

Project Concordia Workshop RSA Conference · April 2008

Presented by Eve Maler (Sun) and Mike Jones (Microsoft),
with guest moderator Dr. Robert Haar (General Motors)

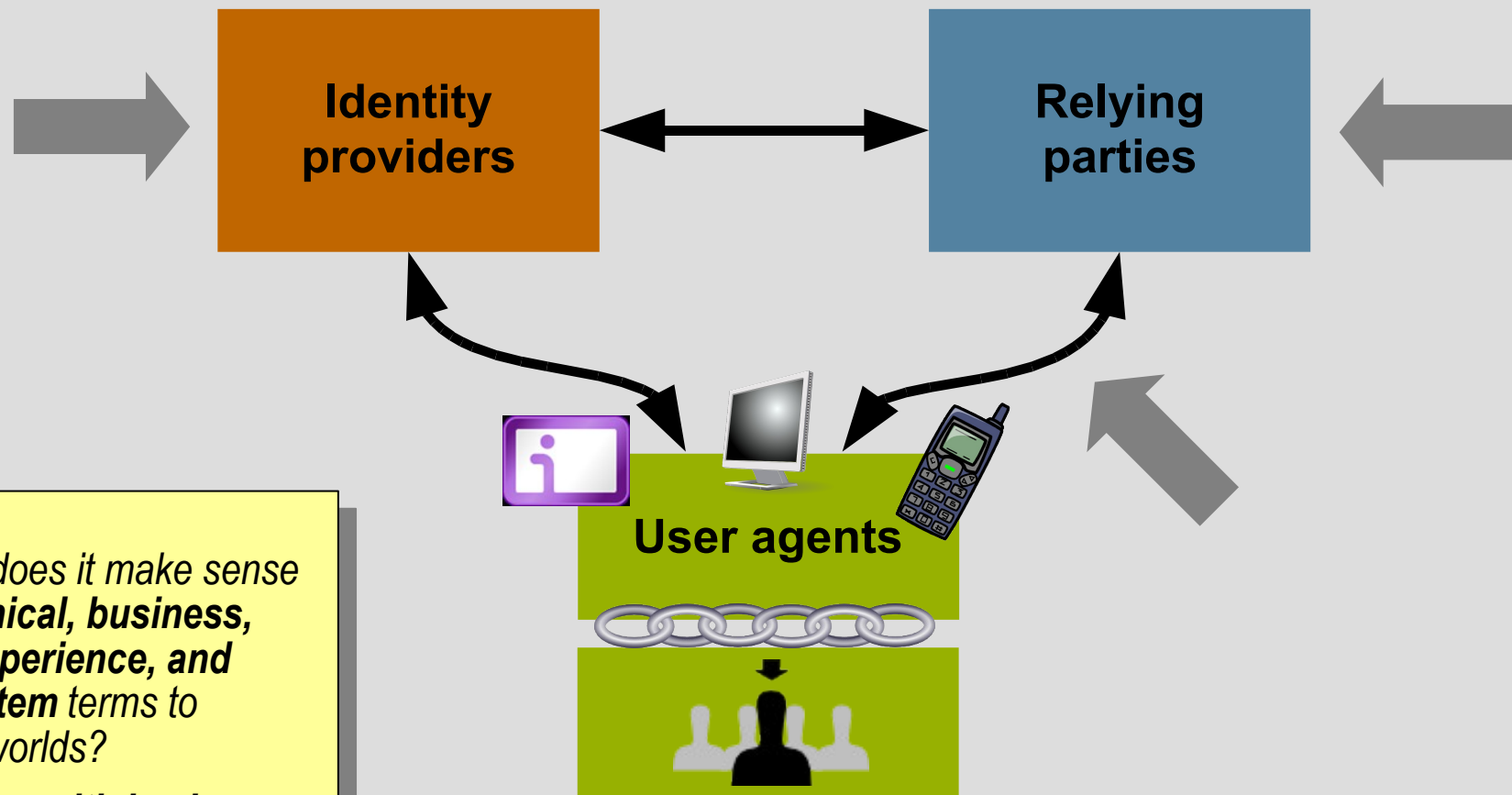
Welcome!

