

Business Continuity Management steeds hoger op agenda

Hoe gaan we om met ambient
intelligence en convergerende
technologie?



'Artikel van het jaar 2008' -
En de winnaar is...

The impact of Cloud
Computing on Identity

Op weg naar convergentie van
IT- en fysieke beveiliging

INFORMATIEBEVEILIGING



Publieke Identity Providers: kip en ei?

Auteur: André Koot > André is Security Manager bij Univé-VGZ-IZA-Trias en hoofdredacteur van dit blad. Hij is per e-mail bereikbaar via a.koot@unive.nl.

Wie heeft er al een digitale identiteit? Foute vraag, iedereen heeft er al minimaal een, naast diverse accounts op internet en intranet heeft iedereen immers ook een DigiD. Ik moet de vraag dan ook iets gerichter stellen: wie heeft er een herbruikbare digitale identiteit - een identiteit die aan verschillende accounts gekoppeld kan zijn? Ook dat geldt voor iedereen: DigiD is herbruikbaar. DigiD kan worden gebruikt binnen het G-C domein (government - consumer) en binnen enkele aanpalende domeinen. Zo mag (bij wijze van uitzondering) DigiD door consumenten ook worden gebruikt om in te loggen bij zorgverzekeraars.

Nu heb ik zelf een paar andere herbruikbare identiteiten. De belangrijkste is een OpenID identiteit. Die identiteit kan ik gebruiken op alle sites die OpenID toelaten. Maar dat gemak levert mij alleen maar een vervanger van een account op de betreffende website op. Mijn OpenID levert geen enkel vertrouwen op: ik heb zelf online een OpenID account aangemaakt, zonder dat iemand mijn identiteit ook maar heeft vastgesteld. Ik heb zo ook een eigen Information Card op mijn eigen pc gemaakt. Zomaar, zelf gedaan, zonder enige validatie. Erg handig, maar het kan ook alleen maar mijn gebruikersnaam en wachtwoord vervangen.

Zoals ik in het vorige nummer schreef (in het artikel over Claims Based Access Control, Informatiebeveiliging nr. 2 2009, pagina 4-8) hebben we wel grote behoefte aan een digitale identiteit om de juiste autorisaties te kunnen toekennen. We willen geen identiteiten beheren, maar wel autorisaties kunnen toekennen, zonder dus de identiteit te kennen, laat staan die te beheren.

In dat artikel schreef ik ook dat er nu wel een fors probleem bestaat. Er bestaan (buiten DigiD) op dit moment geen betrouwbare leveranciers van betrouwbare herbruikbare digitale identiteiten. Geen enkele identity provider doet iets aan verificatie van identiteiten, waardoor het digitale paspoort niet dezelfde mate van betrouwbaarheid heeft als een fysiek paspoort. Ook DigiD blijft qua verificatie eerlijk gezegd beperkt tot een check van het BSN en reikt het digitale paspoort ongezien uit. Ik ben blij dat ik het zelf uit mijn eigen brievenbus heb gehaald...

Hoe dan ook, er zijn geen betrouwbare publieke identity providers. Waarom niet? Op zich een eenvoudig antwoord: niemand heeft nog een herbruikbare digitale identiteit nodig. Want je kunt nog vrijwel nergens met een herbruikbare digitale identiteit inloggen. En dat kan niet omdat vrijwel geen enkele site nog een gebruikersgroep heeft die met een herbruikbare digitale identiteit wil inloggen. Tja, je hebt een enkele blog waar je met OpenID kunt inloggen, maar dat is toch wel iets voor 'geeks'. De LinkedIn groep van OpenID gebruikers in mijn netwerk van 4,5 miljoen personen omvat 545 leden. En de Information Card group heeft maar tien leden. Dat is niet veel. Voor die mensen ga je geen eigen inlogschermpje bouwen.

Zoals ik in het vorige nummer ook schreef is de waarde van een identiteit eigenlijk volkomen afhankelijk van de betrouwbaarheid van de identity provider. Als de Identity Provider te vertrouwen is, dan is de identiteit die door de provider wordt verstrekt ook te vertrouwen. Wat is het voordeel daarvan? Een betrouwbare identiteit maakt grote kans om hergebruikt te kunnen worden.

