Federated Identity Management

Options and Issues

Digital Identity of a person

- Credit card
- Driver’s license
- email id

  - Unlike physical identity, digital identities might change.
  - Pose management challenges

Federated Management

- Coalescing all identities and managing them together
- Enables computer systems to dynamically distribute identity across security domains
- Most prominent capability – SSO (Single Sign-On)
- Has various risks and concerns to be addressed

Scope

- Describe the federated identity model
- Discuss its security, privacy and architectural challenges
- Discuss the three popular federated identity protocols

Identity Management

- Enterprise
  - User accounts for employees
  - Managed through a store, usually LDAP
  - Scalability issues
- Web sites and web applications
  - Accounts hosted on behalf of users
  - email, online shopping, social networking, etc
  - Users assume ownership
  - Problem borne by users in remembering username/password

Federated Identity Management

- Provides solution to many problems shared by both the cases
- SSO is prominent capability that gets attention
- Involves sharing information about user between sites

Logical Components

- User – assumes a particular identity
- User Agent – the means through which the user interacts with the system
- Service Provider – web application that provides the service. Offloads authentication to third party and relies on external information. Also called Relying Party.
- Identity Provider – web site that users log in to. Stores attributes that needs to be shared with various SPs.

Authentication Patterns

- *SP-initiated*
  - Service provides initiates an authentication request to the identity provider
- *IdP-initiated*
  - Identity provider acts as a portal for the user to navigate to various participating service providers

Separating Identity from its Usage

- User logs in to IdP once – accesses multiple SPs
- Service Providers delegate account management tasks and always receive accurate real-time data
- Identity Providers can focus on improving authentication methods and interface

Challenges - Security

- Basic loose coupling pitfalls like replay attacks, man-in-the-middle-attacks, session hijacking, etc
- In HTTP context, SSL/TLS can be the baseline
- User authentication
  - Pros: Small initial burden
  - Cons: Weak link in the security chain – prone to phishing attacks
- Increased scope of a compromised identity
  - Identity renewal mitigates the risk to some extent

