansluiten van dienstenaanbieders. Met contractueel aansluiten wordt bedoeld wat een dienstenaanbieder contractueel moet regelen om gebruik te maken van alle identiteitsproviders.

Onderdeel van het trust framework is een governance orgaan waarin belanghebbenden vertegenwoordigd zijn. Dit orgaan controleert de afspraken, en is verantwoordelijk voor de verdere ontwikkeling van het trust framework. De markt bepaalt wie de identiteitsproviders worden, en welke authenticatiemiddelen ze leveren. Voor de marktintroductie is het essentieel dat er een goed business model onder het trust framework ligt, en dat er al bij de start een hoge penetratie is onder consumenten.

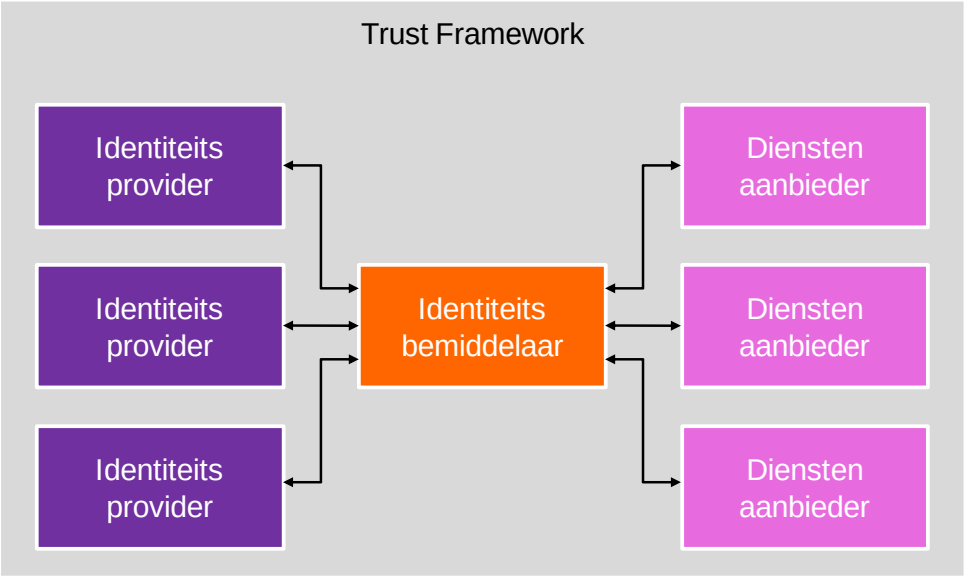
Een trust framework kan gezien worden als een manier om de noodzakelijke openheid te combineren met voldoende vertrouwen. Immers, een marktbenadering betekent dat allerlei partijen in staat worden gesteld hun diensten aan te bieden, maar er zijn wel afspraken en controle hiervan nodig om vertrouwen te creëren in deze diensten.

Er zijn tal van invullingen mogelijk voor een trust framework voor consumenten identiteit. De detail uitwerking hiervan is geen onderdeel van cidSafe, wel staan hieronder de voornaamste keuzes rondom de veiligheid, business model, mobiel en privacy:

- *Veiligheidsniveaus* - Het trust framework zal een zekere variëteit aan middelen en processen toe moeten staan om toekomstvast en schaalbaar te zijn. Dit leidt tot het vaststellen van veiligheidsniveaus, die afhangen van de sterkte van het authenticatiemiddel en de kwaliteit van de processen van uitgifte van die middelen. Gezien de initiële focus van cidSafe op de financiële sector zijn verzekeraars de grootste groep aan potentiële dienstenaanbieders die gebruik kunnen gaan maken van dit trust framework. Uit een inventarisatie onder drie grote verzekeraars blijkt dat bestaande bancaire authenticatiemiddelen en registratieprocessen ruimschoots voldoen aan de eisen van deze verzekeraars[10].
- *Business model* – Uit studies in het buitenland blijkt dat consumenten niet of slechts heel beperkt willen betalen voor een identiteit. Dit zal dus een indirect onderdeel moeten zijn van de

[10] Het gaat hier om STORK Levels of Assurance 2 en 3.

