Authenticatie-middelenscan

Overzicht van technieken, dreigingen, en factoren voor succes en falen

Colofon

DATE	November 2010
VERSION	1.0
PROJECT REFERENCE	cidSafe AuthN-scan
URL	http://www.novay.nl
ACCESS RIGHTS	Consortium intern
STATUS	Final
EDITOR	Martijn Oostdijk
COMPANY	Novay
AUTHOR(S)	Martijn Oostdijk

Synopsis

Deze scan geeft de huidige stand van zaken op het gebied van authenticatiemiddelen- en technologieën weer. Gekeken wordt naar technieken, dreigingen en mogelijk oplossingsrichtingen die binnen geschetste kaders ondersteunend kunnen zijn voor een high-trust identiteitsoplossing welke met name toegepast kan worden voor authenticatie van consumenten in het financiële domein.

Contents

1 Introductie

Dit rapport bevat een scan van authenticatiemiddelen. Authenticatie is het proces dat, met een bepaalde mate van zekerheid, vaststelt of een gebruiker van een dienst over een geclaimde identiteit beschikt. In het kader van dit rapport wordt vooral gekeken naar authenticatie ten behoeven van *online* diensten, en in het bijzonder naar high-trust online diensten die via het Internet worden aangeboden aan eindgebruikers (“consumenten”). Typische voorbeelden van high-trust online diensten zijn te vinden in het financiële domein. Te denken valt, bijvoorbeeld, aan Internet-bankieren of het online afsluiten of beëindigen van een verzekering. Voor deze diensten is het voor zowel de gebruiker als voor de dienstaanbieder van belang dat de identiteit van de gebruiker met een hoge mate van zekerheid wordt vastgesteld.

Deze scan wordt uitgevoerd in het kader van het cidSafe (safe Consumer Identity) project. cidSafe beoogt een doorbraak te bewerkstelligen voor een veilige, gemakkelijke en toekomstbestendige digitale sleutel voor algemeen gebruik door consumenten op het internet. Het gaat hier om een high-trust oplossing, die gebruikt kan worden voor privacy en fraudegevoelige transacties. De initiële focus van het cidSafe project is op de financiële sector, met de ambitie in de toekomst ook high-trust scenario’s in andere sectoren te bedienen.

1.1 VRAAGSTELLING

De vraag die dit rapport tracht te beantwoorden bestaat uit twee deelvragen, die elk weer onderverdeeld kunnen worden in verdere deelvragen.

- Wat is de huidige stand van zaken op authenticatiemiddelengebied?
    - Wat is er voorhanden aan technieken? Hoe ondersteunen deze het authenticatieproces? Wat zijn de onderliggende principes?
    - Wat lijkt in de praktijk goed te werken? Waarom werken bepaalde technieken of middelen (wel of niet)?
- Wat zijn belangrijk kenmerken voor een succesvol high-trust consument-ID?
    - Hoe meet je de kwaliteit van authenticatie? Wat zijn succesfactoren?
    - Wat zijn de gevolgen van keuzes voor bepaalde technieken (kosten, implicaties voor back-end systemen)?

Hoewel authenticatie geen nieuw probleem is, technisch zijn een aantal zaken al lange tijd opgelost, vinden er nog steeds wel technische innovaties plaats. Het in kaart brengen van deze innovaties is een van de belangrijkste doelen van deze scan. Veel van de nieuwe ontwikkelingen worden gedreven door en richten zich op het voorkomen van nieuwe, inventieve en vaak specifieke aanvallen. Niet zelden gaat dit ten koste van gebruiksvriendelijkheid. Acceptatie van authenticatiemiddelen voor online diensten (als onderdeel van een totale identiteitsoplossing) door eindgebruikers is voornamelijk uitdagend vanwege schaalgrootte, gebruiksvriendelijkheid en het kostenmodel.

2 De Context

Dit hoofdstuk schetst de context waarin authenticatie gebruikt wordt. Dit hoofdstuk kijkt niet naar technologie (deze wordt in Hoofdstuk 3 beschreven) maar naar authenticatie in de brede zin van het woord. Het doel is om trends te signaleren die van belang kunnen zijn bij het slagen of falen van de technologie.

2.1 DE ROL VAN AUTHENTICATIE IN HET IDENTITEITSMANAGEMENT PROCES

Doorgaans gaat authenticatie vooraf aan autorisatie. Autorisatie regelt toegang tot diensten door toegangsrechten (indirect) toe te wijzen aan gebruikers. In zogenaamde autorisatie-policies wordt door de dienstaanbieder vastgelegd welke rechten gebruikers hebben voor het gebruik van diensten en de resources die ontsloten worden door die diensten. Autorisatie-policies kunnen alleen uitgevoerd worden als duidelijk is welke gebruiker toegang probeert te krijgen, i.e. alleen als authenticatie op orde is.

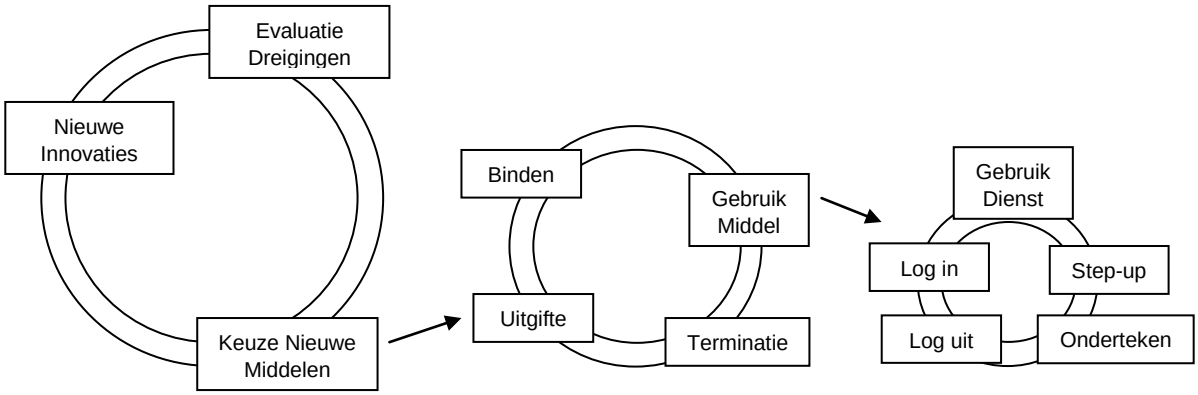
Bij dit “klassieke” authenticatie-voorafgaand-aan-autorisatie patroon vallen twee kanttekeningen te plaatsen: Ten eerste, *perfecte* authenticatie is zeker niet vereist om diensten aan te kunnen bieden of af te kunnen nemen. Het inzetten van authenticatie om online diensten te beschermen kost geld en brengt in de meeste gevallen gebruiksongemak met zich mee. Afhankelijk van de kans en impact van aanvallen zullen dienstenaanbieders wel of niet willen investeren in authenticatiemiddelen. Afhankelijk van de waarde van de dienst en de mate van gebruiksgemak zullen consumenten wel of niet bereid zijn om authenticatiemiddelen te gebruiken om de dienst af te kunnen nemen.

Ten tweede, vaak worden verschillende diensten, van verschillend niveau, aangeboden door een dienstverlener en is het niet nodig (en vanuit gebruiksvriendelijkheid zelf ongewenst) om gebruikers voorafgaand aan het afnemen van de dienst met maximale zekerheid te authenticeren, zelfs al is dit technisch mogelijk. Denk bijvoorbeeld aan het online laten inzien van een bankrekening op basis van gebruikersnaam en wachtwoord maar bij overschrijven een SMS met TAN code naar de gebruiker zijn of haar mobiele telefoon sturen.

Een identiteit (in de context van deze scan) is een verzameling gelabelde gegevens, zogenaamde attributen, over een gebruiker. Een identiteitsmanagementsysteem zou bijvoorbeeld gegevens als voornaam, achternaam, burgerservicenummer (BSN), adres, telefoonnummer en werkgever bij kunnen houden. Authenticatie heeft tot doel om vast te stellen of een gebruiker over een geclaimde identiteit beschikt zodat andere systemen met een zekere mate van zekerheid met de gegevens kunnen werken. Hiertoe worden aan de gebruiker doorgaans middelen verstrekt die de vorm van een fysiek token kunnen hebben (een fysieke sleutel, of een bankpas, of een USB token) maar ook andere vormen zijn mogelijk (een wachtwoord om te onthouden, of een certificaat dat op een desktop computer geïnstalleerd moet worden). In het identiteitsmanagementsysteem worden deze middelen op de een of andere manier gekoppeld aan de gegevens over gebruikers.

In het grotere geheel van een identiteitsmanagementsysteem is authenticatie slechts een klein technisch onderdeel.

Maar wel een essentieel onderdeel met grote consequenties. Identiteitsmanagementsystemen kunnen, voor wat betreft authenticatie, op drie verschillende niveaus beschouwd worden: strategisch, tactisch en operationeel. Het strategische niveau, het niveau van organisaties, beschrijft het verloop van hoe de eisen aan authenticatie veranderen onder invloed van externe factoren. Er worden continu nieuwe diensten ontwikkeld, er worden nieuwe dreigingen onderkend, nieuwe technieken komen beschikbaar, of de regelgeving verandert (op het gebied van privacy of aansprakelijkheid, bijvoorbeeld). Hierdoor zijn aanpassingen in beleid nodig, waardoor de eisen aan authenticatiemiddelen veranderen. Het kan dan bijvoorbeeld nodig zijn om opnieuw "assurance-niveau's" toe te wijzen aan de aangeboden diensten zodat andere klassen van authenticatiemiddelen ingezet moeten worden om de diensten adequaat te beveiligen. Of een innovatie op authenticatiegebied kan bijvoorbeeld de helpdeskkosten sterk doen dalen waardoor het aantrekkelijk wordt om gebruikers te voorzien van nieuwe authenticatiemiddelen.



Figuur 1: Strategisch, tactisch, operationeel niveau.

Het tactische niveau, het niveau van authenticatiemiddelen zelf, beschrijft de zogenaamde life-cycle van authenticatiemiddelen (en, meer in het algemeen, van identiteiten). Authenticatiemiddelen worden uitgegeven. Na of tijdens de uitgifte wordt een middel (al dan niet onder toezicht van de dienstaanbieder of een vertrouwde partij) gekoppeld aan de gebruiker: de zogenaamde binding of registratie (en soms andere namen[1]). De sterkte van deze binding heeft ook invloed op het assurance-niveau van het middel. Een eenmaal uitgegeven authenticatiemiddel kan gebruikt worden in sessies waarin de gebruiker de dienst afneemt. Mochten er problemen zijn tijdens het gebruik, dan moet aan incidentafhandeling gedaan worden door het opstarten van tevoren gedefinieerde procedures. Ten slotte, aan het einde van de life-cycle zal het authenticatiemiddel getermineerd worden. Hoe de life-cycle van een middel er precies uitziet zal gevat moeten worden in de hierboven genoemde policies.

De life-cycle van een authenticatiemiddel (het tactische niveau) maakt onderdeel uit van de grotere life-cycle van een gebruikersidentiteit in relatie tot een dienstverlener. De life-cycle van identiteiten zit ergens tussen het strategische en tactische niveau in. Een gebruiker zal meerdere authenticatiemiddelen "verslijten" gedurende zijn of haar relatie met de authenticatiemiddelenprovider en kan een relatie met een dienstverlener voor kortere of langere tijd onderbreken

[1] In [KPMG-2007] wordt dit aangeduid met "anker". "Issuance" of "uitgifte" is een andere veelgebruikte benaming.

(waarbij het token tijdelijk geen toegang tot de dienst mag verschaffen).

Het operationele niveau, het niveau van authenticatiesessies, beschrijft hoe authenticatiemiddelen toegepast worden tijdens het daadwerkelijk afnemen van een dienst. Een gebruiker meldt zich aan bij een dienst en claimt een bepaalde identiteit. Vervolgens wordt het authenticatiemiddel gebruikt om vast te stellen of de gebruiker daadwerkelijk over de geclaimde identiteit beschikt. De gebruiker kan nu de dienst afnemen maar elke actie van de gebruiker wordt door de dienstaanbieder aan autorisatie-policies getoetst.

Authenticatie wordt vaak uitgevoerd op een vaste plaats binnen een sessie: aan het begin, voorafgaand aan autorisatie. Echter, voor bepaalde deeldiensten is meer zekerheid gewenst. De dienstaanbieder kan de gebruiker om additionele zogenaamde *step-up* of *out-of-band* authenticatie vragen. De dienstaanbieder zal tijdens de sessie bepaalde transacties loggen, bijvoorbeeld ter ondersteuning van incidentafhandeling en kan op basis van “events” besluiten dat meer zekerheid omtrent de identiteit van een gebruiker vereist is. Naarmate diensten complexer worden zal het authenticatieproces wellicht van plaats en rol veranderen en zal de nadruk minder liggen op authenticatie aan het begin van de sessie.

Tenslotte zal, aan het einde van een sessie, de gebruiker zich afmelden zodat een volgende keer weer authenticatie nodig is om de dienst af te nemen. In sommige gevallen, zoals als een authenticatiemiddel onderdeel uitmaakt van een identiteitsoplossing die door meerdere dienstaanbieders gedeeld wordt, is het mogelijk om het aantal authenticaties te verminderen door gebruik te maken van single-sign-on (SSO). Bij SSO kan een sessie waarin een geslaagde authenticatiepoging vereist is meerdere dienstaanbieder-sessies overspannen.

Bepaalde authenticatiemiddelen bieden naast hun primaire authenticatiefunctie ook mogelijkheden om elektronische handtekeningen te genereren. Zo’n handtekening kan gebruikt worden om bijvoorbeeld documenten of email-berichten te ondertekenen, maar biedt ook mogelijkheden om een transactie of challenge te ondertekenen om op die manier de authenticiteit van een geclaimde identiteit te controleren. Door te ondertekenen met een middel dat aan de voorwaarden van de Europese richtlijn [EU directive 1999] elektronische handtekeningen voldoet, kan een rechtsgeldige handtekening gezet worden. Dit heeft juridische consequenties die bijvoorbeeld van invloed zijn op de aansprakelijkheid voor gevolgen die uit de ondertekende transactie voortkomen.

Eigenschappen zoals acceptatie, kosten en veiligheid komen voort uit de combinatie van eigenschappen op alle niveau’s. Het strategische niveau zegt veel over flexibiliteit en toekomstvastheid van het middel, terwijl op het operationele niveau snel duidelijk wordt hoe gebruiks(on)vriendelijk een authenticatiemiddel in de praktijk is. Maar deze aspecten worden ook door keuzes op de andere niveaus beïnvloed. Acceptatie door de consument wordt bijvoorbeeld sterk bevorderd door op operationeel niveau een middel aan te bieden dat intuïtief werkt maar ook door maatregelen op strategisch niveau die de perceptie van veiligheid bij de consument beïnvloeden. Bij de vergelijking van authenticatiemiddelen in §3.2 worden het tactische en operationele niveau beschouwd.

