Van Username tot Federated Identity. En wat daarna?

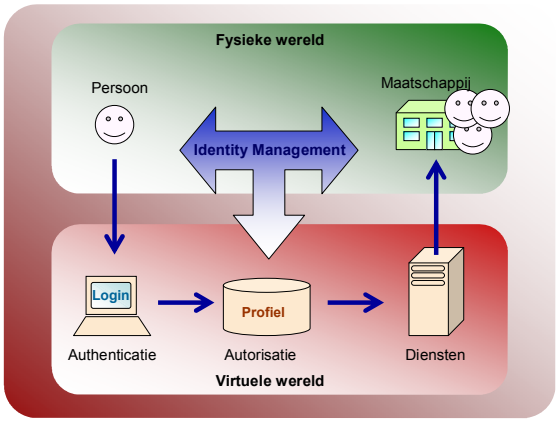
Identity Management een evolutie

We hebben allemaal wel één of meer usernames waarmee we voor onze hobby of werk inloggen op computersystemen. Hier is niets nieuws onder de zon. Bij de eerste mainframes werden al usernames toegekend en in een moderne webservice omgeving is dat nog steeds zo. Alleen onze moderne usernames hebben meer mogelijkheden gekregen en zijn geëvolueerd tot federated identities. Wat dat zijn? Aan de hand van de evolutie in Identity Management worden oude en nieuwe ontwikkelingen als SAML en federatie toegelicht en op hun waarde voor organisaties geschat.

Een evolutie stopt niet zomaar. Is er een volgende stap in de evolutie van Identity Management aan te wijzen? Uiteraard, durven we nu al te zeggen. Kijken we naar de evolutie als een ontwikkeling van virtuele personen in een geautomatiseerde virtuele wereld, dan zal de volgende stap bepaald worden doordat virtuele personen steeds meer op echte personen uit de fysieke wereld gaan lijken.

Identity Management in de virtuele wereld

Voordat we ingaan op de evolutionaire stappen van identity management is het goed om eerst stil te staan bij het fenomeen identity management en wat we daar onder verstaan.

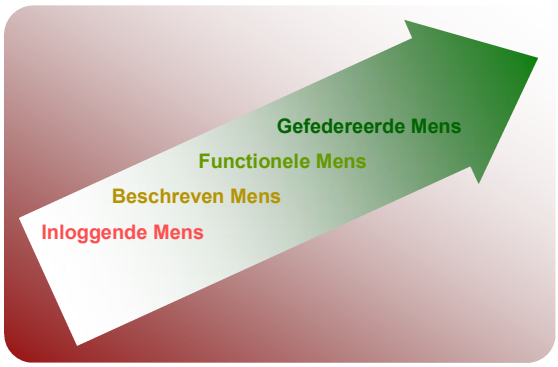


In de fysieke wereld hebben we een virtuele wereld opgebouwd die uit informatiesystemen bestaat. Om toegang tot deze virtuele wereld te krijgen, worden we eerst geauthenticeerd door in te loggen met een eigen ID of username en password. Zo'n electronische identiteit is gelinked aan een fysieke persoon waarmee hij in de virtuele wereld als dezelfde persoon herkend wordt. Vervolgens worden we geautoriseerd aan de hand van ons gebruikersprofiel en toegangsregels die in een directory zijn opgeslagen en waarmee we wel of geen toegang krijgen tot de gevraagde diensten. Diensten zijn hier heel algemeen bedoeld en kunnen variëren van een boekhoudpakket tot deelname aan internet communities.

Identity Management is het geheel van technieken en processen om gebruikers en hun toegang te managen. Rond repositories of directories met alle gebruikergevens zijn een viertal processen gepositioneerd: *Administreren* van gebruikers, *provisionen* van credentials en rechten in directories en informatiesystemen, *access control* ofwel het daadwerkelijk controleren van een actieve gebruiker en toegang verlenen en als vierde proces *monitoren* van de andere processen en opgevoerde rechten op fouten of misbruik [ref: artikel Infosecurity.nl]. Als we naar deze processen kijken dan zullen we zien dat de evolutie begint bij access control en dat stapsgewijs de andere processen en repositories ook de nodige aandacht en invulling hebben gekregen.