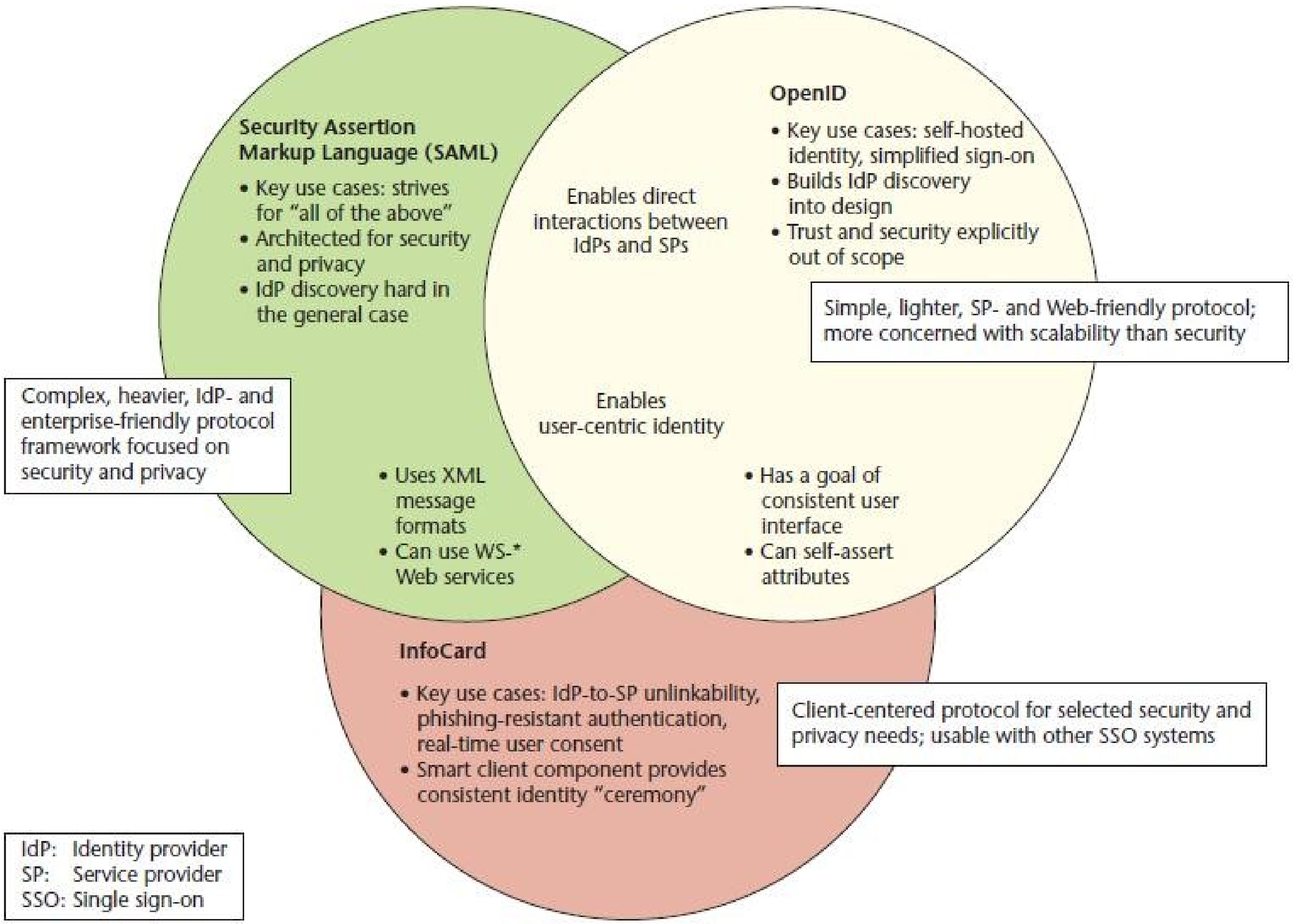
Challenges - Privacy

- SPs might get hold of user info more than required
- Minimal disclosure at foundation level
- Pseudonymous identifiers
  - Based on IdP-SP-User relationship instead of a globally unique identifier of the user
- Informed user consent can safeguard against excessive disclosure

Architectural Challenges

- IdP discovery
  - Partner based solution
  - User provided information
- Identifier Schemes
  - Same identity should be resolved at different scopes across multiple authorities
  - XRI (Extensible Resource Identifier)
    - Abstraction layer for URIs and IRIs
    - Same XRI can resolve into multiple URIs depending on context
- User Empowerment
  - Total user control over identity: service providers may not trust the authenticity of the information
  - Getting user consent for data sharing: requires rich policy and permission tracking environment

Federated Identity Protocols



Security Assertion Markup Language (SAML)

- Key use cases: strives for "all of the above"
- Architected for security and privacy
- IdP discovery hard in the general case

OpenID

- Key use cases: self-hosted identity, simplified sign-on
- Builds IdP discovery into design
- Trust and security explicitly out of scope

Enables direct interactions between IdPs and SPs

Simple, lighter, SP- and Web-friendly protocol; more concerned with scalability than security

Complex, heavier, IdP- and enterprise-friendly protocol framework focused on security and privacy

Enables user-centric identity

- Uses XML message formats
- Can use WS-* Web services

- Has a goal of consistent user interface
- Can self-assert attributes

InfoCard

- Key use cases: IdP-to-SP unlinkability, phishing-resistant authentication, real-time user consent
- Smart client component provides consistent identity "ceremony"

Client-centered protocol for selected security and privacy needs; usable with other SSO systems

IdP: Identity provider
SP: Service provider
SSO: Single sign-on

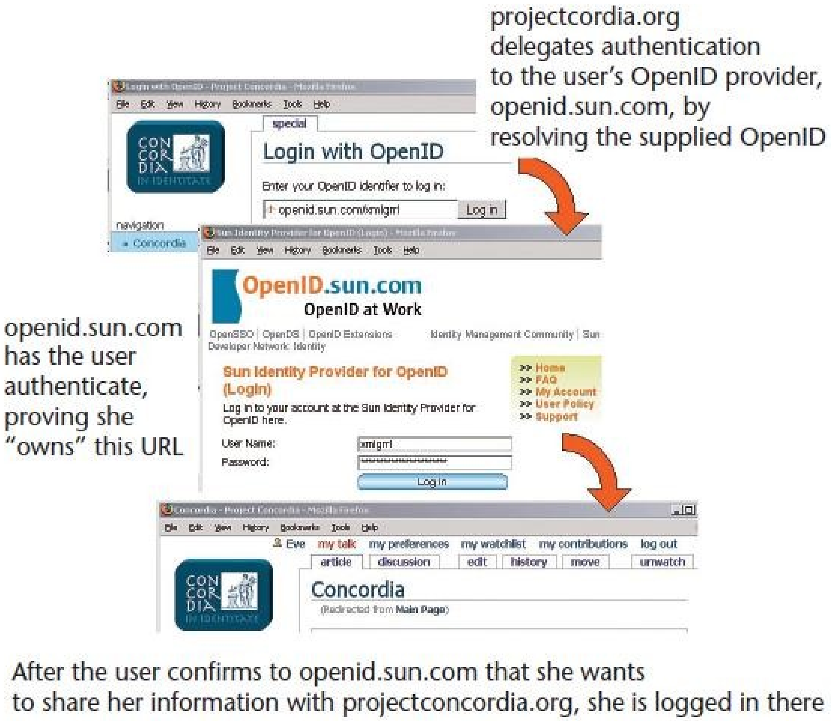
Figure 1. Three popular federated identity protocols. The Security Assertion Markup Language (SAML), OpenID, and the InfoCard protocol used by Windows Cardspace have both common traits and clear differences.