dienstverlening. In het business model zullen de online dienstenaanbieders daarom degenen moeten zijn die de identiteitsproviders betalen. Om het makkelijk te maken voor online dienstenaanbieders om zich aan te sluiten kan het introduceren van een extra partij in het business model helpen. Deze partij (de identiteitsbemiddelaar) zit tussen de dienstenaanbieder en de identiteitsproviders in, zodat dienstenaanbieders zowel technisch als contractueel de aansluiting niet per identiteitsprovider hoeven te doen. Zie Figuur 2 voor een visualisatie van de rol van de identiteitsbemiddelaar. In eHerkenning voor bedrijven heet deze rol de herkenningsmakelaar. Een bijkomend voordeel van het ontkoppelen van de identiteitsproviders en de dienstenaanbieders is dat de eersten geen zicht hebben over het gebruik van specifieke dienstenaanbieders door consumenten.



Figuur 2 Visualisatie van de positie van een identiteitsbemiddelaar in het trust framework

- *Mobiel* – het mobiele kanaal wordt steeds belangrijker. Daarom wordt de mobiele telefoon steeds meer gezien als dé toekomstige drager van het authenticatiemiddel. In het trust framework mogen geen afspraken staan die dit in de weg staan.
- *Privacy* – Een herbruikbare identiteit brengt privacy-risico's met zich mee. Het trust framework moet state-of-the-art privacy enhancing technologieën, privacy-by-design en informed consent verplicht stellen, en bovendien eisen stellen met betrekking tot de privacy-bescherming door de identiteitsprovider en dienstenaanbieders. Onderdeel hiervan is dat het mogelijk moet zijn om alleen specifieke attributen te delen, zoals "ouder dan 18" of "woont in Enschede", zonder dat er uniek identificerende informatie wordt meegestuurd. Een unieke persistente identifier voor elke consument wordt hiervoor niet gebruikt. Verder worden identiteitsproviders, en waarschijnlijk ook dienstenaanbieders, voorgeschreven over hoe ze om moeten gaan met de privacy gevoelige gegevens, zoals wanneer deze te vernietigen en hoe deze te beveiligen.

Hoewel het hierboven geschetste trust framework primair een marktaangelegenheid is, is het om een brede maatschappelijk acceptatie te krijgen, en om het vertrouwen te vergroten, wenselijk zo niet noodzakelijk dat de overheid een rol heeft als toezichthouder. Aangezien de trust framework aanpak goed aansluit op de aanpak van eHerkenning voor bedrijven die het ministerie van EL&I aan het introduceren is, is er een win-win situatie mogelijk wanneer een consumer-2-business trust framework aansluiting vindt bij dat eHerkenning afsprakenstelsel. Dit biedt praktische voordelen voor zowel consumenten als online dienstenaanbieders door de ontstane schaalvergroting in het gebruik van die identiteit. Zie Appendix A voor een korte analyse van mogelijk hergebruik van eHerkenning.

6. Scenario's

Inherent aan het open karakter van een trust framework zoals hierboven geschetst, is dat het op verschillende manieren tot stand kan komen. We schetsen hieronder een tweetal scenario's waarop dit

zou kunnen gebeuren, en ook een tweetal scenario's voor alternatieve oplossingen. Dit is geen uitputtende lijst, maar is bedoeld om concreter te maken hoe een trust framework in de praktijk zou kunnen werken en wat alternatieven zouden kunnen zijn.

Scenario 1: eHerkenning voor consumenten

Het huidige afsprakenstelsel van eHerkenning voor bedrijven wordt hergebruikt en aangepast voor consumer-2-business. In 2011 wordt dit aangepaste trust framework gedefinieerd, waarna eind 2011 pilots starten. De banken in Nederland die online bankieren aanbieden sluiten zich aan als identiteitsproviders, eventueel indirect via een derde partij, waarmee er vrijwel 100% dekking is onder consumenten. Daarnaast zijn er een paar andere partijen actief als identiteitsprovider, zoals bijvoorbeeld de huidige identiteitsaanbieders binnen eHerkenning. Hergebruik van authenticatiemiddelen is zo optimaal. In 2012 lopen een paar innovatieve verzekeraars voorop als afnemer, in 2013 volgen de meeste andere verzekeraars en neemt gebruik buiten de verzekeringssector ook snel toe. Verschillende LoA niveaus worden aangeboden. Identiteitsproviders profiteren van sterk toenemende authenticatievolumes. De overheid stimuleert het tot stand komen van eHerkenning voor consumenten, en draagt blijvend bij aan het vertrouwen en openheid door een toezichthoudende rol. In 2013 zijn er ook banken die in plaats van identiteitsprovider juist afnemer worden, en wordt de rol van identiteitsprovider voor de hogere veiligheidsniveaus geconcentreerd bij een selecte groep gespecialiseerde partijen.