2.2 IDENTITEITSSYSTEMEN IN BINNEN- EN BUITENLAND

Een overzicht van buitenlandse identeitssytemen is in het kader van cidSafe reeds gegeven in [Hulsebosch2010]. Hulsebosch kijkt naar verschillende achterliggende factoren (business model, business case, governance, techniek) die het succes van een identiteitsoplossing zouden kunnen bepalen. De technische middelen die aan gebruikers worden uitgereikt, vormen slechts één van deze factoren. Deze sectie geeft per besproken land een korte analyse van de authenticatiemiddelen die in dat land toegepast wordt.

1. Belgie: De Belgische nationale identiteitskaart, de ".beID", is in 2002 gelanceerd door de Belgische overheid. Het middel is een PKI smart card met contact chip die zowel geschikt is voor authenticatie als voor ondertekenen. Belgie was relatief vroeg met het uitrollen van een nationale eID kaart. De certificaten op de kaart kunnen in principe door iedereen gevalideerd worden, maar alleen de overheid lijkt vooralsnog op te treden als dienstaanbieder.

2. Denemarken

   In Denemarken is sinds 2010 "nemID" gelanceerd door een derde partij ("DanID") opgericht door een aantal banken. De organisatie is wel ondersteund door de overheid. Het gaat om een code kaart (met TAN codes) in combinatie met een gebruikersnaam en wachtwoord. Hoewel de website praat over een digitale handtekening lijkt het middel nemID alleen authenticatie te bieden (en wordt de handtekening waarschijnlijk server-side geplaatst).

3. Duitsland

   Duitsland is voornemens om eind 2010 een nieuwe Nationale "eID" oplossing uit te rollen. Het Bundesambt für Sicherheit in der Informationstechnik (BSI) heeft hiervoor nieuwe standaarden ontwikkeld [BSI website]. Opvallend aan het Duitse initiatief is dat het om een contactloze smart card gaat. Deze hoeft niet in een lezer gestoken te worden alvorens gegevens met een computer uitgewisseld kunnen worden, maar kan op (zeer geringe[2]) afstand uitgelezen worden. Verder zullen vingerafdrukken opgeslagen worden en wordt rekening gehouden met "minimal disclosure" van informatie. De kaart kan zowel voor authenticatie als voor ondertekenen gebruikt worden.

   Duitsland was ook al sinds 2006 bezig om een nationale eHealth smart card te introduceren (die de pasjes van ziektekostenverzekeraars vervangt). Dit project is begin 2010 stopgezet.

4. Estland

   Estland heeft een door de Estse overheid uitgegeven Nationale eID kaart. Deze bestaat al sinds 2000. Het gaat om een PKI kaart met contact chip. De kaart kan voor overheids- en bancaire diensten gebruikt worden en het is zelfs mogelijk om de kaart te gebruiken in het openbare vervoer (in enkele steden, gegevens worden online gekoppeld aan een identiteit).

[2] De fysieke kenmerken van de kaart beperken het actief uitlezen van de kaart tot enkele centimeters.

Een ander Ests initiatief is de “bank eID”. Dit is een concurrerende oplossing door vijf grote banken. Deze maakt gebruik van TAN op papier of PIN calculators. Sinds kort hebben de banken en de overheid afgesproken om over te gaan op eID.

5 Nederland

Nederland heeft een door de overheid aangeboden gebruikersnaam + wachtwoord oplossing (DigiD niveau 1), versterkt met SMS OTP (DigiD niveau 2). Deze mag wettelijk alleen gebruikt worden voor overheidsdiensten, de zorg, en in zeer beperkte mate voor de financiële sector (omdat de dienstverlener het BSN aangeleverd krijgt bij succesvolle authenticatie), (zie [cidSafe flyer BSN]).

De banken in Nederland hebben, voor wat betreft internetbankieren, elk een eigen oplossing. Voor fysieke betalingen in steen-en-cement winkels werken ze samen (PIN). Ook voor online betalingen in Webwinkels wordt samengewerkt (Ideal). In beide gevallen wordt gebruik gemaakt van een centrale partij, een zogenaamde makelaar, die, voor wat betreft authenticatie, de gebruikers doorverwijst naar de eigen authenticatiemiddelenprovider (die in deze context ook wel “issuing” bank genoemd wordt).

Enkele ontwikkelingen die, enigszins op de achtergrond, meespelen bij de Nederlandse overheid zijn PKI-overheid. Dit is een PKI infrastructuur die voorziet in certificaten en sleutels. Een aantal bij de overheid geregistreerde certificaatleveranciers geeft certificaten uit aan natuurlijke personen, maar typisch om een bedrijf of organisatie te representeren. Ook hier geldt dat het gebruik door derden technisch gesproken mogelijk is. Mocht de Nederlandse overheid in de toekomst een eID aan haar burgers aan gaan bieden (de zogenaamde elektronische Nederlandse identiteitskaart, of eNIK) dan zal deze waarschijnlijk gebruik maken van deze PKI.

6 Noorwegen

In Noorwegen is door de gezamelijke banken een “BankID” uitgegeven. Deze heeft de vorm van een PKI smart card (§3.2.10), een applicatie op de SIM kaart (§3.2.12) of een OTP token (waarbij certificaat en sleutel centraal op een server worden opgeslagen) (§0). De oplossing kan gebruikt worden voor authenticatie en voor ondertekening.

Daarnaast heeft Noorwegen ook een door de overheid uitgegeven “minID”, op basis van TAN codes (op papier) en een online trusted third party (de belastingdienst).

7 Verenigde Staten

De VS hebben een authN agnostisch raamwerk waarbinnen verschillende vormen van authenticatie zijn toegestaan. Authenticatieproviders kunnen toegelaten worden als ze aan de gestelde eisen voldoen. Voor low-trust diensten kunnen toegelaten identity providers eenvoudige gebruikersnaam/wachtwoord oplossingen gebruiken. Voor high-trust diensten worden meer eisen gesteld en wordt gebruik gemaakt van smart cards (zoals bijvoorbeeld de CAC-kaart van het ministerie van defensie). Voor deze laatste categorie van diensten heeft de

FIPS een evaluatie programma voor smart cards en gerelateerde producten uitgebracht: FIPS-201[3].

8 Zweden

In Zweden is in 2003 ook een oplossing onder de naam “BankID” gelanceerd door een derde partij ondersteund door een aantal grote banken. Deze is te gebruiken voor overheid en bancair en private sector diensten (in praktijk voornamelijk overheid en bancair). Opmerkelijk is dat gekozen kan worden voor een PKI smart card (§3.2.10) of voor een soft certificate (§3.2.9) en dat deze laatste vorm populairder is bij de meeste Zweden.

Wat opvalt is dat een aantal landen een nationale oplossing heeft die door meerdere dienstverleners gebruikt kan worden. De mogelijkheid tot hergebruik van infrastructuur lijkt onafhankelijk te zijn van de gebruikte techniek. In sommige landen gaat het om gebruikersnaam en wachtwoord, in andere landen om OTP[4] gebaseerde middelen, en weer andere landen gebruiken PKI gebaseerde technieken. In een aantal landen zoals Belgie en Duitsland (maar ook Spanje, Portugal) voorziet de overheid de nationale identiteitskaart van een chip die, naast informatie over de burger, ook binnen een door de overheid beheerde PKI gebruikt kan worden voor authenticatie en ondertekening. In een aantal gevallen kunnen financiële instellingen zoals banken gebruik maken van de geboden infrastructuur. In sommige landen wordt een gemeenschappelijke oplossing zelfs door de (bancaire) markt geïnitieerd en beperken de diensten zich tot overheids- en bancaire diensten.

2.3 TRENDS EN ONTWIKKELINGEN

Deze sectie beschrijft enkele trends en ontwikkelingen die het authenticatieproces beïnvloeden. Het gaat hier om achtergrondontwikkelingen op gebied van identiteitsmanagement en financiële diensten. Gedetailleerde technische ontwikkelingen zoals nieuwe dreigingen en nieuwe innovaties worden in de Hoofdstukken 3 en 5 beschreven.

2.3.1 STANDAARDISATIE VAN HARDWARE EN SOFTWARE

Het platform dat door de consument thuis gebruikt wordt voor het afnemen van e-diensten (de PC) heeft de laatste jaren een aantal veranderingen op het terrein van standaardisatie doorgemaakt. Het besturingssysteem op de gemiddelde PC is minder belangrijk geworden, mits dit het gebruik van standaardgebaseerde web-browsers toestaat. Veel diensten worden immers via het web afgenomen. Ten opzichte van de gespecialiseerde e-banking applicaties, die nog door de gebruiker zelf geïnstalleerd moesten worden, is het afnemen van diensten via het web voor de gemiddelde gebruiker vele malen eenvoudiger.

Randapparatuur heeft tegenwoordig standaard USB, Bluetooth, en Wi-Fi aansluitingen. Hoewel voor veel randapparatuur nog steeds software (drivers) geïnstalleerd moeten worden voordat een besturingssysteem ermee overweg kan, bieden deze standaard koppelvlakken al veel gebruiksgemak boven de situatie die bestond in het pre-USB/Bluetooth/Wi-Fi tijdperk. Bepaalde klassen apparaten (toetsenborden, externe opslag, web-cams) kunnen vaak al driverless worden aangesloten, dat wil zeggen dat het inpluggen van het apparaat voldoende is. Smart cards,

[3] Zie http://fips201ep.cio.gov/apl.php.

[4] OTP, TAN, etc. zie §3.2.

smart card lezers en andere (aangesloten) authenticatietokens lijken in de toekomst ook driverless ondersteund te kunnen worden (zie bijvoorbeeld [ISO24727-3]). Soms kunnen drivers op een veilige manier door het token zelf geïnstalleerd worden (zoals bijvoorbeeld bij de IBM ZTIC die zich (ook) als USB harddisk voordoet, zie [Weigold et al.]). Voor de korte termijn blijft het installeren van drivers waarschijnlijk nodig, hetgeen een bron van problemen bij het uitrollen van (aangesloten) authenticatiemiddelen is.

Software ondersteuning voor authenticatie-en-onderteken-randapparatuur (denk aan browsers, maar ook email programma's en PDF viewers die ondertekenen ondersteunen) is al enigszins gestandaardiseerd [RSA labs] maar zal naar verwachting een verdere standaardisatieslag nodig hebben voordat grote groepen gebruikers naadloos in verschillende applicaties gebruik kunnen maken van een en dezelfde identiteit.

2.3.2 DE OVERHEID ALS ONLINE DIENSTENAANBIEDER

De overheid houdt traditioneel informatie bij over haar burgers. Deze informatie wordt verzameld ten behoeve van de processen van de overheid zelf (om belasting te kunnen heffen, om stempassen aan kiezers te kunnen sturen, etc.). Bovendien faciliteert de overheid identificatie van burgers richting derde partijen (zoals ambtenaren van buitenlandse overheden) door middel van, bijvoorbeeld, het paspoort.

Veel van de diensten die de overheid aan haar burgers aanbiedt worden tegenwoordig via elektronische kanalen aangeboden. De door de Nederlandse overheid ingevoerde authenticatie-standaard DigiD speelt hierbij een belangrijke rol. Het lijkt er niet op dat de Nederlandse overheid voor de middellange termijn dit middel gaat inzetten voor consumer-2-business diensten [Hulsebosch-gebruik BSN 2009]. In andere landen gebeurt dit soms wel, bijvoorbeeld voor diensten in de financiële sector. In sommige gevallen is de overheid juist afnemer van een identiteitsoplossing die uit de markt voorkomt.

2.3.3 VERVAGING VAN DOMEINEN

Het gebruik van computers door consumenten is in de laatste tien jaar enorm gestegen. De computer en andere ge-netwerkte apparaten spelen een steeds belangrijkere rol in het dagelijks leven in het privédomein. ICT ontwikkelingen op de consumentenmarkt gaan soms harder dan de ontwikkelingen op de zakelijke markt. Dit zorgt ervoor dat werknemers, die in hun vrije tijd ook consument zijn, verwachten dat ICT technologie in de werkomgeving zich net zo makkelijk laat bedienen als in de thuissituatie. Deze trend wordt wel aangeduid met "*consumerization*". Een gerelateerde trend is "*het nieuwe werken*"[5]. De rollen van consument en werknemer vloeien steeds meer in elkaar over; denk aan thuiswerken of onderweg werken, werken met apparatuur of programmatuur die eigendom is van de werknemer, etc. Deze trend heeft invloed op de wensen en verwachtingen die werknemers hebben ten aanzien van ICT. Dit heeft invloed op beveiliging in beide domeinen. Authenticatie in de thuissituatie moet net zo veilig en gemakkelijke zijn als in de werksituatie en omgekeerd.

Toegang tot fysieke objecten, bijvoorbeeld tot zakelijke gebouwen, wordt vaak met een elektronische sleutel of RFID

[5] Zie http://www.microsoft.com/netherlands/het_nieuwe_werken/.

tag geregeld. Die tag is soms gecombineerd met een middel dat toegang biedt tot de beveiligde zakelijke computernetwerken. Betalingen in winkels gaan elektronisch, net als betalingen via Internet. In de praktijk van internetbankieren wordt door een aantal banken de betaalkaart, die bij de geld- of betaalautomaat gebruikt wordt, ook tijdens een online transactie gebruikt in een PIN-calculator: in Nederland de Random Reader bij Rabobank, de e.identifier bij ABN AMRO bank. Deze PIN-calculators gebruiken de EMV (zie §2.3.5) functionaliteit op de chip om de PIN code van de gebruiker te controleren en transactie te ondertekenen. Het binden van het authenticatiemiddel voor online gebruik maakt hierdoor gebruik van de uitgiftestructuur van een reeds uitgegeven authenticatiemiddel.

Vanuit gebruikersoogpunt lijkt het logisch om een en hetzelfde authenticatiemiddel te gebruiken voor zowel de thuis- als de werksituatie en voor toegang tot zowel fysieke als virtuele zaken. Des te meer applicaties ontsloten worden met een enkele sleutel des te kleiner is de digitale sleutelbos. Er kleven, echter, beveiligingsbezwaren aan deze aanpak. Door zomaar één en hetzelfde middel te gebruiken voor toegang tot meerdere domeinen wordt een afhankelijkheid gecreëerd die niet altijd wenselijk. Als een aanvaller in de ene context de identiteit van een slachtoffer over kan nemen, dan krijgt deze opeens ook toegang tot zaken in andere domeinen. Ook vanuit privacyoogpunt kan het bezwaarlijk zijn om authenticatie te delen voor verschillende domeinen: het doen en laten van de gebruiker kan over de domeinen heen gevolgd worden.

2.3.4 SEPA: EÉN EUROPESE BETAALMARKT

De Single European Payment Area[6] zorgt ervoor dat er op Europese schaal een zone ontstaat waarin elektronische betalingen over en weer geaccepteerd worden. Voor de consument heeft het onstaan van SEPA tot gevolg dat er geen onderscheid meer gemaakt wordt tussen binnenlandse en buitenlandse betalingen.

SEPA wordt in verschillende fases uitgerold, waarbij de implementatie initieel vooral gevolgen heeft voor de back-office systemen bij financiële instellingen. Het zijn immers deze instellingen die elkaars betalingen over en weer moeten accepteren. De consument, met het internationale rekeningnummer van de begunstigde in de hand, merkt weinig verschil met binnenlandse overschrijvingen (credit transfer) of enkelvoudige machtigingen (direct debit). Uiteindelijk zal SEPA, naar verwachting, ook invloed hebben op de authenticatiemiddelen die door consumenten gebruikt worden, maar onduidelijk is op welke termijn dit gaat gebeuren.

