Project Concordia Update
2nd European Identity Conference
April 22, 2008

Presented by George Fletcher (AOL)
Slides re-used with permission by Eve Maler (SUN)

Agenda

- What is Concordia?
- Current Use-Cases
- RSA Interop Report
- Next steps
- Resources

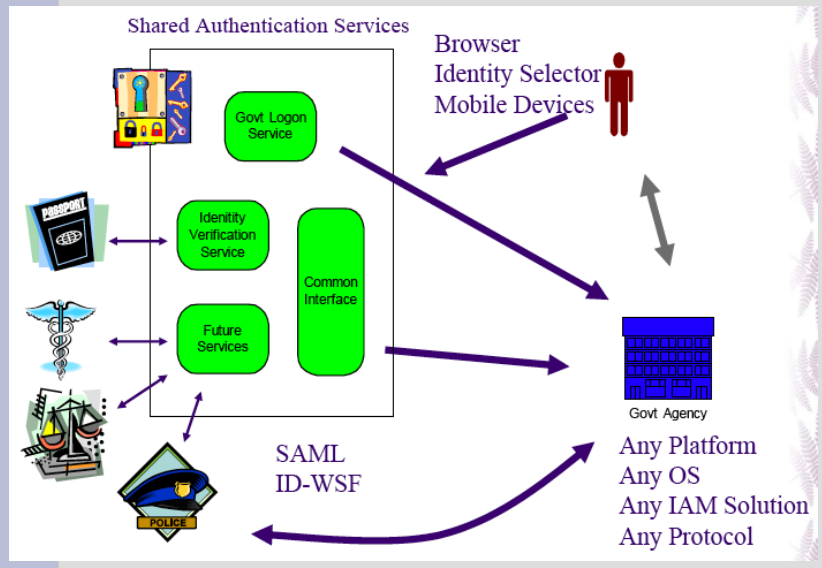
What is Concordia?

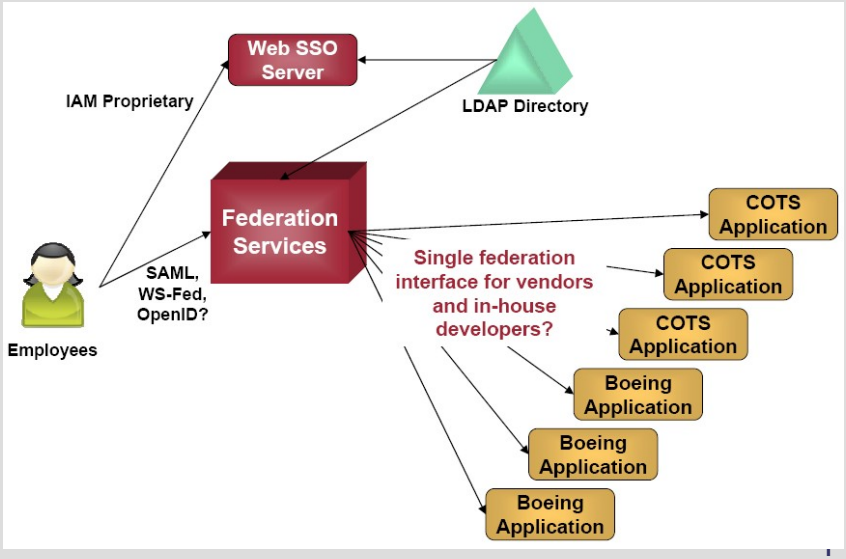
- "Agreement, understanding, and marital harmony"...
- Public forum driving interop *among* identity protocols
  - Used together in practice
  - But not originally designed to fit together
- Practical focus on real-life issues
  - Gathering deployer input is an explicit goal

- No technology is off-limits
  - Discussed so far: PKI, SAML, WS-Fed, OpenID, InfoCard...
- Scenarios are explored, tested, and clarified in turn
  - If further spec work is needed, we will champion its standardization

Who's doing this and how?