Scenario 2: cidSafe trust framework

Vergelijkbaar met scenario 1, maar dan zonder afstemming met eHerkenning. Het vertrouwen in het trust framework komt vanuit branche organisaties en consumentenvertegenwoordigers. Hierdoor duurt het wat langer voordat er hoge volumes zijn. Best practices tussen eHerkenning en cidSafe worden gedeeld, en er vindt afstemming plaats over de technische interoperabiliteit. De governance over het cidSafe framework is gescheiden van die van eHerkenning.

Scenario 3: Tijdelijke SMS oplossing voor de verzekeringssector

In 2011 wordt een sectorspecifieke oplossing uitgewerkt waarin de verzekeraars een identiteitsoplossing delen op basis van een combinatie van gebruikersnaam/wachtwoord en SMS one-time-password (Level of Assurance 2). De binding tussen de consument en zijn/haar mobiele telefoon wordt door elk van de verzekeraars gedaan, maar is wel centraal ontsloten zodat een consument het maar eenmalig hoeft te doen. Er komt een stichting die dit beheert, met vertegenwoordigers van de initiërende verzekeraars en branchevertegenwoordigers (zoals Verbond van Verzekeraars en Adfiz). Eind 2011 begint een handvol verzekeraars hiermee, in 2012 krijgt het bredere opvolging. De kosten van de infrastructuur worden gedeeld tussen de verzekeraars, wat besparingen oplevert. Gebruikers gebruiken hun wachtwoord vaker dan voorheen en vergeten het daardoor minder vaak. Voor de meeste diensten is deze oplossing voldoende, maar voor bijvoorbeeld banksparen en bepaalde mutaties worden per verzekeraar veiliger middelen (smartcards) uitgereikt waardoor een deel van de consumenten meerdere smartcards heeft voor online authenticatie. In 2014 begint de Nederlandse overheid met de uitrol van de elektronische Nederlandse identiteitskaart (eNIK) die in tegenstelling tot DigiD wel gebruikt mag worden voor consumer-2-business. In de periode 2014-2019 krijgen steeds meer Nederlanders hier de beschikking over, en langzaam vervangt de eNIK de gedeelde SMS authenticatie oplossing en smartcards. In 2020 wordt de stichting opgeheven.

Scenario 4: Verzekeringssector specifieke oplossing op basis van bancaire middelen

In 2011 wordt er een sectorspecifieke oplossing uitgewerkt waarin de verzekeraars gebruik maken van de huidige bankauthenticatie oplossingen middels een gedeelde infrastructuur. Het beheer van deze infrastructuur ligt bij een door de sector opgerichte stichting. Verzekeraars kunnen makkelijker via deze stichting aansluiten dan rechtstreeks bij elke bank, en de technische infrastructuur maakt het onmogelijk voor de banken te zien welke consument bij welke verzekeraars inlogt. De banken verzorgen de binding tussen identiteit van de persoon en zijn/haar bankpasje als authenticatiemiddel alsmede het uitgifteproces ervan. In vergelijking met scenario 2 is het geheel wat meer gesloten, waardoor de governance simpeler is, en het minder investeringen vereist om tot stand te komen. Dit scenario kan gezien worden als een beperkt trust framework. In 2012 sluiten de eerste verzekeraars zich aan. In 2015 zijn er ook andere branchespecifieke oplossingen ontstaan, en in 2016 wordt de stichting ondergebracht in een breder trust framework.