2.3.5 EMV: SLIMME BETAALKAARTEN

EMV (dit acroniem staat voor Eurocard-Mastercard-Visa, verwijzend naar de partijen die de standaard oorspronkelijk ontworpen hebben, waarbij opgemerkt dient te worden dat Eurocard sinds lange tijd is overgenomen door Mastercard) is een initiatief afkomstig van creditcard maatschappijen om betaalkaarten van een chip te voorzien. De chip kan gebruikt worden om de authenticiteit van de kaart aan te tonen tijdens een transactie bij een geldautomaat (ATM) of bij een kassa in een winkel (POS). EMV lost zodoende het probleem van geskimde betaalkaarten op doordat het nagenoeg onmogelijk is om de chip te kopieren, in tegenstelling tot de traditionele magneetstrip op de achterkant van de betaalkaart.

[6] Zie http://www.europeanpaymentscouncil.eu.

De chip kan ook gebruikt worden als authenticatiemiddel voor online diensten. Er wordt dan gebruik gemaakt van CAP (Chip Authentication Program), een proprietary protocol van Mastercard bovenop EMV. Visa heeft een eigen implementatie onder de naam DPA (Dynamic Password Authentication). Bij CAP/DPA controleert de chip offline de ingetoetste PIN code van de gebruiker en ondertekent de chip een waarde die de online transactie karakteriseert.

Een belangrijke verandering die door de aanwezigheid van een sterker beveiligde bankkaart wordt bewerkstelligd is de zogenaamde liability shift van uitgevende partij (bank of credit card uitgever) richting de acceptant of zelfs de klant. Een complicerende factor hierbij is dat per land verschillende wetgeving geldt en de aansprakelijkheid anders ligt. Dit betekent dat ook de eisen aan de EMV oplossingen per land anders zullen zijn.

In Nederland voorzien de banken alle betaalkaarten van een EMV chip die CAP aankan. Geldautomaten zijn (anno 2010) uitgerust met mogelijkheden om deze chip op authenticiteit te controleren. Een aantal banken, Rabobank en ABN AMRO, gebruikt als authenticatiemiddel een EMV-CAP calculator (zie §3.2.8).

2.3.6 VERSCHILLENDE NIVEAU'S VAN ZEKERHEID

Niet voor alle diensten is dezelfde sterkte van authenticatie vereist. Bijvoorbeeld de sterkte van de binding aan een gebruiker (bij uitgifte en bij gebruik) kan verschillen per dienst. Bij inzet van een middel over diensten heen kan het nuttig zijn om voor sommige diensten een deel van het gebruiksgemak in te ruilen voor veiligheid: Voor high-trust diensten, moet de gebuiker wellicht per transactie een PIN code invoeren, terwijl voor low-trust diensten deze achterwege gelaten kan worden.

Hoewel deze verschillende niveau's van zekerheid (levels of assurance) geïmplementeerd kunnen worden door verschillende authenticatiemiddelen (bij veel banken is de rekening wel al te raadplegen op basis van gebruikersnaam/wachtwoord, maar moet voor het overmaken van geld een token gebruikt worden), is het vanuit gebruiksgemak eleganter om dit in een en hetzelfde middel te kunnen faciliteren.

2.3.7 MOBIELE APPARATEN

Het tijdperk van de thuis-PC lijkt nog niet ten einde. Maar veel diensten worden niet meer exclusief door gebruikers achter PC's afgenomen en in toenemende mate vanachter mobiele apparaten.

Een aantal authenticatiemethoden maakt juist gebruik van het feit dat veel gebruikers een mobiele telefoon bezitten (zie SMS OTP en Mobile PKI beschreven in §3.2) door het bezit van een mobiel apparaat als extra factor en extra kanaal bij authenticatie in te zetten. De trend om ook diensten af te nemen op het mobiele apparaat zelf, maakt dat het mobiele apparaat op zichzelf geen extra factor meer is. De dreiging van malware op de mobiele platforms lijkt tot nu toe mee te vallen in vergelijking tot de PC wereld [Lenzini et al. 2008], maar dit dreigingsbeeld kan omslaan naarmate de diensten die op of met behulp van het mobiele apparaat worden afgenomen meer waard worden.

De SIM kaart, een smart card die standaard in mobiele telefoons aanwezig is, kan mogelijk ingezet worden als vertrouwd element. Dit vereist medewerking van en vertrouwen op mobiele operators.

Mobiele apparaten zijn over het algemeen voorzien van een user interface met minder faciliteiten dan een PC, hoewel het scherm steeds meer grafische mogelijkheden heeft. Gebruikersnaam en wachtwoord invoeren op een mobiele telefoon blijft echter dusdanig ongebruiksvriendelijk dat veel applicaties de gebruiker de optie bieden om wachtwoorden op het apparaat zelf opslaan. De user interface van een mobiel apparaat is wel uitgebreider dan die van dedicated authenticatietokens.

Het ligt in de lijn der verwachtingen dat door het verbeteren van de gebruikersinterface steeds meer diensten via een mobiel apparaat afneembaar zullen zijn. Dit betekent dat het extra kanaal geen extra beveiliging biedt.

2.4 CONCLUSIE

Op basis van de in dit hoofdstuk geschetste context kan de vraag gesteld worden wat nu de voorwaarden zijn om van een toekomstig authenticatiemiddel voor consumenten een succes te maken.

Authenticatie is een proces dat op verschillende niveau's beschouwd moet worden. Om verschillende middelen te kunnen vergelijken moeten zowel juridische, organisatorische, als technische aspecten meegewogen worden. Om geaccepteerd te worden door consumenten moet een middel bovendien gebruiksvriendelijk zijn: consumenten moeten intuïtief met het middel kunnen werken.

Een aantal trends lijkt ervoor te gaan zorgen dat er een speelveld ontstaat waarin authenticatiemiddelen makkelijker en breder ingezet kunnen worden. Voorbeelden van zulke trends zijn het vervagen van grenzen tussen privé en zakelijk en tussen online en offline. Het ontkoppelen van een specifiek authenticatiemiddel als sleutel voor één specifieke dienst maakt dat een middel voor meerdere diensten gebruikt kunnen worden. Dit is een belangrijke eis om acceptatie door gebruikers mogelijk te maken. Er dient hierbij opgemerkt te worden dat diensten hiermee overweg moeten kunnen gaan. Dat dit nog altijd het geval is, is een potentiële show-stopper voor hergebruik van authenticatiemiddelen en de bijbehorende identiteitsmanagement infrastructuur.

Uit een snelle scan van buitenlandse oplossingen in [Hulsebosch-2010] kan geconcludeerd worden dat de gebruikte technologie niet altijd doorslaggevend is in het bepalen of een oplossing slaagt of faalt. Oorzaken voor slagen of falen lijken veel meer gezocht te moeten worden in bijvoorbeeld de rol van de overheid (zeg, als launching customer), samenwerking van banken, aanwezig zijn van een juridisch raamwerk waarin aansprakelijkheid redelijk verdeeld wordt tussen gebruiker, dienstenaanbieder en andere stakeholders.

Een andere belangrijke factor zou *aansprakelijkheid* kunnen zijn. Het wel of niet aansprakelijk zijn van de consument is van grote invloed op het belang dat door consumenten aan sterkere vormen van authenticatie gehecht wordt. Als de bank, dienstaanbieder te allen tijde volledig aansprakelijk gehouden kan worden, dan zal de eindgebruiker maximaal gebruiksgemak eisen en niet geneigd zijn mee te werken aan sterke vormen van authenticatie (de

consument krijgt zijn geld hoe dan ook terug).

3 Authenticatiemiddelen

Dit hoofdstuk geeft een overzicht van verschillende technologieën die gebruikt worden in authenticatiemiddelen. Uit deze overzichten wordt een classificatie van bestaande authenticatiemiddelen gemaakt waarmee bestaande en nieuwe middelen vergeleken kunnen worden.

Authenticatie is slechts een van de schakels in de veel grotere identiteitsmanagement-keten. Een groot deel van identiteitsmanagement kan zelfs authenticatie-agnostisch beschreven en geïmplementeerd worden. Vaak is het voor de back-end componenten vooral belangrijk te weten *dat* de identiteit van een gebruiker is vastgesteld en maakt het niet zoveel uit *hoe* dat is gebeurt. Eventueel wil het back-end systeem nog wel weten met welke zekerheid de identiteit van een gebruiker is vastgesteld. Heel soms ook onder welke omstandigheden iemand geauthenticeerd is (als dat in verschillende contexten kan gebeuren). Andere processen, zoals autorisatie (dat zich bezig houdt met de rechten van een gebruiker waarvan de identiteit reeds is vastgesteld), komen dan al snel in zicht.

Maar authenticatie is wel een belangrijke schakel in de gehele keten. Twee belangrijke redenen zijn hier debet aan. Ten eerste is authenticatie in de context van een grootschalige consumenten-identiteit oplossing zeer zichtbaar. Het authenticatiemiddel is wat de gebruiker ziet.

Ten tweede is authenticatie een belangrijke schakel vanwege beveiligingsaspecten. Het authenticatiemiddel wordt gebruikt in een relatief onveilige omgeving: bij de consument thuis. De controlerende partij heeft weinig invloed op externe factoren van deze omgeving (vergelijk het met een bankkantoor, of een geldautomaat, een winkel waar betaald kan worden: de thuissituatie is een stuk minder onder controle van de autoriteit). Er wordt gebruik gemaakt van een onvertrouwd platform (denk aan virussen en andere malware op de computer van de gebruiker). De gebruiker zelf houdt zich, al dan niet “onbewust onbekwaam”, niet aan alle afgesproken policies en procedures (wachtwoorden die worden opgeschreven, etc.). Goed gedrag van de gebruiker moet gemakkelijk gemaakt worden, en verkeerd gedrag zo moeilijk mogelijk. Het authenticatiemiddel heeft als eerste schakel in de keten een unieke positie om hierin te faciliteren.

3.1 TECHNIEK ACHTER AUTHENTICATIEMIDDELEN

Het doel van authenticatie is het vaststellen, door een controlerende partij, of een gebruiker over een geclaimde identitieit beschikt. In het kader van een identiteit voor consumenten zal authenticatie hier beperkt worden tot authenticatie voor *online* diensten. Dit betekent dat de gebruiker zich via het Internet aanmeldt bij een dienst en deze voor een groot deel ook via het Internet afneemt. De gebruiker maakt hiertoe gebruik van een desktop computer (thuis, op het werk, in een Internetcafé, etc.). De dienst kan zelf de controlerende partij zijn maar deze taak kan ook uitbesteed zijn aan een andere vertrouwde partij.

Het vaststellen dat een gebruiker over een geclaimde identiteit beschikt, gebeurt doorgaans door tijdens het binden van het authenticatiemiddel de gebruiker te voorzien van een geheime code. In het eenvoudigste geval gaat het om

een wachtwoord of PIN code. In complexere gevallen gaat het om een generator van geheime codes die onderdeel uitmaakt van het authenticatiemiddel. Tijdens een authenticatiesessie probeert de gebruiker de controlerende partij ervan te overtuigen dat hij of zij daadwerkelijk beschikt over de geheime code. Zolang de code een geheim blijft dat alleen de gebruiker kent, is deze code uniek identificerend voor de gebruiker. In sommige gevallen kent ook de controlerende partij de code, maar deze partij wordt vertrouwd deze code niet te delen met anderen.

3.1.1 MULTI-FACTOR

Een authenticatiemiddel kan gebruik maken van meerdere eenvoudigere authenticatiemiddelen, ook wel *factoren* genoemd. Een gebruiker kan namelijk op meerdere verschillende manieren aantonen de eigenaar van een bepaalde identiteit te zijn. Als de combinatie tijdens de binding aan de gebruiker gekoppeld is, dan maakt de combinatie de zekerheid voor de controlerende partij groter. Vaak wordt gebruik gemaakt van de volgende grove categorisering van factoren, vanuit het standpunt van de gebruiker:

- Iets wat men weet; bijvoorbeeld een wachtwoord.
- Iets wat men heeft; bijvoorbeeld een bankpas met chip.
- Iets wat men is; bijvoorbeeld een biometrisch kenmerk.

Soms wordt ook de context van de gebruiker meegenomen als vierde factor [Hulsebosch2006]. Onder de context valt dan bijvoorbeeld het IP-adres of de locatie van de gebruiker.

Vaak wordt aangeraden om bij multi-factor authenticatieoplossingen tenminste twee van de drie hierboven genoemde factoren te gebruiken. Vaak ook wordt dit onderscheid nog verder verfijnd met “uitrol factor” en “geleverd factor”. Maar deze extra factoren worden in dit rapport op verschillende niveau’s (zie §2.1) behandeld. Soms worden ook “analytische factoren” (wat je aan het doen bent) ook wel bekend als “context factoren” beschouwd. Deze worden hier onder de “iets wat men is”-categorie geschaard.

Multi-factor wordt ook wel gebruikt om toegang tot het authenticatiemiddel zelf te regelen. Een PIN code voor een mobiele telefoon wordt niet zozeer als additionele factor door een controlerende partij gecontroleerd maar door de mobiele telefoon zelf (of, iets preciezer, door de SIM kaart in de mobiele telefoon). Pas als de menselijke gebruiker toegang tot het authenticatiemiddel heeft, kan het authenticatiemiddel gebruikt worden om een authenticatiesessie met de controlerende partij op te zetten.

3.1.2 MULTI-CHANNEL

Een middel kan gebruik maken van een *extra* verbinding met de back-end systemen van een controlerende partij. Dit is dus een kanaal dat gescheiden is van het oorspronkelijke kanaal dat tussen de controlerende partij en (PC van) de gebruiker reeds is opgezet ten behoeve van de dienst.

Men spreekt in dit vervand ook wel van een verbonden (“connected”) authenticatiemiddel. Het tweede kanaal kan het middel veiliger maken want de aanvaller moet op twee kanalen gesynchroniseerd de aanval uitvoeren. Voorbeelden

van zulke extra kanalen zijn GSM bij SMS OTP (§3.2.6) of Mobile PKI (§3.2.12).

Het opzetten van de extra verbinding wordt door het middel zelf bewerkstelligd. Ook kan een beveiligd virtueel kanaal via de PC van de gebruiker opgezet worden. Doordat vrijwel elke PC anno 2010 over standaard USB poorten beschikt (§2.3.1), kunnen authenticatiemiddelen hiermee gekoppeld worden. De PC hoeft niet vertrouwd te worden om toch een beveiligde end-to-end verbinding (tussen authenticatiemiddel en back-end van controlerende partij) mogelijk te maken. Een alternatief interface zou Bluetooth kunnen zijn. Bluetooth is standaard aanwezig op laptops en mobiele apparaten. Op desktop computers die er niet over beschikken kan eenvoudig en goedkoop een USB Bluetooth adapter geinstalleerd worden. Nadeel is dat het instellen van een Bluetooth verbinding over het algemeen lastiger is (denk aan het “discoveren”, “vertrouwd koppelen via een PIN code” van apparaten).