- Participants include solution providers and deployers
  - Wiki, mailing list, and workshops – join us! it's easy
  - **projectconcordia.org**
  - **lists.projectconcordia.org/mailman/listinfo/community**
- Formal use-case contributors so far:
  - AOL, Boeing, Chevron, GM, Government of B.C., InCommon Federation, N.Z. State Services Commission, U.S. GSA



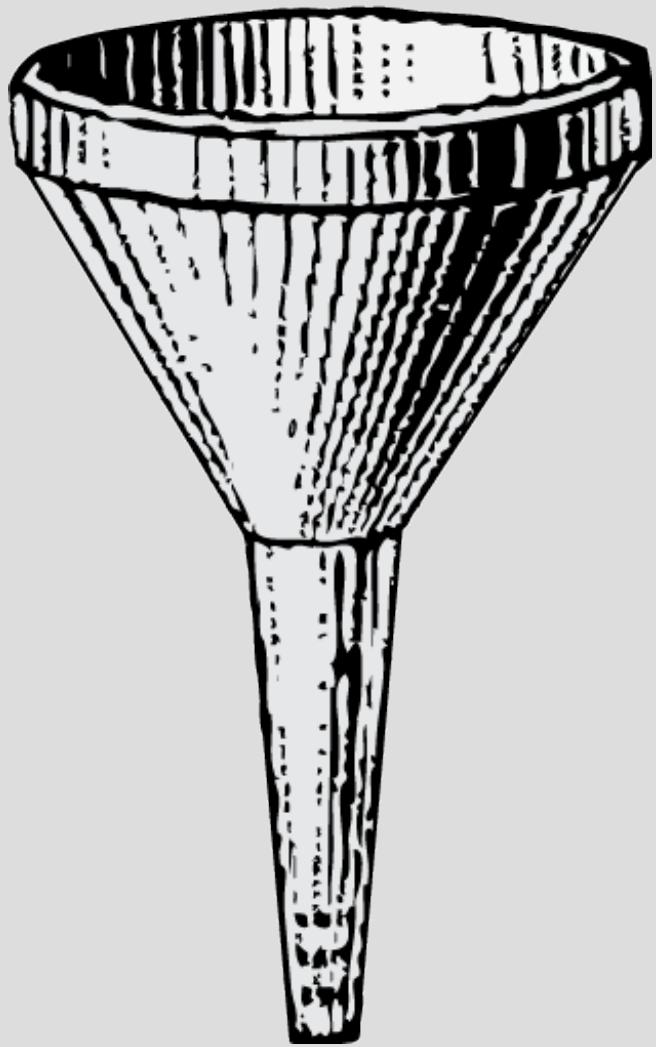


What about similar activities in other groups?

- Problem-solving is good wherever it occurs!
  - Standards venues, community groups, open-source projects, discussion lists, vendor-led initiatives...
- Other groups
  - **OSIS (Open Source Identity System)**
- Concordia's added value:
  - Pain points expressed by deployers, and
  - “inter-interop” problems amenable to protocol-layer solutions

Scenario development timeline

- **Aug 07**: discussed “use-case buckets”
- **Sep 07**: prioritized an initial issue list
- **Nov 07**: analyzed our A-priority issues
- **Dec 07**: selected two interop scenarios
- **Jan-Apr 08**: defined and tested them
- **Soon**: document findings
- Lather, rinse, repeat



General issues, as initially prioritized

A-priority:

- InfoCard + SAML
- SAML + WS-Federation
- IdP discovery
- WS-Fed/SAML metadata

B-priority:

- Single logout
- Level of Assurance encodings
- InfoCard à ID-WSF bootstrap
- SASL+SAML

