IRMA

Attributen in plaats van identiteiten

Attributen zijn eigenschappen van personen die in het dagelijkse leven veel gebruikt worden als basis van transacties. Met nieuwe cryptografische technieken is het ook mogelijk elektronische transacties te baseren op attributen in plaats van op identiteiten. Een concrete realisatie daarvan is het project IRMA, waarbij een betrouwbare digitale infrastructuur op een proportionele wijze omgaat met persoonsgegevens en niet meer gegevens vereist dan strikt noodzakelijk is.

BART JACOBS

In veel situaties, in de gewone *offline* wereld, maar zeker ook in de *online* wereld op het web, is het belangrijk te kunnen vaststellen met wie we van doen hebben. Dit geldt met name voor IT-auditors die moeten vaststellen wie een bepaalde handeling mag en kan verrichten. Daarbij moet bepaald kunnen worden of een persoon ook daadwerkelijk bevoegd is om de betreffende handeling te verrichten. Van belang zijn daarmee niet alleen identiteiten, maar ook attributen. In het algemeen worden attributen hier begrepen als eigenschappen van personen die van belang zijn bij het autoriseren van handelingen of transacties. Attribuutgebaseerde toegang is een belangrijke nieuwe trend, die in dit artikel besproken zal worden. Attributen vormen een zeer flexibel kader waarmee allerlei nieuwe toepassingen mogelijk zijn en waarbij precies die gegevens uitgewisseld worden die voor een transactie noodzakelijk zijn. Dit is privacyvriendelijk en geeft bescherming tegen identiteitsfraude. In dit artikel wordt in het bijzonder ingegaan op het project IRMA, van onder andere de Radboud Universiteit Nijmegen, waarbij persoonlijke attributen door middel van smart cards voor transacties getoond worden.

IDENTITY MANAGEMENT

Identity management is een aparte discipline geworden die zich bezighoudt met het systematische beheer van identiteiten, binnen een organisatie (bijvoorbeeld via toegangspassen), in een land (in Nederland via DigiD), of zelfs op wereldwijde schaal (via paspoorten). Drie basisbegrippen zijn:

- **identificatie:** *zeggen* wie je bent, bijvoorbeeld via een gebruikersnaam of login;
- **authenticatie:** *bewijzen* wie of wat je bent, bijvoorbeeld via een wachtwoord of PIN, of meer in het algemeen via een *credential*;
- **autorisatie:** vaststellen waartoe iemand bevoegd is.

Identity management omvat niet alleen een precieze uitwerking van deze drie begrippen, maar ook een veelheid van daarmee samenhangende onderwerpen: logging, lifecycle management van credentials (productie, personalisatie, uitgifte, gebruik, vervanging, terugname, herroeping, vernietiging), interoperabiliteit, privacy, et cetera. Nu informatie- en communicatietechnologie (ICT) tot in de haarvaten van onze samenleving is doorgedrongen is identity management een integraal en onvermijdelijk onderdeel geworden van onze manier van leven. Dit betreft niet alleen professioneel identity management binnen organisaties, maar ook persoonlijk identity managent. Bij het laatste kan men denken aan het omgaan met verschillende e-mailadressen, gebruikersnamen en wachtwoorden, maar in de toekomst ook aan het omgaan met persoonlijke attributen.

Er bestaat een haast natuurlijke neiging om in ICT-systemen identiteiten te koppelen aan transacties en processen. Dit maakt het makke- ▶

lijker om achteraf, bij eventuele problemen, vast te stellen wie wat gedaan heeft. Bedrijven hebben tegenwoordig vooral online contact met de klant en willen daarbij graag weten met wie ze van doen hebben voor hun *customer relation management* (CRM). Ze proberen uit die online contacten via profilering en *behavioral targeting* zoveel mogelijk secundaire informatie te destilleren om het contact met die klant te verbeteren en om nieuwe commerciële kansen te herkennen. Individuen zijn zich nog niet of nauwelijks bewust van de informatie die ze over zichzelf prijsgeven, impliciet of expliciet, en van de waarde van die informatie.

