

User Centric Identity Management

André Koot >André Koot is security manager bij Univé Verzekeringen en redacteur van dit blad, e-mail: A.koot@unive.nl

Binnen iedere organisatie die IAM in enige vorm inricht, is de eigenaar van de infrastructuur de baas van de digitale identiteiten. Niet geheel onlogisch: als jij in mijn SAP-systeem wilt komen, zal ik jou daarvoor onder mijn condities de mogelijkheid bieden. Dat levert natuurlijk meteen alle complicaties op waarvoor we nu met IAM oplossingen een uitweg proberen te vinden, denk hierbij aan de volgende knelpunten:

- iedereen heeft een groot aantal (verschillende) digitale identiteiten;
- verschillende wachtwoord conventies;
- te veel rechten door inflatie (blijven bestaan uit vorige functies) van autorisaties;
- zero-day employment-achtige zaken (direct de beschikking krijgen van de benodigde autorisaties).

En bovendien: hoeveel identiteiten willen wij nou eigenlijk beheren?

Dit probleem speelt natuurlijk al heel lang binnen organisaties, maar het probleem wordt groter naarmate we ook het internet als werkomgeving gaan gebruiken. Hoe waarborg je daar de digitale identiteit van gebruikers? Voor de systeemeigenaren valt het op zich wel mee. Je laat iedereen zich online aanmelden en je creëert ter plekke een nieuwe digitale identiteit voor het betreffende systeem. Het grootste probleem daarbij is dat je natuurlijk niet weet wie zich aanmeldt, maar ach, dat los je binnen de gemeenschap maar op door beperkte functionaliteit te leveren, een blog bijvoorbeeld. Maar voor de gebruikers wordt het snel onbeheersbaar. Elke verkregen digitale identiteit moet weer beheerd worden en dat houdt gewoon een keer op.

Er zijn organisaties die als intermediairs kunnen fungeren. Je meldt je één keer aan en vervolgens kun je die identiteit gebruiken om elders aan de slag te

'Identity and access management' (IAM) staat volop in de belangstelling. Enerzijds vanuit de toenemende compliance problematiek en anderzijds vanwege de toenemende technologische mogelijkheden om IAM op een effectieve en efficiënte manier in te richten. Steeds meer IAM suites maken het mogelijk om aan de eisen vanuit compliance te voldoen. Maar er is in het afgelopen jaar een nieuwe trend ontstaan. De trend van User Centric Identity Management. User Centric Identity Management betekent dat een gebruiker de baas wordt van zijn eigen digitale identiteit. En dat is een fundamenteel andere denkwijze dan we tot nog toe gewend zijn.

gaan. Een bekend voorbeeld is Microsoft Passport (nu Microsoft Live ID). Je genereert daar een identiteit en vervolgens kun je op alle Passport compliant websites zonder verdere identificatie aan de slag. Ideaal als je veel op het internet rondhangt. Toch blijkt dat niet zo'n succes. Technisch werkt het perfect. Passport verzorgt zo'n één miljard authenticaties per dag! Maar het probleem is dat er buiten de MSN wereld onvoldoende steun is voor een dergelijk identificatiesysteem. Hoe kan dat? Vertrouwt men Microsoft niet? Of wil iedereen het gewoon zelf doen omdat beveiliging een kernproces is?

Deze vraag werd ook gesteld binnen een groep denkers op het internet. Aanvoerder van die groep is Kim Cameron. Hij werkt sedert de overname van zijn eigen bedrijf Zoom-It voor Microsoft (Zoom-It was bekend doordat het bedrijf op basis van ActiveDirectory een identity management oplossing had ontwikkeld). Cameron geldt inmiddels als de goeroe op het gebied van Identity Management. Het eerste belangrijke product van zijn denkwerk werd The Laws of Identity. In dit werkstuk beschrijft Cameron de werkzame principes achter een succesvol identity management systeem. En als je die zeven wetten bekijkt, zie je ook waarom Passport niet kan dienen als een generiek identity management systeem.

