LIBERTY ALLIANCE PROJECT

# Liberty ID-WSF Overview

Conor P. Cahill
Architect
Intel Corporation

# Agenda

- Abridged History of Liberty (how did we get here)
- Identity Federation
- Identity based Web Services
- Future Directions

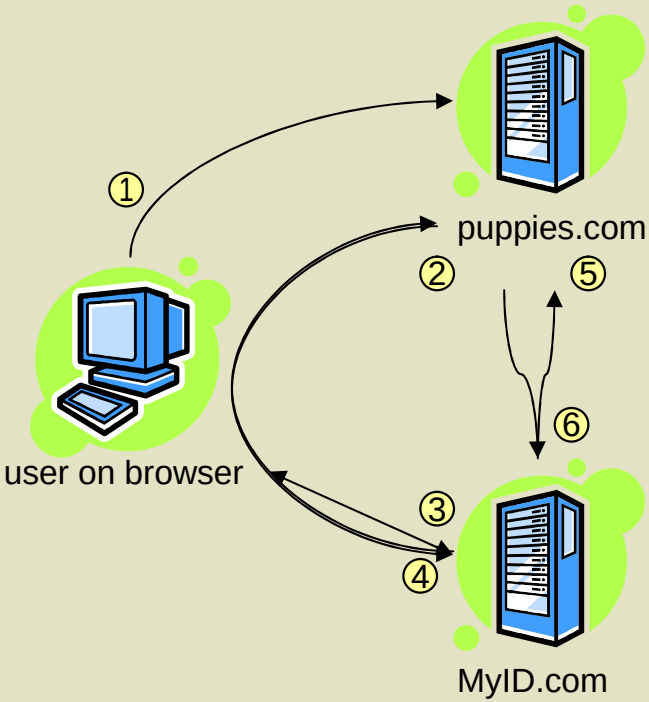
# History

- Founded in late 2001
  - Industry reaction to MS Hailstorm (.NET My Services)
  - Nothing to do with MS Passport
  - To Develop Open Standards for Identity Services
- Evolution
  - Who are you?
  - Who provides services for you and how do I invoke them?
  - How can one user invoke another user's services?

# Identity Federation – Who are you

- Initial Release July 2002
- Features
  - Complete set of SSO/SLO protocols
  - On-the-fly Federation
  - Privacy enablement through
    - Pseudononymous identifiers
    - Anonymous identifiers
    - Consent action points
- Details
  - Based on SAML
  - Additions: Fed, SLO, Auth Context, Passive SSO
  - Extensions folded back into SAML in SAML V2.0