Evolutie in vier stappen

In vier kenmerkende stappen is het management van identiteiten geëvolueerd tot het huidige Federated Identity management. De virtuele wereld is inmiddels het technisch stadium ontgroeid naar een wereld waarin zakelijke en sociale aspecten een rol spelen.



Hierbij zien we dat virtuele identiteiten meer en meer menselijk gedrag gaan aannemen. De virtuele wereld is bezig een echte 'wereld' te worden.

De inloggende mens

Als meer mensen hetzelfde computersysteem of applicaties gebruiken worden aan gebruikers usernames toegekend om ze toegang te verlenen tot hun rechtmatige resources of gegevens. Op verzoek van een gebruiker die wil kunnen inloggen maakt een beheerder op de ICT-afdeling een username aan op het systeem. Als na verloop

van tijd een gebruiker toegang nodig heeft tot een ander systeem dan wordt de desbetreffende beheerder aangesproken.

Lees- en schrijfrechten van gebruikers en gebruikersgroepen worden rechtstreeks als file-attributen of via lokale Access Control Lists vastgelegd. Feitelijk omvat identity management nog niet veel meer dan access control in haar simpelste vorm. In het beste geval worden de uitgegeven usernames op de ICT-afdeling in een klapper bijgehouden en zijn er procedures voor de aanvraag van een username.

In deze eerste evolutie stap is er een sterke focus op toegang tot systemen en gegevens. Met het toenemend belang van deze systemen en gegevens, wordt de trend van sterkere authenticatiemechanismen gestimuleerd. Zo worden tokens, smartcards als de bankpas en biometrische authenticatie ontwikkeld. Met de introductie van digitale certificaten in een Public Key Infrastructure wordt een eerste stap gezet werd met het beschrijven van gebruikersattributen in het certificaat.

Door regelmatige reorganisaties veranderen medewerkers vaker van functie en bureau dan de telefoongids kan bijbenen. Toename van ICT middelen vergroot de complexiteit van beheer. Het is onduidelijk wie en waarom op welk systeem toegang wil hebben.

De beschreven mens
In een continu veranderende organisatie is er een sterke behoefte aan een up-to-date overzicht met alle medewerkers. Directories doen hiervoor hun intrede. Ook het almaar uitdijende ICT-park met grote aantallen PC's en printers kan keurig in zo'n directory worden bijgehouden.

De voordelen van een centrale bedrijfsbrede directory zijn evident en al snel worden directories ook gebruikt om de usernames en rechten van gebruikers in op te nemen. De access control mechanismen van systemen worden aangepast om tegen een bedrijfsbrede directory te authenticeren.

Veel gebruikte directories zijn standaard LDAP of Active Directory van Microsoft, beide gebaseerd op het Lightweight Directory Access Protocol. In deze directories worden gebruikers met gestandaardiseerde attributen beschreven zoals naam, afdeling, kamer, e-mail adres of telefoonnummer. Met deze standaardbeschrijving-en worden personen makkelijk opzoekbaar.

Ondanks centrale directories blijven er om technische en organisatorische redenen toch lokale password files, autorisatietabellen en systeem specifieke directories bestaan. De vele verschillende tabellen maken een helder inzicht in gebruikersrechten onmogelijk en provisioning van usernamens en rechten blijft een arbeidsintensief en foutgevoelig proces. Directories en tabellen raken vervuild door fouten en niet geschoonde usernames en rechten.

De functionele mens
Als grote groepen gebruikers toegangsrechten hebben tot een veelheid aan systemen en objecten wordt het managen ervan problematisch; het is niet meer inzichtelijk welke gebruiker wat mag. De oplossing wordt gevonden in Role Based Access Control. Gebruikers krijgen simpelweg een functionele rol toegewezen en daarmee zijn in principe hun rechten voor alle benodigde systemen bepaald [zie kader].