Het tweede resultaat van het denkwerk van Cameron werd het Identity Metasystem framework, waar ik later op terugkom. Op basis van dit frame-

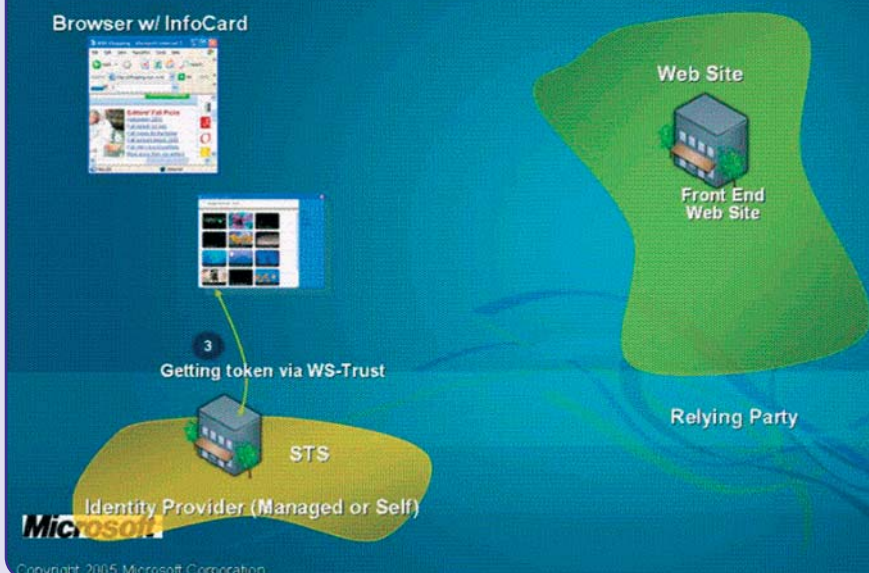
work ontwikkelde Microsoft het CardSpace systeem (voorheen Infocard), heeft de Open Source gemeenschap Higgins ontsloten, bouwde Sun Web SSO en zijn er vele andere initiatieven gestart om aan te sluiten. Als je het ons vraagt, is dit de ontwikkeling waar we de komende tijd veel werk in kunnen steken.

Er is al enorm veel informatie op het internet beschikbaar (onderaan dit artikel staan een paar links), maar laten we toch in het kort een introductie geven. Daarbij moeten we eerst een paar kernobjecten definiëren die we in het vervolg gaan tegenkomen:

- de Relying Party
- de Identity Provider
- een Subject

Een relying party is een doelsysteem waar een individu (het subject) gebruik van wil maken. De relying party kan een website zijn, een blog of een commerciële applicatieserver. Iemand zal zich aanmelden met een identiteit die hij aan de relying party wil mededelen. Deze mededeling is in veel gevallen niet voldoende. Voor verschillende systemen zal bij de relying party de behoefte bestaan om de betrouwbaarheid van de opgegeven identiteit te controleren. Daarvoor wordt dan gebruikgemaakt van een Identity Provider. De identity provider is dan ook de partij waar de relying party op vertrouwt als het aankomt op het toelaten van een aangemelde identiteit. Er bestaan verschillende soorten identity providers. Een individu kan zelf een identity provider zijn (net als nu feitelijk op het internet ook al kan

InfoCard Protocol Flow



De Laws of Identity

1. User Control and Consent

De gebruiker heeft de volledige controle over welke identificatiegegevens in het identificatieproces worden gecommuniceerd. Dat wil zeggen dat er ook niet onder water identificatiegegevens mogen worden verstrekt.

2. Minimal Disclosure for a Constrained Use

Uitsluitend de minimaal noodzakelijke identificatiegegevens worden overhandigd. Dat betekent dat er niet méér wordt overhandigd dan echt noodzakelijk is. Daarmee wordt de privacy van de gebruiker gewaarborgd. Voor de relying party is dit ook interessant: wat je niet hebt, kan niet worden gestolen. Dat betekent dat het voor aanvallers niet zinvol is om een relying party zonder veel interessante informatie aan te vallen. De privacy van de gebruikers is dan ook beter gewaarborgd.

