Food for Thought: SAML, Liberty, and Identity in a Connected World

Eve Maler
eve.maler@sun.com
http://www.xmlgrrl.com/blog

Open Source CMS Summit – Vancouver, BC – 9 February 2006

Identity is stuck – it wants to be free

Enterprise

Collaborative Industry Networks, Outsourcing, New Business Models

Developers

Java, Open Source, Standards Development

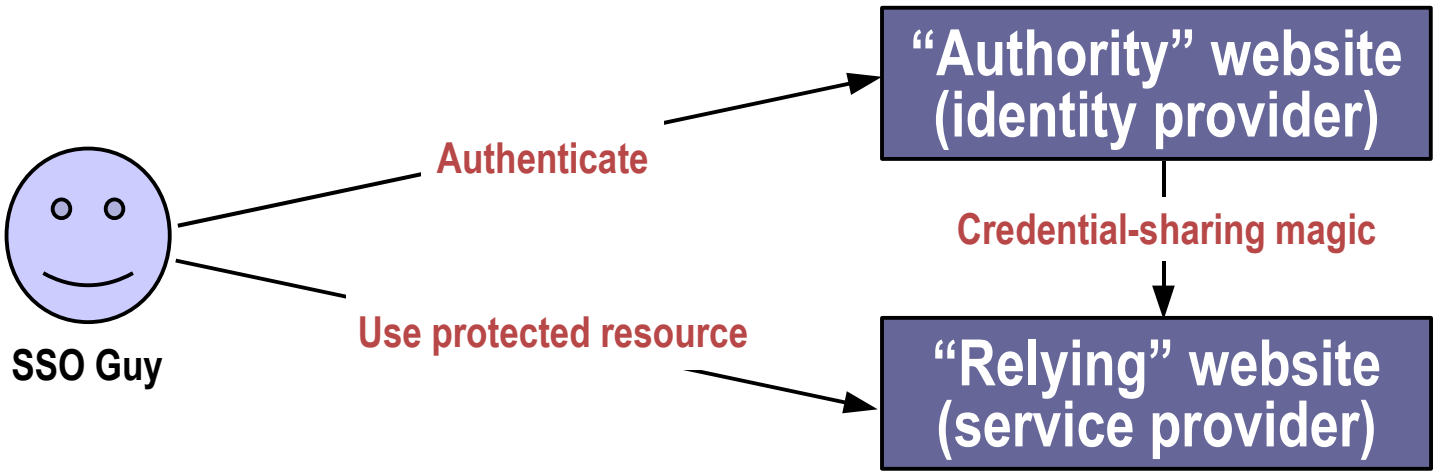
Consumers

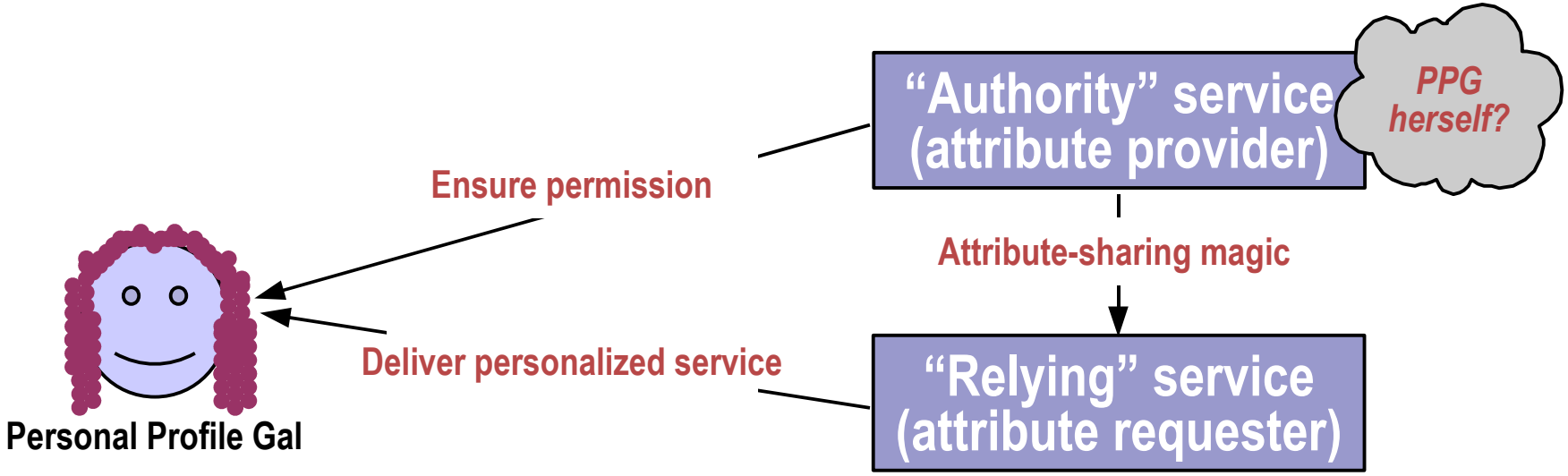
Blogs, Instant Messaging, Personalized Content on Devices, Social and Job Networking, Online Gaming