Wat maakt dan een digitale identiteit betrouwbaar?

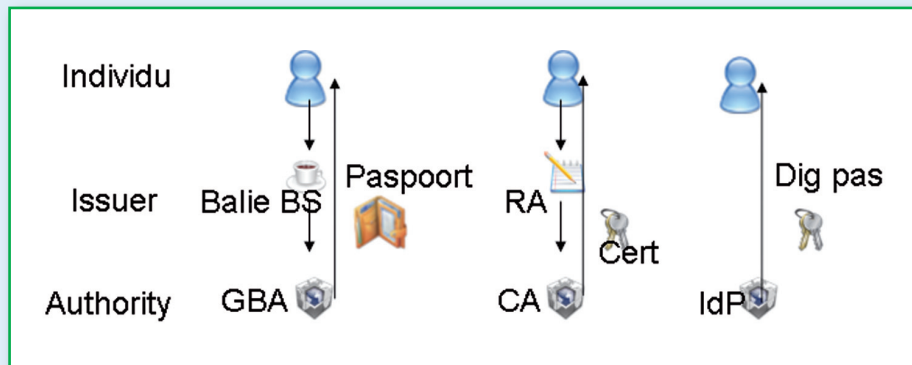
Laat ik even een vergelijking maken tussen diverse vertrouwensmechanismen. In de eerste plaats kennen we het mechanisme waarbij we een fysiek identiteitsbewijs van een hoge autoriteit (de overheid) krijgen. Een individu meldt zich bij een ambtenaar van de Burgerlijke Stand (BS) van de gemeente, die de identiteit verifieert (op

basis van een ander geldig document met een biometrisch kenmerk, de foto). De BS keurt de aanvraag goed, waarna een andere overheidsinstantie een paspoort via de BS uitreikt. Het hergebruik van het paspoort is mogelijk doordat onder meer andere overheden (in binnen- en buitenland) onze overheid vertrouwen en de echtheid van het paspoort kunnen vaststellen. Ook andere organisaties vertrouwen de overheid, zodat het paspoort ook in andere omgevingen bruikbaar is (hoewel het paspoort, als reisdocument, daar in beginsel dus niet voor is bedoeld).

Een tweede soortgelijke methode is die van de Public Key Infrastructure. Een individu meldt zich bij een Registration Authority, die na verificatie van de identiteit van het individu (aan de hand van een fysiek identiteitsbewijs) aan de Certification Authority opdracht geeft een certificaat te verstrekken. In de PKI wereld kunnen certificaten van verschillende CA's worden vertrouwd als de betreffende CA's elkaar vertrouwen (ik ben me ervan bewust dat er diverse niveaus van betrouwbaarheid van certificaten bestaan, maar laten we even de zwaarste classificatie als norm hanteren).

In de 'herbruikbare digitale paspoorten'-wereld bestaat een dergelijke werkwijze nog niet. In het beste geval (DigiD) meldt een individu zich rechtstreeks bij de Identity Provider, die zelf (na een specifieke afweging en wellicht verificatie) besluit een digitaal paspoort aan het individu te verschaffen. Voor de andere IdP's (met name OpenID) gaat het ongeveer hetzelfde, maar daarbij vindt er geen verificatie van de identiteit plaats.

Schematisch kun je dit als volgt weergeven:



Er bestaan op dit moment geen vertrouwensrelaties tussen IdP's, zoals die voor overheden en CA's ('cross certification') wel al bestaan. Hergebruik van identiteiten is dus niet per definitie mogelijk. Hergebruik is echter vooral een kwestie van vertrouwen: als een service provider een identity provider vertrouwt, dan is het al goed. Er bestaat dan ook niet direct de noodzaak van onderling vertrouwen tussen IdP's, dat scheelt wel heel veel zorgen...

Om een herbruikbare digitale identiteit te verkrijgen moeten we dus het nodige organiseren:

- Er moet een identity provider zijn die identiteiten controleert op basis van een ander identiteitsbewijs. Het zou fraai zijn als die IdP gebruik zou willen maken van 'issue-ing parties', zodat een gedistribueerd systeem ontstaat. Dat betekent automatisch dat er al meerdere partijen via dezelfde IdP identiteiten zouden kunnen verstrekken, zodat er meteen een hergebruik potentieel ontstaat. Denk aan de Pass-dienst van Diginotar.
- de 'issue-ing' en 'provisioning' processen bij de betreffende instanties moeten op een transparante en toetsbare manier worden ingericht om het vertrouwen te laten ontstaan. Die processen zouden ook daadwerkelijk getoetst moeten worden. Dat mechanisme kennen we natuurlijk al vanuit de PKI wereld. Daarbij worden op basis van een accreditatieschema audits door onafhankelijke auditors uitgevoerd. Niets nieuws onder de zon.