Het toenemend gebruik van identiteiten heeft echter een duidelijke prijs: identiteitsfraude en privacy-aantasting. Indien je overal moet bewijzen wie je bent, typisch via een kopietje-paspoort, loop je groot risico dat iemand anders van die credentials misbruik maakt. Met zo'n kopie kan een nieuw telefoonabonnement of een lening afgesloten worden, waarbij de kosten op jouw conto kunnen komen, je reputatie aangetast kan worden (bijvoorbeeld via opname bij het bureau krediet registratie BKR), of waarbij je zelfs verdachte of veroordeelde kunt worden (bijvoorbeeld als zo'n telefoon voor een bedreiging wordt gebruikt). Gevallen van identiteitsfraude zijn individueel ontwrichtend doordat 'opschoning' moeizaam en stressvol is. Identiteitsfraude is de plaag van de digitale samenleving, die zelfs maatschappelijk ontwrichtende vormen aan kan nemen.

Mensen hebben gerechtvaardigde verwachtingen dat persoonlijke informatie tot de gepaste context beperkt blijft: wat je met je huisarts bespreekt, wil je niet vervolgens terughoren van een drogisterijketen: 'U heeft kennelijk aambeien, en daar hebben wij speciaal voor u een aanbieding voor!'. Ook willen mensen die aan online medische/psychische hulpgroepen deelnemen dit vaak doen zonder dat bekend is wie ze zijn. Anonimiteit is een gerechtvaardigd belang. Privacy en individuele autonomie vormen de basis voor onze maatschappelijke ordening. Daarnaast is privacy niet alleen belangrijk voor je persoonlijke welbevinden, maar in sommige situaties zelfs essentieel voor je persoonlijke veiligheid: denk aan vrouwen in een blijf-van-mijn-lijfhuis. In de afgelopen jaren waarin terrorisme het angstbeeld bepaalde werd privacy vooral afgeschilderd als 'schuilplaats van het kwaad'. Maar met de huidige zorgen om cybersecurity is het discours veranderd en wordt burgers voorgehouden dat ze vooral zorgvuldig met (persoons)gegevens om dienen te gaan.

Nu de digitalisering van onze samenleving vergevorderd is, begint langzaamaan het besef door te dringen dat privacy systematische bescherming verdient en dat het klakkeloos vastleggen van identiteiten ook risico's met zich meebrengt. Misschien moeten we juist minder identiteiten gebruiken: wanneer mijn identiteit immers niet in het geding is, kan die ook niet gestolen worden en kan mijn privacy niet aangetast worden.

IDENTITY MANAGEMENT MET ATTRIBUTEN

Attributen vormen een flexibel mechanisme om dit gebruik van identiteiten te proportionaliseren. Het gebruik van attributen zet een rem op het ongericht verzamelen van persoonsgegevens. Als ik een fles whisky koop, moet ik bewijzen dat ik boven de achttien ben, maar hoef ik helemaal niet te vertellen wie ik ben. In de praktijk, in een winkel, wapper ik even met mijn paspoort en is het goed. Essentieel hierbij is het idee dat de winkelier niet alle identiteitsgegevens uit mijn paspoort registreert: zij kijkt misschien even naar mijn geboortedatum, maar is die daarna weer snel vergeten. Maar online is zoiets een stuk lastiger te regelen. Wat je daar voor nodig hebt is een mechanisme om enkel het attribuut 'boven de 18' te kunnen bewijzen, en verder helemaal niks.

Als je hier even over nadenkt, herken je dat attributen in het dagelijkse leven een reeds veelgebruikt autorisatiemechanisme vormen: als je boven de 65 bent, mag je bijvoorbeeld gratis met de bus; als je student bent krijg je korting bij een knipbeurt; als je arts bent mag je medicijnen voorschrijven, als je Nederlander en boven de achttien bent mag je wiet kopen; als je een geldig kaartje hebt mag je met de trein; als dit je BSN is mag je dat inzien, et cetera. Sommige attributen zijn identificerend (zoals je BSN), maar andere attributen zijn dat niet (zoals student). In termen van attributen kun je heel precies vastleggen welke informatie noodzakelijk is voor een transactie. Als je een boek bij bol.com wil kopen, zijn de volgende attributen nodig: je bankrekeningnummer voor de betaling, mogelijk je adres voor als het geen e-boek betreft en het dus opgestuurd moet worden, en mogelijk een attribuut dat een minimumleeftijd aantoont, afhankelijk van de aard van het boek. Je feitelijke naam doet er niet toe en hoeft niet vastgelegd te worden. Bij eventuele fraude kan de identiteit van de koper via het bankrekeningnummer wel achterhaald worden. Om te controleren of iemand in een medisch dossier mag schrijven is het artsattribuut nodig en het registratienummer (het zogenaamde BIG nummer), waarmee toegang gelogd kan worden. Een UZI-pas verschaft deze attributen. Voor een online locaal referendum is het attribuut nodig dat iemand inwoner is van de betreffende gemeente, maar juist niet wie hij/zij is, om anonimiteit te waarborgen. Kortom, attributen zijn een intuïtief herkenbaar mechanisme voor autorisatie. Bovendien: via attributen realiseer je data-minimalisatie in identity management.

