Trends in Harmonizing Identity Protocols: Project Concordia

Eve Maler
eve.maler@sun.com
www.xmlgrrl.com/blog
We’re on a quest together for identity portability.

identity providers

identity consumers

identity providers

identity consumers

The user is OUT

user
But the real world intrudes on this goal

• Heterogeneity in systems

• Complexity and duplication

• Interoperability vs. composability

• Adoption trends
Getting to interoperability: the truth is out there

extensions, gateways, profiles

protocol

protocol

protocol

API

API

guidelines, best practices
Introducing Project Concordia

- ProjectConcordia.org
- Public forum driving interop *among* identity protocols
- Practical focus on real-life pain points
- Priority on high-leverage solutions

Thanks to Charles Andres for the graphic concept!
Everyone is welcome at the Concordia table

- Users and deployers
  - E.g., use cases have been contributed by:

- Solution providers
  - E.g., our interop workshop at RSA ’08 saw interop demos from:

- Standards and open-source communities
  - E.g.: InfoCard, Liberty, OAuth, OpenID, OSIS, PKI, SAML, Shibboleth, WS-Fed, WS-Trust
Scenario development timeline

- **Aug 07**: developed initial “buckets”
- **Sep 07**: prioritized initial issues list
- **Nov 07**: analyzed our A-priority issues
- **Dec 07**: selected two major scenarios
- **Jan-Apr 08**: defined, tested, documented
- **Aug 08**: facilitated spec creation
- **Now**: lather, rinse, repeat
# Use-case areas explored to date

<table>
<thead>
<tr>
<th>Protocol Function</th>
<th>OpenID</th>
<th>SAML</th>
<th>InfoCard</th>
<th>WS-Fed</th>
<th>ID-WSF</th>
<th>OAuth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Single sign-on</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Front-channel attributes</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Back-channel attributes</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Single logout</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

- **InfoCard login to SAML2 or WS-Fed**
- **SAML2/WS-Fed chaining**
- **SAML2/OpenID chaining**
- **Bootstrapping: SAML2 to OAuth, InfoCard to ID-WSF**
- **Whitepaper ideas: IdP discovery, attrib mapping, SLO**
- **Workshop: entitlements management**

Thanks to Paul Madsen, Mary Ruddy, and Patrick Harding for the matrix concept!
The (somewhat) larger context

<table>
<thead>
<tr>
<th>Protocol Function</th>
<th>OpenID</th>
<th>SAML</th>
<th>InfoCard</th>
<th>WS-Fed</th>
<th>ID-WSF</th>
<th>OAuth</th>
<th>XRDS</th>
<th>WS-*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Single sign-on</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Front-channel attributes</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Back-channel attributes</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Single logout</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Discovery/metadata</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Service plumbing</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

Liberty TEG: SAML bootstrap to ID-WSF
OpenID and OAuth: XRDS for discovery
Liberty SIG-WSH: web services harmonization
OASIS WS-Fed: leverage SAML metadata
Burton ISWG: identity services
IDtbd?
Tested scenario: InfoCard login to SAML2 or WS-Federation

- **What happens:** User logs in with a card of the requested type while taking part in federated interaction
- **Challenge:** Persist the RP's authentication policy and the actual method used across the protocols
- **What's new:** SAML2 token support in WS-Federation implementations; draft SAML2 InfoCard token profile
- **Issues to solve:** Generic claim structure vs. SAML's authn context structure; well-known identity selector limitation on policy (claim types)
Tested scenario: SAML2/WS-Federation chaining

• **What happens:** User can SSO into a SAML2 federation and proceed to a WS-Fed one, or vice versa

• **Challenge:** IdPs and RPs each acting as protocol bridges

• **What's new:** SAML2 token support in WS-Federation implementations

• **Issues to solve:** Translation between SAML authentication context and WS-Fed `wauth` parameter
SAML2/OpenID chaining

• Use cases submitted in response to call for **level-of-assurance** issues:
  > Outsource authentication from high-assurance SAML IdP to OpenID OP
  > Issue employee OpenIDs with SAML-based strong authentication for high-assurance ‘Net transactions

• Common threads in all InfoCard and chaining scenarios:
  > Accurately “proxying” authentication context
  > Avoiding assurance degradation from protocol-mixing
  > Representing levels consistently in SAML assertions
Heterogeneous bootstrapping

• **Bootstrapping** teaches an RP how to become a **web service client** for a user’s identity data
  > Based on initial transfer of bootstrap data in a login session

• Bootstrapping to **ID-WSF** involves an endpoint reference to a discovery service
  > ...which an **information card** can provide, with profiling

• Bootstrapping to **OAuth** involves a long-lived access token
  > ...which the **SAML** authentication request protocol carrying **OAuth** request tokens can provide, with profiling
We invite you to get involved

• Why?
  > Many other venues focus on prospective development of specs and APIs
  > Concordia is responding to deployers' needs and concerns about heterogeneous environments today

• How?
  > Visit ProjectConcordia.org
  > Provide input today – I’m all ears!
  > Mailing list, wiki, workshops, telecons, interops
  > Planning has just begun for an interop workshop at RSA ‘09
Thanks for your kind attention!

Questions? Comments?

Eve Maler
eve.maler@sun.com
Slides: www.xmlgrl.com/blog/publications