



Liberty Architecture Overview

Conor P. Cahill
Principal Engineer
Intel Corporation

Liberty History

- Founded in response to Microsoft Hailstorm
- Web services as a core of user identity
- First step – enable federation
- Next step – enable web services

Why Liberty?

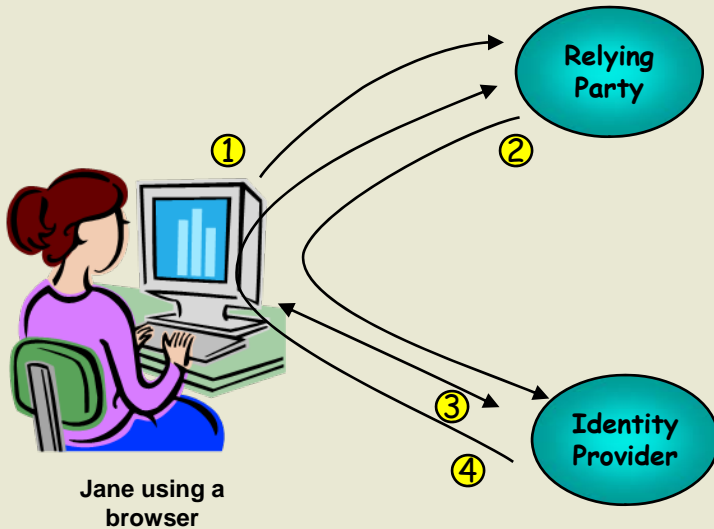
- Response to Microsoft's Hailstorm
- Generate specs in an open environment
- Focus on Identity
- Start with SSO & Federation
- Move to web services

Phase 1: SSO and Federation ID-FF

- Based on SAML 1.0
 - Identity Management (Federation)
 - Authentication Context
 - Extended Authentication Request
 - Single Log-out
 - Enabled Client/Proxy Profile

Sample SSO session

1. After shopping for a few hours, Jane Initiates a checkout at the Relying Party
2. The Relying Party Requests an authentication from the IdP (by redirecting the user's browser to the IdP with Authn request parameters)
3. The IdP may prompt the user for credentials
4. The IdP generates an assertion and returns it to the relying party. The Relying Party now knows it's Jane and can complete the txn.



ID-FF and SAML 2.0

- Liberty contributed all of ID-FF into SSTC
- Converged with work from Shibboleth
- Subsequent Identity Federation work all in SSTC

Phase 2: Identity Based Web Services (ID-WSF)

- Framework for locating and invoking identity based web services
- Supports all types of Web Services
- Permissions-based Attribute Sharing
- Invoking Services under control of user
- At the DS **and** at the WSP