Met RBAC wordt het toekennen van gebruikersrechten transparanter en vereist minder inspanning. Als rollen goed beschreven zijn, kan de provisioning van usernames en rechten naar de achterliggende systemen worden geautomatiseerd aan de hand van logische regels.

Rollen versus usergroups
Rollen lijken enigszins op gebruikergroupen of autorisatiegroepen die al bij het beheer van gebruikers in Access Control List worden gebruikt. Toch is er een wezenlijk verschil.

Een rol is een organisatorische functie of takenpakket waarvoor toegang moet worden geregeld voor één of meer resources. Een rol wordt gekoppeld aan gebruikers en bij toegang tot een resource wordt gecontroleerd of de gebruiker een geldige rol heeft. Door het toekennen of het intrekken van een rol is met één handeling de toegang tot alle resources geregeld

Daarentegen wordt een gebruikersgroep aan een te beveiligen resource gekoppeld. Het opnemen of verwijderen van een gebruiker moet voor elke gebruikersgroep voor alle resources apart worden uitgevoerd.

Om te voldoen aan regelgeving als Sarbanes Oxley en de Wet Bescherming Persoonsgegevens moeten organisaties exact weten wie waar toegang tot heeft en worden geacht hier op toe te zien. Met RBAC was al een grote stap gezet naar de transparantie van identity management door het gebruik van betekenisvolle rollen. Voor de noodzakelijke controles achteraf wordt monitoring een integraal onderdeel van Identity Management

Met de ontwikkeling van internet stellen organisaties zich steeds opener op. Activiteiten

worden uitbesteed aan derden en er wordt meer samengewerkt met ketenpartners waardoor opportunities voor nieuwe diensten ontstaan. Webservice technologie faciliteert deze ontwikkeling naar een open wereld en wordt door organisaties omarmt. Identity management is echter nog steeds op de interne organisatie gericht. Nieuwe standaards zijn nodig zijn om organisaties in een open wereld te helpen identity management in te richten.

De gefedereerde mens

Met de komst van webservices ontstaan federatie standaards. Niet omdat webservices nieuwe authenticatie technieken vereisen, integendeel, maar wel omdat identity management zich net als het gebruik van webservices zich over organisatiegrenzen heen gaat uitstrekken.

Als organisaties elkaar voldoende vertrouwen kunnen er identiteitfederaties worden aangegaan. Gebruikers kunnen dan niet alleen terecht bij hun primaire organisatie maar krijgen ook bij de gefedereerde partijen toegang voor hun activiteiten op basis van hun primaire username. Bijvoorbeeld als een organisatie voor al zijn werknemers een gunstig pakket verzekeringen weet af te sluiten, zouden de primaire inloggevens door de verzekeraar als een accceptabel authenticatie middel beschouwd kunnen worden. Hiermee komen ook de voor de verzekering benodigde personeelsgegevens beschikbaar voor de verzekeraar.

Identity Provider, Service Provider en COT's

Binnen federatief identity management worden vaak een tweetal componenten of business rollen onderscheiden die ook door dezelfde organisatie kunnen worden ingevuld. De Identity Provider of Asserting Party verzorgt de authenticatie en vaak ook single sign-on. De Service Provider, Relying Party of ook wel de Requestor genoemd maakt gebruik van deze authenticatie en SSO-diensten.

Alvorens de Service Provider gebruik kan maken van deze dienst wordt het onderlinge vertrouwen tussen Service Providers en Identity Providers bezegeld in een zogenaamde Circle of Trust of COT.

Binnen een federatie worden gebruikersgegevens die in beheer zijn bij de afzonderlijke gefedereerde partijen gekoppeld. Meestal op initiatief van de gebruiker zelf zodat de gebruiker in control blijft en de gebruiker een maximaal vertrouwen houdt in het beheer van zijn gegevens. De uitwisseling van identiteitsgegevens over organisatorische grenzen heen is hiermee een feit en wordt aangeduid met Federated Identity Management. De afzonderlijke organisaties die hun eigen identity management hebben ingericht behouden daarin hun zelfstandigheid.