Prachtig! Maar zijn er ook attribuutgebaseerde systemen in de digitale, online wereld? Sinds eind jaren negentig van de vorige eeuw zijn er geavanceerde cryptografische mechanismen voorhanden die dit doen. Bij IBM Research in Zürich is het

systeem *Idemix* ontwikkeld. De Nederlander Stefan Brands heeft ook een eigen systeem bedacht dat inmiddels door Microsoft overgenomen is en beschikbaar gesteld wordt onder de naam *U-Prove*. Beide systemen zijn openlijk beschikbaar en kunnen via open source software gebruikt worden. Dit is belangrijk voor breed gebruik en voor vertrouwen. In het gebruik van deze systemen onderscheidt men drie partijen.

- **Users** (gebruikers) zijn individuen op wie attributen (zoals 'boven de 18' of 'student') van toepassing kunnen zijn. Deze attributen kan de gebruiker zelf opslaan, bijvoorbeeld op een eigen smart card.
- **Issuers** zijn de uitgevers van attributen. Overheden zijn voor de hand liggende *issuers* van attributen als 'boven de 18', 'inwoner van Nijmegen', 'BSN is ...' et cetera. Maar ook banken, internet service providers, medische instanties, et cetera. kunnen attributen uitgeven. Bij zo'n uitgifte is het belangrijk eerst vast te stellen met wie men van doen heeft en of de betreffende attributen wel gelden; daarna kan de gebruiker de eigen attributen zelf opslaan en gebruiken zonder tussenkomst van de uitgever.
- **Verifiers** zijn de dienstverlenende partijen die attributen gebruiken in hun autorisatieproces. Typische *verifiers* zijn webwinkels, of website/database beheerders, winkeliers, controleurs van toegang of rollen, et cetera. Gebruikers 'tonen' hun attributen aan deze verifiers en kunnen daarmee een transactie of handeling verrichten.

Het gaat te ver om de onderliggende wiskunde en cryptografische protocollen van Idemix en U-Prove hier in detail te beschrijven. Het is wel zinvol in te gaan op de security en privacy eigenschappen die door deze attribuutgebaseerde systemen gerealiseerd worden.

- **Integrity & authenticity:** eenmaal uitgeven attributen kunnen niet veranderd worden en hun herkomst kan gecontroleerd worden. Een verifier kan dus vaststellen dat een 'boven de 18' attribuut daadwerkelijk door de overheid is uitgegeven. Technisch is dit gegarandeerd via een digitale handtekening van de issuer.
- **Non-transferrability:** attributen zijn strikt persoonlijk en kunnen niet van de ene persoon op de andere persoon overgedragen worden. Dit wordt gerealiseerd door in de attributen een speciale persoonlijke cryptografische sleutel (een *private key*) op te nemen die op een beveiligde smart card staat. Die sleutel is noodzakelijk voor het cryptografische protocol dat gebruikt wordt bij het tonen van de attributen. Om de smart card te kunnen gebruiken is een PIN vereist, die wederom persoonlijk is.
- **Confidentiality:** de inhoud van attributen is afgeschermd: voor het lezen/tonen is de betreffende geheime sleutel noodzakelijk.
- **Issuer unlinkability:** de uitgever van een attribuut kan het eenmaal uitgeven attribuut niet meer herkennen of traceren, ondanks het feit dat deze uitgever er zelf een digitale handtekening op gezet heeft. Daarmee is het bijvoorbeeld voor de overheid die mij mijn 'boven de 18' attribuut gegeven heeft niet mogelijk te volgen bij welke slijters ik dit attribuut toon, zelfs niet als al die slijters meewerken. Deze niet-traceerbaarheid wordt typisch gerealiseerd door zogenaamde blinde digitale handtekeningen.
- **Verifier unlinkabiltiy:** als ik bij twee verschillende slijters heb aangetoond dat ik boven de 18 ben, kunnen zij gezamenlijk niet vaststellen dat achter deze twee vertoningen dezelfde persoon schuilgaat. Deze eigenschap kan gerealiseerd worden via een *zero knowledge proof*.
- **Revocation:** het kunnen terugtrekken van kaarten en/of attributen. Deze herroepbaarheid is moeilijk te combineren met de voorgaande eisen. Toch is het technisch realiseerbaar, zij het op dit moment niet op een praktische en efficiënte wijze. Verbetering van zulke herroepbaarheid is een actief onderzoeksonderwerp.