Public Sector

Inter-Agency Collaboration, Healthcare Networks, Political Campaigning, International Coalitions

Two common use cases





SAML: a universal solvent for identity information

- **Formats** for authentication, attribute, and entitlement information, plus...
- **Protocols/profiles** for various human-centred patterns of identity info sharing and syncing
  - Many inherited from Liberty's Identity Federation Framework
- Mature
- Extensible and yet interoperable
- Developed out in the open at OASIS
- Free of patent royalties
- Widely supported
  - Vendors, academia, commercial deployments, open source...

Common portions of a SAML assertion

```
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  Version="2.0"
  IssueInstant="2005-11-15T14:07:00Z">
  <saml:Issuer>
    www.pitchtree.com
  </saml:Issuer>
  <saml:Subject>
    <saml:NameID Format=
     "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
      sam.smith@pitchtree.com
    </saml:NameID>
  </saml:Subject>
  <saml:Conditions
    NotBefore="2005-11-15T14:07:00Z"
    NotOnOrAfter="2005-11-15T14:37:00Z">
  </saml:Conditions>
    ... statements go here ...
</saml:Assertion>
```

Example of an Authentication Statement

```
<saml:AuthnStatement
  AuthnInstant="2005-11-15T14:07:00Z"
  SessionIndex="0">
  <saml:AuthnContext>
    <saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI
    </saml:AuthnContextClassRef>
  </saml:AuthnContext>
</saml:AuthnStatement>
```