Security Assertion Markup Language

- Oasis and ITU standard (ITU-T X.1141)
- XML based framework for exchanging security and identity information across domains
- Assertions
  - XML packets containing identity information
- Assertions are signed, encrypted into profiles
- Offers pseudonyms in several forms
- Ties up with Liberty Alliance's Identity Web Services Framework (ID-WSF) for offline users
- Deployed in a trusted circle for IdP discovery
- InCommon Federation: IdP discovery in universities

OpenID

- Originally developed by Brad Fitzpatrick for LiveJournal authentication and avoiding spam
- Operates like a closed-loop email-address



projectcordia.org delegates authentication to the user's OpenID provider, openid.sun.com, by resolving the supplied OpenID

Login with OpenID

Enter your OpenID identifier to log in:

openid.sun.com/xmlgrrl

openid.sun.com has the user authenticate, proving she "owns" this URL

Sun Identity Provider for OpenID (Login)

Log in to your account at the Sun Identity Provider for OpenID here.

User Name: xmlgrrl

Password: ••••••••••••••

After the user confirms to openid.sun.com that she wants to share her information with projectconcordia.org, she is logged in there

File Edit View History Bookmarks Tools Help
special
Log in
navigation
Concordia
OpenID.sun.com
OpenID at Work
OpenSSO | OpenDS | OpenID Extensions Identity Management Community | Sun Developer Network: Identity
>> Home
>> FAQ
>> My Account
>> User Policy
>> Support
Log in
Eve my talk my preferences my watchlist my contributions log out
article discussion edit history move unwatch
Concordia
(Redirected from Main Page)

Figure 3. OpenID. Originally developed for an online community, the rapidly evolving OpenID treats Web addresses as user identifiers.

OpenID

- Expanded to support XRI and more sophisticated discovery of IdPs.
- Users provide the IdP information
  - Pros: Scalable model like the web
  - Cons: Privacy issues in sharing user information
    - Different SPs could correlate user activity
    - Version 2 in 2007 supported pseudonymous logins
- Not true SSO, only Simplified Sign On.

InfoCard Protocol and Windows Cardspace

- dot net component designed to provide consistent digital identity
- Digitally signed security token like SAML
- Two types or cards
  - Self-asserted
  - Managed
- Need to meet the SP’s policy requirements
- Elegant solution for IdP discovery even though requires special client technology

InfoCard Protocol and Windows Cardspace

- Identity Selector
  - Can use managed cards to enhance phishing resistance
  - Gatekeeper between SP and IdP
  - Applies user-centric principles in identity selection
- Currently compatible with web service protocols. Eclipse higgins project is working on a plugin-API architecture for multiple protocols.

Interoperability Issues

- SAML and OpenID address simplified sign on in a different way
- InfoCard and SAML have smart clients, but optimized for different purposes
- OpenID and InfoCard both target user centric identity, but have multiple and sometimes incompatible goals

Current Development Efforts

- NTT laboratories’ Sasso project
  - Seeks to let users authenticate to browser based SSO using mobile SIM cards over SAML protocol
- Identity Commons has established Identity Rights Agreements working group
  - Create small set of standardized agreements to specify terms under which personal information is shared
- ACM Digital Identity Management Workshop
  - In 2007, focus was on user acceptance of digital identity paradigms in Web 2.0 online apps
  - Strengthening authentication and increasing usability