Het gebruik van attributen kan men zich als volgt voorstellen. Gebruikers hebben een smart card – of een andere beveiligde drager zoals een secure USB/SD-geheugen, of een SIM-kaart – waarop ze attributen kunnen plaatsen, na (online) contact met een of meer issuers. Vervolgens kan een gebruiker deze attributen tonen, zowel online als offline, om transacties te kunnen verrichten. Omdat het attribuutbegrip zo open is, zijn zeer veel verschillende gebruiksscenario's denkbaar. Natuurlijk zijn er voor de hand liggende scenario's, zoals verificatie van 'boven de 16' voor het kopen van drank of sigaretten of voor toegang tot bepaalde webpagina's. Te denken valt aan uitzendinggemist.nl, voor toegang tot programma's die op televisie pas na tien uur te zien zijn. Eenzelfde privacyvriendelijke leeftijdcheck kan gebruikt worden bij het kopen van games of films met een leeftijdindicatie. Een andere mogelijke toepassing is een 'micro-EPD', waarbij essentiële medische gegevens als attributen op de smart card opgeslagen worden, voor gebruik in noodgevallen. Daarnaast zou de rol van medisch personeel vastgelegd kunnen worden als attribuut, waardoor zo'n attributenkaart ook als UZI-pas gebruikt kan worden voor toegang tot medische dossiers. Natuurlijk kun je ook andere rollen, bijvoorbeeld in een militaire of bedrijfsmatige context, vastleggen als attributen op een kaart. Je zou ook toegang tot terreinen, gebouwen of afdelingen afhankelijk kunnen maken van aanwezigheid van bepaalde attributen op een kaart. Ook kun je klantnummers en loyalty status (zoals goud/zilver/brons) als attributen op een kaart opnemen, waarbij één smart card als drager van verschillende klantenkaarten van verschillende winkels gebruikt kan worden. In de toekomst kun je mogelijk treinkaartjes, vlieg- ▸

tickets, of concertkaartjes als attributen op je kaart zetten. Door een open infrastructuur te gebruiken is zo'n attributenkaart door veel verschillende partijen te gebruiken, waardoor allerlei nieuwe vormen van interactie mogelijk worden. Op een vergelijkbare wijze heeft juist het open karakter van internet ongekende innovatie en nieuwe (commerciële) diensten mogelijk gemaakt.

Belangrijk bij al deze toepassingen is dat attributen een geldigheidsduur hebben en daardoor niet onbeperkt bruikbaar zijn. Je adresattribuut kan bijvoorbeeld een geldigheidsduur hebben van zeg een jaar, waardoor een verifier er op kan vertrouwen dat het getoonde adres redelijk recent is. Een gevolg van zo'n beperkte geldigheidsduur is dat attributen van tijd tot tijd ververst moeten worden. Dit betekent dat de gebruiker terug moet gaan naar de oorspronkelijke issuer. Voor gevoeligere attributen, zoals voor bedrijfstoegang, kan een kortere geldigheidsduur gekozen worden, van zeg een of drie maanden.

Gebruikers zullen hierbij te maken krijgen met een nieuwe activiteit, namelijk beheer van hun eigen attributen. Dit is enigszins te vergelijken met beheer van de applicaties (apps) op smartphones. Belangrijk voor acceptatie is dat er begrijpelijke en intuïtief heldere interfaces komen voor het beheer en gebruik van attributen.