3.1.3 STRONG AUTHENTICATION

De term “sterke authenticatie” kan verschillende dingen betekenen. Meestal wordt bedoeld dat een middel over meerdere factoren beschikt waarbij de werking van minstens één van de factoren gebruik maakt van sterke cryptografie. Met sterke cryptografie worden versleutel-technieken bedoeld waarvan in theorie aangetoond is dat er voor een aanvaller niets anders opzit dan alle mogelijk combinaties uit te proberen. In de praktijk worden sleutels dan zo gekozen dat zo’n uitputtende aanval tijd- en rekenkrachtig gezien zinloos is. Versleuteltechnieken worden door experts voortdurend onderzocht, en pas nadat een bepaalde techniek lange tijd ongeschonden de kritische analyses doorstaan heeft, mag erop vertrouwd worden dat deze veilig is. De Amerikaanse veiligheidsdienst NSA geeft bijvoorbeeld van tijd tot tijd een lijst van aangeraden versleutelalgoritmes en sleutellengtes uit die, gegeven de huidige inzichten, veilig gebruikt kunnen worden[7].

Een sterk authenticatiemiddel bevat dan doorgaans een geheime sleutel opgeslagen in hardware die gebruikt kan worden tijdens transacties. Groot voordeel van dit type middel is dat naast authenticatie ook elektronisch ondertekenen in principe mogelijk wordt. Authenticatie vindt dan eigenlijk plaats door een - voor de sessie - uniek bericht (vaak een door de controlerende partij opgestuurde “challenge”) te ondertekenen met behulp van de sleutel in het authenticatiemiddel.

Als voor de versleutel-technieken public key cryptografie gebruikt wordt, dan is het nodig om een zogenaamde public key infrastructure (PKI) op te zetten. Een PKI maakt het mogelijk om op een hiërarchische manier informatie over publieke sleutels in een organisatie uit te wisselen. Het betreffende authenticatiemiddel wordt vaak aangeduid met PKI token.

3.1.4 TAMPER RESISTANT HARDWARE

Voor “iets dat men heeft” factoren is het van belang dat de integriteit van het authenticatiemiddel niet aangetast kan worden. Vaak berust het vertrouwen van de controlerende partij in het inderdaad aanwezig zijn van het middel tijdens een transactie op de aanname dat het middel ongehinderd zijn werk kan doen (en dat sub-componenten van het

[7] Zie http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml.

middel, zoals intern geheugen, niet kunnen worden afgeluisterd of aangepast). Dit kan van belang zijn als het middel sterke authenticatie probeert te bewerkstelligen en geheime sleutels zich intern in het middel bevinden. De *authenticiteit* van het middel is dan alleen gegarandeerd als deze sleutels niet uit het middel geëxtraheerd kunnen worden, i.e. als de *integriteit* van het middel onaangetast is. In veel gevallen heeft tamper resistance als gevolg dat het nagenoeg onmogelijk is om het authenticatiemiddel te kopiëren.

De mate waarin het middel weerstand biedt tegen aanvallers die de werking van het middel proberen te beïnvloeden (tamperen) wordt aangeduid met kwalificaties zoals “tamper evident”, “tamper resistant” of “tamper proof”. Een authenticatiemiddel kan bijvoorbeeld zo geconstrueerd zijn dat pogingen om het te beïnvloeden het middel beschadigen zodat dit herkenbaar is (tamper evident) of het middel kan actief proberen te achterhalen of een dergelijke aanval plaatsvindt en zichzelf in dat geval al-dan-niet permanent uitschakelen (tamper proof). De term tamper resistant wordt gebruikt als verzamelnaam voor dit scala aan maatregelen.

Bijzondere aandacht bij het ontwerpen (of beoordelen) van tamper resistant hardware moet geschonken worden aan de gebruikersinterface (display en toetsenbord) omdat het koppelvlak tussen het middel en de gebruiker vaak de zwakke plek is. Er moet een “vertrouwd pad” zijn tussen de in- en uitvoercomponenten en de (cryptografische) verwerkingseenheid van het middel.

3.1.5 SMART CARDS

Smart cards vormen een bijzonder geval van tamper proof hardware en worden voornamelijk ingezet voor offline authenticatie in de niet-virtuele wereld (toegang tot gebouwen en dergelijke). Voordeel om deze ook in te zetten voor online authenticatie is dat dan hetzelfde middel gebruikt wordt, dit verhoogt het gebruiksgemak.

Een consument beschikt reeds over een tweetal smart cards die mogelijk gebruikt zouden kunnen worden als authenticatiemiddel voor een consument-ID. Ten eerste, met de invoering van EMV bevat elke bankkaart een chip (en is dus een smart card). Een authenticatiemiddel voor een consument-ID in de vorm van een kaartlezer kan hier gebruik van maken. Het middel kan de gebruiker identificeren met behulp van de bankkaart (een unieke identifier kan uit de chip gelezen worden), zodat het middel zelf generiek kan zijn. Bovendien kan zo’n middel duidelijk om consent aan de gebruiker te vragen: deze voert namelijk zijn of haar PIN code in. Zie ook §3.2.8.

Ten tweede, elke mobiele telefoon bevat als smart card een SIM kaart. Ook deze kan gebruikt worden om een gebruiker uniek te identificeren en via een PIN code te authenticeren. Zie ook §3.2.12.

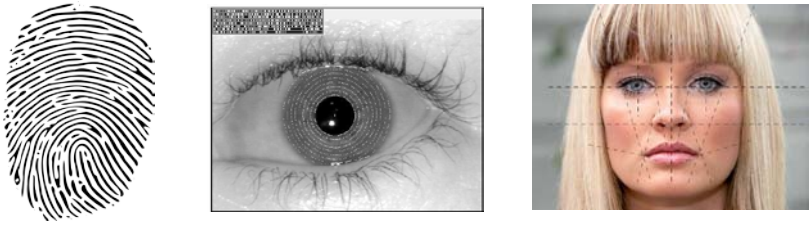
Een andere mogelijke kandidaat voor een breed ingevoerde smart card oplossing in Nederland is een door de overheid uitgegeven eID. In een aantal Europese landen is dit gedaan of zijn plannen om dit binnenkort te gaan doen (België, Duitsland, zie §2.2). In Nederland is een initiatief om te komen tot een elektronische Nationale Identiteitskaart (de eNIK) in 2007 gesneuveld vanwege een fout in de aanbesteding.

Nadeel van een smart card oplossing is dat er, in het algemeen, een aparte kaartlezer voor nodig is. Hoewel reeds

lang geleden gestandaardiseerd, zitten smart card readers niet standaard in de PC van de gebruiker. In Belgie heeft de overheid, bij de invoering van de Belgische eID, afgesproken met de sector, industry om smart card lezers in te bouwen in elke PC. Toch lijken smart card oplossingen, tot nu toe, vooral aan te slaan in een enterprise omgeving en minder geschikt voor consument-ID. Hoewel in sommige landen (België, Duitsland) de eID in de vorm van een smart card geïmplementeerd is of wordt.

3.1.6 BIOMETRIE

Een andere mogelijkheid om een controlerende partij van de identiteit van een gebruiker te overtuigen is door gebruik te maken van biometrische kenmerken van de gebruiker zelf. Tijdens de binding wordt uit een lichamelijk kenmerk van de gebruiker een zogenaamde template gegenereerd die gekoppeld wordt aan de identiteit van de gebruiker. Tijdens een authenticatiesessie wordt een opnieuw afgelezen biometrisch kenmerk vergeleken ("ge-matched") met de opgeslagen template. Populaire biometrische kenmerken voor authenticatiegebruik zijn stemherkenning, vinger- of palmafdruk, aderpatroon (vein), iris en gezichtsherkenning. Zie afbeelding.



Figuur 2: Vingerafdruk, Iris met iriscode (uit [Daugman]), Gezichtherkenning.

Bij stemherkenning worden karakteristieken van het door een gebruiker geproduceerde stemgeluid gemeten. Stemherkenning heeft als voordeel in een consument-ID scenario dat het op een natuurlijke manier op afstand te gebruiken is, namelijk via de telefoon. Er is geen speciale hardware aan de gebruikerskant nodig. Bovendien vormt de telefoon een tweede kanaal naar de gebruiker toe. Hoewel stemgeluid opgenomen zou kunnen worden, kunnen replay-aanvallen onmogelijk gemaakt worden door een challenge te laten voorlezen. Het dynamisch synthetiseren van stemgeluid is door de controlerende partij te herkennen.

Bij vingerafrukherkenning worden karakteristieke patronen in de (diepte van de) huid van de vingers van een gebruiker gemeten. Vingerafdrukherkenning heeft als voordeel dat er redelijk wat off-the-shelf hardware is en het in het gebruik als non-intrusive ervaren wordt[8]. Een groot nadeel is dat vingerafdrukken wel makkelijk na te maken zijn, zelfs op basis van een onvermoed achtergelaten vingerafdruk [Putte_Keuning:2001]. Off-the-shelf readers voor uitrol op grote schaal zullen waarschijnlijk niet over de echtheidsdetectie (lifeness) beschikken die nodig is om namaakvingers te detecteren.

[8] Dit is een redenen waarom vingerafdrukken als een van de eerste kenmerken wordt ingevoerd in ePaspoorten in Europa. Het andere kenmerk in de ICAO standaard is irisscan dat doorgaans als meer obstrusive ervaren worden.

Aderpatroonherkenning (vein recognition) lijkt in opkomst te zijn. Hierbij worden door een scanner infra-rood foto's gemaakt van de vingers of de palm van de hand van de gebruiker. Op basis van deze foto's wordt een 3D template gemaakt van de aderpatronen. Voordelen ten opzichte van vingerafdruk is dat aderpatronen op dit moment lastig na te maken zijn op basis van de template en dat uit de template vooralsnog geen eigenschappen van de gebruiker afgeleid kunnen worden. Vein scanners zijn al commercieel te koop.

Iris-scan wordt door Privium op Schiphol gebruikt voor geautomatiseerde grensovergang (voor leden die enrolled zijn, in 2006 waren er 31.000 Privium leden [Bron Interview met Conny Lanza, mt.nl, November 2006]). Dit gebeurt in combinatie met een contactloze smart card. Een iris-scan wordt als intrusive beschouwd. Bovendien is off-the-shelf hardware voor toepassing bij de gebruiker thuis duur.

Andere nadelen van biometrie in het algemeen zijn:

1. Een veel genoemd nadeel is de gevoeligheid voor valse positieven en negatieven (False Acceptance Rate / False Rejection Rate, FAR/FRR). Dit speelt minder bij gebruik als extra factor voor online authenticatie van welwillende gebruikers (zogenaamde positieve identificatie) dan bij andere toepassingen (zoals single factor, zogenaamde negatieve identificatie waarbij de eigenschappen van een individu vergeleken moeten worden met een grote collectie van templates).
2. Templates zijn extreem privacy gevoelig. In sommige gevallen (bijvoorbeeld bij gelaat-, vingerafdruk-, DNA-herkenning) kunnen uit een template allerlei eigenschappen van de gebruiker afgeleid worden (bijvoorbeeld het geslacht [Wang et al. 2008], erfelijke aanleg voor ziektes). De template wordt typisch door de controlerende partij opgeslagen in een database met bijbehorende privacy risico's. Mogelijk oplossingen zijn: het opslaan van een versleutelde [Cavoukian en Stoianov] of gehashde versie van de template (bijvoorbeeld BioHash van priv-ID[9]), het opslaan van de template in een (tamper-proof) token en deze de vergelijking laten doen (zogenaamde match-on-card).
3. Als de 'geheime code' (een template) wordt gekopieerd , kan geen nieuwe code worden gekozen of uitgedeeld, juist omdat deze biologisch verankerd is.
4. Het is in sommige gevallen op afstand moeilijk controleren of een gebruiker inderdaad een biometrisch kenmerk laat zien of dat een kopie gepresenteerd wordt (archetypisch voorbeeld is een foto die ten behoeve van gezichtherkenning voor de camera gehouden wordt).
5. Een ander probleem is dat enrollment zeer omslachtig is. Dit kan in de praktijk alleen bij face-to-face binding onder toeziend oog van medewerkers van de dienstverlener (of vertrouwde partij). Stemherkenning is hierop wellicht een uitzondering als het kanaal naar de gebruiker toe veilig is.

Gedragskenmerken (hoe je praat, loopt, typt) kunnen ook gebruikt worden voor biometrische authenticatie. Het gaat hierbij niet zozeer om fysiologische kenmerken van de gebruiker maar om gedragspatronen die door een aanvaller

[9] Priv-ID B.V., http://www.priv-id.com.

moeilijk over te nemen of na te doen zijn. Een voorbeeld is toetsenbord-biometrie, waarbij niet (alleen) naar wat er getypt wordt gekeken, maar ook naar hoe een wachtwoord of PIN code ingetypt werd. Door tijdsverschillen tussen aangeslagen toetsen te analyseren kan een gebruiker herkend worden. Stemherkenning (hierboven besproken) valt in hoge mate ook onder deze categorie (hoewel de fysiologische kenmerken van de spraakorganen zeer bepalend zijn voor het geproduceerde geluid).

In een consument-ID scenario, waarbij op afstand authenticatie van een gebruiker plaats moet vinden, is biometrie lastig (zie punt 4 hierboven). Wel kan het, op termijn, als gebruiksvriendelijk variant van binding van middel aan gebruiker toegepast worden, zowel bij enrollment (controle op identiteit bij uitreiking token) als tijdens een authenticatiesessie (ter vervanging van PIN code).

3.2 OVERZICHT DAADWERKELIJK TOEGEPASTE AUTHENTICATIEMIDDELEN

Op basis van productoverzichten van authenticatiemiddelen-technologie leveranciers is de volgende lijst met bestaande authenticatie-technologieën voor consumenten-identiteit samengesteld. Per authenticatiemiddel zijn voor het tactische en operationele niveau een aantal voor- en nadelen samengevat (in de linkerkolom van elke tabel). Het gaat hierbij om typisch gebruik in de huidige praktijk. Ook is per authenticatiemiddel aangegeven welke onderliggende mechanismen gebruikt worden om de beveiliging te bewerkstelligen (in de rechterkolom van elke tabel, waarbij MF staat voor multi-factor, MC voor multi-channel, SA voor strong authentication (op basis van sterke cryptografie) en TR voor tamper-resistant.

3.2.1 GEBRUIKERSNAAM/WACHTWOORD

De gebruiker heeft een gebruikersnaam en bijbehorend geheim wachtwoord. Bij binding kunnen deze uitgedeeld worden, of de gebruiker mag ze zelf kiezen. Daarna kan de gebruiker ze eventueel nog veranderen afhankelijk van het wachtwoordenbeleid van de controlerende partij. Soms wordt zelfs afgedwongen dat het wachtwoord na een *N* aantal dagen veranderd moet worden (waarbij eerder gekozen wachtwoorden kunnen worden uitgesloten). Tijdens een authenticatiesessie voert de gebruiker zijn gebruikersnaam en wachtwoord in. De controlerende partij kan ook om enkele tekens van het wachtwoord vragen (bijvoorbeeld: “voer het tweede, derde en achtste teken in”) zodat een onderschepte authenticatiesessie voor de aanvaller niet direct het volledige wachtwoord oplevert.

