Identity Federation & Web Services

Fulup Ar Foll, Sun Microsystems
fulup@sun.com

Why Federation
Why Standard & Interoperability Matter

• **Global Connectivity**
  • Across repository, domain, ...
  • Seamless to User (complexity advert)
  • Want to be both consumer and provider

• **Increasing Demand for ID**
  • Everyone wants your identity, but do users want it?
  • Need adequate privacy mechanisms before exposing it.

• **Heterogeneous world**
  • Multi vendors, services provider and consumers are heterogeneous.
  • Multi channel, cross devices, cross networks, ...

A high level Interoperable standard

• **ID-FF**: Identity Federation Framework
  • "Liberty Federation"
  • Focused on human-to-application interaction
  • Now converged with SAML V2.0

• **ID-WSF**: Identity Web Services Framework
  • Focused on application-to-application interaction

• **ID-SIS**: Service Interface Spec
  • ID-SIS plus ID-WSF equals "Liberty Web Services"
  • Defines particular useful services
  • Personal profile, geolocation...
Design goals

- A standards-based architecture for Federation & identity web services
  - Ecosystems of services that expose interfaces on behalf of individual users' identities
- Privacy and Security as a 1st class citizen
  - Identity information requests access-controlled
  - Minimal disclosure of identity information
  - Protection against disclosure of identifiers
- Flexible foundation for application development
  - Across security domains and computing platforms
  - Across time, allowing for service location flexibility

Privacy is a MUST

- Ensuring that your data is shared on your terms by:
  - Capturing your usage directives and consent status in service messages
  - Allowing for interaction with you at critical junctures to obtain your consent and privacy policies
    - Interaction Service, Interaction Redirect
- Inhibiting correlation of your activities by:
  - Offering different pseudonyms to different parties
    - Identity Mapping Service
- Protecting your data in transit
  - WS-Security for confidentiality
Global Architecture

An all-singing, all-dancing sample flow
Protocol architecture piece-parts

Major benefits of ID-WSF's design

- Peer to Peer (no big brother)
- Authentication, authorization, and application of usage policy against consumers of identity data
- User privacy through use of pseudonyms
- Dynamic service discovery and addressing
- Common web services transport mechanisms to apply identity-aware message security
- Abstractions and optimizations to allow anything – including client devices – to host identity services
- Unified data access/management model for developers
- Flexibility to develop arbitrary new services
- Identity model for social network & cross users (ID-WSF2)
ID-WSF 2.0: What's new?

• 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

• 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
ID-WSF-2: People Service

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

Technology is Mature