Daarnaast is het belangrijk dat het gehele attributenstelsel transparant beheerd wordt en dat issuers en verifiers zich houden aan bepaalde regels en afspraken. Zo zullen ze voor het uitgeven en tonen van attributen allen dezelfde herkenbare interface moeten gebruiken, net zoals online betalingen via iDEAL er ook bij iedereen hetzelfde uitzien. Een belangrijk ander punt is: hoe weet ik eigenlijk zeker dat een verifier die zegt alleen het attribuut 'boven de 16' te willen controleren niet ondertussen ook alle andere beschikbare attributen uitleest? Op dit punt aangekomen spitst dit verhaal zich verder toe op een concrete realisatie, waarbinnen deze zaken meer in detail besproken kunnen worden.

IRMA: I REVEAL MY ATTRIBUTES

Binnen de *Digital Security*-afdeling van de Radboud Universiteit Nijmegen wordt sinds enige jaren onderzoek gedaan naar attribuutgebaseerde authenticatie. Daarbij zijn voor verschillende beschikbare cryptografische systemen (Idemix, U-Prove, maar ook andere) snelle implementaties op (contactloze) smart cards ontwikkeld. Omdat de onderliggende cryptografie niet-triviaal is, zijn ingewikkelde berekeningen nodig die alleen op moderne geavanceerde smart cards uitgevoerd kunnen worden. Het Idemix-systeem van IBM is het meest veelzijdig. Daarom is Idemix als cryptografische basis gekozen, in een groter project met de naam 'IRMA', als afkorting voor: *I reveal my attributes*. Binnen dit IRMA-project wordt met verschillende andere partijen samengewerkt waaronder Surfnet, TNO en SIDN. Uitgangspunt is om al het werk volgens open standaarden (zover reeds aanwezig) en met open source software uit te voeren. Dit bevordert het vertrouwen en maakt het mogelijk om IRMA-kaarten als open drager te gebruiken voor een veelheid aan toepassingen.

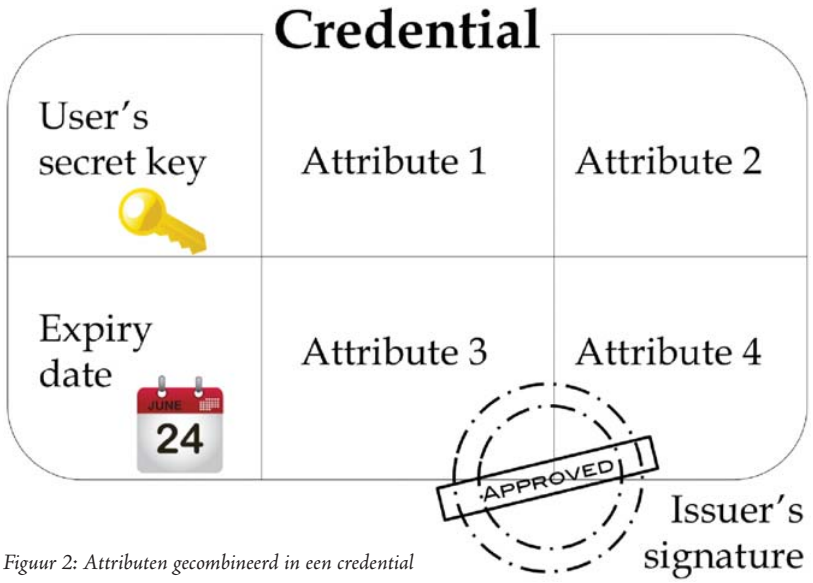
In het kader van dit IRMA-project wordt (open source) software ontwikkeld voor de verschillende aspecten van identiteitsmanagement gebaseerd op attributen: aanvraag en overhandiging van nieuwe IRMA-kaarten, uitgifte van attributen, verifiëren van attributen en het beheer van de eigen attributen op de kaart. Het laden vindt plaats via speciale webpagina's waarbij de gebruiker de attributen die hij/zij wil selecteert en de issuer vervolgens rechtstreeks (en beveiligd) communiceert met de kaart om de geselecteerde attributen te plaatsen. Het tonen van attributen kan ook via een webpagina, bijvoorbeeld om toegang tot bepaalde webpagina's te beperken tot mensen boven de 16 of onder de 12. Maar ook kunnen attributen via een speciale app op een Android tablet of telefoon met NFC smart card lezer aan een verifier getoond worden. Gebruikers hebben een eigen kaartlezer nodig, of zo'n tablet/telefoon