- 9:00-10:00** Update on Concordia activities
- 10:00-12:00** Interop demos and Q&A's
Visit stations individually, or join us for the rotating mainstage demo/discussion
- 12:00-12:30** Gather at mainstage for next steps
General Q&A and review of input gathered throughout the morning
- 12:30** Exit the room expeditiously!
A Liberty workshop is being held this afternoon in the same room

Classic interoperability issues in federated identity

- Heterogeneity is a boon but also a challenge
 - Application platforms
 - Legacy systems
 - Devices at the edge of the network
- Issues to address across solutions include:
 - Multiple protocols and implementations
 - Mix of common and distinct features
 - Abstraction mismatches
 - Compliance issues
 - Satisfying both composability and interoperability

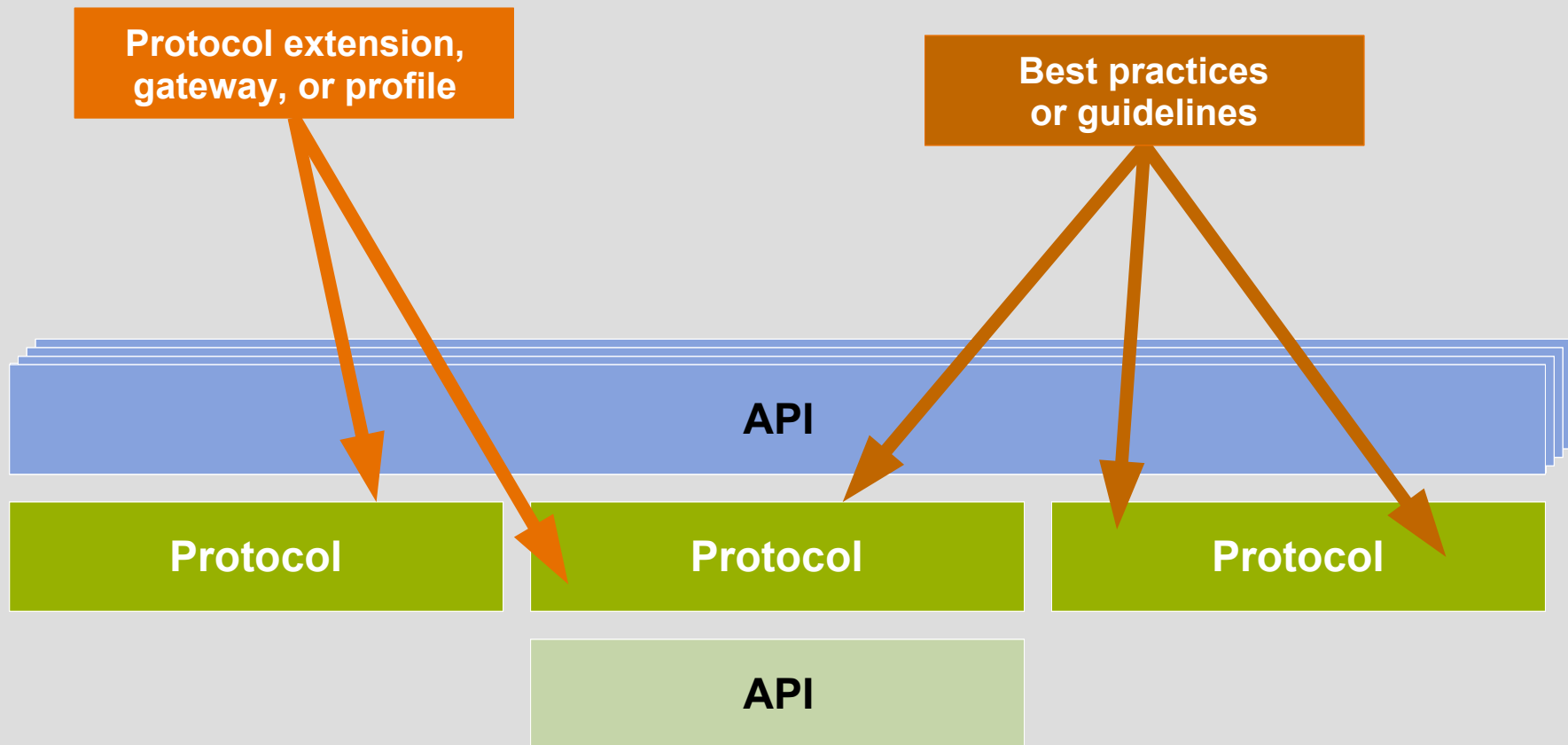
Where is it useful to define additional “smarts”?



Where does it make sense in **technical, business, user experience, and ecosystem** terms to bridge worlds?

Possibly **multiple places**, depending on the use case

How can we get at the “interop truth”?



