Passport die Zweite

Authentifizierung und Autorisierung über Windows CardSpace

W3L AG
info@W3L.de

2007

Inhaltsverzeichnis

zurück

Identity-Management - Probleme

- **Jeder Internet-Dienst verlangt Authentifizierung**
  - viele Benutzername/Passwort-Kombinationen erforderlich
  - Konsequenz
    - Anwender benutzt immer die gleichen Kombinationen
    - erhöhtes Risiko
  - Das Internet ist potenziell gefährlich!
    - viele Angriffsmöglichkeiten: Phishing, Spoofing, Man-In-The-Middle-Angriffe, XSS …
- **Viele unterschiedliche Anmeldeprozesse**
- **Identitätsproblem**
  - Feststellung der Identität einer Web-Site überfordert häufig den Anwender

Identity-Management - Probleme

- **Datenschutz**
  - Benutzer hinterlässt im Netz Spuren
  - bei jedem Anbieter sind (evt. vertrauliche) Informationen hinterlegt
  - einfache Erstellung eins detaillierten Anwenderprofils
- **Zusatzinformationen**
  - Durch vertrauenswürdige Instanz gesicherte Zusatzinformationen zum Anwender aus der Sicht des Anbieters wünschenswert
    - Geschäftsfähigkeit, Liquidität, Staatsbürgerschaft etc.
- **Anbieter haben Probleme erkannt**
  - aber Standardisierung erforderlich
  - viele Initiativen, keine einheitliche Linie, schwer zu überblicken!

Überblick Identity-Management

- **Neue Ansätze unter dem Schlagwort „Identity 2.0“**
  - OpenId, Prime, CardSpace
- **Zwei Hauptthemen**
  - Federation
    - firmenübergreifende Nutzung von Identitätsinformationen
  - User Centric Identity
    - Endbenutzer erhält Kontrolle über seine Daten

Überblick Identity-Management

- **Grundszenario benötigt drei Parteien**
  - Anwender, Dienstanbieter, Identitätsprovider
- **Aus Problemen leiten sich Anforderungen ab**
  - Vereinfachung
    - einfache Registrierung und Authentifizierung durch den Benutzer
    - Reduzierung von Benutzername/Kennwort-Kombinationen
    - möglichst Single Sign On
  - Sicherheit
    - Verhinderung bekannter Angriffe
  - Verbesserung des Datenschutzes
  - Zusatzinformationen zum Anwender
    - Nutzung von durch einen Dritten gesicherten Identitätsinformationen

Überblick Identity-Management

- **Erfüllung der Anforderungen erfordert zwingend ein standardisiertes Identity Management!**
- **Nutzen wir doch einfach Microsoft Passport!**

Inhaltsverzeichnis

zurück

Was ist mit Passport ?

- **Passport hat sich (zwangsweise) als Identitäsprovider im Microsoft Umfeld durchgesetzt**
  - MSN > 300.000.000 Benutzer
  - > 1.000.000.000 Logons/Tag
- **Universeller Identitätsprovider für das Internet**
  - Fehlschlag!
  - Vertrauen
    - Warum soll Microsoft in die Kommunikation eingebunden werden, wenn ein Anwender sich bei seiner Bank authentifiziert?
- **Microsoft hat dazu gelernt!**
  - Laws of Identity
    - Aufgestellt von Kim Cameron, Microsoft Chief Identity Architect

Laws of Identity

- **Die Kontrolle liegt beim Benutzer; jede Aktion muss genehmigt werden**
- **Es werden nur unbedingt notwendige Informationen übermittelt**
- **Nur direkt beteiligte Parteien erhalten Informationen**
- **Parteien müssen sich gegenseitig ausweisen**
- **Identität ist zielgerichtet**
  - Nutzung z.B. nur für einen bestimmten Zweck
- **Pluralismus von Systembetreibern und Technik**
- **Besserer Schutz des Anwenders vor Angriffen**
- **Konsistenter Umgang mit Identitätsdaten**

Inhaltsverzeichnis

zurück

Identity-Management - Standards

- **Noch einmal: Erfüllung der Anforderungen erfordert zwingend ein standardisiertes Identity Management!**