Gelijk met de ontwikkeling van standaards voor Federated Identity Management wordt het idee om identity management functies uit te besteden aan specialistische partijen in de praktijk gebracht. Deze zogenaamde Identity Providers [zie kader] verzorgen authenticatie en single sign-on en leveren zonodig real-time gebruikerskenmerken die nodig zijn voor autorisatie. Dit ontlast de uitbestedende organisatie ofwel de Service Provider van het dure beheer van authenticatie middelen. Een fraaie exponent hiervan is de ontwikkeling van een product als A-select waardoor een gebruiker kan kiezen met welk authenticatie middel hij wil inloggen [zie kader].

A-select

A-select is een open source product dat meerdere soorten authenticatiemiddelen ondersteunt. In principe kan een organisatie middels A-select ook gebruik maken van andere partijen die voor haar als authenticatieprovider willen optreden. Vooraf worden moeten hierover uiteraard wel afspraken gemaakt zijn.

Het voor iedere belastingplichtige bekende DigiD is gebaseerd op A-select. Afhankelijk van de toepassing kan een belasting-plichtige zich authenticeren met een DigiD code, een aanvullende SMS-code, een PKI-overheidscertificaat of een bankpas.

Voor het aangaan van identiteitfederaties zijn standaards als SAML, het Liberty initiatief, WS-Fed, SPML en XACML van groot belang. Dé standaard voor het uitwisselen van verzoeken en beweringen over authenticatie, attributen en autorisaties in een web- of SOAP-omgeving is SAML. De Security Assertion Markup Language is een XML-taal die alles van doen heeft met access control. SAML biedt mogelijkheden voor single sign-on in een webomgeving maar vervangt hiermee niet de traditionele authenticatie technieken. Sterker nog, SAML voert een authenticatie niet zelf uit en geeft in feite alleen het resultaat van de authenticatie als een gestandaadiseerde bewering door. De meest traditionele usernames kunnen dus ook nu nog gebruikt worden. SAML is als standaard in beheer bij OASIS.

Liberty is een initiatief van meer dan 150 bekende marktpartijen dat op initiatief van SUN is gestart als reaktie op Microsofts Passport. De kracht van Liberty in tegenstelling tot het weinig succesvolle Passport is dat Liberty uitgaat van de privacy en het in control zijn van een consument over zijn eigen gegevens op het internet. Liberty heeft daarnaast een business insteek en biedt handvatten voor het daadwerkelijk aangaan van een federatie

waarbij het onderlinge vertrouwen van twee of meer partijen moet worden vastgelegd en in systemen ingericht. Liberty maakt meer en meer gebruik van de SAML standaard.

WS-Federation of Webservice Federation focust zich meer op de technische kant van het beveiligen van samenwerkende webservices. WS-Federation biedt als initiatief van IBM en Microsoft de kans om ongeacht de eigen technologie een federatie aan te gaan met een Microsoft Active Directory omgeving waardoor single sign-on over beide werelden heen mogelijk wordt. MS-AD was voorheen een tamelijk gesloten wereld tenzij je eigen technologie ook Microsoft was. Inmiddels is WS-Federation net als SAML ook in beheer bij OASIS.

SAML, Liberty en WS-Federation hebben de focus op Access Control. Maar zoals we gezien hebben zijn er meer processen van belang voor identity management. SPML ofwel de Service Provisioning Markup Language maakt het geautomatiseerd provisionen tussen webservices mogelijk. Hierbij is provisioning niet beperkt tot identiteitsgegevens als naam, adres, username en e-mailbox; ook een mobiele telefoon of werkplek met PC kan geprovisioned worden. Voor het flexibel beschrijven, distribueren en gebruiken van toegangspolicies is XACML, Extensible Access Control Markup Language, ontwikkeld.