Figuur 1: Voorbeeld IRMA kaart

met ingebouwde lezer. Nu steeds meer van zulke draagbare apparaten een kaartlezer hebben zullen ze vermoedelijk meer gebruikt gaan worden dan losse kaartlezers. Echter, voor gevoelige toepassingen is de veiligste oplossing een aparte kaartlezer met geïntegreerd display en toetsenbord voor het invoeren van de PIN.

De IRMA-kaarten zelf zien eruit zoals aangegeven in figuur 1, met de voorkant links en de achterkant rechts. Op de voorkant staat alleen de foto van de drager van de kaart en verder niets. Dit is belangrijk voor privacybescherming. Bij het kopen van een fles whisky is je naam niet relevant: een winkelier moet kunnen zien dat de kaart bij jou hoort, en daarvoor is de foto voldoende; vervolgens moet je de winkelier tonen dat je boven de 18 bent, en dit kan plaatsvinden door de kaart op een daarvoor bestemde kaartlezer van de winkelier te leggen. Het is de bedoeling dat zo'n kaartlezer geïntegreerd kan worden met de (nieuwe) betaalterminals voor draadloos betalen.
Op de achterkant van de kaart staat praktische informatie voor het retourneren van gevonden kaarten. Daarbij is een specifiek nummer toegevoegd dat enkel gebruikt wordt om bij teruggestuurde kaarten op te zoeken wie de eigenaar is. Dit nummer is gevoelig omdat het gebruikt zou kunnen worden voor het traceren van kaarten (en dus mensen); het nummer staat dan ook enkel op de achterkant, en niet in de (chip in de) kaart.

Binnen Idemix worden attributen gecombineerd in *credentials*, die men zich voor kan stellen als in figuur 2. We zien dat zo'n credential een geheime sleutel bevat, een vervaldatum, en een aantal attributen. Het geheel is digitaal ondertekend door de issuer van het credential. Ieder van de vier attributen is afzonderlijk te tonen. Dit mechanisme van zogenoemde *selective disclosure* is erg belangrijk om het principe van data-minimalisatie te handhaven. Zo kun je op basis van een IRMA-kaart waarin onder meer je leeftijd staat, aantonen dat je 18+ bent, zonder ook je naam vrij te moeten geven. Er is gekozen voor vier attributen, om pragmatische redenen: bij een groot aantal attributen in één credential worden berekeningen trager en duren transacties dus langer terwijl bij een klein aantal attributen het lastiger is om coherente credentials te ontwerpen.
Een mogelijke invulling van een credential staat hieronder. Daarbij zijn voor het gemak de geheime sleutel en de vervaldatum weggelaten.



Figuur 2: Attributen gecombineerd in een credential

Adres
Land
Stad
Straat + Nummer
Postcode

De eerste regel beschrijft de naam van de credential en geeft een indicatie van de inhoud. De vier regels daaronder beschrijven de verschillende attributen. Zoals gezegd, deze zijn afzonderlijk toonbaar. Met deze credential kun je dus bewijzen dat je Nederlander bent of dat je in Nijmegen geregistreerd staat, zonder dat je verder ook maar iets anders over jezelf onthult. Een voor de hand liggende issuer van dit credential is je eigen gemeente, omdat die op basis van de Gemeentelijke Basis Administratie (GBA) een autoriteit is met betrekking tot adressen. Eventueel zou ook een andere organisatie met toegang tot de GBA als issuer kunnen optreden, zoals de website mijnoverheid.nl.
Andere mogelijke credentials staan hieronder.

Naam
Achternaam
Roepnaam
Volledige voornamen
Initialen

Identiteit
Burger Service Nummer
Geboortedatum
Geboorteplaats
Geslacht

Bedrijfstoegang
Hoofdingang
Parkeren
Intranet
Kluis

De eerste twee van deze credentials kunnen weer door mijnoverheid.nl uitgegeven worden. De laatste moet van het betreffende bedrijf komen, of van een derde partij die deze *issuing* namens het bedrijf (commercieel) uitvoert. De precieze inrichting van zulke credentials vergt enige zorg. Ook de onderlinge samenhang, om overlap en onduidelijkheid te voorkomen, is een onderwerp op zich.

