Pieter Bos en Sven Vintges zijn werkzaam bij Atos Origin

Windows Cardspace

UNIFORME REPRESENTATIE VAN IDENTITEIT OP HET INTERNET

Windows Cardspace is één van de nieuwe onderdelen van het .NET 3.0 Framework en is Microsoft's nieuwste benadering voor het creëren van een oplossing voor het beheren van digitale identiteiten. In dit artikel gaan de auteurs in op de problemen die er zijn met het beheren van digitale identiteiten en leggen ze uit hoe dat met Windows Cardspace wordt opgelost.

Wie ben ik? Dit lijkt een heel simpele vraag, waarop echter geen simpel antwoord bestaat. De identiteit van de gebruiker is afhankelijk van de context waarin hij zich bevindt. Als iemand in de winkel staat en met een creditcard wil betalen, dan wordt aangenomen dat degene die de creditcard kan overhandigen de eigenaar is van de kaart en er ook mee mag betalen. Het maakt de winkelier niet uit wanneer de persoon geboren is, zolang er maar met een geldige creditcard betaald wordt. Staat iemand op het vliegveld bij de douane, dan wordt het paspoort overhandigd aan de douanier om daarmee de identiteit te bevestigen. De douanier zal vervolgens het paspoort op een aantal echtheidskenmerken controleren en er daarmee op vertrouwen dat de persoon is wie hij zegt dat hij is.

Wat is digitale identiteit?

Digitale identiteit is een set van claims die betrekking heeft op de gebruiker of een bepaald onderwerp. Bijvoorbeeld: "Mijn naam is Pieter Bos", "Ik woon in Nederland", "Ik werk bij Atos Origin", "Ik heb een rijbewijs". Elk van deze claims kan door de partij aan wie de claim wordt voorgelegd worden geverifieerd. Als iemand bij een autoverhuurbedrijf een auto wil huren en daar de claim neerlegt dat hij in het bezit is van een geldig rijbewijs, dan zou dit bedrijf de claim kunnen vertrouwen, het rijbewijs van de persoon kunnen controleren, of deze claim ook verifiëren bij de Rijksdienst voor het Wegverkeer. Er bestaan vele identiteiten voor verschillend gebruik, zowel in de echte wereld als online. Vaak heeft men in de echte wereld vele vormen van identiteit bij zich zoals een paspoort, rijbewijs, zorgpas, toegangspas voor het werk en bibliotheekpas. In de online wereld bestaan er ook veel verschillende vormen van identiteit en daarmee ook veel verschillende manieren om die identiteit te bevestigingen. De ene keer moet er worden ingelogd met een gebruikersnaam en wachtwoord, de andere keer is daarvoor een token nodig. Vaak hebben gebruikers voor de diverse contexten een andere combinatie van username en wachtwoord; bij de ene partij moet dit worden ingevoerd in twee velden op het scherm, bij een andere website dient dit in een andere context op te worden gegeven.

Microsoft Passport

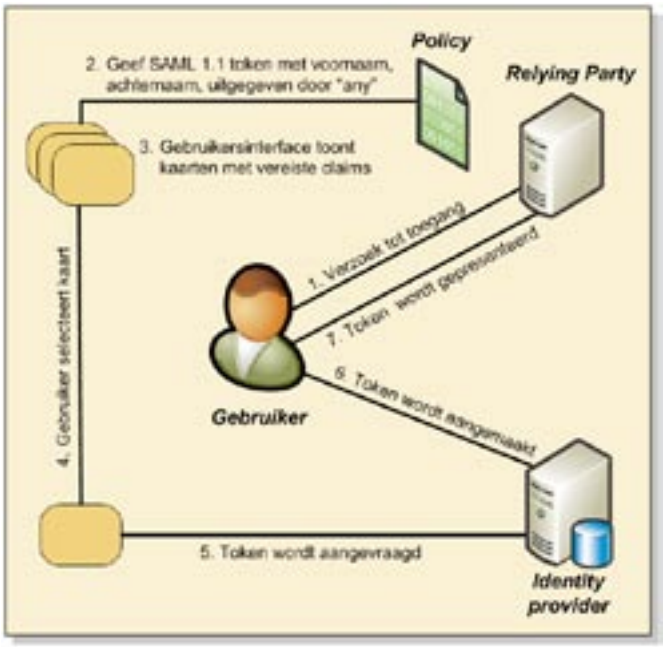
Een aantal jaren geleden is Microsoft Passport gelanceerd als een webservice voor identity management. Hoewel het Passport, tegenwoordig Windows Live ID, nog steeds gebruikt wordt voor de Microsoft-diensten als MSN, is het geen succes geworden worden voor andere internetservices. eBay heeft enige tijd gebruikgemaakt van het Microsoft Passport, maar dit later weer gestopt. De belangrijkste reden voor het niet gebruiken van het Microsoft Passport is dat zowel gebruikers als bedrijven geen gedwongen relatie met Microsoft willen hebben, en dat alle gegevens rondom hun identiteit bij Microsoft geregistreerd zijn. Dit is een van de belangrijke punten uit de Seven Laws of Identity.