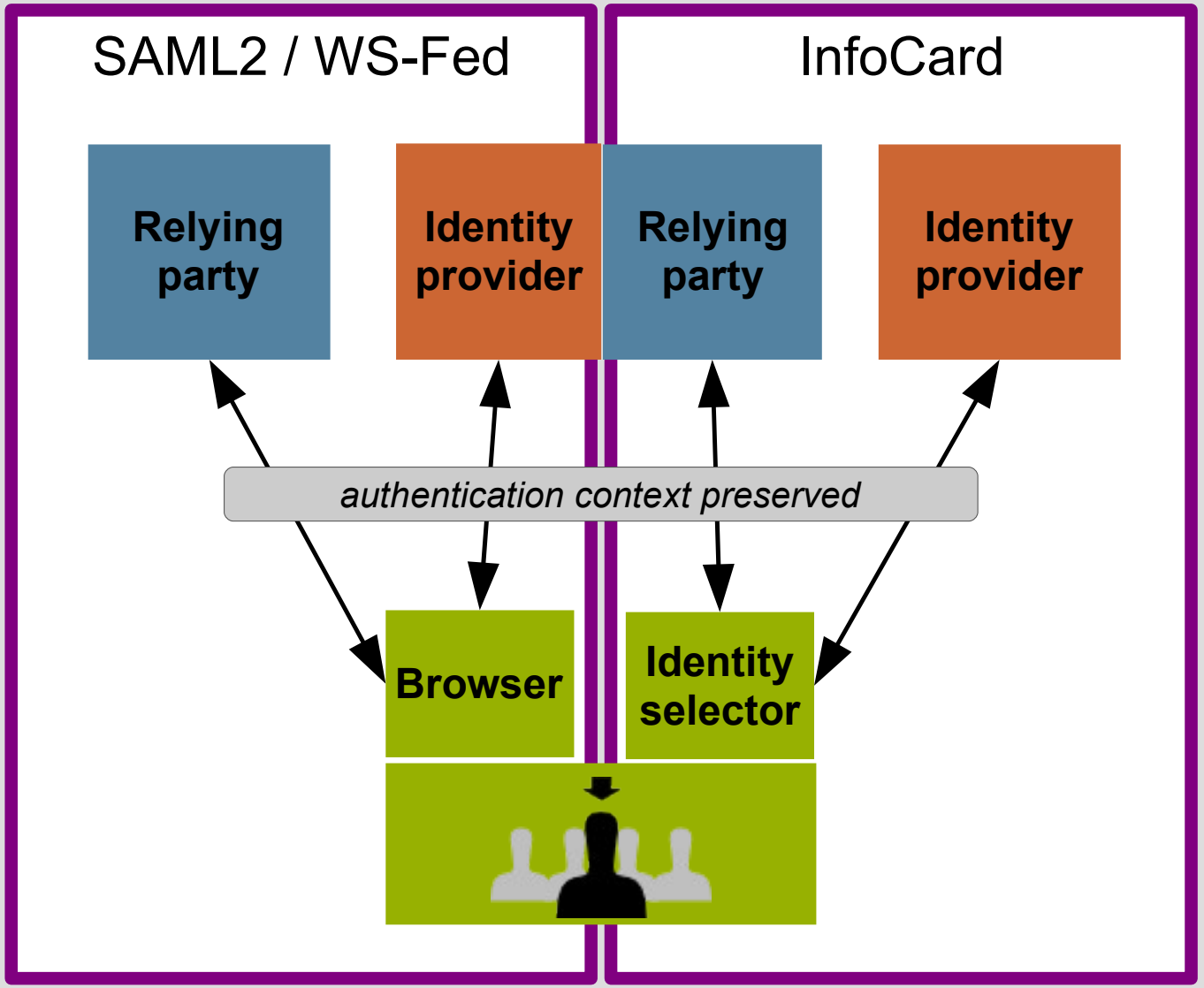
Keep an eye on:

- Roaming network access
- Dynamic web SSO use cases
- Attribute schema mapping
- OpenID + SAML