3. Justifiable Parties

Alleen partijen die bij een transactie betrokken moeten zijn, zijn ook daadwerkelijk betrokken bij de transactie. Overbodige relaties worden niet aangegaan. Met name deze wet laat zien waardoor de Passport dienst van Microsoft is mislukt als generieke authenticatiedienst: het gaat een partij als MS niet aan dat ik een boek koop bij Amazon. Of dat ik inlog op een bepaalde weblog. MS is in die gevallen geen gerechtvaardigde partij. Toepassing van bijvoorbeeld DigiD voor niet-overheidstransacties

stuit daarmee op hetzelfde bezwaar: de overheid hoeft niet te weten dat ik een boek koop bij Amazon, of inlog op een weblog.

4. Directed Identity

Identificatiegegevens mogen alleen worden doorgegeven aan relevante partijen. De identificatiegegevens worden niet zomaar verspreid over de verschillende netwerken heen.

5. Pluralism of Operators and Technologies

Een relying party moet er rekening mee houden dat gebruikers zelf kiezen welke infrastructuur of welke applicaties ze gebruiken. Of welke identity provider ze kiezen. Evengoed kan een gebruiker niet weten welke infrastructuur een relying party gebruikt. Dat betekent dan ook dat alle componenten ongeacht de leverancier of gebruikte technologie met elkaar moeten kunnen communiceren

6. Human Integration

De mens is een onmisbare schakel in het identificatieproces. Dat betekent dat het voor de mens ook een bruikbaar proces moet zijn en dat het dus gebruikersvriendelijk en intuïtief moet zijn.

7. Consistent Experience Across Contexts

Identificatie moet voor diverse transactie/werkprocessen op eenzelfde manier plaatsvinden. Of iemand zich nu wil aanmelden bij een weblog of bij een elektronische webshop of bij een ERP-systeem, het moet op dezelfde manier werken.

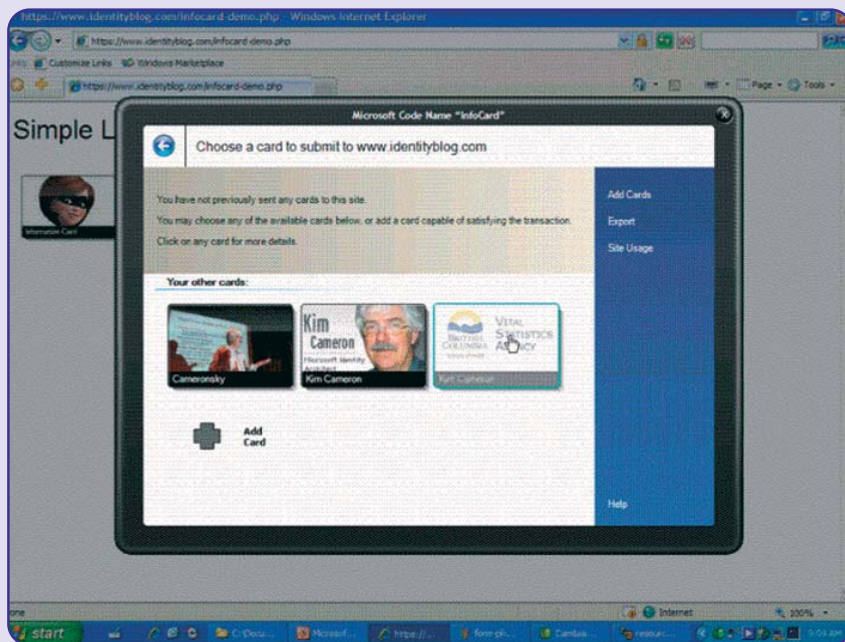
doordat je op een website zelf een account aanmaakt), maar hij kan ook een identiteit die hij van een andere provider heeft gekregen aanbieden. Dat betekent meteen dat iemand meerdere digitale identiteiten kan hebben. Voor elk gebruiksdoel kan iemand zelf kiezen welke digitale identiteit hij wil gebruiken en welke identificerende gegevens hij dus wil prijsgeven. Het is dus ook helemaal niet erg als iemand meerdere identiteiten heeft, als hij ze zelf maar beheert!