De huidige IRMA-kaart implementatie maakt gebruikt van MULTOS-smart cards, maar kaarten van andere fabrikanten worden ook onderzocht. Op een kaart is ruimte voor tientallen credentials, hetgeen voldoende lijkt voor gewoon dagelijks gebruik. De transactietijden voor het tonen van attributen zijn in de orde van één seconde, en voor het uitgeven in de orde van drie à vier seconden. Voor het laden van credentials is altijd de PIN van de kaart nodig. Bij het tonen van attributen kan er voor gekozen worden of de PIN noodzakelijk is of niet. Voor toegang tot de bedrijfsparkeerplaats is dat mogelijk niet handig en/of nodig, maar voor 'boven de 18' waarschijnlijk wel, bijvoorbeeld om te voorkomen dat andermans kaart te gemakkelijk geleend kan worden voor ongeschikte activiteiten door kleine kinderen. Voor het eigen beheer van attributen is een speciale kaart-PIN voorzien die extra toegang geeft tot de kaart, bijvoorbeeld om de transactielogs te kunnen inzien die aangeven waar en wanneer de kaart op welke wijze gebruikt is.

Eerder is het probleem aangekaart dat verifiers mogelijk meer uit de kaart uitlezen dan de bedoeling is. Wanneer zoiets plaatsvindt is dit te zien in de transactielogs van de kaart, waarna de gebruiker mogelijk (juridisch) in actie wil komen in geval van onterecht uitlezen. Dit geeft *a posteriori* bescherming. *A priori* bescherming is ook mogelijk, op technische wijze. Men zou de kaart zo in kunnen richten dat het tonen van een of meerdere attributen alleen mogelijk is wanneer de verifier eerst een certificaat naar de kaart stuurt waarin staat dat de verifier gerechtigd is deze attributen uit te lezen. Daarvoor is een IRMA-beheerder nodig, liefst in stichtingsvorm, die verifiers zulke certificaten verleent, natuurlijk alleen voor legitieme doeleinden met proportionele toegang tot attributen. Zo heeft een webwinkel als bol.com geen recht op een certificaat waarmee het burger service nummer, of het micro-EPD, uit te lezen is.

Binnen het IRMA-project is een pilot voorzien met ongeveer honderd studenten van de Kerckhoffs master opleiding in computer security uit Eindhoven, Twente en Nijmegen. Zij krijgen de beschikking over een eigen IRMA-kaart en kunnen die gebruiken voor een aantal toepassingen: korting op koffie, toegang tot speciale webpagina's, gratis printen, et cetera. Deze studenten zullen hopelijk zelf ook nieuwe toepassingen bedenken; tevens vormen ze een kritische testgroep die op zoek zal gaan naar mogelijke beveiligingszwakheden in het systeem. Bij deze pilot zal de zojuist genoemde terminal-authenticatie nog niet geïmplementeerd worden.

In figuur 3 staan drie schermen die een terminal weergeeft wanneer een klant bij een bepaalde kapper (zie het logo rechtsonder) moet aantonen dat hij of zij een student is, om in

Figuur 3: Interactieschermen bij het tonen van het 'student' 'attribuut'

aanmerking te komen voor een korting. De kapper moet hierbij nog wel zelf de foto op de kaart controleren. Het linker scherm geeft de rusttoestand aan, waarbij de terminal wacht op een kaart om daarop een eventueel student attribuut te controleren. Het middelste scherm is gedurende een seconde zichtbaar, wanneer de verificatie plaatsvindt, nadat een IRMA-kaart bij de kaartlezer gehouden wordt. Het rechter plaatje verschijnt wanneer er inderdaad een student attribuut aanwezig is.