7. Business case

De business case voor dienstenverleners en identiteitsproviders voor een betrouwbare en herbruikbare consumenten identiteit op basis van een trust framework is niet eenvoudig te maken. De business drivers als kostenbesparing, toegenomen efficiency, betere beheersing van risico's en compliance laten zich moeilijk in harde valuta vertalen. De nadruk zal daarom vooral moeten liggen op de kwalitatieve winstpunten.

We gaan in deze sectie uit van een business model waarbij dienstenaanbieders aan de identiteitsproviders een vergoeding betalen voor het leveren van de identiteiten. We beschrijven eerst kwalitatief de business case voor zowel dienstenaanbieders als identiteitsproviders, en geven vervolgens een indicatieve kwantificatie van de business case voor de gehele verzekeringssector.

Dienstenaanbieders – kwalitatieve business case

De business case voor een dienstenverlener kent als belangrijkste voordelen:

- *Kostenbesparingen voor authenticatie* – de consument zal minder vaak de helpdesk hoeven bellen, omdat het authenticatiemiddel vaker wordt toegepast en het resetten van wachtwoorden of uitdelen van nieuwe authenticatietokens zal minder vaak voorkomen. Daarnaast is een gezamenlijke aanpak kostenefficiënt.
- *Hogere conversie* – doordat het aanmelden sneller gaat, kunnen nieuwe klanten makkelijker en sneller diensten beginnen af te nemen.
- *Kostenbesparingen door efficiëntere processen* – omdat de externe identiteit in principe veiliger is, zullen er minder controles en veiligheidsstappen nodig zijn waardoor processen efficiënter ingericht kunnen worden.
- *Kostenbesparingen door meer gebruik online kanaal* – er ontstaan meer mogelijkheden voor self-service en dienstverlening in het algemeen via het online kanaal. Dit is goedkoper dan andere kanalen, zoals bijvoorbeeld telefoon of bezoek aan een kantoor.
- *Klantvriendelijkheid* – totdat het gemeengoed wordt, is het ondersteunen van externe identiteiten onderscheidend qua klantvriendelijkheid ten opzichte van concurrenten.

De voornaamste nadelen zijn:

- *Risico* – Er is een afhankelijkheid van een groep identiteitsproviders qua veiligheid maar ook qua beschikbaarheid. Er zijn hierover wel afspraken gemaakt in het trust framework, inclusief aansprakelijkheid;
- *Identifier mapping* – Bestaande klanten die zich aanmelden via een externe identiteitsprovider hebben geen uniek nummer dat ook voorkomt in de klantendatabase. Het is nodig om de eerste keer dat een bestaande klant inlogt via een externe identiteitsprovider deze te 'mappen' op de interne klantidentifier. Dit kan bijvoorbeeld aan de hand van naam, adres, geboortedatum en plaats, maar dit zal niet altijd voldoende zijn;
- *Branding* – de dienstenaanbieder verliest in vergelijking tot een eigen identiteitsoplossing een mogelijkheid voor branding, bijvoorbeeld een logo op een smartcard. Het is mogelijk dat een concurrent als identiteitsprovider op treed.
- *Investeringen* – er zijn initiële investeringen nodig in de ICT infrastructuur om gebruik te kunnen maken van externe identiteitsproviders, en zaken zoals Levels of Assurance. Ook zal het in de meeste gevallen in de beginperiode ook mogelijk moeten zijn nog dienstenaanbiederspecifieke identiteiten te gebruiken.

Identiteitsprovider – kwalitatieve business case

De business case voor een identiteitsprovider kent als belangrijkste voordelen:

- *Inkomsten* – de dienstenaanbieders betalen aan de identiteitsprovider. In het geval dat een identiteitsprovider bestaande identiteiten kan hergebruiken, zijn er weinig additionele kosten nodig.
- *Churn reduction* – het zal 'gedoe' zijn voor consumenten om van identiteitsprovider te wisselen, er wordt een extra binding opgebouwd met de consument.

- *New business* – voortbouwend op het vertrouwen van de consument zijn aanpalende diensten mogelijk zoals digitale kluisjes, portals en machtigingen.
- *Maatschappelijk imago en zichtbaarheid*– identiteitsprovider zijn voor grote aantallen consumenten is een zichtbare rol, die bijdraagt aan gebruikersgemak, het stimuleren van de online diensteneconomie en tegengaan van de diefstal van identiteiten.