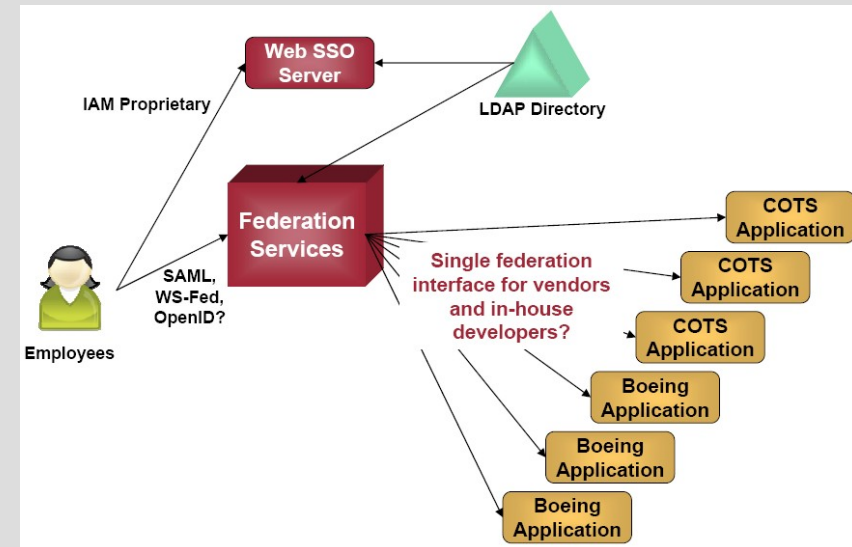
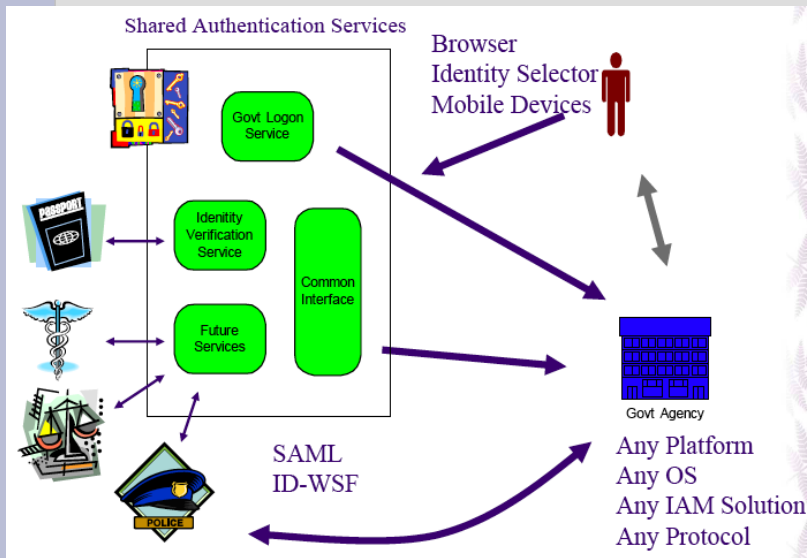
What is Concordia?

- “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



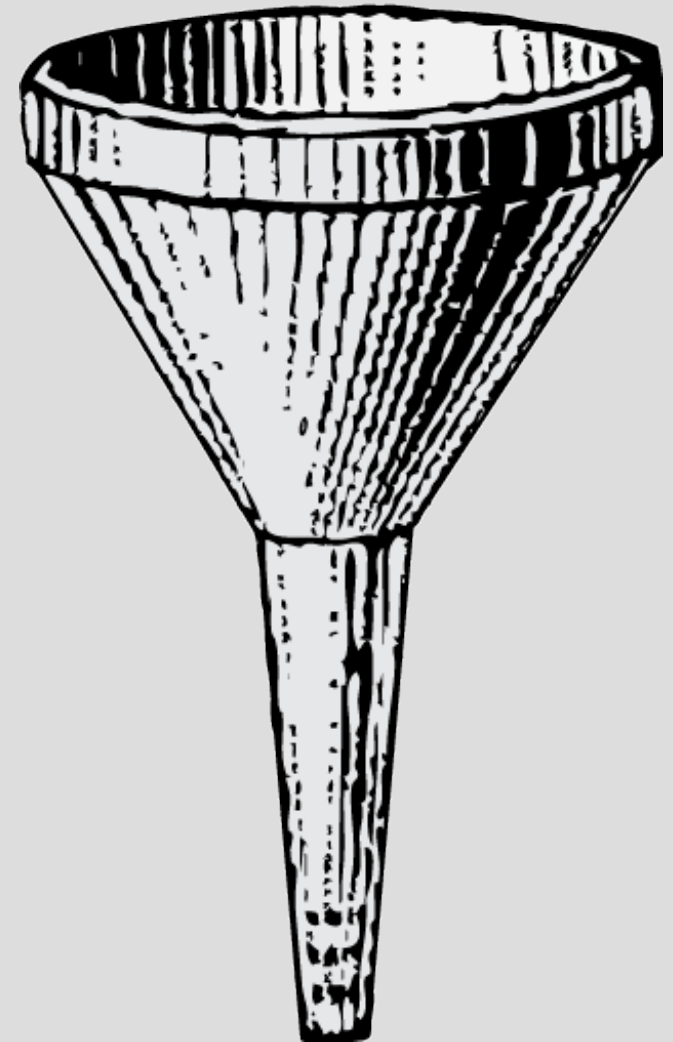
What about similar activities in other groups?