Seven Laws of Identity

Kim Cameron, Identity Architect bij Microsoft, stelt op zijn blog dat er behoefte is aan een metasysteem voor online identiteit. Hij heeft zeven wetten geformuleerd, de 'Seven Laws of Identity', die de basis vormen voor een goed werkend Identity Management-systeem.

De Seven Laws of Identity zijn:

1. **User Control and Consent**
   Het systeem moet zodanig worden ontworpen dat de gebruiker de controle heeft over de digitale identiteiten die worden gebruikt, en over welke informatie wordt vrijgegeven. Indien de gebruiker beslist informatie over de identiteit te verstrekken, moet de ontvanger van deze informatie ondubbelzinnig bepaald zijn, zodat het mechanisme transparant is voor de gebruiker. Daarnaast vergt het systeem een mechanisme dat de gebruiker bewust maakt van de doeleinden ongeacht welke informatie wordt verzameld.
2. **Minimal Disclosure for a Constrained Use**
   Er wordt niet meer informatie rondom de identiteit verstrekt dan strikt noodzakelijk is. Als gevraagd wordt om een claim op een bepaalde leeftijd, dan is het beter een leeftijdscategorie door te geven dan de geboortedatum. Een systeem dat volgens de principes van informatieminimalisme is opgebouwd, wordt daardoor een minder aantrekkelijk doel voor identiteitsdiefstal.
3. **Justifiable Parties**
   Het identiteitssysteem moet zijn gebruikers bewust maken van het feit dat er identiteitsgegevens worden vrijgegeven. Elke partij die om het vrijgeven van de identiteit vraagt, moet aan de publicerende partij (de gebruiker) dan ook een verklaring over het gebruik van deze gegevens kunnen overleggen.
4. **Directed Identity**
   De gebruiker geeft zijn identiteit alleen door aan een bepaalde ontvanger. De identiteit wordt niet rondgebazuind, zoals dit bijvoorbeeld bij RFID-technologie wel het geval is.
5. **Pluralism of Operators and Technologies**
   Het system moet gebaseerd zijn op open standaarden, zodat het de gebruiker vrij staat te kiezen welke 'product identity provider' hij of zij gebruikt om de identiteit door te geven.
6. **Human Integration**
   De gebruiker maakt onderdeel uit van het metasysteem. Dat betekent ook dat de hulpmiddelen die de gebruiker ondersteunen in het identificatieproces eenvoudig te bedienen moeten zijn.
7. **Consistent Experience Across Contexts**
   Het metasysteem moet op een eenduidige manier werken en dit moet onafhankelijk zijn van de context waarin de identiteit gevraagd wordt, zoals bij het browsen of chatten.