De voornaamste nadelen zijn

- *Risico* – als er wat mis gaat, ook als dit slechts incidenten zijn, kan dit tot aansprakelijkheid leiden en zorgen voor schade aan het publieke vertrouwen.
- *Onzekerheid* – omdat dit een nieuwe markt betreft, zal er onzekerheid zijn over opbrengsten, succes en de validiteit hiervan over langere termijn.

Kwantitatieve business case voor de verzekeringssector

De kosten van een identiteit liggen met name in het authenticatiemiddel, en het registratie- en uitgifteproces hiervan. De kosten van het authenticatiemiddel zijn natuurlijk afhankelijk van het middel, waarbij het niet zo is dat het direct gerelateerd is aan de betrouwbaarheid. Bijvoorbeeld gebruikersnaam/wachtwoord brengt op zich geen hardware kosten met zich mee, maar wel kosten voor de helpdesk als de gebruikersnaam vergeten wordt. SMS authenticatie is vaak bovenop gebruikersnaam/wachtwoord, en brengt SMS kosten met zich mee. Het derde voor de hand liggende authenticatiemiddel is een smartcard. Dit brengt kosten voor de smartcard zelf, en voor de reader met zich mee, maar geen kosten per gebruik.

De kosten van het registratieproces zijn wel grotendeels afhankelijk van de betrouwbaarheid, waarbij ook het her-registeren meegenomen moet worden. Dit her-registeren is het proces dat doorlopen wordt als een gebruiker zijn authenticatiemiddel niet meer heeft (bijvoorbeeld wachtwoord vergeten). Dit her-registeren moet natuurlijk even veilig zijn als de oorspronkelijke registratie, wat in de meeste gevallen betekent dat hetzelfde proces nogmaals doorlopen wordt.

Om een indicatie te krijgen van de kwantitatieve business case voor de verzekeringssector hebben we drie cases doorgerekend. Hierbij hebben we alleen de variabele kosten per gebruiker van de identiteitsoplossingen meegenomen. Allerlei andere kosten zoals bijvoorbeeld voor aanpassen van de ICT infrastructuur zijn buiten beschouwing gelaten. We doen dit zo omdat de besparingen bij een herbruikbare identiteit met name zitten in het minder vaak uitgeven van identiteiten. Of concreter: als een consument nu drie verzekeraars heeft, krijgt deze consument drie identiteiten. Bij een herbruikbare identiteit worden dit er één of zelfs nul (bijvoorbeeld bij hergebruik van de bancaire identiteit). Ook baten zoals kwalitatief geschetst hierboven, bijvoorbeeld simpelere processen, zijn niet meegenomen in de berekeningen.

De drie cases zijn:

1. *Ieder-voor-zich gebruikersnaam en wachtwoord* – zoals beschreven in sectie 2 is dit de huidige situatie bij de meeste verzekeraars.
2. *Branchebreed uitbesteden SMS* – hierbij gaat de verzekeringsbranche gezamenlijk een identiteitsinfrastructuur introduceren op basis van SMS one-time-password. Dit komt overeen met scenario 3 “Tijdelijke SMS oplossing voor de verzekeringssector” zoals geschetst in voorgaande sectie.
3. *Branchebreed hergebruik van bankauthenticatie* – dit komt overeen met scenario 4 “Verzekeringssector specifieke oplossing op basis van bancaire middelen”, en ook met de scenario’s 1 en 2 zonder gebruik buiten de verzekeringsbranche.

De volgende aannames naam gemaakt bij de berekeningen:

- Er zijn 10 miljoen klanten;
- Elke klant heeft verzekeringen bij drie verschillende verzekeraars;
- De tijdsspanne voor afschrijving is 5 jaar;
- Elke consument logt per jaar 4 keer in;
- Aangezien de 10 grootste verzekeraars samen bijna 85% van de markt in handen hebben[11], zal ervan uitgegaan worden dat er in Nederland 10 verzekeraars zijn;

[11] Uit 'Verzekerd van cijfers 2010' (Verbond van Verzekeraars).

- Verrekening van de kosten gaat per keer inloggen van een consument (dit kwam het meeste voor bij de buitenlandse cases, zie sectie 3).