- Problem-solving is good wherever it occurs!
 - Standards venues, community groups, open-source projects, discussion lists, vendor-led initiatives...
- Other interop events taking place this week:
 - **OSIS user-centric identity interop** Tue/Wed
 - **OASIS XACML interop** on the Expo show floor
- 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 → ID-WSF bootstrap
- SASL+SAML

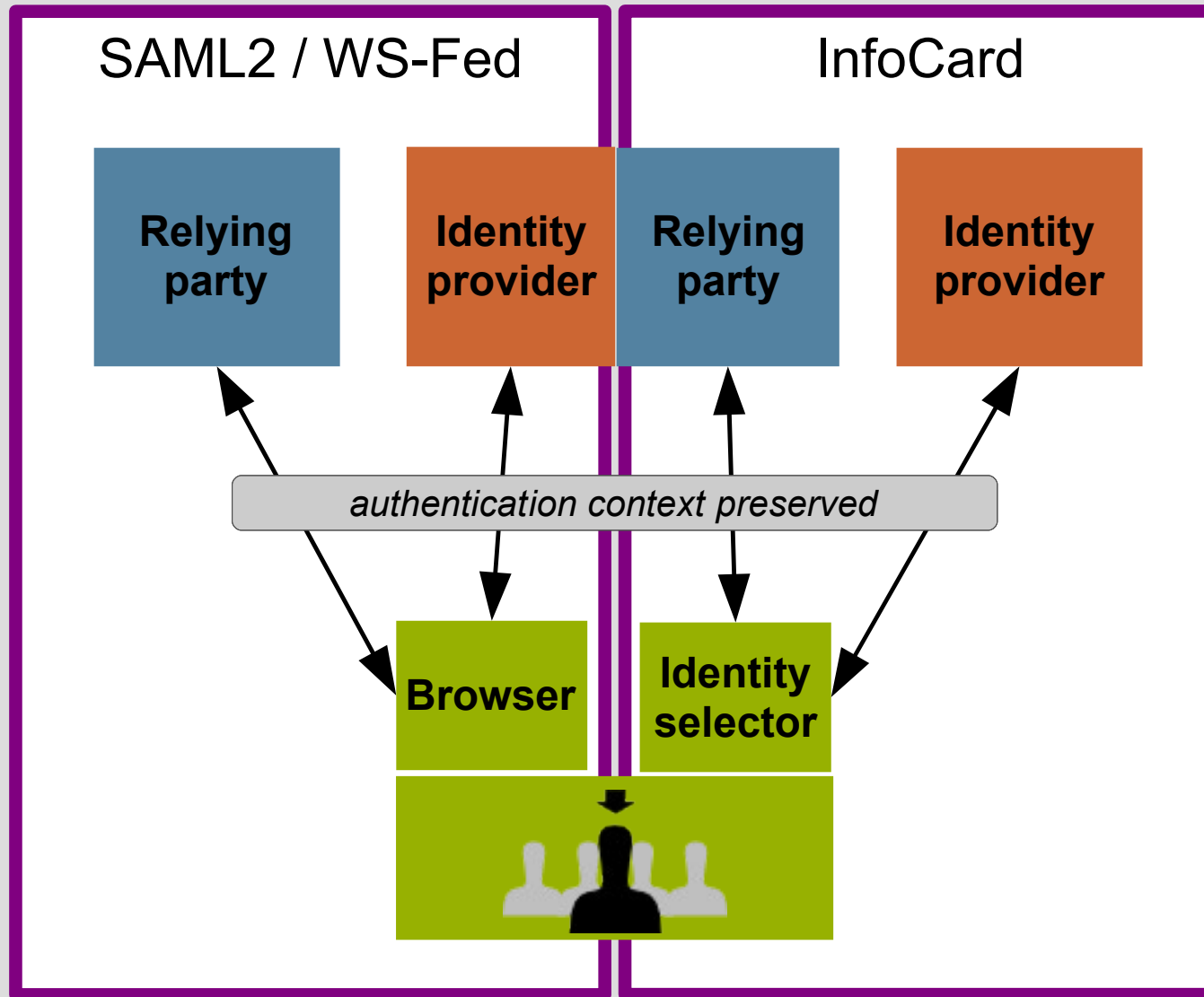
Keep an eye on:

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

High-level scenarios collected in A-priority issue discussion

- (SAML2 | WS-Federation) + InfoCard authentication
 - InfoCard-related authn context preserved through interaction
 - Metadata profiles for this integration
 - InfoCard mechanism for SAML2 IdP discovery
- Interfederation between SAML2 + WS-Federation
- SAML authn context as Level of Assurance context holder
- InfoCard + ID-WSF Interaction Service
- InfoCard + SAML2 Enhanced Client profile
- Higgins integration of SAML2 assertion query profile
- WS-Trust + ID-WSF token issuance/exchange services
- Delegation

Scenario 1: Authenticating to Federations with Information Cards



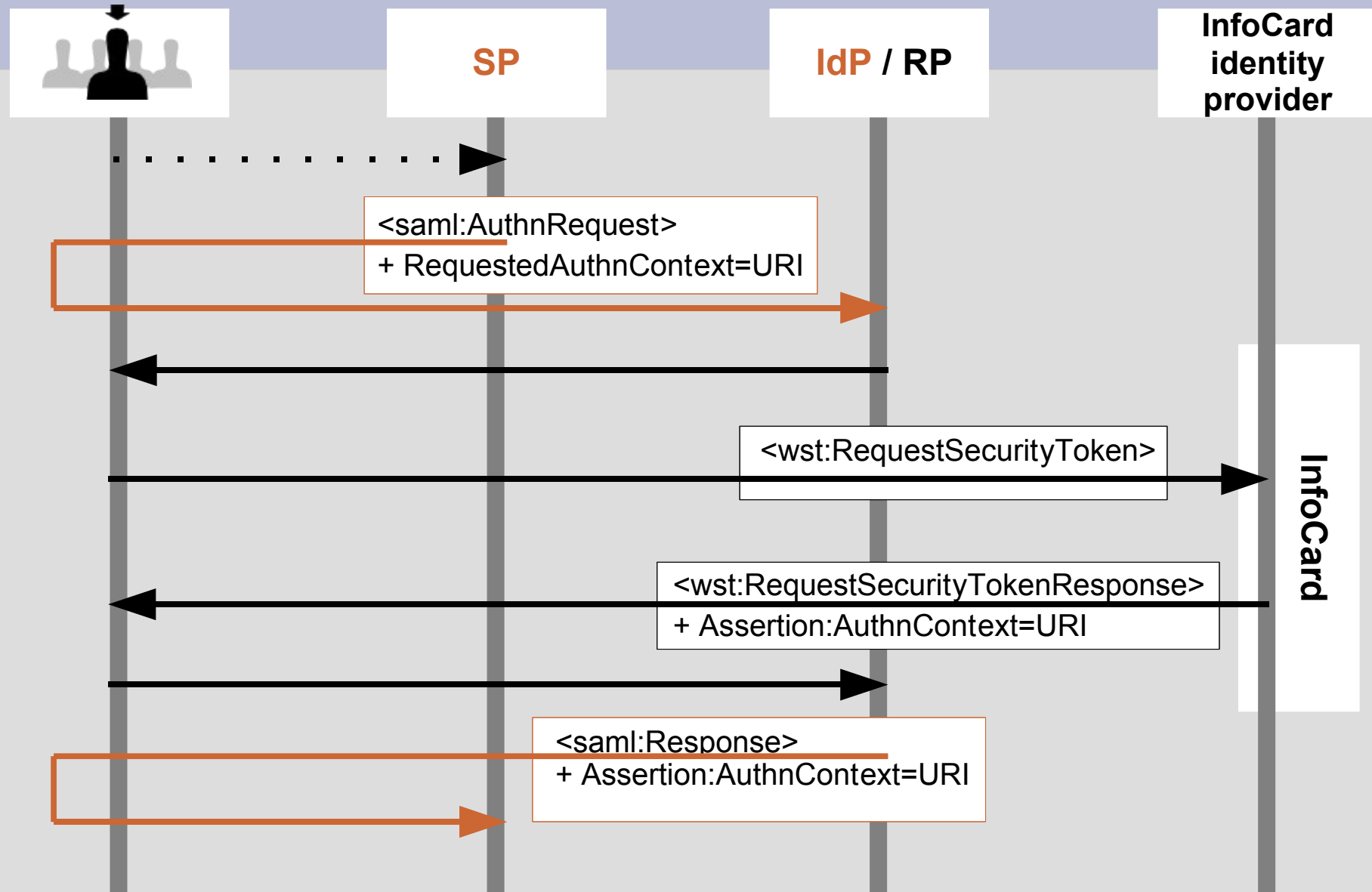
Scenario 1: InfoCard + (SAML2 | WS-Federation)