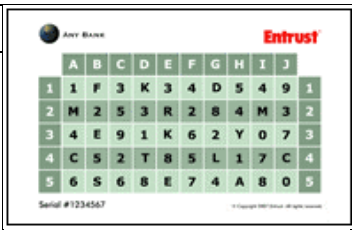
<table>
<tr><td>Tactisch</td><td rowspan="3"> 

<table>
<tr><th>MF</th><th>MC</th><th>SA</th><th>TR</th></tr>
<tr><td>0</td><td>0</td><td>0</td><td>0</td></tr>
</table></td></tr>
<tr><td>[Goed] Grote keuzevrijheid voor het wachtwoord in combinatie met “low-tech” middel biedt gebruiksgemak. Binden kan op afstand (afhankelijk van gewenst zekerheidsniveau).
[Slecht] Kosten vergeten wachtwoorden.</td></tr>
<tr><td>Operationeel</td></tr>
</table>

[Slecht] Makkelijk kopieerbaar en bovendien totaal afhankelijk van gedrag gebruiker of wachtwoord geheim blijft.	

3.2.2 MATRIXKAART WACHTWOORDGENERATOR

Deze (low-tech) kaart bevat een Bingo-achtig rooster (horizontaal A t/m J, vertikaal 1 t/m 5). Bij een challenge van de dienstverlener (bijvoorbeeld A5, B7, C9, D8) moet de gebruiker de corresponderende cijfers uit het rooster overtypen (de zogenaamde response). Elke kaart heeft een serienummer (dus kaart kan geblacklist worden indien gestolen). Het voorbeeld in de tabel hieronder is van Entrust[10].

Tactisch	
[Goed] Binden: Kan in back-end door serienummer te koppelen aan identiteit van gebruiker. Helpdesk kan nieuwe binding uitvoeren bij verlies/diefstal.	
Operationeel	
[Matig] Gebruiksgemak ietwat bewerkelijk. Vergelijkbaar met bijvoorbeeld TAN codes §3.2.5. [Matig] In principe makkelijke kopieerbaar, maar gebruiker ervaart dit meer als iets-wat-men-heeft dan wachtwoord.	**MF** 1 **MC** 0 **SA** 0 **TR** 0

3.2.3 OTP-WACHTWOORDGENERATOR

Tactisch	
[Goed] Binden: Kan in back-end door serienummer token te koppelen aan identiteit van gebruiker. Helpdesk kan nieuwe binding uitvoeren bij verlies/diefstal.	
Operationeel	
[Matig] Gebruiksgemak: overtypen door gebruiker niet ideaal, maar wel beter dan TAN code op papier of matrixkaart. [Matig/Goed] Veiligheid: serieuze drempel voor passieve aanvaller, maar kan geen transactiedetails	**MF** 1 **MC** 0 **SA** 1 **TR** 1

[10] Entrust (vendor). Zie http://www.entrust.com/.

weergeven naar gebruiker.	

Een OTP wachtwoordgenerator is een token dat op basis van een ingebouwde teller (in persistent geheugen) of klok en een geheime sleutel onvoorspelbare unieke wachtwoorden kan genereren. Bij binding krijgt de gebruiker een dergelijk token en wordt deze gekoppeld aan de identiteit van de gebruiker. Tijdens een authenticatiesessie laat het token de gegenereerde wachtwoorden via een display zien aan de gebruiker, die deze vervolgens op de PC overtypt. De controlerende partij kan de gegenereerde wachtwoorden herkennen als geldig en afkomstig van het token van de gebruiker. Soms is toegang tot het authenticatiemiddel nog beveiligd met een persoonlijke PIN code, maar in eenvoudige gevallen beperkt de interface zich tot een enkele drukknop naast het display. Bij verlies of diefstal kan het token ge-blacklist worden. Voorbeelden: RSA SecurID[11] familie, VASCO Digipass[12] GO familie (zie afbeelding), Entrust IdentityGuard minitoken (en ongetwijfeld andere leveranciers).

3.2.4 EEN USB-TOETSENBORD WACHTWOORDGENERATOR

Een USB toetsenbord wachtwoordgenerator (het standaard voorbeeld is de Yubikey[13]) is een variant van de OTP generator die de gebruiker het werk van overtypen bespaart. Bij binding wordt een uniek gediversificeerd token aan de identiteit van de gebruiker gekoppeld. Tijdens een authenticatiesessie wordt dit token in een vrije USB poort van de PC van de gebruiker gestoken. De PC herkent dit apparaat als een extern USB toetsenbord. Vervolgens ”focust” de gebruiker op een wachtwoord-invul-veld op de webpagina van de controlerende partij en het token typt een sessie-uniek wachtwoord. Aan de interne structuur van dit wachtwoord herkent de controlerende partij het token en de authenticiteit.

Tactisch	
[Goed] Binden: sleutel (op basis van serienummer) in back-end. Bij verlies of diefstal een nieuw token binden.	
Operationeel	
[Goed] Gebruiksgemak: Geen code overtypen. [Matig/Goed] Veiligheid: kan geen transactiedetails doorgeven aan gebruiker.	

MF	MC	SA	TR
1	0	1	1

Security-onderzoeker Didier Stevens beschrijft een zwakte[14] van deze vorm van authenticatie in een scenario waarbij meerdere authenticaties nodig zijn (inloggen en vervolgens step-up authenticatie om een transactie te doen) waarbij

[11] RSA (vendor). Zie http://www.rsa.com/.

[12] VASCO (vendor). Zie http://www.vasco.com/.

[13] Yubikey (vendor). Zie http://www.yubico.com/.

[14] Zie http://blog.didierstevens.com/2009/08/26/yubikey-trojans-and-twitter/.

een man-in-the-middle aanvaller een storing bij het inloggen simuleert om een tweede code te genereren voor een transactie. Het probleem lijkt vooral te liggen in de betekenisloosheid (i.e. geen transactiedetails) van de gegenereerde random wachtwoorden.

3.2.5 TAN-LIJST

Een TAN-lijst is een papieren afdruk met TAN-codes die ter beschikking van de gebruiker wordt gesteld.

Tactisch	
[Slecht] Gebruiksgemak: opzoeken en overtypen code. [Slecht] Binding: lijst moet vervangen worden als alle codes gebruikt zijn.	
Operationeel	
[Matig] Veiligheid vergelijkbaar met OTP middelen. Kan geen transactiedetails doorgeven aan gebruiker. [Goed] Gebruiksgemak: Low-tech, schrikt digibete gebruiker minder af. [Slecht] Gebruiksgemak: Overtypen en gebruiker zal niet in alle situaties lijst bij zich hebben.	

MF	MC	SA	TR
1	0	1	0

Bij binding krijgt de gebruiker een lijst met TAN-codes welke gekoppeld wordt aan de identiteit van de gebruiker. TAN-codes zijn wachtwoorden voor eenmalig gebruik. Als de volledige lijst opgebruikt is, vindt opnieuw binding plaats en krijgt de gebruiker een nieuwe lijst. Tijdens een authenticatiesessie wordt door de gebruiker een TAN-code uit de lijst overgetypt. De controlerende partij kan zien dat deze niet eerder gebruikt is en afkomstig van de gebruiker. Tegenwoordig kiest de controlerende partij meestal een indexnummer dat aan de gebruiker getoond wordt, en moet de gebruiker de corresponderende TAN-code invoeren (iTAN[15]).

In vergelijking met gebruikersnaam/wachtwoord biedt een TAN-lijst een aantal voordelen. In principe vormt de papieren lijst een tweede kanaal dat ook door de aanvaller (die de gebruiker bijvoorbeeld naar een phishing site gelokt heeft) onderschept moet worden om een aanval op te kunnen zetten. In een MitM aanvalsmodel, echter, kan de aanvaller TAN codes eenvoudig doorgeven richting controlerende partij. Er is voor de gebruiker geen mogelijkheid om te controleren of de TAN code daadwerkelijk gebruikt wordt voor de veronderstelde transactie (zie ook de aanval

[15] In http://www.redteam-pentesting.de/advisories/rt-sa-2005-014.txt worden de voordelen van dit systeem ten opzichte van niet-geindexeerde TAN-codes “marginaal” genoemd.

van Stevens waar in §3.2.4 naar verwezen wordt).

De TAN lijst heeft als voordeel dat er een eenvoudig migratiepad is naar SMS OTP, dit vergt minimale aanpassingen aan de controlerende partij. In Nederland gebruikt ING nog steeds TAN lijsten, o.a. om de groep gebruikers die niet over een mobiele telefoon beschikt te kunnen bedienen.

3.2.6 SMS OTP / MTAN

Bij SMS OTP, ook wel mobile TAN of mTAN genoemd, worden TAN-codes naar de mobiele telefoon van de gebruiker gestuurd en is het verstrekken van een papieren TAN-lijst niet meer nodig. Bij binding verkrijgt controlerende partij het mobiele nummer van gebruiker en controleert of gebruiker daadwerkelijk de eigenaar is van dat nummer. Tijdens een authenticatiesessie wordt een verse TAN-code gegenereerd door de controlerende partij en via SMS naar de mobiele telefoon van de gebruiker gestuurd. Het SMS bericht kan ook additionele transactiedetails bevatten die door de gebruiker gecontroleerd kunnen worden. Het belangrijkste verschil met andere externe tokens is dat GSM/SMS een extra kanaal vormt en het dus voor de aanvaller moeilijker maakt om op grote schaal gebruikers aan te vallen. Alleen een gecoördineerde (gerichte) aanval op zowel de PC als de mobiele telefoon is mogelijk. Mogelijk nadeel is dat SMS nooit bedoeld is voor het veilig transporteren van data (een verzender weet bijvoorbeeld niet zeker of een bericht ook daadwerkelijk aankomt). De encryptie op het SMS kanaal, A5, is kraakbaar gebleken [GOVCERT, Nohl] alhoewel een praktische aanval nog niet gedemonstreerd is, zeker niet voor SMS authenticatie, neemt een aantal dienstverleners nu al maatregelen[16]. Naarmate het mobiele platform complexer en meer gebruikt gaat worden, bijvoorbeeld om high-trust diensten af te nemen, zal ook het malware dreigingsbeeld hier wijzigen.

Tactisch
[Matig] Binden en rebinden kan lastig zijn omdat gebruikers van toestel / abonnement wisselen.
Operationeel
[Goed] Veiligheid: Hoewel dit ter discussie staat vanwege zwakheid in GSM. Transactiedetails kunnen tot op zeker hoogte doorgegeven worden aan gebruiker. Niet veilig tegen man-in-browser. [Goed] Gebruiksgemak: Gebruiker zal mobiel vaker bij zich dragen dan los token.

MF	MC	SA	TR
1	1	0	0

[16] Zie http://www.telegraaf.nl/binnenland/7676918/__Geheime_dienst_vreest_afluistering__.html?p=1,1.

3.2.7 CHALLENGE-RESPONSE TOKEN MET TOETSENBORD EN DISPLAY

Een niet-aangesloten challenge response token heeft een numeriek toetsenbord en display. Bij binding wordt een unieke identifier (het serienummer van het token) aan de identiteit van de gebruiker gekoppeld. Tijdens een authenticatiesessie wordt via de browser op de PC een challenge aan de gebruiker getoond die ingevoerd moet worden via het toetsenbord van de token. De token laat vervolgens op het display een response zien die door de gebruiker op de PC overgetypt moet worden.

Er zijn een aantal nadelen. Er is redelijk wat administratie nodig om tokens aan gebruikers te kunnen binden. Het gaat om een extra token dat door de gebruiker meegenomen moet worden als deze in verschillende contexten (thuis, werk, internetcafé) gebruik wil maken van diensten. En het over en weer overtypen van challenge en response is bewerkelijk. Transactiedetails zullen niet door het token getoond kunnen worden (de challenge bevat te weinig informatie, want deze moet kort genoeg zijn om overgetypt te kunnen worden).

.

Tactisch	
[Goed] Binden vergelijkbaar met OTP tokens (§3.2.3).	
Operationeel [Goed] Beveiliging: serieuze drempel, maar kan geen transactiedetails doorgeven aan gebruiker.	

MF	MC	SA	TR
1	0	1	1

Een geheel andere manier om toch via het PC platform een verbinding met het token te bewerkstelligen is door gebruik te maken van optische leesbare codes op het scherm van de PC. Deze codes kunnen ingescand worden door het token. Meestal gaat het om bewegende streepjescodes. Kobil[17] heeft hier een oplossing voor die ook echt wordt toegepast door een bank in Luxemburg, Todos (A200 Optic), Gemalto (Ezio) en Vasco hebben ook oplossingen.

3.2.8 PIN-CALCULATOR

Een PIN-calculator (ook wel CAP reader) is een challenge response token met toetsenbord, display *en* ingebouwde smart card reader. De bankpas van de gebruiker wordt als extra “iets wat men heeft” factor toegevoegd. De chip op de bankpas kan ook nog gebruikt worden om toegang te controleren. De gebruiker moet dan via de PIN-calculator

[17] KOBIL Systems (vendor). Zie http://www.kobil.com/.

zijn PIN code (die hij of zij ook bij de geldautomaat gebruikt). Een en ander werd in Nederland al enige tijd toegepast (op basis van Chipknip functionaliteit). Recenter is dit, onder invloed van de invoering van EMV, min of meer gestandaardiseerd op EMV-CAP. In Duitsland is voor dit soort tokens zelfs een echte standaard: [HBCI-ZKA]. Details over de EMV-CAP implementatie zoals toegepast in Groot-Britannie is te vinden in [Drimer2009], voor de Nederlandse middelen is een soortgelijke analyse gedaan door de Radboud Universiteit [Schouwenaar2010].

Wordt toegepast door twee grote banken in Nederland. Middelen van Vasco (de Random Reader van Rabobank en versie 1 van de e.dentifier van ABN AMRO).

Tactisch	
[Goed] Binden lift mee op binden van bankkaart. Enige helpdesk kosten als batterij leeg is.	
Operationeel	
[Goed] Beveiliging: Huidige generatie geeft tot op zeker hoogte mogelijkheid om transactiedetails met gebruiker te delen. Vatbaar voor man-in-browser als gebruiker transactiedetails niet leest of snapt. Lift mee op PIN code die ook bij betaal- en geldautomaat gebruikt wordt. [Matig] Overtypen codes.	

MF	**MC**	**SA**	**TR**
1	0	1	1

Het is ook mogelijk om dit connected te doen (versie 2 van de e.dentifier van ABN Amro kan via USB aangesloten worden). In principe is het mogelijk om op deze manier een end-to-end beveiligde verbinding op te zetten tussen back-office en authenticatiemiddel bij de gebruiker thuis. In Nederland is Todos de leverancier van de.e.dentifier 2 van ABN AMRO[18].