Scenario	Eenmalige kosten	Jaarlijkse kosten	Totale kosten na 5 jaar	Totale kosten per klant per jaar na 5 jaar
Case 1 ieder-voor-zich gebruikersnaam en wachtwoord	€ 24.000.000	€ 18.000.000 - € 36.000.000	€ 114.000.000 - € 204.000.000	€ 2,28 - € 4,08
Case 2 branchbreed uitbesteden SMS	€ 10.000.000 - € 50.00.000	€ 15.000.000 - € 25.300.000	€ 85.000.000 - € 176.500.000	€ 1,70 - € 3,53
Case 3 branchebreed hergebruik van bankauthenticatie	€ 0	€ 800.000 - € 20.000.000	€ 4.000.000 - € 100.000.000	€ 0,08 - € 2,00

Business case 1 schetst min of meer de huidige situatie waarbij de cijfers zijn gebaseerd op gegevens van enkele verzekeraars. De eenmalige kosten bedragen € 0,80 per klant. Dit zijn de kosten voor het versturen van de brieven met daarin de toegangscredentials naar een reeds bekend huisadres. De jaarlijkse kosten bedragen tussen de € 0,60 en € 1,20 per klant. Dit zijn o.a. de kosten voor de helpdesk en het resetten van wachtwoorden. Met 10.000.000 klanten, die elk bij 3 verzekeraars een verzekering hebben, komt dit neer op een bedrag tussen de 114 en 204 miljoen euro na 5 jaar.

In case 2 wordt gebruik gemaakt van een gedeelde, branchebrede SMS authenticatie infrastructuur onder beheer van een derde partij. De kosten van deze case zijn gebaseerd op de kosten van DigiD zoals publiceert oor Logius[12]. Hierbij wordt niet aangenomen dat DigiD deze derde partij zal zijn, maar wel dat deze derde partij vergelijkbare kosten zal maken. De eenmalige kosten liggen dan tussen de € 1,00 en € 5,00 (‘educated guess’, hier geeft het jaaroverzicht van Logius geen inzicht in). De jaarlijkse kosten liggen tussen de € 1,50 en € 2,53 (wel af te leiden uit het jaaroverzicht). In totaal komt dit dan neer op een bedrag tussen de 85 en ongeveer 177 miljoen Euro na 5 jaar.

Tot slot de derde case waarin bestaande bankauthenticatiemiddelen worden hergebruikt door alle verzekeraars. Hierdoor zijn er geen eenmalige kosten meer. De jaarlijkse kosten in deze case bestaan alleen uit de kosten die de verzekeraars moeten betalen aan de uitgevers van de bestaande authenticatie middelen (bijvoorbeeld banken) voor het gebruik maken hiervan. Deze kosten zijn erg afhankelijk van de commerciële beslissing (van de banken) en zullen waarschijnlijk liggen tussen de € 0,02 (huidige kosten in Scandinavië) en € 0,50 (kosten voor betaling via iDEAL[13]). De jaarlijkse kosten (voor vier authenticaties) liggen dan tussen de € 0,08 en € 2,00. De totale kosten komen dan neer op een bedrag tussen de 4 en 100 miljoen euro na 5 jaar. Omdat in deze case uiteindelijk veel meer identiteitsproviders en dienstenaanbieders kunnen participeren, zal het aantal authenticatietransacties vele malen hoger kunnen liggen waardoor de prijs per transactie meer naar de ondergrens zal gaan.

In bovenstaande cases neemt het hergebruik van identiteiten toe: geen hergebruik bij de ieder-voor-zich oplossing (case 1), via wel hergebruik maar alleen binnen de verzekeringsbranche (case 2) naar ook buiten de branche hergebruik in case 3. Daarnaast neemt ook de betrouwbaarheid toe van gebruikersnaam/wachtwoord oplossing (LoA1) via een SMS oplossing (LoA 2) naar LoA 3 voor de bankoplossing. Tenslotte neemt ook de gebruikersvriendelijkheid toe door het toenemende hergebruik, en nemen de kosten af ondanks de toegenomen veiligheid en hergebruik.