Identity-Management - Standards

- **Im Wesentlichen zwei große Gruppen**
- **Liberty Alliance um Sun**
  - geplant als Konkurrenz zu Passport
- **Web-Service-Interoperability-Organistion (WS-I)**
    - IBM, Microsoft, …
- **Teilweise überlappende, teilweise konkurrierende Implementierungen**
  - Gemeinsamkeit
    - Standards von OASIS (**O**rganization for the **A**dvancement of **S**tructured **I**nformation **S**tandards)
    - XML-Dialekt SAML (Security Assertion Markup Language)

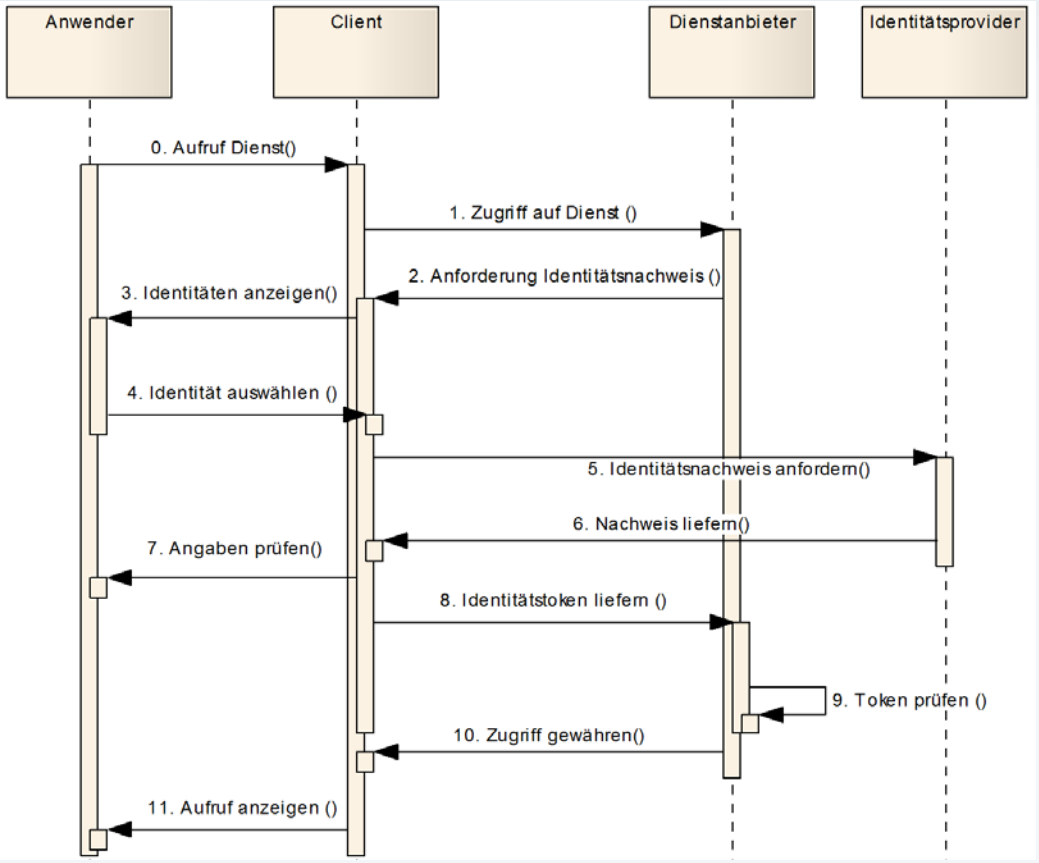
Identity-Management - Standards

- **Was ist eine digitale Identität?**
  - Subjekt
    - z.B. Person oder Sache
  - Aussagen (Claims)
    - Name, Alter, Wohnort ...
  - Nachweis (Security Token)
    - z.B. Reisepass
  - eine digitale Identität ist die Summe aller Aussagen über ein Subjekt in einem Sicherheitstoken (digitaler Container)

- **Beteiligte Parteien**
  - Anwender (Subjekt), Identitätsprovider, Dienstanbieter (Identitätsempfänger)