Het Identity Metasystem

Het metasysteem is een ontwerp van een globaal identificatie en authenticatie mechanisme. Het is niet een kant-en-klaar systeem, maar een set (bestaande!) protocollen en processen (Kerberos, SAML, PKI zijn allemaal in te passen) waarmee een samenhangend identificatie mechanisme kan worden ontwikkeld. Het door Cameron ontwikkelde Metasysteem voldoet aan de zeven wetten, zodat het in theorie zou moeten kunnen werken. Maar het gaat inmiddels verder dan theorie. Er zijn inmiddels werkende prototypes en ook de eerste implementaties staan voor de deur. Sterker nog, als in 2007 Windows Vista wordt uitgeleverd, komt een belangrijke component, de identiteiten selector, op een aanzienlijk aantal systemen standaard beschikbaar.

De identiteiten selector

Om dit identificatieproces te faciliteren, moet een gebruiker wel in staat zijn om op verzoek een identiteit te kunnen selecteren om die vervolgens zelf aan te bieden. Dit mechanisme is de Identity Selector. Dat is een component die min of meer vergelijkbaar is met de portefeuille waarin iemand alle bankpasjes, creditcards en lidmaatschapskaartjes bewaard. Afhankelijk van het beoogde gebruik selecteert iemand de relevante kaart om die vervolgens te kunnen presenteren als identificatiemiddel (de ID selector verzorgt geen authenticatie, dat is een separaat proces). Het Identity Selector mechanisme is feitelijk volledig conform de metafoor van de portefeuille ontwikkeld. Het oogt ook vergelijkbaar en dus in het geheel niet spectaculair. De Identity Selector is aanwezig in Windows Vista en CardSpace wordt



Dit is een voorbeeld van de Identity Selector in Windows. Het scherm toont verschillende digitale identiteiten die voor de gebruiker beschikbaar zijn. De gebruiker kan zelf kiezen welke identiteit aangeboden moet worden.

ook door .NET 3.0 ondersteund. Maar ook andere leveranciers bieden dergelijke functionaliteit, die, zoals bedoeld, ook uitwisselbaar is. Te denken valt aan OpenID en OSIS (Open Source Identity System).

Claims

Een ander belangrijk onderdeel van het metasysteem is het begrip 'Claim'. Een claim is een mededeling waarmee een subject (iemand dus, een individu) aangeeft de noodzakelijke identificatiegegevens te bezitten. Het is een bewering, geen bewijs. Het soort bewering kan wel tenderen naar een

vorm van bewijs, maar daar komen we nog op terug.

Kenmerk is dat een relying party van een individu een identiteit vraagt die voldoet aan de gevraagde claims. Voorbeeld: een webserver wenst een identiteit die is voorzien van een geldig burger servicenummer. Of een identiteit met bijvoorbeeld een CISSP certificering...

Daarbij is dan van belang dat de relying party de betrouwbaarheid van de identiteit kan vaststellen. Dat doet de relying party niet door bij een identity

provider de identiteit te controleren, want dat zou wet 3 doorbreken. Nee, de relying party vraagt welke echtheidskenmerken de identity provider heeft aangebracht die voor de digitale identiteit aanwezig moeten zijn bij een claim. Daardoor weet de identity provider niet welke identiteit een relatie heeft met de relying party, daardoor is de privacy ook niet in geding.

Wat te denken van de volgende ontwikkeling:

Zouden wij als verzekeraar niet een webservice op een assurantiëtussenpersonen applicatie aan kunnen bieden, waarbij we de claim van een diploma Assurantie B vereisen. Iedere individu die een identiteit met deze claim kan overleggen zou dan gewoon van die service gebruik mogen maken. Je kunt je wel voorstellen dat een dergelijke claim bevestigd moet worden door een betrouwbare identity provider, maar wij hoeven dan die identiteit niet te beheren.

