IDENTITY MANAGEMENT AND FEDERATION – BC.Net Conference April 25, 2006

Lauren Wood
Senior Technical Program Manager
Business Alliances, CTO Office
Sun Microsystems

Alex Acton
Software Specialist
Client Solutions
Sun Microsystems

Talk Plan

- Concept Reviews - Identity Services and Federation
- Liberty Alliance
- Single Sign-On/Federation Demo
- Other Federation Examples
- Identity in Web Services
- Liberty-based User-Centric Identity Demo
- More Examples
- Summary

Welcome to the Participation Age

Enterprise

Collaborative Industry Networks, Outsourcing, New Business Models

Developers

Java, Open Source, Standards Development

Consumers

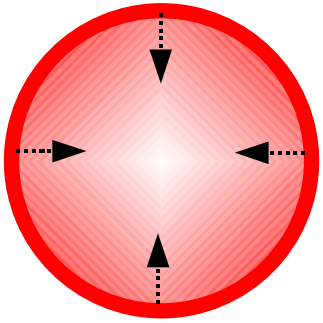
Blogs, Instant Messaging, Personalized Content on Devices, Social and Job Networking, Online Gaming

Public Sector

Inter-Agency Collaboration, Healthcare Networks, Political Campaigning, International Coalitions

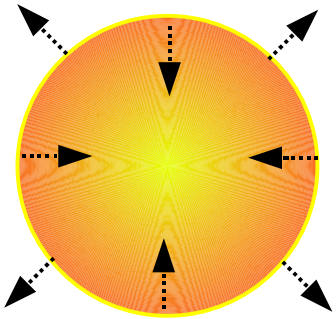
Can Identity Keep Up with Distributed Applications?

- Perimeters are dissolving
- Access is any time, anywhere, through any device
- We need security, control, manageability, privacy, scalability, and accountability