Identity-Management - Standards

- **SAML übernimmt u.a. den standardisierten Transport von Identitätsdaten**



Inhaltsverzeichnis

zurück

Windows Cardspace

- **Im Gegensatz zu Passport beliebige Identitätsprovider möglich**
  - Verwendung von Standards (SAML)
- **GUI zur Verwaltung von Identitäten in Form von „Infocards“**
  - es werden zwei Fälle unterschieden
    - Infocard wird vom Anwender selbst erzeugt
    - Anwender erhält die Infocard von einem Identitätsprovider (managed card)
- **Infocard**
  - Anmeldung bei Website mit Hilfe von ausgewählter Infocard
  - enthält nur Verweis auf Identitätsprovider (keine sensiblen Inform.)
  - bei einer durch den Anwender ausgestellten Infocard übernimmt der eigene PC die Rolle des Identitätsproviders

Windows Cardspace

- **Demo**
- **Was passiert hinter den Kulissen?**

Identity Selector einbinden

```
<object type="application/x-informationcard"
    name="ctl00_MainContentPlaceHolder_cardButton_token"
    id="ctl00_MainContentPlaceHolder_cardButton_token">
    <param name="tokenType" value="urn:oasis:names:tc:SAML:1.0:assertion" />

    <param name="requiredClaims"
      value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
      http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
      http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
      http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier" />

    <param name="optionalClaims"
      value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddress
      http://schemas.xmlsoap.org/ws/2005/05/identity/claims/locality
      http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince
      ...
      http://schemas.xmlsoap.org/ws/2005/05/identity/claims/webpage" />
</object>
```

Formular für Anmeldung

```
<form name="aspnetForm" method="post" action="signin.aspx?..." id="aspnetForm">
            ...

   <a onclick="javascript:ctl00_MainContentPlaceHolder_cardButton_submit();"
                        href="javascript:void(0);">
           <img src="images/informationcard.gif" alt="Sign In" style="border-width:0px;" />
   </a>
</form>
```

Identity Selector aufrufen

```
<script language='javascript'>
   function ctl00_MainContentPlaceHolder_cardButton_submit()
   {
      /*ctl00_MainContentPlaceHolder_cardButton_token = id des Identity Selectors!*/
      var token =
         document.getElementById('ctl00_MainContentPlaceHolder_cardButton_token');
      try {
         //Identity Selector wird geöffnet!
         var test = token.value;
         //Request zum Server schicken
         //der Request wird dort vom Control cardButton verarbeitet
         __doPostBack('ctl00$MainContentPlaceHolder$cardButton',test);
      } catch ( e ) {}
   }
</script>
```

Verarbeitung auf der Serverseite

```
void IPostBackEventHandler.RaisePostBackEvent(string tokenXml)
{
        if( tokenXml != null && tokenXml.Trim() != string.Empty )
        {
                Token token = new Token( tokenXml );
                string uniqueId = token.UniqueID;
                string nachname = token.Claims[SelfIssued.Surname];
                string vorname = token.Claims[SelfIssued.Nachname];
                ... //weitere Verarbeitung
        }
}
```

Literatur

- **Online**
  - Decrypting a Security Token; Microsoft; http://cardspace.netfx3.com/files/folders/pdf_documents/entry8932.aspx
  - SAML; OASIS; http://www.oasis-open.org/specs/index.php#samlv2.0
- **Identity Management**
  - Mezler-Andelberg C.: Ich und Ich; Weichenstellung für das Identity-Management; iX 10/2007; S. 124 ff.
- **Zusammenhängendes Fallbeispiel ASP.NET AJAX, WF, WCF, WPF, CardSpace**
  - www.dinnernow.net

Vielen Dank für Ihre Aufmerksamkeit!

Inhouse-Schulungen

Wir bieten Inhouse-Schulungen und Beratung durch unsere IT-Experten und –Berater.

Schulungsthemen

- Softwarearchitektur (OOD)
- Requirements Engineering (OOA)
- Nebenläufige & verteilte Programmierung

Gerne konzipieren wir auch eine individuelle Schulung zu Ihren Fragestellungen.

Sprechen Sie uns an!
Tel. 0231/61 804-0, info@W3L.de

W3L-Akademie

In Zusammenarbeit mit der Fachhochschule Dortmund bieten wir

zwei Online-Studiengänge

- B.Sc. Web- und Medieninformatik
- B.Sc. Wirtschaftsinformatik

und 7 Weiterbildungen im IT-Bereich an.

Besuchen Sie unsere Akademie!
http://Akademie.W3L.de