# Ecommerce SSO

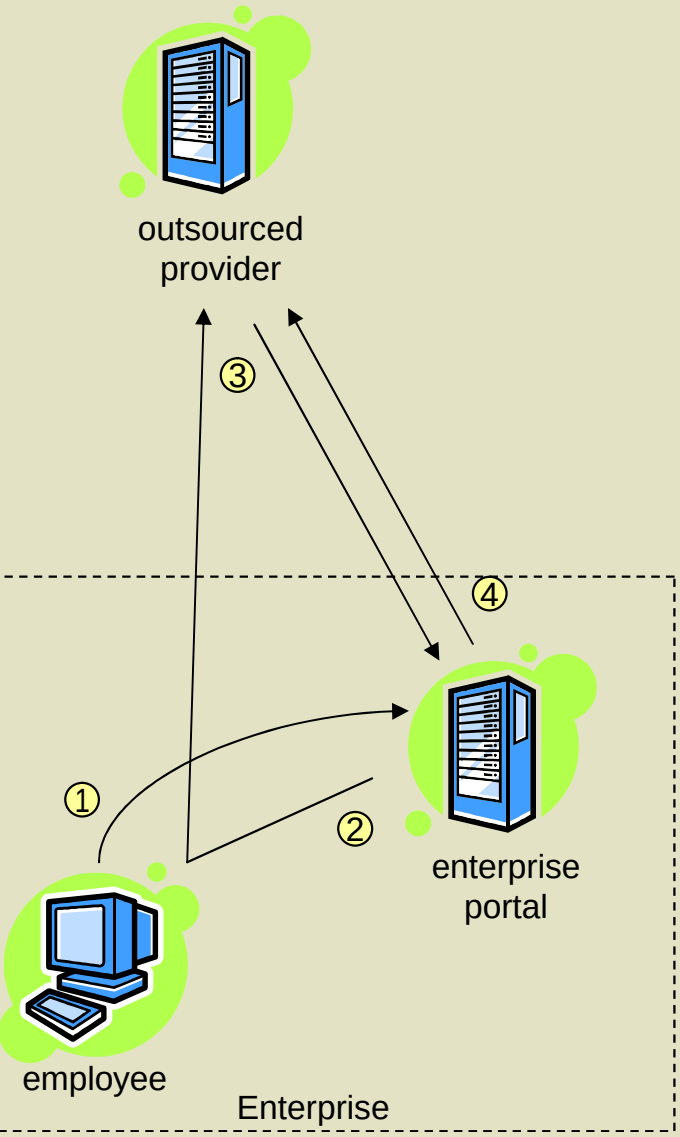



1. The user selects “checkout” on the SP (puppies.com)
2. The SP redirects the browser to the IdP (MyID.com) with an authentication request
3. The IdP interacts with user for auth & consent
4. The IdP redirects browser to SP w/Artifact
5. The SP sends Artifact to IdP
6. The IdP responds with Assertion with user identity

# Typical Ecommerce Features

- Federations take place in-line
- Consent for Federation and for SSO obtained from user when IDP has control of browser (first redirect)
- Federation handles pseudononymous to protect privacy of user
- SSO initiated on request from SP

# Enterprise outbound SSO




1. The user selects the service (i.e. 401k, health plan, etc) on the enterprise portal
2. The Portal redirects user to provider with a SAML artifact
3. The SP submits artifact to Enterprise IdP
4. Enterprise IdP responds w/Assertion containing employee identity

# Typical Enterprise Features

- Federations typically done in out-of-band batch provisioning
- SSO pushed from Enterprise to provider
- Frequently Identity *not* pseudononymous
- Consent as part of employment agreement
- Benefits for SP
  - Reduced support & maintenance (no user accounts to maintain/passwords to reset)
  - Easier integration to Enterprise
- Benefits for Enterprise
  - Better employee experience
  - Easier first day/last day process

# Ongoing Federation Work

- Specification work in OASIS SSTC
- Liberty operates Conformance Interoperability Testing Program for SAML

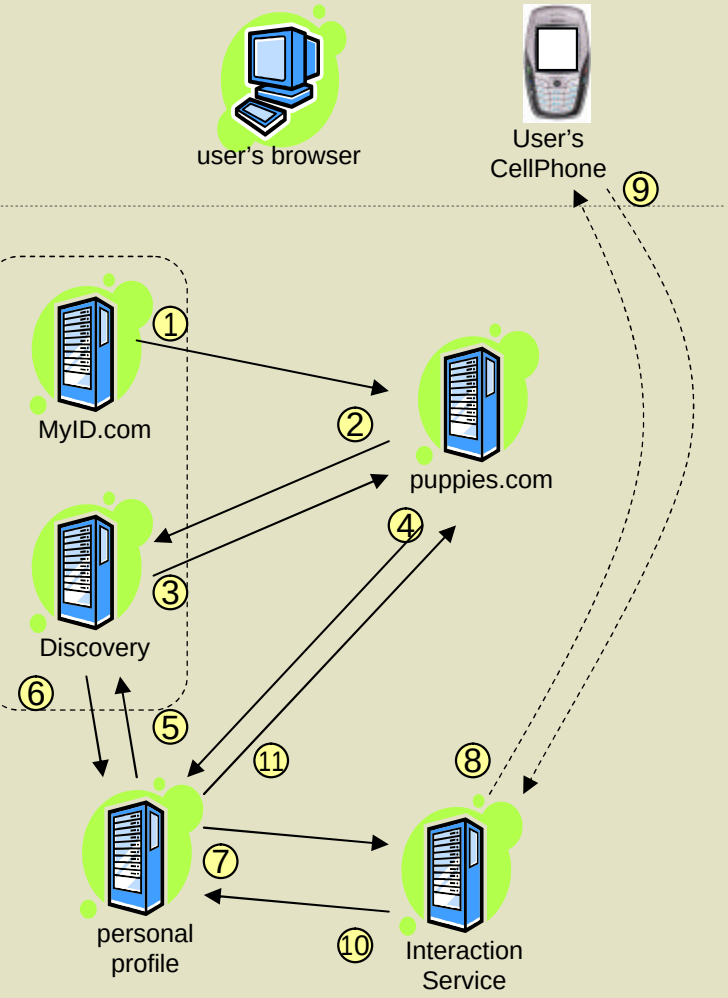
# Liberty ID-FF a success?