Tactisch	
[Goed] Binden lift mee op binden van bankkaart. Updates kunnen (in theorie) zelfs over beveiligde verbinding naar middel gepushed worden.	
Operationeel	

[18] Bron: http://www.todos.se/downloads/ABN_AMRO_CS_Todos.pdf

[Goed] Beveiliging: in principe kan een end-to-end beveiligde verbinding met de back-end systemen opgezet worden. [Goed] Gebruiksgemak connected: geen noodzaak om codes over te typen. Transactiedetails kunnen aan gebruiker getoond worden	1	1	1	1	

3.2.9 PKI SOFT CERTIFICATE

Alle browsers ondersteunen authenticatie via TLS/SSL. De gebruiker heeft hiervoor een sleutelpaar nodig, waarvan het publieke deel ondertekend is door een autoriteit die vertrouwd wordt door de controlerende partij. Dit sleutelpaar (ook wel aangeduid met “user certificaat”) wordt opgeslagen op de PC van de gebruiker.

Het grote voordeel is dat ondertekenen met een certificaat mogelijk is. Een groot nadeel is dat bij binding het certificaat (eigenlijk de private sleutel) op de PC van de gebruiker geïnstalleerd wordt. Dit is lastig voor de gebruiker, o.a. omdat een groot aantal handelingen noodzakelijk is om het certificaat naar een andere PC te exporteren. Bovendien is deze aanpak vatbaar voor malware op de PC, die immers bij het certificaat zou kunnen komen.

Tactisch	
[Goed] Binden in back-end eenvoudig (serienummer, standaard attributen voor gebruikers). [Matig] Binden/gebruiksgemak: Maar (her)installatie op PC is notoir probleem.	
Operationeel	
[Slecht] Beveiliging: malware kan in principe bij certificaat en privésleutel.	

MF	**MC**	**SA**	**TR**
1	0	1	0

3.2.10 PKI USB TOKEN / PKI SMART CARD (MET READER)

Bij binding krijgt de gebruiker een PKI token of smart card. De reader is gewoon off-the-shelf. Nadeel: voor zowel de reader als het specifieke type kaart moet software geïnstalleerd worden. Nieuwe standaarden (ISO 24727, onder andere gebruikt voor de Duitse eID) zorgen ervoor dat dit beperkt blijft tot driver voor de reader. Een voordeel is dat ondertekenen mogelijk is.

Tactisch	
[Goed] Binden: Eenvoudig in back-end. Token heeft unieke identifier/serienummer. [Matig] Gebruiksgemak: installatie drivers kan lastig zijn en helpdesk kosten genereren.	
Operationeel	
[Goed] Beveiliging [Goed] Gebruiksgemak: als eenmaal goed geïnstalleerd geen probleem.	

MF	MC	SA	TR
1	0	1	1

3.2.11 MOBIELE TELEFOON MET APPLICATIE

Tactisch	
[Goed] Binden: kan in principe over-the-air, dan lift men mee op identieit van mobiele abonnee.	
Operationeel	
[Slecht] Beveiliging: Malware op mobiel kan in principe bij sleutels. (Op dit moment is dreiging nog niet heel groot.) [Goed] Gebruiksgemak: Gebruiker heeft mobiel altijd bij zich.	

MF	MC	SA	TR
1	1	1	0

Een authenticatietoken zou de vorm van een applicatie op de mobiele telefoon kunnen aannemen. Een voordeel is dat moderne mobiele telefoons over een relatief rijke gebruikersinterface beschikken en gebruikers hebben mobiele telefoon vaker bij zich (missen hem eerder in geval van diefstal) dan een dedicated token. Nadeel ten opzichte van de in 3.2.11 beschreven SIM gebaseerde oplossing is dat ondertekenen niet mogelijk is (in ieder geval geen geavanceerde handtekening). Een ander nadeel is de platform-fragmentatie op het mobiele platform (wil men een brede basis van gebruikers kunnen bedienen, dan moet een versie van de applicatie voor verschillende besturingssystemen zoals Windows Mobile, Android, iPhone en Symbian, ... ontwikkeld worden). Het lijkt niet waarschijnlijk dat hier op korte of zelfs langere termijn op één platform gestandaardiseerd gaat worden (zo'n uniform platform, Java J2ME, bestond wel op de vorige generatie mobiele telefoons maar lijkt in de huidige generatie smart-phones veelal niet ondersteund te worden). Zie verder §2.3.7 en §5.6.

3.2.12 SIM MET APPLICATIE (MOBILE PKI)

Op de SIM kaart in een mobiele telefoon kunnen applicaties geïnstalleerd worden die ingezet kunnen worden voor authenticatie en ondertekenen. Deze zogenaamde SIM toolkit applicaties kunnen (speciaal geformateerde) SMS berichten afvangen en verwerken en kunnen ook een eenvoudige menu-gebaseerde gebruiksinterface naar de gebruiker presenteren.

Binding gebeurt tijdens het uitreiken van de SIM kaart aan de gebruiker door de mobiele operator door een SIM toolkit applicatie op de SIM te installeren, of eventueel op een later tijdstip waarbij de gebruiker aan de controlerende partij bewijst over een bepaalde SIM te beschikken. Eventueel kunnen applicaties, sleutels en andere codes post-issuance nog over-the-air op de SIM geïnstalleerd worden. Hiervoor is medewerking van de mobiele operator nodig die de toegang tot de SIM regelt. Dit middel heeft bovendien als voordeel dat de mobiele telefoon een relatief rijke interface biedt aan een middel dat de veiligheid van een smart card heeft. Nadeel is dat een geavanceerde, duurdere SIM gebruikt moet worden (o.a. meer geheugen dan een standaard SIM). Een SIM vervangingstraject beslaat enkele jaren (aangenomen dat een gebruiker hetzelfde abonnement blijft gebruiken).

Tactisch
[Goed] Binden: kan over-the-air, dan left men mee op identiteit van mobiele abonnee.
Operationeel
[Goed] Gebruiksgemak: vergelijkbaar met mobiele telefoon applicatie (als zal user interface eenvoudiger zijn vanwege beperkingen SIM toolkit) [Goed] Beveiliging: vergelijkbaar met smart card.

MF	MC	SA	TR
1	1	1	1

Dat medewerking van een extra stake holder (de mobiele operators) vereist is voor deze oplossing maakt het maken van een business case extra moeilijk.

3.3 CONCLUSIE

Er zijn veel verschillende authenticatiemiddelen, maar slechts een beperkt aantal basisprincipes ligt ten grondslag aan deze middelen. Gebruikersnaam/wachtwoord (§3.2.1) is het eenvoudigst maar kampt met ernstige beveiligingsproblemen. Dit wordt veel gebruikt voor low-trust diensten, bijvoorbeeld bij het online inzien van een bankrekening (in Nederland bij ING).

OTP is veiliger dan gebruikersnaam/wachtwoord, en heeft in veel gevallen (§3.2.5, TAN codes en §3.2.6 mTAN via

SMS) veilig tweede kanaal naar de gebruiker toe. Een alternatief wordt gevormd door challenge-response tokens. In de Nederlandse e-banking situatie voor het daadwerkelijk doen van online transacties kiest ING op dit moment voor TAN codes en mTAN (OTP) via SMS, en Rabobank en ABN AMRO voor een PIN calculator die gebruik maakt van EMV-CAP (§3.2.8, waarbij de gebruiker codes over moet typen van PC naar token en terug). Voordeel bij deze oplossingen is dat gebruik wordt gemaakt van bestaande infrastructuur (mobiel resp. bankpas met PIN).

Authenticatietokens kunnen in principe ook gebruikt worden om elektronische handtekeningen te plaatsen. Naarmate authenticatiemiddelen beter beveiligd zijn (gebaseerd op sterke cryptografie en tamper resistant) en naarmate deze de gebruiker de mogelijkheid geven om daadwerkelijk goed geïnformeerd toestemming te geven om een handtekening te zetten kan dit ook op een toekomstbestendige manier (in lijn met de EC richtlijn elektronische handtekeningen). Dit kan in ieder geval zeker met PKI tokens (§3.2.10) en (dus) met Mobile PKI (§3.2.12).

Voor wat betreft beveiliging lijken de connected PIN calculator () en Mobilre PKI de beste papieren te hebben. Het eerste middel heeft als nadelen dat de gebruiker een extra apparaat bij zich moet dragen en dat het opzetten van de verbinding iets meer voeten in de aarde heeft (via een USB poort van de PC van de gebruiker). Het tweede middel heeft als nadeel dat het de medewerking van (en dus een business case voor) de mobiele operators vereist.

4 Dreigingen

Een belangrijke aanname in dit hoofdstuk is dat bij consumenten identiteit uitgegaan mag worden van aanvallen die niet op een specifiek slachtoffer gericht zijn (niet-gerichte, “non-targeted”). Aanvallers vinden online authenticatie interessant vanwege de schaalgrootte waarop het toegepast wordt. Het uitsturen van een phishingmail naar miljoenen slachtoffers in de hoop dat er een paar gebruikers intrappen is al snel lonend voor een aanvaller.

4.1.1 FOUT BIJ INITIELE BINDING

Als bij de binding (het moment dat de identiteit van een gebruiker gekoppeld wordt aan een authenticatiemiddel) fouten gemaakt worden, kan een gebruiker een valse identiteit krijgen. Alle beveiligingsmaatregelen die daarna (tijdens een authenticatiesessie) volgen zijn vervolgens zinloos. Het is dus van belang om te investeren in het bindingsproces om dit risico zo laag mogelijk te houden.

Doorgaans wordt vertrouwd op een nog sterkere identiteitsprovider zoals de overheid: de gebruiker moet zich in persoon met zijn of haar paspoort melden bij de controlerende partij die controleert aan de hand van de echtheidskenmerken of het om een authentiek paspoort gaat en of deze toebehoort aan de gebruiker die zich meldt.

4.1.2 VERLOREN OF GESTOLEN AUTHENTICATIEMIDDEL

Omdat de meeste authenticatiemiddelen voor een deel op “iets dat men heeft” berusten, kan het authenticatiemiddel fysiek ontvreemd worden. In sommige gevallen kan een token zelfs door een aanvaller opnieuw gebonden worden, bijvoorbeeld als een mobiele telefoon gebruikt wordt in een SMS-OTP (§3.2.6) scenario[19].

Het helpt om het authenticatiemiddel op een sterke manier te koppelen aan de gebruiker, niet alleen bij uitgifte, maar tijdens elke transactie. Bijvoorbeeld, PIN calculators verifiëren eerst of de gebruiker de PIN van de bankkaart kent, alvorens aan een transactie te beginnen. Biometrie is hier een andere mogelijkheid. In het algemeen zal een aanvaller door een (fysiek) authenticatiemiddel te stelen slechts één van de factoren in handen krijgen en is het wenselijk om de kans dat meerdere factoren gelijktijdig ontfutseld worden, zo klein mogelijk te maken.

Een andere mogelijkheid om dit risico af te dekken is het snel en doelmatig blokkeren (revoken, blacklisten) van authenticatiemiddelen als deze als gestolen of verloren gerapporteerd worden door gebruikers. Daarbij is het wel belangrijk dat gebruikers zich tijdig realiseren dat een authenticatiemiddel verdwenen is. De kans hierop wordt natuurlijk groter naarmate een gebruiker een middel vaker gebruikt.

4.1.3 BEWUST AFSTAAN VAN AUTHENTICATIEMIDDEL VOOR FRAUDE

Een variant op de in 4.1.2 beschreven dreiging is het bewust en vrijwillig afstaan van een authenticatiemiddel door een gebruiker opdat een aanvaller het middel kan gebruiken. De rechtmatige gebruiker kan vervolgens richting de

[19] Zie http://webwereld.nl/nieuws/66536/ing-past-zwakste-schakel-internetbankieren-aan.html.

authenticatiemiddelenprovider claimen dat het middel buiten zijn of haar medeweten gebruikt is en/of dat de transacties hem of haar vreemd zijn.
Het authenticatiemiddel kan, indien op een sterke manier gebonden aan de gebruiker, gebruikt worden om met enige zekerheid aan te tonen dat niet de gerechtigde gebruiker de transactie initieerde. Maatregelen om het restrisico te beperken zijn voornamelijk te vinden in het delen van de aansprakelijkheid met de gebruiker

4.1.4 PASSIEVE AANVALLER OP HET NETWERK

Het probleem van een passieve aanvaller op het netwerk is in de praktijk goed op te lossen. Door het opzetten van een beveiligde verbinding tussen de PC van de gebruiker en de webservers van de controlerende partij kan zelfs het zwakste authenticatiemiddelen (gebruikersnaam/wachtwoord combinatie) afdoende tegen deze aanval beschermd worden: Een internetbrowser beschikt over een trust-store met daarin de root-certificaten van vertrouwde partijen, de zogenaamde Certification Authorities (CA's). Hierdoor kan de browser een beveiligde verbinding opzetten met de dienstaanbieder via het intussen breed geaccepteerde TLS/SSL protocol.

Zwakheden in (implementaties van) TLS/SSL worden van tijd tot tijd gevonden, zie bijvoorbeeld http://www.thoughtcrime.org/papers/null-prefix-attacks.pdf en http://extendedsubset.com/?p=8. Deze worden relatief snel opgelost. Vaak is op zijn minst een actieve aanvaller (§4.1.5 en §4.1.6) nodig om deze zwakheden uit te buiten.

Met een passieve aanvaller op het GSM netwerk moet, sinds de succesvolle aanvallen op de versleuteling van GSM telefoonverkeer [GOVCERT.NL, Nohl and Paget], rekening gehouden worden. Authenticatiemiddelen die gebruik maken van GSM gebruiken dit kanaal echter alleen om eenmalig te gebruiken codes door te geven (door de aanvaller vergaarde informatie via GSM zal dus in een actieve aanval gebruikt moeten worden).

4.1.5 PHISHING

Bij phishing wordt een gebruiker verleidt om naar een door de aanvaller gecontroleerde nep-website te gaan en daar een authenticatiesessie te starten. Dit gebeurt meestal via een email met daarin een uitnodigende link naar de website. Als gebruikt wordt gemaakt van gebruikersnaam/wachtwoord dan zal de gebruiker hier zijn of haar wachtwoord invullen. Met deze credentials kan de phisher dan op een later tijdstip bij de daadwerkelijke controlerende partij authenticeren en zo diensten afnemen in naam van het slachtoffer.

Phishing wordt voor een groot deel ook via TLS/SSL opgelost. Wel vereist dit van de eindgebruiker dat deze bijvoorbeeld goed controleert dat zijn of haar browser inderdaad erin geslaagd is een beveiligde verbinding op te zetten met de dienstaanbieder. Bewustzijnscampagnes zoals "3 x kloppen" trachten de gebruiker hiervan bewust te maken.

Wanneer geen gebruik gemaakt wordt van gebruikersnaam/wachtwoord, maar van een OTP authenticatiemiddel of een eenvoudig challenge-response authenticatiemiddel, dan heeft de phishende aanvaller geen kans van slagen. De controlerende partij zal herkennen dat de gebruikte codes niet bij de nieuwe sessie horen.

4.1.6 MAN-IN-THE-MIDDLE OP HET NETWERK

Een aanvaller kan zich ten opzichte van een gebruiker voordoen als de controlerende partij (bijvoorbeeld door via een phishing email de gebruiker te verleiden om naar een door de aanvaller gecontroleerde nep-website te gaan) en tegelijkertijd, *tijdens de authenticatiesessie* van de gebruiker zich voordoen ten opzichte van de controlerende partij als de gebruiker. De aanvaller speelt tijdens de transactie voor een groot deel alleen de rol van doorgeefluik, maar kan op essentiële punten wellicht transactiedetails veranderen.