RSA Interop Report

- Scenarios
- Details
- Participants
- Conclusions

Scenario 1: Authenticating to Federations with Information Cards



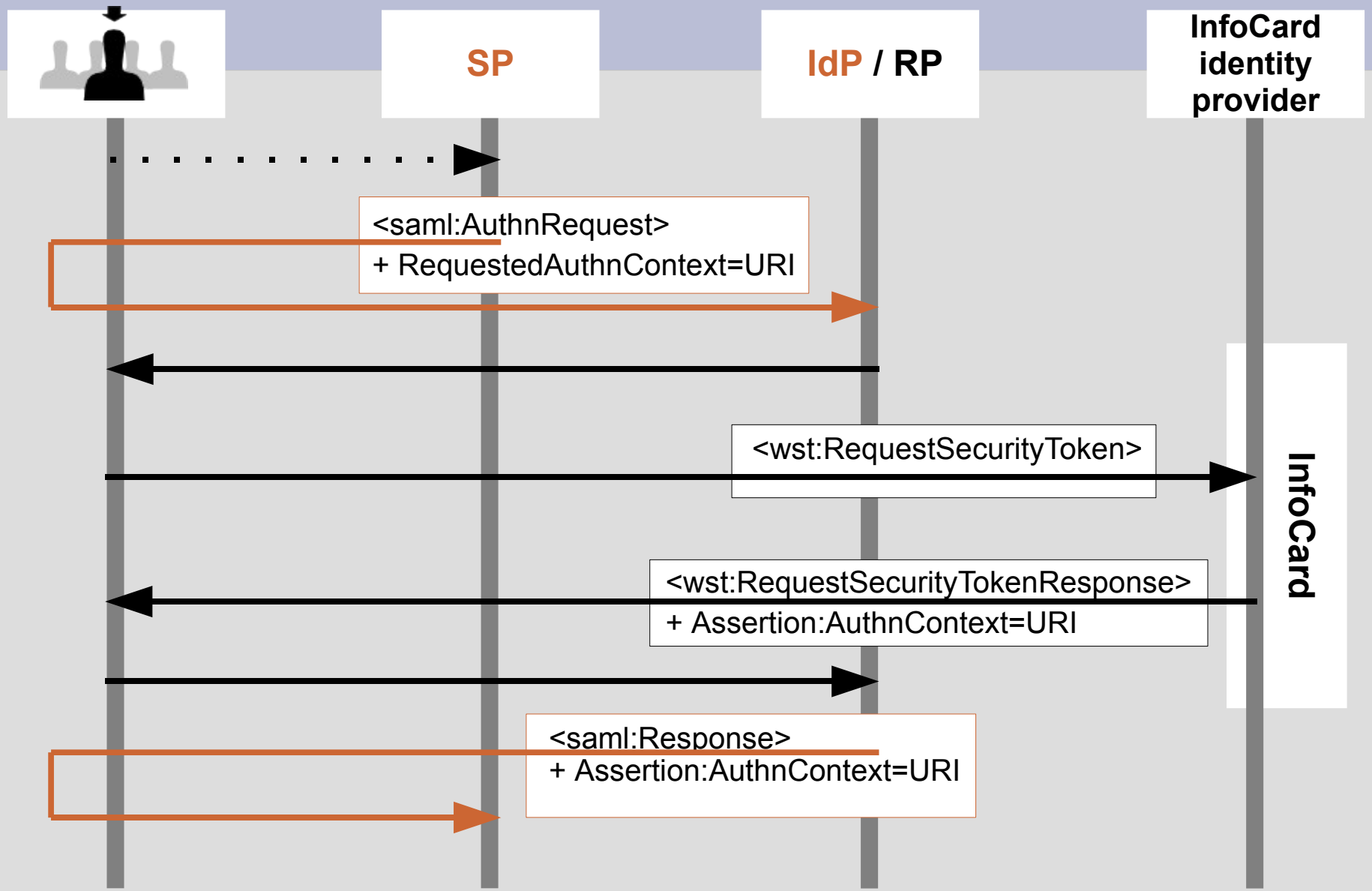
Scenario 1: InfoCard + (SAML2 | WS-Federation)

- **What happens:** User logs in with an Information Card while taking part in a federated interaction
- **Challenge:** Persist the details of the RP's authn policy and the actual authn method used
  - Chaining environments remains necessary
  - Exploring protocol implications of carrying InfoCard authn info in various ways
- **What's new:**
  - SAML2 token support in WS-Federation implementations
- **Issues to solve:**
  - Generic claim structure vs. SAML's authn context structure
  - Well-known identity selector limitation on policy (claim types)

Authentication context class URLs-of-convenience

```
http://projectconcordia.org/rsainterop/authnmech/personal
http://projectconcordia.org/rsainterop/authnmech/managed/password
http://projectconcordia.org/rsainterop/authnmech/managed/kerberos
http://projectconcordia.org/rsainterop/authnmech/managed/x509
http://projectconcordia.org/rsainterop/authnmech/managed/personal
```

1a: InfoCard + SAML2 flow



Scenario 2: Chaining SAML2 and WS-Federation

- **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
  - Chaining between environments remains necessary
  - A common deployment reality today
- **What's new:**
  - SAML2 token support in WS-Federation implementations
- **Issues to solve:**
  - Translation between SAML authentication context and WS-Fed **`wauth`** parameter

Interop participants

Participant	SAML	WS-Fed	Chain
FuGen Solutions	1a		
Internet2	1a	1b	
Microsoft		1b	
Oracle	1a	1b	2
Ping Identity	1a	1b	
Sun Microsystems	1a	1b	
SymLabs	1a	1b	2

Honorable mention:

NZ SSC 1a

RSA “Conclusions”

- Concordia is focusing on conventions, not inventions
  - only innovations were the InfoCard authentication descriptor strings and the agreement around the pairing of an expressed SP requirement and an IdP's description of what it did
  - need to formally document (“profile”) these conventions
- Concordia is focusing on scenarios involving protocols that are used together, but weren't originally designed for that purpose

Next Steps

- Identify the use-cases for the next interop
  - OpenID+SAML?
  - InfoCard+(L)ECP?
- Formally document the “profiles” used for this interop
- Seek additional industry participation
  - New use cases
  - Participation in interop events

Resources

- Wiki
  - http://www.projectconcordia.org/
- Teleconference Calls
  - Usually every other Tues. from 10-11am PT
- Use Case descriptions
  - http://projectconcordia.org/index.php/Main_Page#Current_Work
- RSA Interop 2008
  - http://projectconcordia.org/index.php/Concordia_workshop_RSA_2008_notes

Questions