Dat gaat natuurlijk nog wat meer betekenen. Aan de relying party kant moet nagedacht worden over de aan te bieden diensten en de daarvoor benodigde claims. Dat betekent dat inzicht moet bestaan ten aanzien van de achterliggende processen en de benodigde beveiligingseisen, AO enzo. Dat betekent ook dat we aanzienlijke inspanningen moeten verrichten op het gebied van audit trails en log-analyse en alerting en reporting. Maar daar moet je toch al veel voor doen.

Interview met Don Schmidt

Don Schmidt van Microsoft was keynote speaker op het IIR Identity 2006 congres in Lisse, dat in oktober plaatsvond. Schmidt is een vriend en collega van Kim Cameron, die zelf helaas verhinderd was te spreken. Schmidt is verantwoordelijk voor de ontwikkeling van diverse IAM producten bij Microsoft, met name Active Directory Federation Server (ADFS) en hij is de architect achter veel WS-* protocollen.

De Keynote was een prima inleiding op het Identity Metasysteem. Het fenomeen is blijkbaar nog zo nieuw dat er op het congres verder nog geen aandacht voor was, maar we mogen volgend jaar beslist meer verwachten,

zeker als Vista en .NET 3.0 gemeengoed worden.

We hebben kort met Schmidt gesproken en op enkele punten een toelichting gevraagd.

>>

Don Schmidt
(met dank aan Dré de Man)



V. Betekent het Identity Metasystem dat we eigenlijk voldoende hebben aan vertrouwen tussen de Relying Party en de Identity Provider, hoeven we het individu zelf niet meer te vertrouwen?

A. "Het aspect Trust is inderdaad vitaal, maar het vertrouwen tussen Relying Party en Identity Provider betreft alleen de managed Cards. De gebruikers zullen zelf in staat zijn om ook cards te beheren, via zelfuitgifte van kaarten."

V. Zullen er wereldwijde Identity Providers ontstaan?

A. "Nee, er zullen wel binnen contexts Identity Providers ontstaan, dat zou natuurlijk wel wereldwijde context kunnen zijn. Wat we wel voorzien zijn gedistribueerde Identity Providers."

V. Als we kijken naar ADFS, conflicteert dat niet met wet 5, pluralism of technology?

A. "Nee, want ADFS is al volledig gebouwd om te kunnen praten met

allerhande industriestandaard protocollen. Zo fungeert ADFS (ActiveDirectory Federation Server) als een identity provider. CardSpace biedt een laagdrempelige interface. ADFS en CardSpace zullen wel samen gaan komen. R2 van ADFS zal, evenals Longhorn server, WS-federation en passive clients gaan ondersteunen. De volgende release ondersteunt WS-Trust en integreert volledig met CardSpace."

V. Is Identity Metasystem te beschouwen als federation in het kwadraat?

A. "Nee, Identity Metasystem betekent wel het eind van phishing. Federation is wel min of meer de basis."

V. Hoe past CardSpace in het Identity Metasystem?

A. "CardSpace neemt het gokwerk weg ten aanzien wie geauthenticeerd wordt. De portefeuillemetafoor maakt het aan de gebruikerskant bruikbaar."

V. Gaat User Centric Identity Management de domain authenticatie vervangen, melden we ons in de toekomst ook aan met een Infocard in plaats van een authenticatieslag op ActiveDirectory?

A. "Ja, dat zal ooit gebeuren. Nu nog niet, maar het ligt in de lijn van de verwachte ontwikkelingen. Domain authenticatie zal ook gebruikt kunnen blijven voor groepen waartoe je behoort."

Tot zover deze bijdrage. Wellicht voor velen een eerste kennismaking met een nieuw fenomeen. Wij verwachten dat het hier beslist niet bij zal blijven. Als wij voorspellende gaven hebben, dan zal het Identity Metasystem binnen afzienbare tijd de basis zijn waarop het nieuwe internet verder zal groeien. Ik denk dan ook dat we dit aspect binnen het GvIB wel mee moeten nemen in een expert sessie rond identificatie, authenticatie en autorisatie.

Belangrijkste bron:

Kim Cameron's weblog: www.indentityblog.com (met de whitepapers en bijvoorbeeld ook de php implementatie van een relying party inlog).