OTP of challenge-response tokens helpen niet tegen deze aanval doordat de aanvaller tijdens dit deel van de transactie alleen als doorgeefluik optreedt.

Door een beveiligde verbinding met de controlerende partij op te zetten (via TLS/SSL) en de gebruiker ook te laten controleren dat de bestemming klopt (de authenticiteit van de server is geconstateerd door een CA en de browser van de gebruiker kan een SSL certificaat controleren en laten zien aan de gebruiker) kan deze aanval voorkomen worden. Wederom (zoals beschreven in §4.1.5) vereist dit oplettendheid bij de gebruiker.

4.1.7 MAN-IN-THE-BROWSER

Een man-in-the-middle kan op het netwerk maar ook op de PC van de gebruiker voorkomen. Dit laatste geval is veel gevaarlijker en kan bijvoorbeeld geïmplementeerd worden door een geïnstalleerd malware programma (een trojan). Als deze malware voldoende privileges heeft kan deze bijvoorbeeld certificaten toevoegen aan de database van vertrouwde certificaatautoriteiten.

Maar malware hoeft hier niet noodzakelijk privileges op administratorniveau te hebben. Een *man-in-the-browser* is een variant van deze aanval waarbij een trojan een browser-plugin[20] aan de browser toevoegt welke ingrijpt in lopende websessies, bijvoorbeeld tijdens een sessie met de echte controlerende partij. In een typisch geval kan een man-in-the-browser de gebruiker een scherm laten zien met transactiedetails die niet overeenkomen met de transactie die de gebruiker aan het uitvoeren is.

Het is erg lastig om onder dergelijke omstandigheden de gebruiker een veilige transactie te laten uitvoeren.

Malware neemt toe in hoeveelheid (aantal drive-by download sites), en inventiviteit. Niet al te lang geleden werden exploits eerst in theorie in de zogenaamde white-hat gemeenschap bedacht en werden ze pas veel later in het wild ontdekt (blijkbaar door de zogenaamde black-hat gemeenschap als aanval geïmplementeerd). Tegenwoordig is het eerder andersom. De gebruiker lijkt kansloos tegen dit soort malware.

Verschillende oplossingen kunnen op de korte termijn het probleem beheersbaar houden. Er zijn bijvoorbeeld mogelijkheden om op de back-end verdachte transacties te detecteren (en terug te draaien). De PC van de gebruiker kan beter beschermd worden (zie §5.5). En het kan de geïnstalleerde trojan moeilijker gemaakt worden om de

[20] Alle grote browsers staan hulpprogramma's toe om bepaalde additionele features toe te voegen.

website van de bank aangepast weer te geven (dit vereist oplettendheid bij de gebruiker).

Het risico wordt nu ook al tot aanvaardbare proporties worden teruggebracht door voor hoge bedragen transactiedetails door gebruiker te laten controleren via het authenticatiemiddel. Als het authenticatiemiddel invoermogelijkheden heeft (een toetsenbord) kan gevraagd worden om het bedrag en eventueel het tegenrekeningnummer in te voeren. Als het authenticatiemiddel uitvoermogelijkheden heeft (een scherm) kunnen deze zaken getoond worden. Omdat dit met de huidige generatie tokens nogal gebruiksonvriendelijk is, vooral bij hoge volumes, moet er eerst iets veranderen aan de tokens, voordat dit bij elke transactie gedaan kan worden.

Een echte oplossing is om over te stappen van authenticatie naar *transactieintegriteit* en dit ook door de gebruiker te laten controleren. De transactiedetails moeten dan meegenomen worden en, na consent van de gebruiker, ondertekend worden door het authenticatiemiddel.

4.1.8 INSIDER BIJ DE DIENSTAANBIEDER OF CONTROLLERENDE PARTIJ

Werknemers bij de dienstaanbieder of controlerende partij die niet te vertrouwen zijn (aanvallen uitgevoerd door zogenaamde insiders) zijn een probleem. Aangenomen is steeds dat de controlerende partij door de dienstaanbieder *en* door de gebruiker te vertrouwen is. Met een combinatie van geavanceerde authenticatiemiddelen (waarbij de controlerende partij slechts hoeft te beschikken over publieke informatie, en geen geheime informatie die in het middel aanwezig is) en organisatorische maatregelen is het goed mogelijk om aanvallen tijdens authenticatiesessies te voorkomen of in ieder geval te detecteren. Vooral bij binding, echter, moet voorkomen worden dat insiders verkeerde invloed op processen kunnen uitoefenen (§4.1.1).

4.2 CONCLUSIE

Sinds de invoering van online financiële diensten zoals internetbankieren is het dreigingslandschap op essentiële punten veranderd. Waar de dreiging initieel van passieve aanvallers op het internet uitging, is deze de laatste jaren verschoven naar het verleiden van slachtoffers om *phishing* sites te bezoeken en daar gebruikersnaam en wachtwoord achter te laten. Door een combinatie van technische maatregelen (o.a. OTP en challenge-response tokens), verkeerd gedrag bij de consument onmogelijk te maken (denk aan overlay banking dat op de back-end systemen gedetecteerd kan worden) en het bewust en alert maken van de consument (door campagnes als “3 x kloppen”) is deze dreiging tot nu toe redelijk hanteerbaar.

Nieuwe aanvallen op basis van geïnstalleerde malware (zogenaamde man-in-the-browser aanvallen beschreven in §4.1.7) zorgen ervoor dat browser-gebaseerde internetbankieren niet veel langer beschermd kan worden met die relatief eenvoudige OTP of challenge-response authenticatiemiddelen. Een aanvaller die op de PC van de gebruiker controle krijgt over de browser kan door een zogenaamde man-in-the-browser invloed uitoefenen op de transactie. De kans dat een grote groep gebruikers getroffen wordt door zo’n trojan lijkt, ondanks pogingen om het besturingssysteem en de browser te beschermen, groter te worden. Om de risico’s voortkomend uit deze dreigingen tot aanvaardbare niveaus terug te kunnen brengen, zullen, naast authenticeren van transacties, het meenemen van transactionele context en het beter betrekken van de eindgebruiker hierbij, technische innovaties op het gebied van

authenticatiemiddelen nodig zijn.

5 Innovaties en oplossingen

In de onderzoeksgemeenschap en in de financiële sector wordt voortdurend gekeken naar technische innovaties om authenticatieproces te verbeteren. Dit hoofdstuk geeft een selectie van ontwikkelingen en bekijkt de relevantie ten opzichte van de in de eerdere hoofdstukken gegeven state-of-the-art.

5.1 ALTERNATIEVE WACHTWOORDEN

De problemen bij gebruikersnaam/wachtwoord combinaties ontstaan eigenlijk door twee factoren. Ten eerste moet de entropie van een wachtwoord laag zijn want een wachtwoord moet door een mens onthouden kunnen worden. Dit heeft tot gevolg dat wachtwoorden vaak makkelijk te raden zijn en ook makkelijk doorgegeven, afgeluisterd (of ge-shoulder-surfed) kunnen worden.

Ten tweede, wordt een wachtwoord ingevoerd op een (in principe) onvertrouwd apparaat. Dit geldt voor de desktop computer bij de gebruiker thuis (die mogelijk een phishing site in de browser geladen heeft, of waar een malware programma meeluistert) en voor de geld- of betaalautomaat waar een aanvaller mogelijk skimming-apparatuur op heeft geïnstalleerd.

Voor beide problemen zijn alternatieve vormen van wachtwoordauthenticatie bedacht, waarbij de gebruiker meestal iets anders moet onthouden dan een wachtwoord. Een voorbeeld is GRIDSure[21]: de gebruiker onthoudt niet een PIN maar een patroon, vervolgens wordt een cijfermatrix getoond waaruit de gebruiker cijfers moet overtikken om een sessie-PIN te krijgen. Een ander voorbeeld is MyVidoop waarbij de gebruiker een drietal verschillende foto-categorieën onthoudt (“een computer”, “een trein”, “een telefoon”) waarvan vervolgens concrete foto’s (een foto van een laptop, een foto van een stoomtrein, een foto van een ouderwetse draaischijftelefoon) met bij elke foto steeds een andere letter. Ook hier moet het sessie-wachtwoord bestaande uit de letters ingetypt worden voor authenticatie. Een variant is PassFaces[22] waar de gebruiker een sequentie bekende gezichten moet aanwijzen uit een gepresenteerde matrix van foto’s.

Al deze oplossingen pakken vooral het tweede probleem aan door een sessie afhankelijkheid in te bouwen. Als een aanvaller een aantal keer mag meekijken is, door de relatief lage entropie, het onderliggende patroon in veel gevallen te achterhalen.

5.2 CONNECTED DEVICES

Een end-to-end secure connectie tussen authenticatiemiddel en back-end systeem, waarbij de gebruiker geen berichten hoeft over te typen, biedt zowel voordelen op het gebied van gebruiksgemak als op het gebied van beveiliging. De “iets wat men heeft” factor kan zo eenvoudiger gecontroleerd worden, de token kan direct met de

[21] GrIDsure (vendor). Zie http://www.gridsure.com/.

[22] PassFaces (vendor). Zie http://www.realuser.com/.

back-end systemen communiceren. Om zo'n connectie te bewerkstelligen zou een authenticatiemiddel aangesloten kunnen worden op de PC van de gebruiker. Alternatief zou zijn om het authenticatiemiddel uit te rusten met autonome netwerkmogelijkheden (met multi-channel als bijkomend voordeel).

- Automatisch inscannen van challenge/response (camera / optische scanner die voor beeldscherm gehouden wordt). Dit kan gebruikt worden om een end-to-end verbinding met het token te maken.
- Automatisch invoeren (bijvoorbeeld een wachtwoordgenerator die eentoetsenbord nadoet zoals de Yubikey (besproken in §3.2.4).
- Connected PIN-calculators, via USB (niet duidelijk of dit driverless kan; e.dentifier2 van ABN AMRO vereist bijvoorbeeld een software installatie en bied fall-back door ook een niet connected mode te ondersteunen).
- IBM ZTIC (IBM research in Zurich, zie afbeelding, zie [Weigold et al.]) combineert een authenticatie-token met (read-only) USB opslag. Software om een verbinding met de bank op te zetten (een driver) staat op het token en kan eenvoudig geinstalleerd worden. De verbinding wordt vervolgens versleuteld met behulp van TLS/SSL op basis van sleutels op het middel. Het middel beschikt over een display om transactiedetails te laten zien.

Figuur 3: IBM ZTIC.

5.3 BIOMETRIE

Biometrie is uitgebreid beschreven in §3.1.6. Hoewel de techniek al lang bestaat, wordt biometrie als onderdeel van authenticatie voor online diensten voor consumenten nog niet breed toegepast[23]. Wel worden biometrische kenmerken sinds enkele jaren wereldwijd toegepast in de chip die door veel overheden in reisdocumenten geïntegreerd worden. Een ontwikkeling die de industrie rond biometrische authenticatie ongetwijfeld een duwtje inde rug zal geven.

[23] Er gaan geruchten dat gezichtsherkenning onderdeel zal uitmaken van Windows 8: http://msftkitchen.com/2010/06/windows-8-plans-leaked-numerous-details-revealed.html. Sommige laptops beschikken al over gezichtsherkenning software die werkt met de webcam. Dit blijkt echter niet echt veilig te zijn: http://www.blackhat.com/presentations/bh-dc-09/Nguyen/BlackHat-DC-09-Nguyen-Face-not-your-password.pdf.

De meerwaarde van biometrische authenticatiefactoren ten opzichte van andere factoren zijn gebruiksgemak en veiligheid omdat een “iets wat men is” factor vanzelfsprekend zeer persoonsgebonden is. Biometrische kenmerken kunnen niet vergeten worden en zijn (als het goed is) niet door anderen dan de rechtmatige eigenaar te gebruiken. Er kleven ook nadelen aan biometrie, vooral op privacygebied. Echter als extra factor is het zeker denkbaar dat biometrie in de toekomst voor een sterke binding van gebruiker aan token gaat zorgen.

5.4 GEDRAGSKENMERKEN

Gedrag van de gebruiker kan ook als biometrisch kenmerk gezien worden, zie ook §3.1.6. Een voorbeeld van gedragsauthenticatie is toetsenbord-biometric [Ordal 2005]. De gebruiker authenticeert zichzelf door een wachtwoord in te voeren, waarbij niet alleen gekeken wordt wat het ingetoetste wachtwoord is, maar ook naar de manier waarop dit ingevoerd wordt door te meten hoe lang de gebruiker over toetsaanslagen doet.

Gedragsinformatie, zoals gebruikt bij gedragsbiometrie, is een speciaal geval van context informatie. Andere contextuele factoren, zoals bijvoorbeeld de typische tijden dat een gebruiker inlogt ,kunnen ook meegenomen worden tijdens het authenticatieproces (en zelfs daarna tijdens het gebruik van de dienst) om meer zekerheid te krijgen dat echte gebruiker daadwerkelijk de dienst afneemt. Mobiele apparaten beschikken vaak over sensoren (bijvoorbeeld GPS) die nog meer informatie over de context van de gebruiker kunnen verschaffen. De GPS locatie van het mobieltje kan eenvoudig gecombineerd worden met de locatie van een geldautomaat waarmee geverifieerd kan worden of de gebruiker daadwerkelijk bij de betreffende geldautomaat een geldopname doet of iemand anders. Een ander voorbeeld van een sensor is de accelero-meter die in veel smart phones zit[24].

5.5 VEILIGER MAKEN VAN CONSUMER PLATFORM (DE PC)

Eén van de grote risico’s wordt gevormd door de onvertrouwde PC bij de gebruiker thuis. De PC wordt regelmatig gebruikt wordt om high-trust diensten af te nemen en kan verborgen malware bevatten die ingrijpt in transacties. Dit wordt op dit moment als de zwakste plek gezien. Hoewel veel aanvallen nu nog op het netwerk plaatsvinden (denk aan phishing sites) is de verwachting dat op een gegeven moment dit zal verschuiven naar de desktop computer ij de gebruiker thuis (bijvoorbeeld MitB, zie Hoofdstuk 4).

[24] Accelerometers waren eerder al te vinden in sommige laptops (om een val van het apparaat te kunnen detecteren zodat de harddisk in parkeerstand gezet kan worden), in navigatiesystemen (om bij uitval van het GPS signaal een schatting te kunnen maken van de relatieve positie van het voertuig), en in digitale camera’s (om ‘portrait’ of ‘landscape’ posititie meta-data aan opnamen te kunnen toevoegen).

De voor de hand liggende oplossing, het platform gewoon veiliger maken, lijkt niet realistisch te zijn. Ondanks innovaties op dit gebied (besturingssystemen zoals Microsoft Windows zijn de laatste jaren op het gebied van bescherming tegen softwaremisbruik door malware behoorlijk verbeterd[25]) blijven exploiteerbare bugs in het platform gevonden worden. Sterker nog, exploits nemen in aantallen toe en de tijd tussen theoretische mogelijkheid en in het wild voorkomen van exploits wordt steeds korter.