[12] Zie Logius Jaaroverzicht DigiD 2009

[13] De kosten van een betaling via iDEAL verschillen per bank, aantallen transacties en abonnementsvormen. € 0,50 lijkt een realistische bovengrens (zie bv. tarieven Fortis, Rabobank en TargetPay).

Hoewel bovenstaande berekeningen door de simplificaties en aannames alleen indicatief beschouwd kunnen worden, komt er duidelijk uit naar voren dat een trust framework oplossing voor een veilige en herbruikbare identiteit door het hergebruik goedkoper is dan de huidige identiteitsoplossing, waarbij elke dienstenaanbieder gebruik maakt van gebruikersnaam/wachtwoord dienstenaanbieder. Hierbij zijn voordelen zoals toegenomen veiligheid en gebruikersvriendelijkheid nog niet meegerekend.

8. Discussie

In dit whitepaper hebben we het probleem en met name ook de kansen rondom digitale consumenten identiteiten geschetst. Hierbij staat een betrouwbare en herbruikbare identiteit centraal, en is de wenselijkheid van een trust framework aangetoond.

De haalbaarheid van deze aanpak hangt af van het commitment van drie (groepen van) partijen:

1. Dienstenaanbieders – zij moeten duidelijk maken dat ze externe identiteitsproviders gaan gebruiken, en welke eisen ze daaraan stellen.
2. Identiteitsproviders – hoewel het trust framework open is, en identiteitsproviders ook later kunnen toetreden, is het nodig dat het bereik van de identiteitsoplossing onder consumenten al bij de start van de oplossing voldoende groot is.
3. De overheid – niet alleen om vertrouwen in het trust framework te vergroten, maar ook om te voorkomen dat er alsnog een overheidsoplossing op de markt wordt gebracht die investeringen van de identiteitsproviders teniet doet.

Als de noodzaak en urgentie niet bij al deze drie (groepen van) partijen in voldoende mate gevoeld wordt, is een succesvolle marktintroductie onwaarschijnlijk. Voor dienstenaanbieders is het voor de business case immers nodig een vrijwel volledige dekking te hebben van haar consumenten. Voor de business case van identiteitsproviders, en dan met name voor banken als meest voor de hand liggende betrouwbare identiteitsproviders die gezamenlijk vrijwel de gehele Nederlandse bevolking afdekken, is het belangrijk voldoende zicht te hebben op volume en dus potentie voor omzet.

Appendix A – Hergebruik eHerkenning

eHerkenning is een in 2010 geïntroduceerd trust framework (afsprakenstelsel) voor business-2-government identiteit. Het ondersteunt zowel authenticatie als machtigingen. Zie http://www.eherkenning.nl voor meer informatie.

Hieronder staat een korte analyse wat er wel en niet hergebruikt kan worden van eHerkenning voor een consument-2-business trust framework.

Hergebruik is mogelijk voor:

- *Authenticatiemiddel en binding* – het mogelijk maken dat gebruikers de keuze hebben om hetzelfde middel te gebruiken voor verschillende toepassingen (C2B/B2B/B2G), en ook de binding/registratie hiervoor te hergebruiken. Hiermee zijn immer grote efficiency winsten te behalen (authenticatiemiddelen en binding is erg duur) alswel leidt dit tot gebruikersgemak.

- *Governance & audit richtlijnen* – hergebruik van audit richtlijnen leidt tot duidelijke efficiency winsten en lijkt mogelijk, eventueel met specifieke C2B extensies. cidSafe zou ook een vergelijkbare governance structuur kunnen adopteren, en deze eventueel zelfs kunnen delen met eHerkenning. Voordeel van dat laatste is het bewaken van consistentie van het afsprakenstelsel in toekomstige versies . Voor het operationele deel heeft dit alleen zin als ook de infrastructuur gedeeld wordt. Voor een C2B governance structuur zijn wel extra stakeholders die waarschijnlijk een rol moeten krijgen, denk aan consumentenorganisaties.

- *Standaarden* – eHerkenning heeft gekozen voor SAMLv2 (en XACML) en het gebruik van STORK Levels-of-Assurance, beiden zijn heel valide keuzes voor cidSafe/C2B.