Afbeelding 1. Inlogstappen

Open Source Identity System

Een aantal grote partijen als Microsoft, Sun, IBM en Verisign heeft samengewerkt aan het definiëren en specificeren van een identiteitsmetasysteem gebaseerd op open standaarden. Deze standaarden zijn gebaseerd op SOAP en XML en omvatten onder meer de standaarden WS-Security, WS-Trust, WS-MetadataExchange en WS-SecurityPolicy. Onderdeel van het identiteitsmetasysteem is een identiteitsselector, van welke de identiteitsselector van Windows Cardspace één van de eerste implementaties is. Bij het identiteitsmetasysteem zijn drie partijen betrokken, te weten:

1. De gebruiker. Ook wel aangeduid als 'subject'. De gebruiker is de entiteit die met een digitale identiteit wordt geassocieerd. Gebruikers zijn vaak mensen, maar ook organisaties, toepassingen, machines, en andere dingen die een digitale identiteit hebben.
2. De leverancier van de identiteit (Identity provider). De identiteitsleverancier verstrekt de identiteit aan de gebruiker. In een bedrijfsnetwerk is dit in de meeste gevallen een Active-directory. Voor een site als Amazon is dit de gebruiker zelf, aangezien de gebruiker zelf zijn login en wachtwoord bepaalt.
3. De vertrouwende partij (relying party). Een vertrouwende partij is een toepassing die zich op één of andere manier op een digitale identiteit baseert. De vertrouwende partij gebruikt de identiteit van de gebruiker om deze te authenticeren en te autoriseren. Typische voorbeelden van vertrouwende partijen op het internet zijn de online shops.

Identificatiescenario

In afbeelding 1 worden de stappen weergegeven die genomen worden alvorens een gebruiker met behulp van een identity is ingelogd.

1. De gebruiker vraagt via een Windows Cardspace compatible client (IE7) toegang tot een site van een vertrouwende partij.
2. De vertrouwende partij (Relying party) stuurt een policy (met behulp van ws-* specificaties) terug met het vereiste token-formaat (in ons voorbeeld SAML 1.1), de vereiste claims en het type.
3. Windows Cardspace toont de kaarten die aan de policy voldoen. De gebruiker kan geen kaarten selecteren die niet aan de vereiste policy voldoen.
4. De gebruiker selecteert een geschikte kaart die voldoet aan de eisen die de vertrouwende partij heeft gesteld.
5. Er wordt een token aangevraagd bij de leverancier van de identiteit.
6. De leverancier van de identiteit maakt een token aan en stuurt deze terug naar de client.
7. Na toestemming van de gebruiker wordt dit token doorgegeven aan de vertrouwende partij. De vertrouwende partij zal vervolgens de gebruiker authenticeren en toegang tot de site te geven (of niet).

De identity selector

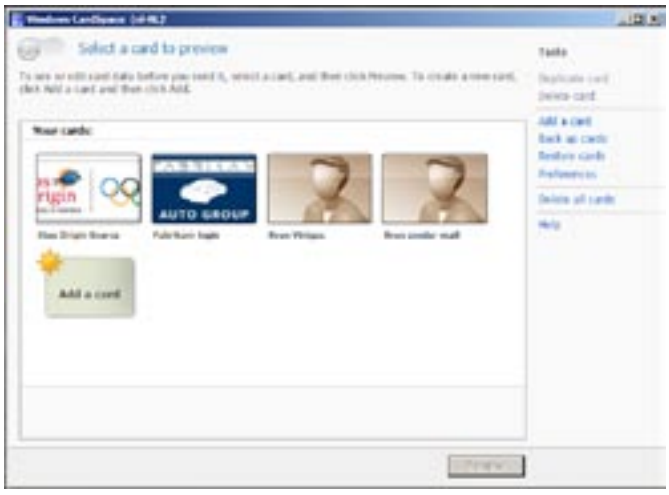
In stap 3 van het hierboven beschreven scenario komt de identity selector in beeld. De identity selector is onderdeel van Windows Cardspace en wordt geïnstalleerd met de installatie van het .NET 3.0 Framework. De identity selector wordt uitgevoerd in een geïsoleerde - en daardoor beter beveiligde - modus. Op het moment dat de identity selector wordt getoond, is de rest van het scherm uitgeschakeld. Afbeelding 2 toont de identity selector.