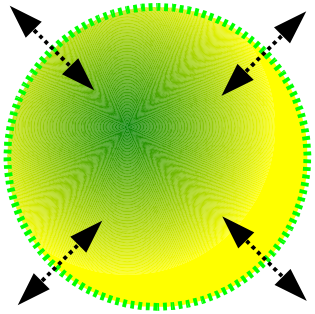
The Era of the Firewall

Keep data inside the firewall



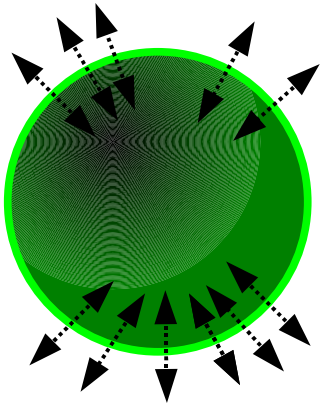
The Era of the Intranet/Internet

Manage data inside and outside the firewall



The Era of the Extranet

Manage data through the firewall

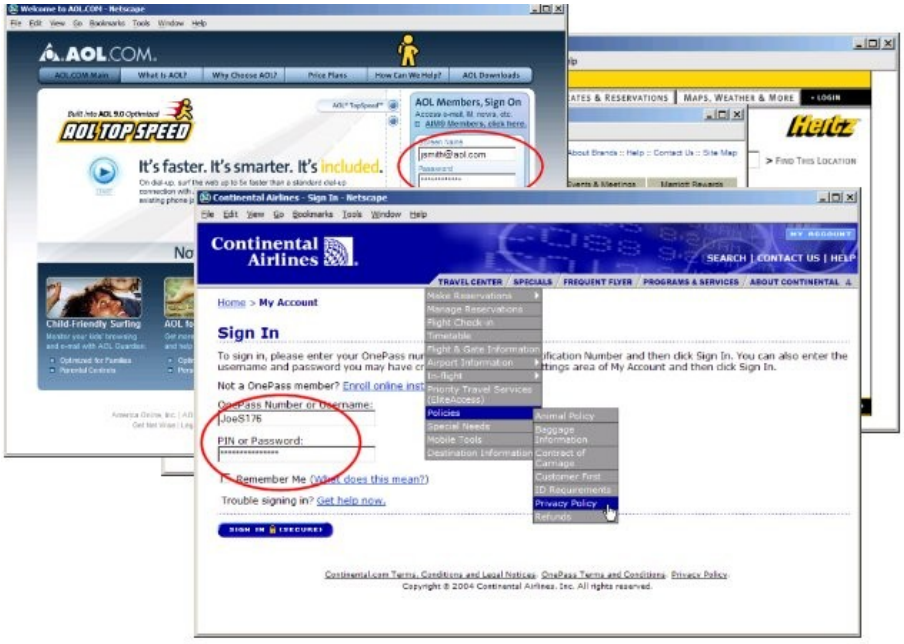


Nothing But Net

Just access and entitlement

Issues with Digital Identity Today

- Users have a proliferation of logins and passwords
- Redundantly stored attributes get out of synchronization
- Security, privacy, trust, and cost are concerns
- When identity is not as “distributed” as the applications that need to use it, business opportunities are missed



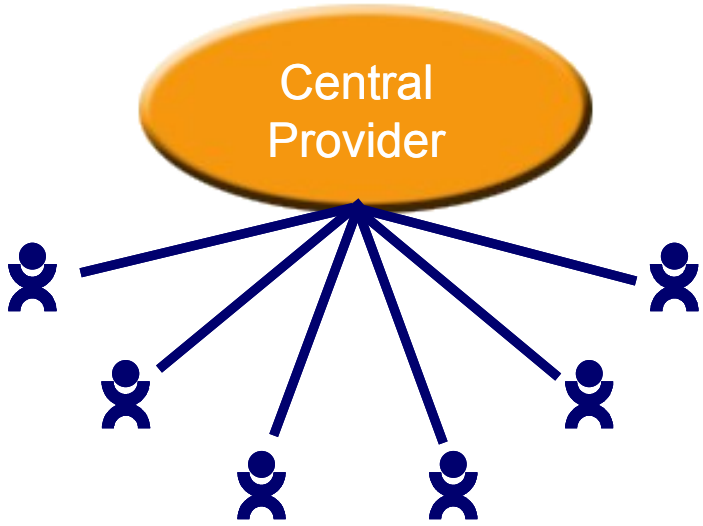
Why Federation?

- People have lots of unconnected identities
- Problems affect lots of Internet applications:
  - Consumer (portal providers, wireless operators, websites)
  - Intranet (students accessing library resources)
  - Extranet (between trading partners, or between employees and benefit administration sites)
- Need to be able to connect together these identity islands

Models of Connection

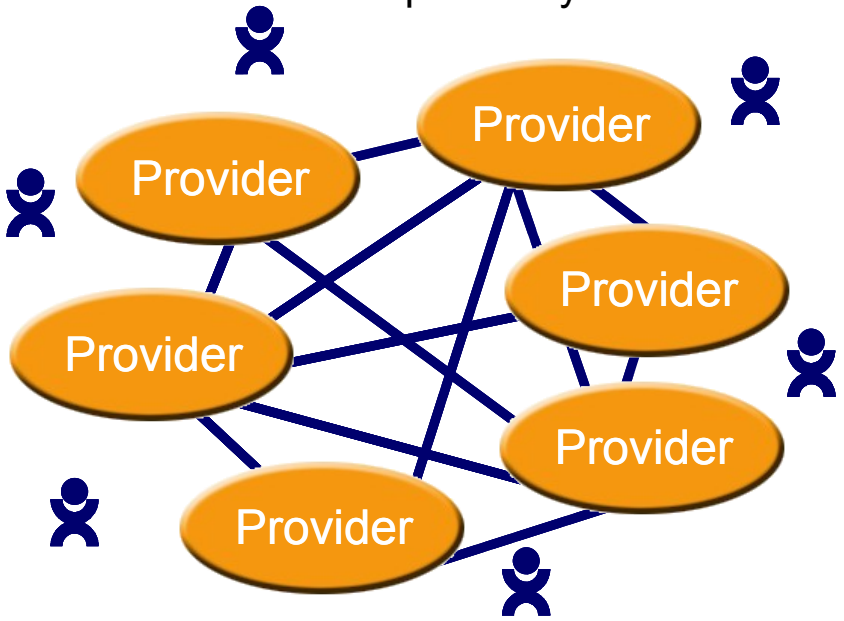
Centralized Model

- Network identity and user information in single repository
- Centralized control
- Single point of failure
- Links similar systems