- *Terminologie en semantiek* – hergebruik van eHerkenning terminologie/definities zoals gebruikt in het afsprakenstelsel (en toekomstige aanpassingen hiervan), en van de semantiek van parameters in uitgewisselde berichten, leidt tot meer begrip en betere interoperabiliteit.

Hergebruik van de volgende punt is niet goed mogelijk vanwege de andere eisen die een C2B oplossing stelt ten opzichte van een B2G oplossing:

- *Attributen* – eHerkenning ondersteunt geen attributen, voor een C2B oplossing is dit een absolute eis (NAW, geboortedatum etc). Als gevolg hiervan zal ook privacy een grotere issue worden (o.a. informed consent is nodig). Een attribuut-gebaseerde aanpak heeft ook impact op de inrichting van de achterliggende autorisatie-infrastructuur (welke dienstenaanbieder mag toegang krijgen tot welke attributen). Ook de authenticiteit van de aangeleverde attributen speelt een rol. De discussie rondom attributen speelt ook nog binnen eHerkenning (dit is een wens van dienstenaanbieders), mogelijk wordt dit onderdeel van C2G in eHerkenning. Gezamenlijk optrekken is hierbij gewenst.

Onduidelijkheid bestaat nog over de onderstaande punten:

- *Machtigen* – in eHerkenning treedt een natuurlijk persoon op namens een bedrijf, en zijn allerlei complexe machtigingsconstructies mogelijk (ketens etc). Voor C2B kan dit waarschijnlijk simpeler, en moet het in ieder simpel zijn vanuit een consumentenperspectief. Hoe dit precies zal moeten werken en urgentie hiervan is nog niet in voldoende diepte naar gekeken in cidSafe. Onder andere zouden we naar de Gemeenschappelijke Machtigings Voorziening moeten kijken (niet om te gebruiken, maar om concepten mogelijk te hergebruiken), en use-cases moeten opstellen i.o.m. verzekeraars en andere dienstenaanbieders (zoals bijvoorbeeld intermediairs). Pas daarna kan goed bepaald worden of het (technisch) past in de huidige aanpak van eHerkenning.

- *Liability* – Op grond van de 1.0 versie van het stelsel blijft er onduidelijkheid bestaan of er in C2B en B2G settings verschil in aansprakelijkheid is. Dit is een onderwerp van nadere studie of de huidige aansprakelijkheidsrichtlijnen voor eHerkenning ook passen voor C2B.

- *Rollen in het business model* – eHerkenning kent t.o.v. van het traditionele 3-party model van gebruiker-identiteitsprovider-dienstenaanbieder meer partijen. Met name gaat het uit van een 4-corner model met de Herkenningsmakelaar als vierde rol, en onderscheidt het verder authenticatiedienst, middelenuitgever, ondertekendienst en machtigingsregister. In de praktijk vallen de rollen authenticatiedienst en middelenuitgever samen, en is ondertekendienst nog niet ingevuld, maar dan nog zijn er vijf (en op den duur) 6 partijen. De vraag is of dit simpeler kan voor een C2B oplossing, bijvoorbeeld door de rollen van authenticatiedienst, middelenuitgever, ondertekendienst, machtigingsregister samen te nemen.Verder gaat eHerkenning er vanuit dat de bedrijven betalen voor authenticaties en machtigingenvoorzieningen terwijl de dienstenaanbieders het werk van de Herkenningsmakelaar vergoeden.

- *Verrekening binnen het business model* – dit lijkt nog een lopende discussie te zijn binnen eHerkenning, maar i.i.g. is het anders of een (werknemer van een) bedrijf de eindgebruiker is, of een consument, als het gaat om het betalen van de identiteitsprovider (authenticatiedienst, middelenuitgever, ondertekendienst, machtigingsregister). Consumenten zullen naar verwachting alleen indirect willen betalen voor een generieke identiteitsdienst; ze zullen niet gaan betalen voor elke authenticatietransactie.

- *Digitale handtekeningen* – dit is een belangrijke functionaliteit die nodig is voor C2B, indien niet in een eerste versie dan toch wel in een volgende versie. Het is op het moment van schrijven niet duidelijk hoe en wanneer dit onderdeel wordt van eHerkenning, dit zal in een later stadium bekeken moeten worden.