- **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)

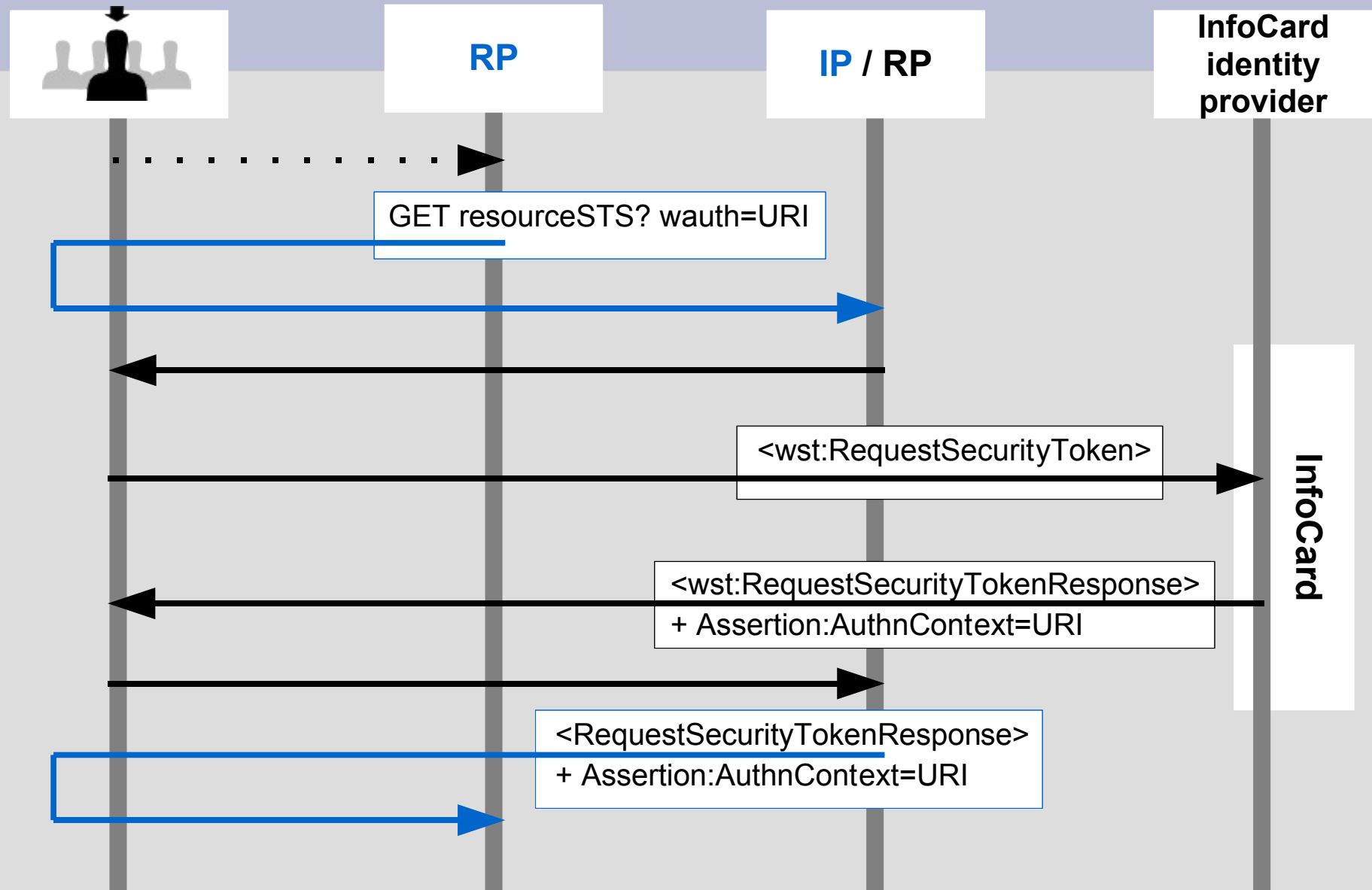
Authentication context class URLs-of-convenience

```
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



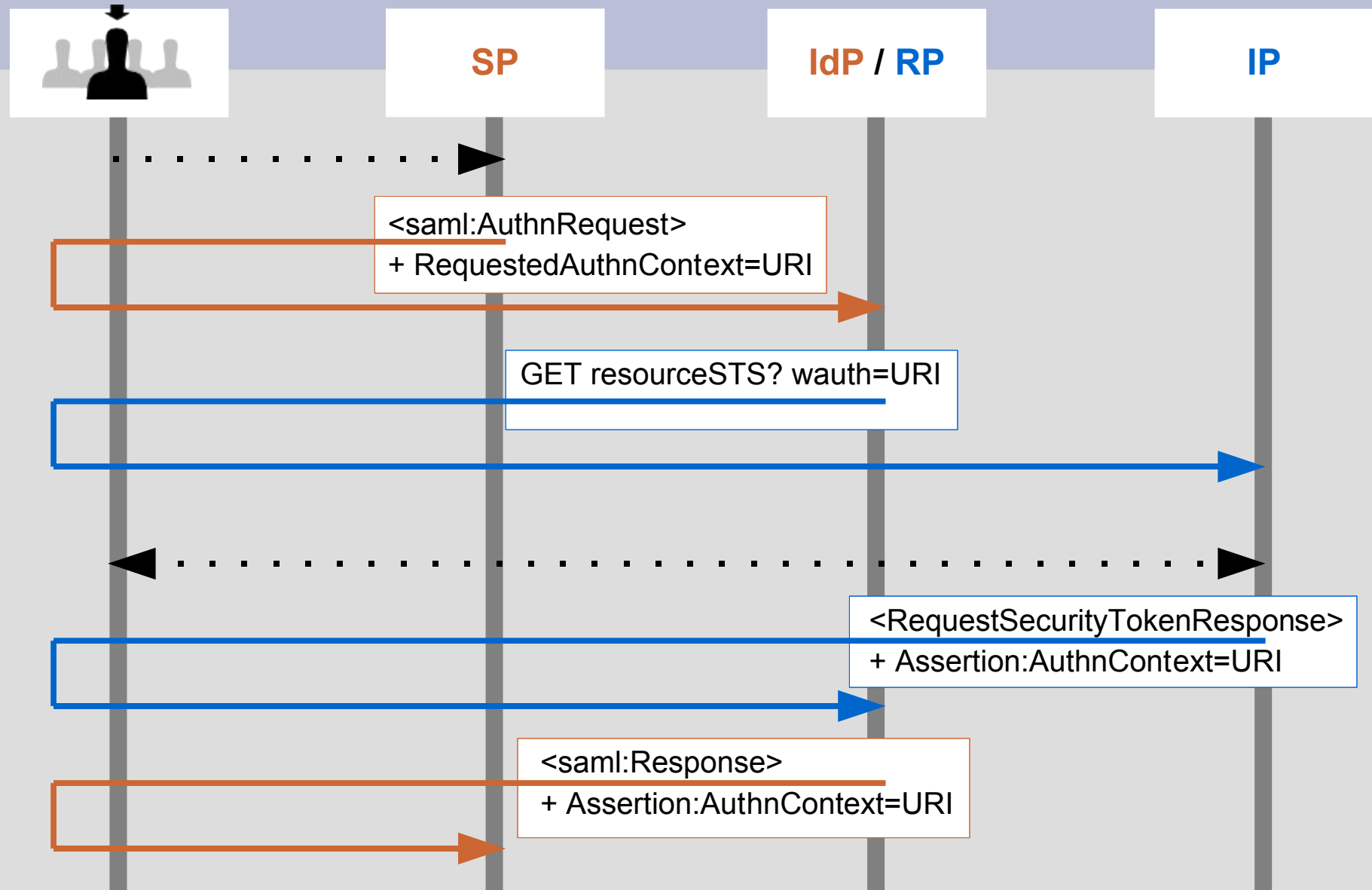
1b: InfoCard + WS-Fed 1.1 flow



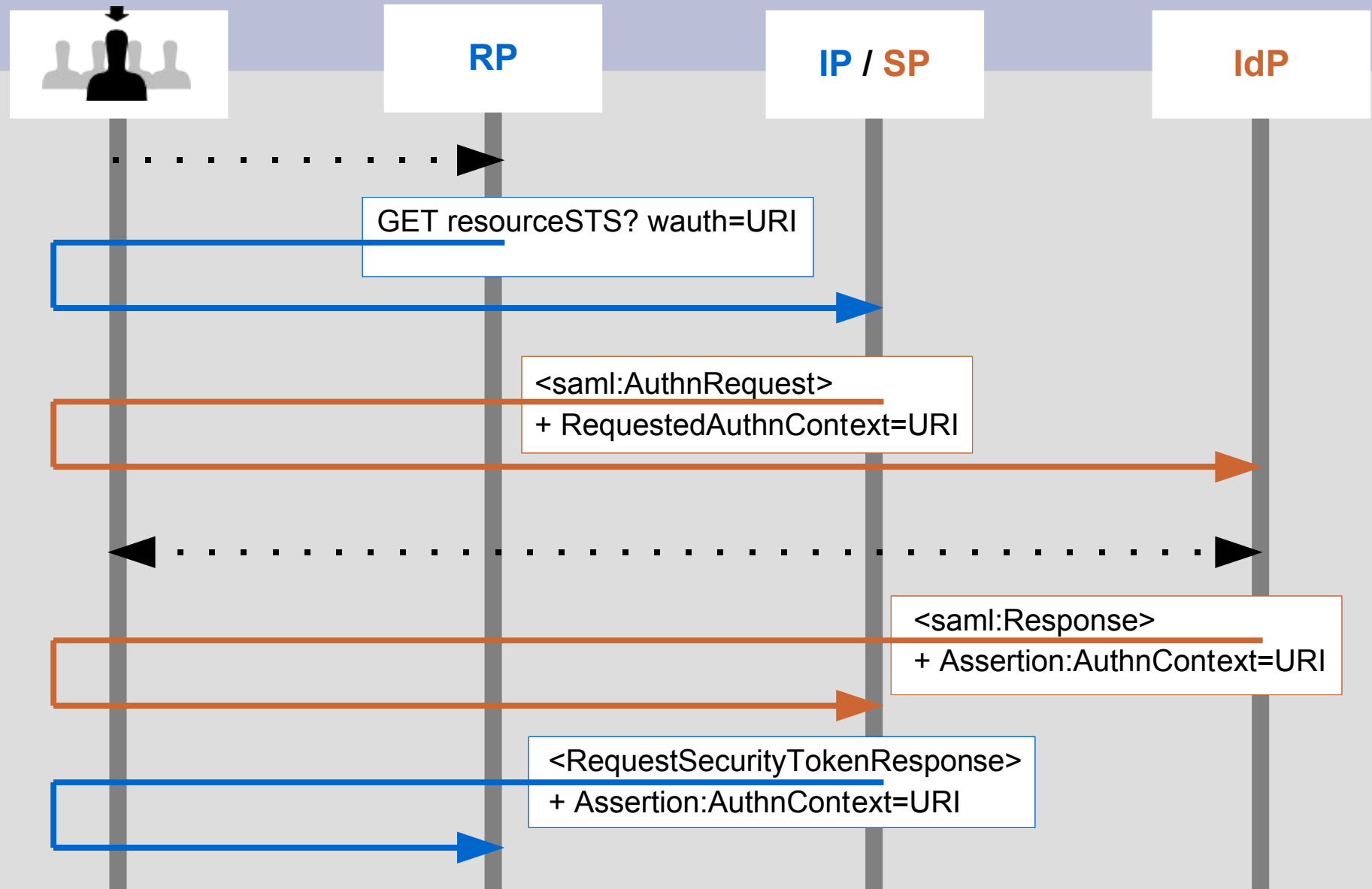
Scenario 2: Chaining SAML2 and WS-Federation

- **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












SAML2 → WS-Federation flow



WS-Federation → SAML flow



Interop participants

	Participant	 SAML	 WS-Fed	Chain
	FuGen Solutions	1a	1b	
	Internet2	1a	1b	
	Microsoft		1b	
	Oracle	1a	1b	2
	Ping Identity	1a	1b	
	Sun Microsystems	1a	1b	
	SymLabs	1a	1b	2
 	<i>Honorable mention:</i> NZ SSC	1a		

Deployers: today we're asking for your feedback and expertise

- In what ways is Concordia's mission valuable to you?
- Which issues and scenarios we've identified so far are important to you?
- For Scenarios 1a, 1b, and 2, what must we ultimately deliver to ensure we're improving the interop picture?
- What other issues, scenarios, and pain points are important to you?
- Are you willing to join our mailing list and share your needs with us over time?

Let's get to the interop demos

- Please feel free to visit the individual demo stations
- Interop participants will also present and respond to comments and questions on the mainstage
- Please join the mainstage wrap-up at **noon**, when we will:
 - Analyze the data we've collected
 - Conduct a general Q&A session
- Don't forget that we must exit promptly at **12:30**
 - For the Liberty workshop this afternoon in the same room
- And don't forget to join us at **projectconcordia.org!**