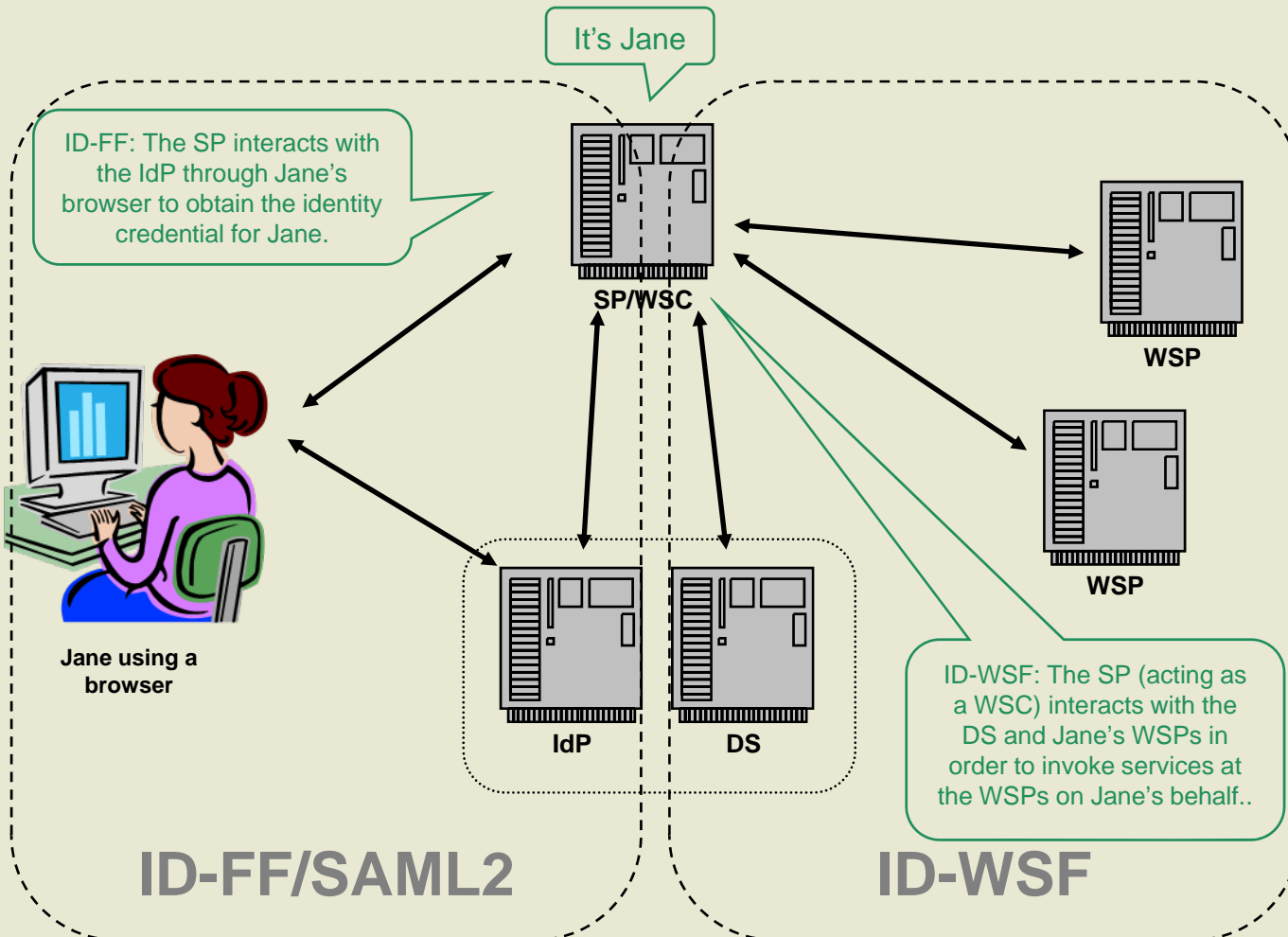
Service Invocation Framework

- Message structure for invoking service
- Separation of messaging/application info
- Identity carried in messaging headers
- Adoption of WS-Security

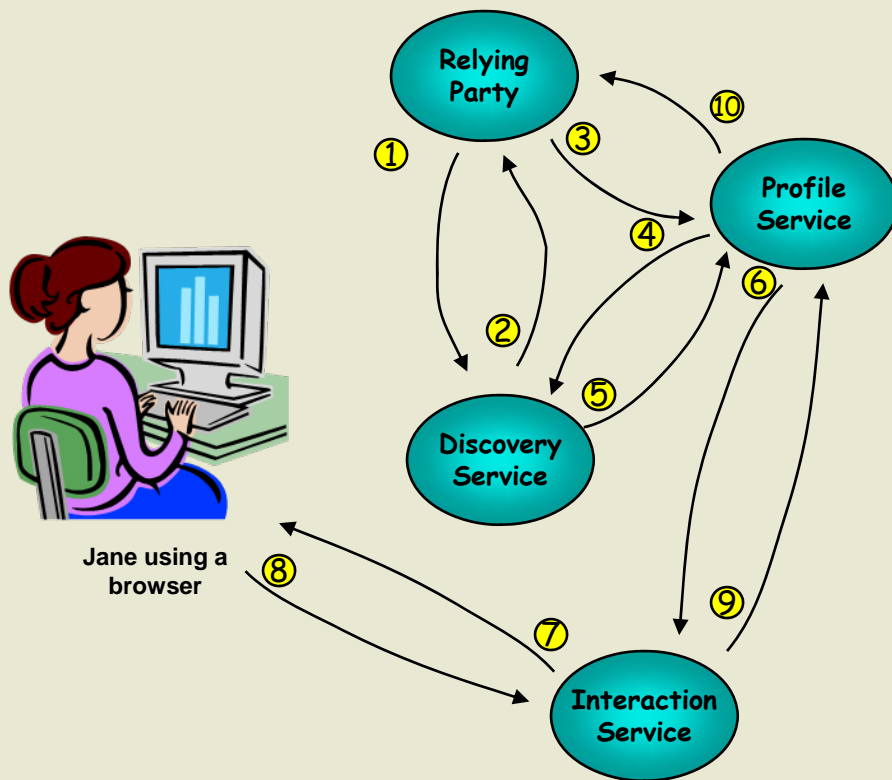
Liberty ID-WSF Discovery Service

- Identity based service discovery
 - Who provides Service X for Conor?
 - At what endpoint?
- Protocol/Framework mapping
 - Which framework and service protocol should I use at that endpoint?
- Token exchange
 - What security token(s) should I use when invoking the service?

Liberty ID-FF & ID-WSF



ID-WSF Invocation following SSO



1. The RP pulls the DS EPR from the SSO token and uses it to invoke the DS asking for the location of the user's Profile Service
2. The DS matches the requested service parameters to the instance of the Profile Service for Jane and returns the EPR for that instance
3. The RP parses the EPR from the DS and uses it to invoke Jane's Profile Service asking for Name/Address, etc.
4. The Profile service, having not gotten permission from Jane to release data to the Relying Party, needs to contact Jane. So it invokes the DS asking for Jane's Interaction Service
5. The DS responds with the IS EPR
6. The Profile Service invokes the IS using the EPR returned from the DS and asking for consent for data release to the RP
7. The IS sends the request to Jane
8. Jane Responds with OK
9. The IS returns the OK response to the Profile Service
10. The Profile service records Jane's response and sends the requested data to the RP

Identity Services (ID-SIS)

- Profile Service (Employee & Personal)
 - Name, address, phone, etc.
- Contact Book Service
- Directory Access Protocol
- Presence Service
- Geolocation Service
- Content SMS & MMS

Phase 3: Web Services extended (ID-WSF 2.0)

- Multi-party transactions
 - People service, Target/Invoking identities
- Extended DST
 - Subscription/Notification
 - Multiple record management
- Convergence
 - Adoption of WS-Addressing
- Advanced Client
 - Provisioning
 - Trusted Module (delegated IDP)

People Service

- Identity Federation between *individuals*
 - Conor establishes a connection with Paul
- Supports Invocation of another user's service
 - Conor can access Paul's Calendar (w/Permission, of course)
- Group (Collection) management
- Invitation model for cross-IDP federations

ID-WSF 2.0: Invocation Context

- Extended Invocation Context to include:
 - Invocation Identity
 - Who is submitting the request
 - Target Identity
 - Who's resource is targeted in the request
 - Sender
 - Server sending the request
 - Destination
 - Server receiving the request

Continuing Work

- Robust Client
- Strong Authentication
- Identity Governance

A decorative graphic consisting of several overlapping, semi-transparent squares in various shades of blue and purple, arranged in a cluster that tapers to the right.

Questions?