Example of an Attribute Statement

```
<saml:AttributeStatement>
  <saml:Attribute
    NameFormat="http://pitchtree.com">
    Name="Role"
    <saml:AttributeValue>
      Mgr
    </saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute
    NameFormat="http://pitchtree.com">
    Name="PurchaseLimit"
    <saml:AttributeValue xsi:type="pitchtree:type">
      <pitchtree:amount currency="USD">
        5000.00
      </pitchtree:amount>
    </saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

SAML profiles

- Web SSO, including authentication (and sometimes attribute) information:
  - Using standard commercial browsers
  - Using enhanced clients and proxies
- Identity federation – setting up privacy-enabled agreements among providers for referring to a subject
- Direct attribute retrieval
- Single logout – coordinated logout from multiple providers
- Your own customized profiles...

Binding SAML protocol messages to transport protocols

- **SOAP over HTTP**
- **Reverse SOAP** ("PAOS") for HTTP clients acting as SOAP responders
- **HTTP redirect**
- **HTTP POST**
- **"Artifact"** for passing a base-64 string that you can dereference with a SOAP exchange
- **URI** for basic HTTP GET retrieval
- Your own custom bindings...
  - If you hate XML Signature, a binding can use alternate means
  - If you hate SOAP, a profile can pick other bindings
  - If you hate XML, uh, um...

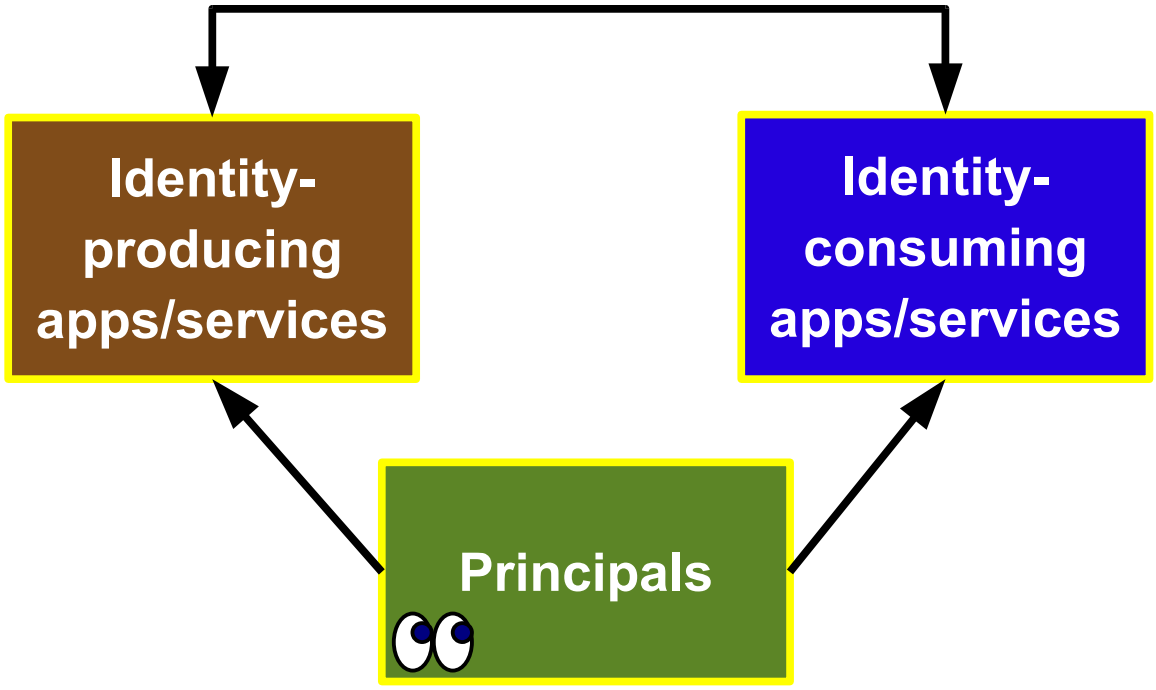
Liberty: a ubiquitous, interoperable, privacy-respecting identity layer

- Offering technology specs and guidelines, business and privacy guidelines, and interoperability assurances to help grow a trusted ecosystem
- Designed to work with all network devices
- Useful for human-facing and machine-to-machine communications
- Enables many patterns involving anonymity and user consent
- Has gone through gauntlets of regulatory and commercial requirements on privacy and security

Liberty technology scope

ID-WSF: Identity Web Services Framework
- Focused on application/application interaction

ID-SIS: Service Interface Specifications
- Focused on particular identity-based services



ID-FF: Identity Federation Framework
- Focused on human/application interaction
- Now converged with SAML V2.0

Liberty identity services for social scenarios

- The Liberty **People Service** is part of ID-WSF 2.0
  - Allows for “identity connections” among humans, with managed exceptions for privacy
  - Even if they don't share blogging tools, photo-sharing services, online calendars...
- People remain the primary actors in even “non-social” scenarios
  - Business networking, collaborative spec editing...
  - Identity sometimes wants to cross these silos

A few additional thoughts

- As a general rule, with multiple ways to do the same thing, policy/metadata retrieval can bridge the gap:
  - RDDL with namespace URL
  - YADIS with identity URL
  - SAML/Liberty metadata with published URL location
  - Web SSO Metadata Exchange Protocol with WS-MEX
- eWeek article:
  - “Security May Dog Software as a Service”
  - http://www.eweek.com/article2/0,1895,1918663,00.asp
  - Businesses have the incentive to solve this; personal use will simply decline in the “bad neighborhoods”

Some resource suggestions

- Some bloggers who are SAML and Liberty fans:
  - Paul Madsen: http://connectid.blogspot.com/
  - John Kemp: http://appliedlife.blogspot.com/
  - Pat Patterson: http://blogs.sun.com/roller/page/superpat
  - Peter Davis: http://identity4all.blogspot.com/
  - Robin Wilton: http://blogs.sun.com/racingsnake
  - Kim Cameron: http://www.identityblog.com/ :-)
- Open-source projects:
  - **OpenSAML**.org
  - **Lasso**.entrouvert.org
  - **OpenSSO**.dev.java.net
  - www.**SourceID**.org
- Java API efforts:
  - JSR 196 (authn SPI)
  - JSR 279 (mobile WS)
- Liberty People Service paper:
  - http://projectliberty.org/about/whitepapers.php

Food for Thought: SAML, Liberty, and Identity in a Connected World

Eve Maler
eve.maler@sun.com
http://www.xmlgrrl.com/blog