Het gedistribueerde karakter van webservices heeft direct gevolgen voor het autoriseren. Het gebruik van RBAC over organisatiegrenzen heen wordt lastig omdat de exacte betekenis van een gebruikersrol per organisatie kan verschillen of sterker nog, een willekeurige webservice in het geheel geen weet heeft van rollen. Toch wil een webservice zijn werk doen voor rechtmatige gebruikers. ABAC, Attribute Based Access Control biedt hiervoor de oplossing. Aan de hand van verschillende gebruikerskenmerken die zijn op te vragen bij een Identity Provider, bijvoorbeeld met SAML-berichten wordt wel of geen toegang verleend.

Met de vele samenwerkingen en federaties is de virtuele wereld afstandelijker geworden. Hoewel er steeds meer feitelijke gegevens van gebruikers zijn te achterhalen om een autorisatiebeslissing op te baseren is de afstand tussen gebruiker en dienstverleners groot. Voor handel is dat niet bezwaarlijk zolang de gebruiker betaalt en hij zijn diensten of producten geleverd krijgt. Maar voor communities is dat wat anders, daar zijn meningen van anderen en eigen ervaringen belangrijk criteria voor verdere contacten.

SAML, Liberty en WS-Federation
SAML berichten met informatie over authenticatie en attributen worden uitgewisseld tussen een Asserting party en de Relying party Aan de hand van de uitgewisselde informatie kan een autorisatiebesluit genomen worden door het Policy Descision Point dat meestal bij de Relying party zelf is ingericht. Daarna krijgt de gebruiker of subject wel of geen toegang tot de gevraagde dienst.

SAML definieert profiles, een voorgeschreven flow van het berichtenverkeer met assertions tussen de verschillende SAML componenten. Een voorbeeld van zo'n profile is het 'Webbrowser Single Sign-On' profile waarmee gebruikers eenmalig hoeven in te loggen om van verschillende sites gebruik te kunnen maken.

Liberty maakt steeds meer gebruik van de SAML standaard, maar Liberty gaat verder dan louter de uitwisseling van assertions zoals SAML doet. Beschreven zijn onder andere webservice definities voor de uitwisseling van identiteiten en op welke wijze dat kan plaatsvinden en webservice definities voor toegevoegde waarde diensten zoals een presence service (hoe ben ik bereikbaar), geo location (waar bevindt zich een identiteit) en een contact book dat ook geschikt is voor het delen van contactgegevens met anderen.

Liberty heeft een business insteek en biedt handvatten voor het daadwerkelijk aangaan van een federatie waarbij het onderlinge vertrouwen van twee of meer partijen moet worden vastgelegd en in systemen ingericht.

WS-Federation gebruikt niet alleen SAML-berichten voor het uitwisselen van security tokens maar ook WS-security profiles voor X509 certificaten en Kerberos tickets. Een specifieke rol is weggelegd voor de Security Token Service die na controle van het getoonde authenticatie token een specifiek access of toegangstoken voor de gewenste resource aan de gebruiker teruggeeft.

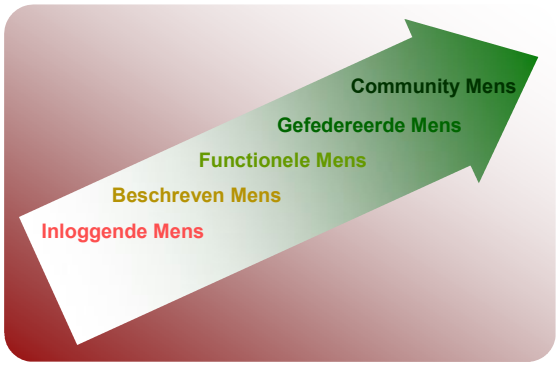
WS-Fedaration wordt gedragen door WS-security standaards als WS-Policy, WS-Trust en WS-Metadata.