- Er moeten Service Providers opstaan die de door de IdP verstrekte identiteiten willen vertrouwen. Dat zal natuurlijk alleen gebeuren als het vertrouwen bestaat dat de verstrekte digitale identiteiten betrouwbaar zijn. Dus eis 2 is daartoe direct voorwaardelijk.
- Het is nodig dat aangesloten wordt bij open standaarden. Wil hergebruik mogelijk zijn, dan moeten open standaarden als SAML op grote schaal worden toegepast - op dit moment waarschijnlijk het grootste obstakel.

Maar waarom bestaat het nu nog niet? Er bestaan volgens mij verschillende redenen:

- De eerste reden is misschien wel het concurrentieaspect, het in de markt onderscheidend zijn. De meeste bestaande identity providers maken gebruik van eigen oplossingen, niet van open standaarden. Denk maar aan de banken, iedere bank heeft zijn eigen oplossing voor een digitaal paspoort. Kwestie van wantrouwen in plaats van vertrouwen: ik vertrouw alleen wat ik zelf beheer. Hergebruik is nog niet mogelijk.
- Daarnaast wordt blijkbaar de noodzaak nog niet voldoende gevoeld. Consumenten zijn gewend om op elke website met een andere account in te loggen. Dat hoort erbij. Het is wel lastig, maar we zijn het gewend. Blijkbaar zijn de ideeën van Identity 2.0 nog niet voldoende doorgedrongen, de markt (de consument) vraagt er nog niet om.
- Een andere reden zou wel eens kunnen zijn dat er nog geen evidente standaard

bestaat. OpenID is een standaard uit de open wereld, maar het is een authenticatieservice, net als DigiD. Maar hoe gaat OpenID zich ontwikkelen? Hoe zit het met privacy, hoe zit het met spoofing? Het alternatief Information Card is ook nog geen winnaar. Niemand kent Cardspace nog, dus hoe dat te gebruiken is?

- Vierde reden is een kostenafweging. Identity Management is een duur proces. Iedere organisatie weet daarvan. Als we nu opeens identity management als een nieuw identity provisioning product in de markt willen zetten, wie heeft daar dan baat bij? De consument, dat is duidelijk, de service provider profiteert echter ook, want die vervangt zijn eigen IdM proces door een (goedkoper) 'federatief proces. Wanneer er genoeg afnemers zijn om 'economies of scale' te laten gelden, is er voor de IdP ook een businesscase te maken, maar niet voor de early adopters... Vraag blijft: wie gaat dit initieel betalen? Zeker als er een heel accreditatieschema ten grondslag ligt aan de betrouwbaarheidstoets, dan moet de rekening ergens terechtkomen. De consument zal dat niet zonder meer willen betalen: liever een extra digitale identiteit, dan te betalen voor het gemak van herbruikbaarheid.

In het voorgaande ging ik impliciet uit van een digitale identiteit met een hoge kwaliteit, een identiteit die wordt verstrekt na verificatie tegen een fysiek paspoort. Nu is een identiteit met een dergelijke hoge kwaliteit natuurlijk niet altijd noodzakelijk. Een dergelijke identiteit is natuurlijk ook kostbaar. Verificatie is een duur proces. Als je dat als service provider niet nodig hebt, als je dus niet een hoger niveau van betrouwbaarheid van digitale identiteiten nodig hebt dan regulier gebruikersnaam en wachtwoord, wat let je dan om OpenID en Information Card inlogmogelijkheden beschikbaar te stellen?

De aanpassing aan je website die hiervoor nodig is, kost vrijwel niets, levert de gebruiker winst op door herbruikbaarheid van een bestaande digitale identiteit en doorbreekt daarmee de kip-ei cyclus. Lijkt mij een eenvoudige overweging.