- Qualified Yes
  - Many Enterprise->outsource provider implementations
    - Big win for outsourcers & enterprises
  - Some big wins in ecommerce (Orange)
  - But not ubiquitous
    - Some resistance outside of enterprise
      - potential loss of connection to user
      - lack of user demand
      - lack of perceived benefits
    - Changing now
      - ID-Theft driving Strong Authentication
      - Strong Authentication driving SSO acceptance for SPs & Users
- Identity world is converging on SAML 2
  - definitive success of ID-FF
  - drivers:  Identity Theft and Strong Authentication

# ID-WSF 1.0

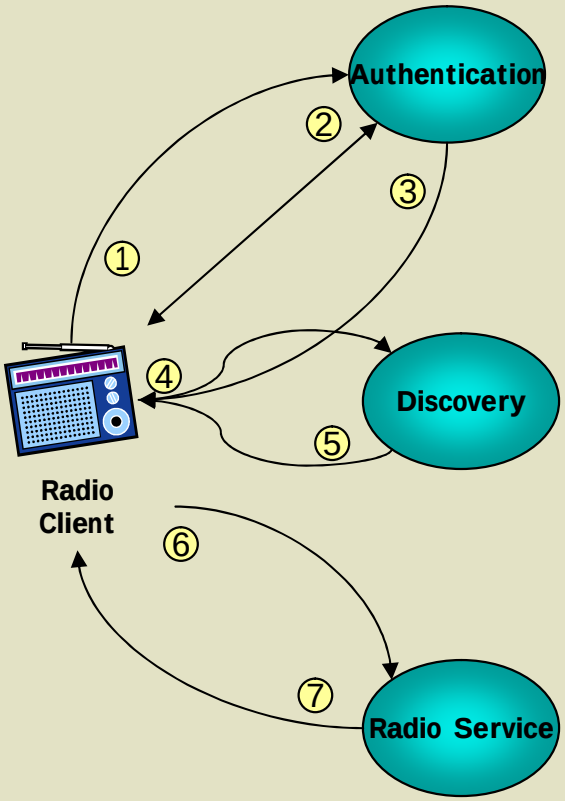
- Initial Release November 2003
- Features
  - Support Per-User sets of services
  - Security Contexts may vary
  - Client->Server and Server->Server invocations
  - Invocation in the context of a principal
- Components
  - Service Invocation Framework
  - Foundation Services
    - Authentication Service
    - Discovery Service
    - Interaction Service
  - Identity Services
    - Personal Profile
    - Employee Profile

# ID-WSF bootstrapped from SSO




1. SSO completion (Assertion to SP (Puppies.com) with nameID 123).
2. SP discovers user's PIP
3. DS Responds with RO for PIP
4. SP asks PIP for user's Name, Addr, etc.
5. PIP needs consent from user and so discovers user's IS
6. DS Responds with RO for IS
7. PIP Invokes IS (ask user for consent for SP to get info)
8. IS sends SMS to User's Cellphone (non-Liberty)
9. User responds with OK (non-Liberty)
10. IS Responds to PIP with OK
11. PIP Responds to SP with data

# Client Initiated ID-WSF




**Authentication**

1. The RC initiates Authentication with AS
2. The RC completes authentication process with AS
3. The AS returns RO for DS.

**Discovery**

4. The RC discovers RS at the principal's DS.
5. The DS returns RO for RS

**Service Invocation**

6. The RC invokes the RS.
7. The RS responds to the RS

# ID-WSF 2.0

- Public Draft 3
- Features
  - Cross-user transactions
  - Asynchronous messaging
  - Subscription/Notification
  - Adoption of SAML2
- Components
  - Framework enhancements
    - Adoption of WS-Addressing
    - Multi-user invocation context
  - People Service
    - Who are my “friends”?

# ID-WSF 2.0: Cross-User Txns

- 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
- 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: Asynchronous Messaging

- Adoption of WS-Addressing
- Adds Asynchronous Messaging support
- Multi-path messaging
  - Responses can be directed to an address
  - Useful in server-to-server messaging with clusters

# ID-WSF 2.0: Subscription/Notification

- Template for service based subscriptions
- Usable by all services
- Notification when data changed
- Supports Notifications with:
  - Data changed flag (recipient has to go get data)
  - Changed data

# ID-WSF Beyond 2.0

- Trusted Module
- Strong Authentication
- Provisioning
- Further Convergence with WS-*