Buiten de academische context is groeiende belangstelling waarneembaar voor attribuutgebaseerde authenticatie in het algemeen en voor het IRMA-project in het bijzonder. Dat is positief, want een uitbreiding naar een pilot met meer dan honderd deelnemers zal niet lukken zonder medewerking van externe partners. Het is ook niet de voor de hand liggende rol voor een universitaire onderzoeksgroep om grotere pilots te organiseren. Het beheer van het IRMA-systeem wordt dan bij voorkeur overgedragen aan een onafhankelijke stichting, bijvoorbeeld vergelijkbaar met hoe de stichting SIDN domeinnamen beheert. Juist zo'n onafhankelijk rol is belangrijk om van een open infrastructuur een maatschappelijk succes te maken.
In de huidige tijd met alomtegenwoordige smartphones komt de vraag als vanzelf op: kan ik mijn attributen niet gewoon op mijn telefoon zetten, in plaats van op een aparte smart card? Technisch is dat zeker mogelijk, maar er is een aantal redenen waarom dat niet zo'n goed idee is. Ten eerste is het cruciaal voor de beveiliging en privacy dat de geheime sleutel in credentials echt geheim blijft. Smart phones zijn niet ontworpen om zulke geheime sleutels op een extern ontoegankelijk, beveiligde wijze op te slaan. Sterker nog, smartphones beginnen net zulke onbetrouwbare platformen te worden als gewone PC's, waarop allerlei oncontroleerbare software draait die de geheime sleutel mogelijk compromitteert. Daarnaast is er nog een aantal praktische redenen waarom telefoons niet de ideale drager van persoonlijke attributen zijn: telefoons raken regelmatig kwijt en worden ook snel vervangen, waardoor vernieuwing van geheime sleutels en van attributen noodzakelijk is. Ook hebben veel mensen een telefoon van de zaak, mogelijk met beperkingen op het gebruik. Het is niet zuiver en handig om je strikt persoonlijke attributen te beheren op een apparaat dat niet van jou is en dat je mogelijk plotseling in moet leveren (bijvoorbeeld bij ontslag). Ten slotte is er nog een psychologische reden waarom voor smart cards gekozen is. Bij een nieuwe technologie als deze attribuutgebaseerde authenticatie is een zekere gewenning noodzakelijk, waarbij de juiste associaties belangrijk zijn. Attributen zijn gevoelige persoonlijke zaken, die toegang geven tot mogelijk nog veel gevoeliger gegevens. Het is dus belangrijk dat mensen bij het gebruik van die attributen op een intuïtief niveau in een hoge staat van alertheid komen, enigszins vergelijkbaar met het beheer van je eigen sleutelbos of bankpas. Het is daarom juist goed dat het een klein beetje moeite kost om een attribuut-authenticatie te verrichten: je moet eerst een fysieke handeling verrichten, namelijk je IRMA kaart uit je portemonnee te voorschijn halen, waardoor je je realiseert dat je iets belangrijks gaat doen; pas door die kaart bij een kaartlezer of bij je smartphone (met kaartlezer) te houden kun je een belangrijke eigenschap van jezelf tonen.
IT-auditors hebben een nadrukkelijke taak om te controleren of transacties door de juiste daartoe bevoegde partijen verricht zijn. Maar in het huidige tijdsgewricht met een overdaad aan informatie en persoonsgegevens mag ook van IT-auditors verwacht worden dat ze er op toezien dat niet meer dan de noodzakelijke gegevens vastgelegd worden. Het is precies deze proportionaliteit waar attribuutgebaseerde authenticatie op gericht is.
Aanvullende, actuele informatie over het IRMA-project is te vinden op de website irmacard.org. ■

Prof. dr. B. (Bart) Jacobs is hoogleraar computerbeveiliging aan de Radboud Universiteit Nijmegen. Met zijn onderzoeksgroep heeft hij de afgelopen jaren aan een aantal maatschappelijk relevante onderwerpen gewerkt rond onder andere chipkaarten, kilometerheffing en EPD. In 2007 is hij lid geworden van de commissie Korthals Altes die over de herinrichting van het Nederlandse stemproces moest adviseren.In 2008 kreeg zijn onderzoeksgroep wereldwijde aandacht voor de aangetoonde zwakheden in de chipkaart. Momenteel is hij lid van de Nationale Cyber Security Raad. Verdere informatie, onder andere over wetenschappelijke activiteiten zijn te vinden op het webadres van Jacobs: www.cs.ru.nl/B.Jacobs