Information Card Interoperability

Michael B. Jones – Microsoft
October 2008
Information Card Interop Pillars

• Existing Standards
• Identity Selector Interoperability Profile
• OSIS (Open Source Identity Systems) Interops
• Concordia demo of cards with SAML 2.0 tokens
• Information Card Foundation
• Shipping Information Card Software
• New OASIS Information Card Work
Information Cards and Existing Standards

• Information Cards built using existing standards

• Relies on these WS-* standards:
  – SOAP
  – WS-Addressing
  – WS-MetadataExchange
  – WS-Policy
  – WS-Security
  – WS-SecurityPolicy
  – WS-Trust
Identity Selector Interoperability Profile

• Documents protocols and data formats used by Windows CardSpace, enabling others to build interoperable software
  – ISIP V1.0 corresponds to CardSpace .NET Framework 3.0, published May 2007
  – ISIP V1.5 corresponds to CardSpace .NET Framework 3.5 SP1, published August 2008
Microsoft Open Specification Promise (OSP)

• Perpetual legal promise that Microsoft will never bring legal action against anyone for using the protocols listed
  – Includes all the protocols underlying CardSpace

• Issued September 2006

OSIS (Open Source Identity Systems) User-Centric Identity Interops

• Opportunities for implementers to try their code against one another’s
  – I1: San Francisco Catalyst, June 2007
    • (with warm-up at IIW, May 2007)
  – I2: Barcelona Catalyst, October 2007
  – I3: San Francisco RSA, April 2008
  – I4: Anaheim DIDW, September 2008

• Tests and results all public since I2
• Not conformance testing
  – Participation in all aspects of each Interop is voluntary
• I3 & I4 added OpenID solutions as well
Barcelona OSIS Interop Oct ’07
Barcelona OSIS Interop Oct ’07

Projects

OpenID
SignOn.com
openXRI
SourceID
XMLLDAP
inames
Bandit
Shibboleth
identitycommons
LID
Higgins
sxip
OpenSSO
Yadis

/* THE Pamela PROJECT */
San Francisco OSIS Interop Apr ’08
San Francisco OSIS Interop Apr ’08

Projects

OpenID
SignOn.com
DISO
XRI
identityModel
inames
SourceID
Bandit
Shibboleth
identitycommons
XMLLDAP
/* THE Pamela PROJECT */
myOpenID
OpenSSO
myvidoop
Yadis
Higgins
Anaheim OSIS Interop Sep ’08

• Shifted focus from previous Interops
  – I1 through I3 primarily cross-solution testing
  – I4 focused on systematically testing specific features of solutions

• Test coverage
  – Tests for > 50% of key Information Card features
  – Test for < 25% of key OpenID features

• By the numbers:
  – 58 Participants
  – 89 Solutions
  – 246 Features
  – 93 Feature Tests
  – O(1000) recorded test results

• Significant interop achievements but still plenty to do!
Concordia demo of using SAML 2.0 tokens in Information Cards

- San Francisco RSA, April 2008
- Used Information Cards carrying SAML 2.0 tokens to authenticate to two federations
  - WS-Federation federation
  - SAML 2.0 federation
- 7 participating organizations
Information Card Foundation

- Industry association to promote Information Cards – formed June 2008
- Corporate board members:
  - Deutsche Telekom
  - Equifax
  - Google
  - Intel
  - Microsoft
  - Novell
  - Oracle
  - PayPal
- Sponsor members:
  - backgroundcheck.com
  - Gemalto
  - CipherTrust
  - PingIdentity
  - Privo
  - wave
- Other members include: Arcot Systems, Aristotle, A.T.E. Software, CORISECIO, Crypto-Pro, Eduserv, ETRI, Figlo, Fraunhofer Institute FOKUS, FuGen Solutions, Fun Communications, Internet 2, Liberty Alliance, ooTao, Wisekey S.A., WSO2
Information Card Foundation Initiatives

• Issuing cards with Verified Claims
  – Claims such as Age, Name, Address
• Relying Party adoption campaign
  – Particularly to accept cards with verified claims
• Best practices recommendations for RPs
• Providing input to related standards efforts
  – OASIS IMI TC
  – OASIS SAML 2.0 Information Card Profile
Shipping Information Card Software

• Shipped:
  – Windows CardSpace
  – IBM Tivoli Federated Identity Manager
  – Sun OpenSSO Enterprise 8.0
  – Bandit DigitalMe Identity Selector for Linux and Mac + IdP and RP software
  – Higgins Eclipse Rich Client Selector and Identity Framework
  – Open Source Relying Party packages:
    • Zend Framework (PHP)
    • Fraunhofer Institute FOKUS (Java)
    • ThoughtWorks (Ruby)
    • Ping Identity (C)

• In Beta:
  – Microsoft “Zermatt” Identity Framework and Visual Studio support
  – Shibboleth (Internet 2 academic federation software)

• Announced:
  – CA SiteMinder
  – Oracle Access Manager
  – Novell Identity Manager
  – Sun Access Manager
  – Siemens DirX
New OASIS Information Card Work

- Identity Metasystem Interoperability Technical Committee (IMI TC), September 2008
  - Identity Metasystem Interoperability 1.0 spec
  - Editors of the spec the presenters in this session

- Proposed SAML 2.0 token profile for Information Cards
Let’s go online now...
For More Information

• Open Source Identity Systems (OSIS)
• Information Card Foundation
• CardSpace Information
• Kim Cameron’s blog
• Mike Jones’ blog
• Or e-mail Mike at
  – mbj@microsoft.com
Backup Slides
CardSpace User Experience

Choose a card to send to: www.identityblog.com

To see or edit card data before you send it, select a card, and then click Preview. To create a new card, click Add a card and then click Add.

Cards you've sent to this site:

Minimal InfoCard

Your other cards:

Anonymous Card  Full Information Card  Kerberos AD Card  Managed InfoCard

To send this card now, click Send. To review the data before you send it, click Preview.
DigitalMe User Experience

This site requires you to send an Information Card. Select a card to send or cancel to quit.

Cards
- pamela card
  - https://cards.pamelaproject.com/TokenService/services/Trust

- HelloWorld
  - http://www.identityblog.com

- My New Card

Select all

<table>
<thead>
<tr>
<th>Send</th>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td><a href="http://k">http://k</a>...</td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td><a href="http://k">http://k</a>...</td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Private Pe...</td>
<td></td>
</tr>
</tbody>
</table>
Relying Party using an OBJECT Tag

```html
<html>
<head>
  <title>Welcome to Fabrikam</title>
</head>
<body>
  <img src='fabrikam.jpg'/>
  <form name="ctl00" id="ctl00" method="post"
    action="https://www.fabrikam.com/InfoCard-Browser/Main.aspx">
    <center>
      <img src='infocard.bmp' onClick='ctl00.submit()'/>
      <input type="submit" name="InfoCardSignin" value="Log in"
        id="InfoCardSignin" />
    </center>
    <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/emailaddress
                                      http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
                                      http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">
    </OBJECT>
  </form>
</body>
</html>
```