En wat daarna? De community mens!
In de fysieke wereld is de beleving van 'identiteit' meer dan een verzameling eigenschappen in een directory. Voor mensen draait het om het gevoel deel uit te kunnen maken van groepen en tegelijkertijd om zich daar juist van te onderscheiden. Dat is de laatste tijd ook terug te zien in discussies over de Nederlandse identiteit en is fraai verwoord door prinses Maxima[1] bij de aanbieding van het WRR rapport 'Identificatie met Nederland'. Als de virtuele wereld zich meer en meer gaat ontwikkelen van ondersteuning van de fysieke wereld tot een zelfstandige uitbreiding op de fysieke wereld dan zal de evolutie van identity management zich moeten bewegen naar de beleving van 'identiteit'.

[1] Nederland is veel te veelzijdig om in één cliché te vatten. 'De' Nederlander bestaat niet. Als troost kan ik u zeggen dat 'de' Argentijn ook niet bestaat.'

De toekomst van identity management wordt wel voorspeld als Identity 2.0. Kern is dat de gebruiker en het beheer van zijn gegevens centraal staan en niet de dienstenleverancier die nu zijn klanten en de reeds verzamelde gebruiker-gegevens afschermt van de rest van de wereld. In het artikel "Digitale Identiteitsportefeuilles beperken verkeer gevoelige data" betoogt Rob van de Staaij dat het hiermee niet zo'n vaart zal lopen, vooral omdat niemand het voortouw voor een kostbare praktische implementatie zal nemen waarbij anderen de vruchten ervan plukken [Automatiseringsgids, 30 augustus 2007]. Of de evolutie van Identity 2.0 nu wel of niet doorzet, feit is dat de beleving van de menselijke identiteit ook hiermee nog seeds niet door identity management wordt ondersteund.

Eén kant van de beleving van identiteit is om deel uit te kunnen maken van één of meer communities waarbij de gebruiker bewust en eenvoudig zijn profiel samenstelt, toegespitst op de deelname aan een specifieke community. De andere kant van de beleving houdt in dat anderen wat van je gaan vinden, uit eigen ervaring of uit de ervaring van anderen. Kortom je bouwt een reputatie op. Een eenvoudig voorbeeld van identiteitsbeleving is het vertrouwen dat we aan een e-mail adres schenken. Na een aantal e-mailen naar een bepaald adres hebben we ervaren dat het adres daadwerkelijk aan de bedoelde persoon toebehoort en gaan we het gebruiken voor echte zaken.
Een evolutionaire stap is als ervaringen, aanbevelingen en reputaties deel gaan uitmaken van het gebruikersprofiel, zonder dat je als persoon daar direct zeggensschap over hebt. De community mens is ontstaan.



Aanbevelingen van andere gebruikers geven jouw identiteit een bepaalde vertrouwenswaarde. Hoe meer aanbevelingen hoe betrouwbaarder je bent. En dat kan binnen communities door de communitie zelf geregeld worden, zonder dat daar officiële overheidsorganen of identiteitsproviders aan te pas komen. Net zoals in de fysieke wereld bepaalt reputatie grotendeels de mogelijkheden van je zakelijke transacties, het krijgen van een lening of de mogelijkheid om door de ballotage heen te komen en dat zal in de virtule wereld niet anders zijn.

In de praktijk zien we beoordelingen en recensies al volop op het internet. Denk aan restaurantrecencies of de vermeende betrouwbaarheid van een verkoper op e-bay. De koppeling van dit soort betrouwbaarheids-kenmerken en aanbevelingen aan profielen van virtuele identiteiten voorspellen we als de volgende ontwikkeling van identity management.

Conclusie
Identity management is een continue evolutie van technieken en processen. Bestaande functionaliteit en technieken worden niet zo zeer vervangen maar uitgebreid. Er is een complexiteit ontstaan die vereist dat ICT- en businessafdelingen gezamenlijk een identity management strategie ontwikkelen.

De volgende stap in de evolutie van identity management wordt bepaald door de koppeling van ervaringen en betrouwbaarheid aan identiteiten.

Wim Geurts en Guido Bezemer zijn consultant bij Largos. Largos adviseert over informatiebeveiliging en risicobeheersing sinds 2001.

Contact: wim.geurts@largos.nl of www.largos.nl