Er bestaan twee type identiteitskaarten, te weten: een zelf uitgegeven kaart (self issued card) en een beheerde kaart (managed card). Zelf uitgegeven kaarten zijn kaarten die in de identity selector worden aangemaakt en beheerd. De claims rondom de identiteit worden ook lokaal beheerd. Dit zijn zeer nuttige kaarten voor situaties waar een derde niet de claims hoeft te bevestigen. Als iemand bijvoorbeeld geabonneerd is op een nieuwsbrief die op basis van een gebruikersprofiel wordt samengesteld, dan volstaat het gebruik van een zelf uitgegeven kaart om toegang te krijgen tot dit profiel. Uiteraard kan een specifieke kaart voor meer websites worden gebruikt, maar is het ook mogelijk meer kaarten te maken, bijvoorbeeld een kaart met een spammailadres, of een kaart met alle persoonlijke gegevens die al dan niet wordt gebruikt, afhankelijk van het gestelde vertrouwen in de bezochte website.

Om self-issued cards te ondersteunen, heeft Microsoft Cardspace een interne security token service (STS). Deze token service zorgt er voor dat de kaarten op de juiste manier van herkenningsgegevens worden voorzien, zodat de vertrouwende partij deze op de juiste manier verifieert. Deze STS is overigens wel afhankelijk van de gebruikte machine en daardoor moeten bepaalde keys dus worden meegenomen alvorens de kaarten op een andere installatie gebruikt kunnen worden. Als een gebruiker via het web de belastingaangifte wil invullen, dan volstaat de zelf uitgegeven kaart niet. De belastingdienst wil er zeker van zijn dat de gebruiker ook is wie hij claimt te zijn. Deze zekerheid kan pas worden verkregen als een derde partij de identiteit van de gebruiker kan bevestigen. In dat geval spreken we over een beheerde kaart. De claims rondom de identiteit van de gebruiker worden bij een derde partij beheerd. De belastingdienst kan in de policy aangeven dat alleen kaarten uitgegeven door bijvoorbeeld de overheid geaccepteerd worden. Bedrijven als banken en creditcardmaatschappijen vervullen vaak de rol van vertrouwende partij en leverancier van identiteit.

Gebruik van de identity selector

De identity selector van het .NET 3.0 Framework wordt alleen ondersteund onder Internet Explorer 7. Voor Firefox is er een plugin beschikbaar die te downloaden is op de Codeplex-site. In Internet Explorer kan de Windows Cardspace-identity selector met behulp van de code uit codevoorbeeld 1 worden opgeroepen. In dit codevoorbeeld willen we één parameter uitlichten, namelijk de parameter 'requiredClaims'. Met behulp van deze parameter kan de ontwikkelaar opgeven welke claims de kaart minimaal moet doen over degene die de kaart aanbiedt. In dit geval moet de kaart in ieder geval claims bevatten over



Afbeelding 2. Windows CardSpace

de voornaam, achternaam en het e-mailadres van de gebruiker. De waarden van deze parameters zijn vastgelegd bij de W3C- organisatie, als het om managed cards gaat, kunnen hier ook eigen claims worden opgenomen. In codevoorbeeld 2 hebben we een stukje voorbeeldcode gemaakt, waarmee de claims uit een bepaald token kunnen worden opgevraagd. In codevoorbeeld 1 hebben we het token de naam 'xmlToken' gegeven, deze laden we in een Token-class. Deze class wordt meegeleverd in de sample kit van Microsoft en zorgt voor de decryptie van het token. Vervolgens kunnen we via de claimcollectie uit deze class de verschillende claims die worden gedaan uitlezen.

7 Laws of Identity versus Identity Metasystem

Eerder in het artikel zijn reeds de Seven Laws of Identity beschreven, zoals deze zijn vastgelegd door Kim Cameron. Het Identity Metasystem claimt een invulling aan deze zeven wetten te hebben gegeven. De invulling kan als volgt worden samengevat:

1. **User Control and Consent**
   Tijdens het vragen om de identiteit van de gebruiker geeft de website duidelijk aan welke claims deze graag wil hebben. De gebruiker zal nooit zomaar worden ingelogd op een website met behulp van in het verleden doorgegeven credentials. De identity selector wordt altijd aan de gebruiker gepresenteerd en toont enkel de kaarten die voldoen aan de claims die de website nodig heeft.
2. **Minimal Disclosure for a Constrained Use**
   De STS zal nooit meer informatie verstrekken dan de vertrouwende partij verwacht. Met andere woorden, de vertrouwende partij krijgt nooit meer informatie dan deze van de gebruiker heeft gevraagd. Hierdoor is het verkrijgen van data die niet bestemd zijn voor deze partij niet meer mogelijk en wordt er voor gezorgd dat slecht de strikt noodzakelijk informatie wordt verstrekt
3. **Justifiable Parties**
   Een van de zaken waardoor Microsoft Passport niet is aangeslagen, is dat mensen zich afvroegen waarom Microsoft betrokken moest zijn bij het autoriseren van de gebruiker bij een website waar Microsoft niets mee te maken heeft. Dit gaf veel gebruikers het gevoel dat Big Brother, in dit geval Microsoft, meekijkt met wat de gebruiker uitvoert.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://
www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
  <head>
    <title>.NET Magazine Codevoorbeeld 1</title>
  </head>
  <body>
    <form id="form1" method="post" action="login1.aspx">
      <button type="submit">Click here to sign in with your
       Information Card</button>
      <object type="application/x-informationcard" name="xmlToken">
        <param name="tokenType"
               value="urn:oasis:names:tc:SAML:1.0:assertion" />
        <param name="issuer"
               value="http://schemas.xmlsoap.org/ws/2005/05/identity/
               issuer/self" />
        <param name="requiredClaims"
        value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
        givenname
          http://schemas.xmlsoap.org/ws/2005/05/identity/claims/sur
        name
          http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
        emailaddress
        "/>
      </object>
    </form>
  </body>
</html>
```

Codevoorbeeld 1

```
Token token = new Token(Request.Params["xmlToken"]);
givenname.Text = token.Claims(ClaimTypes.GivenName);
surname.Text = token.Claims(ClaimTypes.Surname);
email.Text = token.Claims(ClaimTypes.Email);
```

Codevoorbeeld 2

In het identity metasystem zijn alle partijen duidelijk betrokken bij de transactie. De STS, de vertrouwende partij en het onderwerp zijn duidelijk bij de transactie betrokken en wekken dan ook geen argwaan op van de gebruiker.

4. **Directed Identity**
   Door het gebruik van STS wordt de kaart op een dusdanige manier van informatie voorzien dat de kaart alleen verstuurd kan worden door de bron van de verzending en de kaart alleen gelezen kan worden door de ontvanger van de kaart. Ook een 'man in the middle attack' is hiermee uitgesloten. Door het opnemen van zeer specifieke kenmerken van de verzender van het token, is het niet mogelijk hier een relay in te bouwen, waardoor het niet mogelijk is een verzendende partij na te bootsen
5. **Pluralism of Operators and Technologies**
   Het identity metasystem is een open systeem dat gebaseerd is op open ws-*-standaarden. Microsoft heeft een eerste aanzet gedaan door een identity selector door een STS te leveren. Het is nu aan de ontwikkelaar hiervoor alternatieven te ontwikkelen (IBM is hier reeds mee bezig) en eigen STS-en te programmeren.
6. **Human Integration**
   De gebruiker is altijd betrokken bij het selecteren van de identiteit waarmee deze inlogt bij een bepaalde vertrouwende partij.
7. **Consistent Experience Across Contexts**
   Doordat voor iedere vorm van kenbaar maken van identiteit dezelfde selector wordt gebruikt, is er een uniforme manier van autoriseren. Hierdoor is het voor gebruikers duidelijk en overzichtelijk wat er gebeurt met zijn of haar identiteit en is het autoriseren zeer expliciet.

Pieter Bos is Lead Architect en **Sven Vintges** is .NET-architect bij Atos Origin Nederland B.V. Beiden hebben jarenlange ervaring met het ontwikkelen en onderhouden van .NET-applicaties. Pieter Bos is te bereiken via Pieter.Bos@atosorigin.com en Sven Vintges is te bereiken via Sven.Vintges@atosorigin.com.

Referenties

Blog van Kim Cameron: http://www.identityblog.com
http://cardspace.netfx3.com
http://www.codeplex.com/IdentitySelector