Figuur 4: Qubes

Virtualisatie en sandboxing bieden mogelijk oplossingen. Onduidelijk is in hoeverre dit ten koste van het gebruiksgemak gaat. Een voorbeeld van virtualisatie is de "Qubes[26] hypervisor[27]" waarbinnen verschillende applicaties op verschillende virtuele machines gedraaid worden. In Figuur 4 draait de web browser waarmee een aankoop in een web winkel wordt gedaan (met gele randen) op een andere virtuele machine dan de web browser waarmee een krantenartikel gelezen wordt (met rode randen). De desktop computer van de gebruiker heeft beide virtuele machines tot gast en bied mogelijkheden tot interactie met gebruiker en netwerk voor beide virtuele machines, maar ze zijn verder strikt gescheiden.

Virtualisatie en sandboxing zorgen voor een redelijk betrouwbare platform binnen het onbetrouwbare platform van de consument. Onduidelijk blijft of een en ander gerealiseerd kan worden zonder in te boeten op gebruiksgemak wanneer de oplossing vergeleken wordt met externe tokens.

---

[25] Zie http://msdn.microsoft.com/en-us/library/bb430720.aspx.

[26] Zie http://qubes-os.org/.

[27] De term hypervisor (de overtreffende trap van supervisor) verwijst naar het (streng beveiligde) instantie van een besturingsysteem dat een aantal virtuele machines beheert (en in de gaten houdt) waarin minder veilige instanties van besturingssystemen draaien.

5.6 MOBIELE TELEFOON

Een mobiele telefoon kan ingezet worden als authenticatiemiddel. Dit heeft als grote voordeel dat de mobiele telefoon door consumenten als zeer persoonsgebonden beschouwd wordt. Een verloren of gestolen mobiele telefoon wordt door de eigenaar binnen enkele minuten opgemerkt, in tegenstelling tot bankpas, portemonnee, laptop, agenda, sleutels, etc. Een moderne smart-phone heeft bovendien een groot scherm en invoermogelijkheden die de meeste andere authenticatiemiddelen te boven gaan.

Veel potentie voor de mobiele telefoon als authenticatiemiddel ligt in het feit dat een GSM (of UMTS) mobiele telefoon over een smart card lezer met smart card beschikt: de SIM kaart. Deze feature lost in één klap de problemen van hardware- en softwareondersteuning op die doorgaans optreden bij smart card oplossingen. Bij Mobile PKI (§3.2.12) [Oostdijk-Wegdam-2009] wordt de SIM ingezet voor ondertekening of authenticatie (ondertekening van transacties). Het resultaat is een zeer veilig middel met behoorlijk gebruiksgemak.

Nadeel is dat de mobiele operator de sleutels tot de SIM kaart beheert. De technische standaarden staan toe dat de mobiele operator een deel van de SIM verhuurt aan andere partijen die zelf applicaties kunnen beheren. De mobiele operator zal echter altijd een rol spelen in het business-model als gebruik wordt gemaakt van de SIM. Bij de minder geavanceerde varianten van gebruik van de mobiele telefoon voor authenticatie, SMS OTP (§3.2.6) en een op het apparaat geïnstalleerde applicatie (§3.2.11) is de rol van de mobiele operator bescheidener.

5.7 GEBRUIKER INFORMEREN OVER TRANSACTIEDETAILS EN LATEN AKKORDEREN

De huidige generatie authenticatiemiddelen voor internetbankieren (o.a. Random Reader van Rabobank en e.dentifier van ABN AMRO) eisen bij omvangrijkere transacties (bedragen boven een bepaalde grens) dat de gebruiker, naast challenge of TAN, ook nog transactiedetails in het token invoert. Voorbeelden van additionele details zijn bedrag en tegenrekeningnummer. Een alternatief is om de gebruiker te informeren over transactiedetails via de display van het token en expliciet toestemming te laten geven voor het uitvoeren van de transactie. In beide gevallen wordt gebruiksvriendelijkheid ingeruild voor meer bewustzijn bij de gebruiker.

Wanneer het token aan bepaalde eisen uit de Europese richtlijn elektronische handtekeningen [EU Directive 1999] voldoet, dan kan de gebruiker een rechtsgeldige handtekening over essentiële transactiedetails doen. De richtlijn eist bijvoorbeeld dat het token op een sterke manier aan de gebruiker gebonden is, en dat deze onweerlegbaar is.

5.8 CONCLUSIE

De meeste innovaties zijn slechts verbeteringen (op punten) van bestaande middelen, denk bijvoorbeeld aan alternatieven voor wachtwoorden en PIN codes. Sommige innovaties doen in hun huidige vorm nogal exotisch aan (accelerometers, gezichtsherkenning, …). Afgewacht moet worden hoe nuttig deze zijn.

Het tot stand brengen van een beveiligde verbinding van het authenticatiemiddel te verbinden met de back-end systemen via de dektop computer van de gebruiker kan het overtypen van challenge en/of response overbodig gemaakt worden. Om man-in-the-browser tegen te kunnen gaan, moet in plaats van authenticatie overgegaan

worden op het beschermen van *transactieintegriteit en -authenticiteit*. Nodig hiervoor zijn: connectedness van het token en goede mogelijkheden om transactiedetails naar de gebruiker te communiceren (een groot display) om WYSIWYS (what-you-sign-is-what-you-see) zo dicht mogelijk te benaderen. Dit soort maatregelen gaat wel gepaard met de introductie van complexiteit in het authenticatieproces waardoor sneller fouten kunnen optreden of gebruikers afhaken. Hiermee dient rekening gehouden te worden bij de introductie ervan.

6 Conclusies

Uit analyse van de context waarin authenticatiemiddelen ingezet worden, in Hoofdstuk 2, blijkt dat vele factoren van invloed zijn op het succes van een authenticatiemiddel. Perfecte beveiliging bestaat niet; en het versterken van authenticatie zal vaak ten koste gaan van gebruiksvriendelijkheid. De succesfactoren zijn niet alleen te vinden in het directe gebruik van het middel door de consument, maar ook in processen zoals uitgifte en juridische raamwerken waarin zaken als aansprakelijkheid vastgelegd zijn. Een aantal ontwikkelingen en trends, beschreven in §2.3, lijkt in de richting te wijzen voor domeinoverstijgende authenticatie (inzetbaar voor diensten van verschillende dienstaanbieders).

Authenticatiemiddelen die op dit moment gebruikt worden, beschreven in Hoofdstuk 3, zijn gebaseerd op een beperkt aantal onderliggende technieken zoals challenge-reponse, OTP, multi-factor, multi-channel, tamper-resistance. In combinatie met standaard beveiligingspraktijk bij de dienstaanbieders en standaard Internettechnologie voor het opzetten van beveiligde verbindingen tussen browser en web-server bieden deze middelen voldoende technische bescherming tegen traditionele aanvallen waarbij de aanvaller zich op het netwerk bevindt, zoals phishing.

Dat een authenticatietoken in handen van een kwaadwillende persoon misbruikt wordt, kan voorkomen worden door het op een sterkere manier te binden aan een persoon. Biometrie of een andere extra factor kan hier een oplossing zijn, maar het toepassen van biometrie in de situatie bij de gebruiker thuis is lastig. Een sterkere binding van het authenticatiemiddel aan de gebruiker biedt als voordeel dat daadwerkelijk gepleegde transacties moeilijker te ontkennen zijn door de gebruiker. Fraude met medeweten van de gebruiker wordt moeilijker.

Het dreigingslandschap, geschetst in Hoofdstuk 4, laat twee zwakke plekken zien: de consument en de PC van de consument. Bewustwordingscampagnes (3 x kloppen) en ontmoedigen van “verkeerd” gedrag (zoals bijvoorbeeld overlay banking[28]) zijn belangrijk om de eerste zwakke plek te versterken.

De tweede zwakke plek, de PC van de gebruiker, betekent dat het browser-gebaseerde internetbankieren op middellange termijn niet langer beschermd kan worden met de eenvoudige challenge-response en OTP authenticatiemiddelen die nu populair zijn bij dienstaanbieders. Een aanvaller die op de PC van de consument controle krijgt over de browser (een zogenaamde man-in-the-browser trojan) kan invloed uitoefenen op de transactie. De kans dat een grote groep gebruikers getroffen wordt door deze aanval lijkt groter te worden. Hoewel er veel

[28] Bij overlay banking wordt door een externe dienstaanbieder (de overlay bank) aan gebruikers gevraagd om de toegangscodes (wachtwoorden, TAN codes) van financiele dienstverleners zoals banken in te leveren zodat deze door de overlay bank gebruikt kunnen worden om namens de gebruiker in te loggen. De overlay bank biedt gebruiksgemak en organisatorische en juridische maatregelen ter beveiliging (garantie, certificering). Maar het principe druist in tegen bewustwordingscampagnes als ‘3 x kloppen’ waarin gebruikers juist aangeraden wordt om nooit toegangscodes met anderen te delen.

geïnvesteerd wordt in het veiliger maken van het besturingssysteem en de browser, neemt het aantal gemelde exploiteerbare weeffouten in software alleen maar toe en lijkt er ook steeds meer actief misbruik van dit soort weeffouten gemaakt te worden nog voordat beveiligers er weet van hebben.

Een end-to-end beveiligde verbinding tussen authenticatiemiddel en back-end systeem biedt zowel voordelen op het gebied van gebruiksgemak als op het gebied van beveiliging. De gebruiker hoeft geen berichten over te typen en een man-in-the-browser wordt gepasseerd. Om zo'n connectie te bewerkstelligen kan een authenticatiemiddel uitgerust worden met autonome netwerkmogelijkheden: geïntegreerd in een mobiele telefoon bijvoorbeeld. Alternatief is om het middel aan te sluiten op het apparaat dat gebruikt wordt om de dienst af te nemen en een beveiligde *virtuele* netwerkverbinding op te bouwen. In beide gevallen is er feitelijk sprake van multi-channel.

Daarnaast moet het de consument zo eenvoudig mogelijk gemaakt worden om geldige transacties op een bewuste manier te kunnen accorderen. Dit betekent dat een authenticatiemiddel over in- en uitvoermogelijkheden moet kunnen beschikken waarmee de transactie in voldoende detail door en aan de gebruiker gepresenteerd kan worden (voor deze presentatie is ook een rechtstreekse veilige verbinding met de back-end systemen vereist). Het ondertekenen van een transactie door het authenticatiemiddel met een elektronische handtekening is een voor de hand liggende manier te zijn om dit te doen. Indien een geavanceerde elektronische handtekening gebruikt wordt, kan hetzelfde middel ook gebruikt worden om documenten en email te ondertekenen.

Nieuwe ontwikkelingen op het gebied van authenticatie worden gekenmerkt door complexiteit en zijn nog slecht uitrolbaar in een consumentensetting.

DANKWOORD

Wim Hafkamp en Henny van der Pavert van Rabobank Nederland / IBA hebben tijdens de initiële fase van het onderzoek input geleverd en gedurende het onderzoek verschillende versies van commentaar voorzien. Vanuit het cidSafe kernteam hebben Jaap Kuipers en Marcel Jak van Diginotar en Florus van der Linden van SIVI kritisch naar de scan gekeken en veel waardevol commentaar geleverd. Tijdens het onderzoek is een aantal experts-uit-het-veld op informele wijze geïnterviewd over de bestudeerde materie. Allen hartelijk dank!

Referenties

BSI, *Website met documenten,* https://www.bsi.bund.de/english/publications/, Juli 2010

Bundesverband deutscher Banken e.V, ZKA-TAN-Generator: Belegungsrichtlinien für das chipTAN-Verfahren, versie 1.4, http://www.hbci-zka.de/, 2008

Cavoukian A. and Stoianov A., *Biometric encryption: A Positive-Sum Technology that achieves Strong Authentication,* Beschikbaar via http://www.privacybydesign.ca/pbdbook/PrivacybyDesignBook-ch7.pdf, Maart 2007

Daugman, J., *How Iris Recognition works,* IEEE Trans. Circuits Syst. Video Techn. 14(1): 21-30, Beschikbaar via www.cl.cam.ac.uk/~jgd1000/irisrecog.pdf, 2004

Drimer, S., Murdoch, S. J., Anderson, R., *Optimised to Fail: Card Readers for Online Banking,* Financial Cryptography and Data Security '09, LNCS, Springer, pp. 194—200, February 2009

EPC, *Customer-to-bank, Security Good Practices Guide,* EPC397-08v1.1, Maart 2009

EU, *EU e-signature directive,* 1999/93/EC, OJ L 13, p. 12, 1999/2000

GOVCERT.NL, *Afluisteren van GSM-communicatie dichterbij,* Factsheet FS 2009-05 – Versie 1.0, December 2009

Guhring, P., *Concepts against Man-in-the-Browser attacks*, http://www2.futureware.at/svn/sourcerer/CAcert/SecureClient.pdf, 2006

Hulsebosch, R.J., *Contextinformatie maakt dienstverlening veiligerr,* Automatisering Gids, nr 12, p.15—16, 24 Maart 2005

Hulsebosch, R.J., *CidSafe buitenlandse Cases flyer,* Mei 2010

Hulsebosch, R.J., *CidSafe gebruik BSN flyer,* Juni 2010

ISO, *ISO/IEC 24727-3:2008 Identification cards – Integerated circuit card programming interfaces – Part 3: Application interface,* 2008

KPMG, *Verkenning Authenticatie: Roeien met de riemen die je hebt?, R.2007.ISC.18,* voor: Forum Standaardisatie, Maart 2007

KPMG/Everett, *2009 European Identity and Access Management Survey,* October:2009

Nohl, K. and Paget, C., *GSM – SRSLY?,* Presentatie op Chaos Computer Club Congress, December 2009

Lenzini, G., Oostdijk, M., Van Pelt, X., *Security aspecten van mobile learning,* SURFnet, Beschikbaar via http://www.surfnet.nl/nl/nieuws/Pages/mobilelearning.aspx, November 2008

Oostdijk, M. en Wegdam, M., *Mobile PKI - A technology scouting for security and use of mobile authentication technologies,* SURFnet, Beschikbaar via http://www.terena.org/news/community/download.php?news_id=2528, 2009

Ordal, P. et al., *Continuous Identity Verification trhough Keyboard Biometrics,* JUR vol. 4 – issue 1, 2005

Putte, Ton van der en Keuning, Jeroen, *Biometrical Fingerprint Recognition – Don't get your fingers burnt,* IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, pages 289-303, Kluwer Academic Publishers, 2000

RSA Labs, *PKCS standards,* Available from http://rsa.com/rsalabs, 2009

Schouwenaar, M., *Dutch EMV cards and Internet banking,* Thesis Number 635, Radboud University, 2010

Schneier, B., *Secrets and Lies: Digital Security in a Networked World,* Wiley 2000

Wang, J-F et al., *Gender Determination using Fingertip Features,* Internet Journal of Medical Update, Vol. 3, No. 2, pp. 75–91, 2008

Weigold, T. et al., *The Zurich Trusted Information Channel – An Efficient Defence against Man-in-the-Middle and Malicious Software Attacks,* In proc. Trust 2008, LNCS 4968, Springer, pp. 75–91