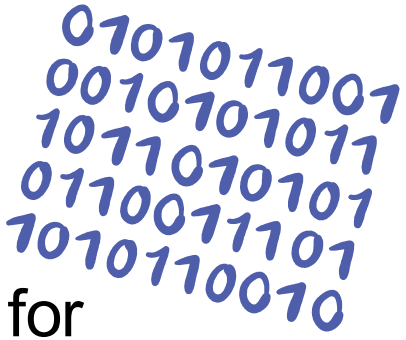


Open Federated Model

- Network identity and user information in various locations
- No centralized control
- No single point of failure
- Links similar and disparate systems

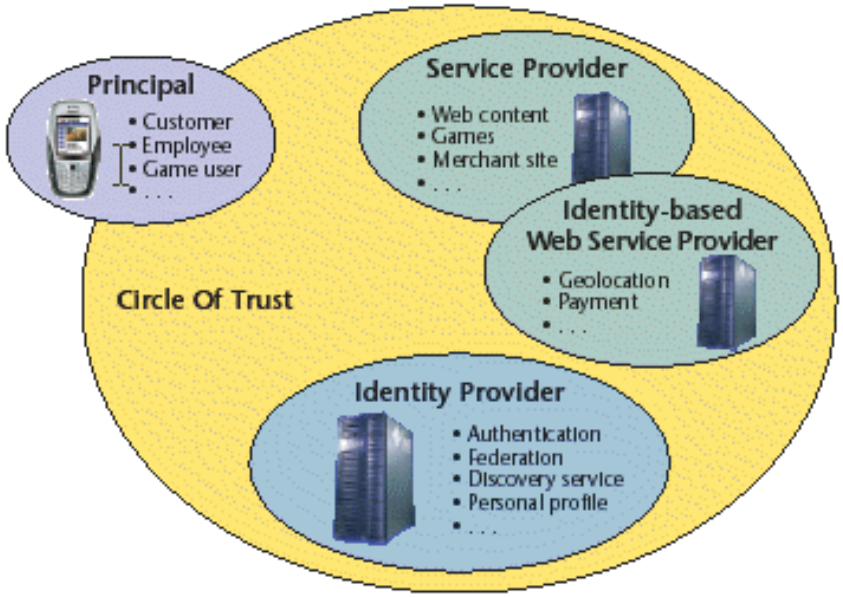


Requirements for Federated Identity



- Standard **formats** for identity information
  - Able to represent all existing authentication and attribute technologies
- Standard, secure, privacy-enabled **protocols** for exchanging identity information between components of distributed applications
  - Technology-neutral, well-specified, and interoperable
- A way to set up **trust relationships** between entities that share identity information
  - Within technical, business, and legal frameworks

Key Terms



- **Principal** – a person or "user", a system entity whose identity can be authenticated
- **IdP** – Identity Provider – a service which authenticates and asserts a Principal's identity
- **SP** – Service Provider
- **Federation** – The act of establishing a relationship between two entities, an association comprising any number of Service Providers and Identity Providers
- **Single Sign-On (SSO)** – the Principal's ability to authenticate with one system entity (Identity Provider) and have that authentication honored by other system entities, often Service Providers

Key Terms (cont.)

- **Circle of Trust** – a group of service providers and identity providers that have business relationships based on Liberty architecture and operational agreements and with whom users can transact business in a secure and apparently seamless environment.
- **Pseudonyms** are arbitrary names assigned by the identity or service provider to identify a Principal to a given relying party so that the name has meaning only in the context of the relationship between the relying parties.
  - Example: student logging into University Library – the Library may only need to know the person is a student to grant access, not the name or other identifying details
- **Anonymity** enables a service to request certain attributes without needing to know the user's identity. For example, in order to provide personalized weather information to a user, a weather service provider can ask for a user's zip code using anonymous service request without knowing the identity (even pseudonymous identity) of that user

Liberty Alliance

The Liberty Alliance is the only global body working to define and drive open technology standards, privacy advice, and business guidelines for digital identity interactions

150+ diverse member organizations:

- Government organizations
- End-user companies
- System integrators
- Software and hardware vendors

Liberty Alliance Activities

- Technical Specifications and Implementation Guidelines, guided by Use Cases
- Interoperability conformance testing – required before specs are published
- Business guidelines, deployment guidelines, and case studies
- Policy guidelines
- Developer resources and User Groups
- Adoption and evangelism
- Liaison and collaboration with other organizations (e.g., OASIS and Internet 2 for SAML)

SSO/Federation Demo

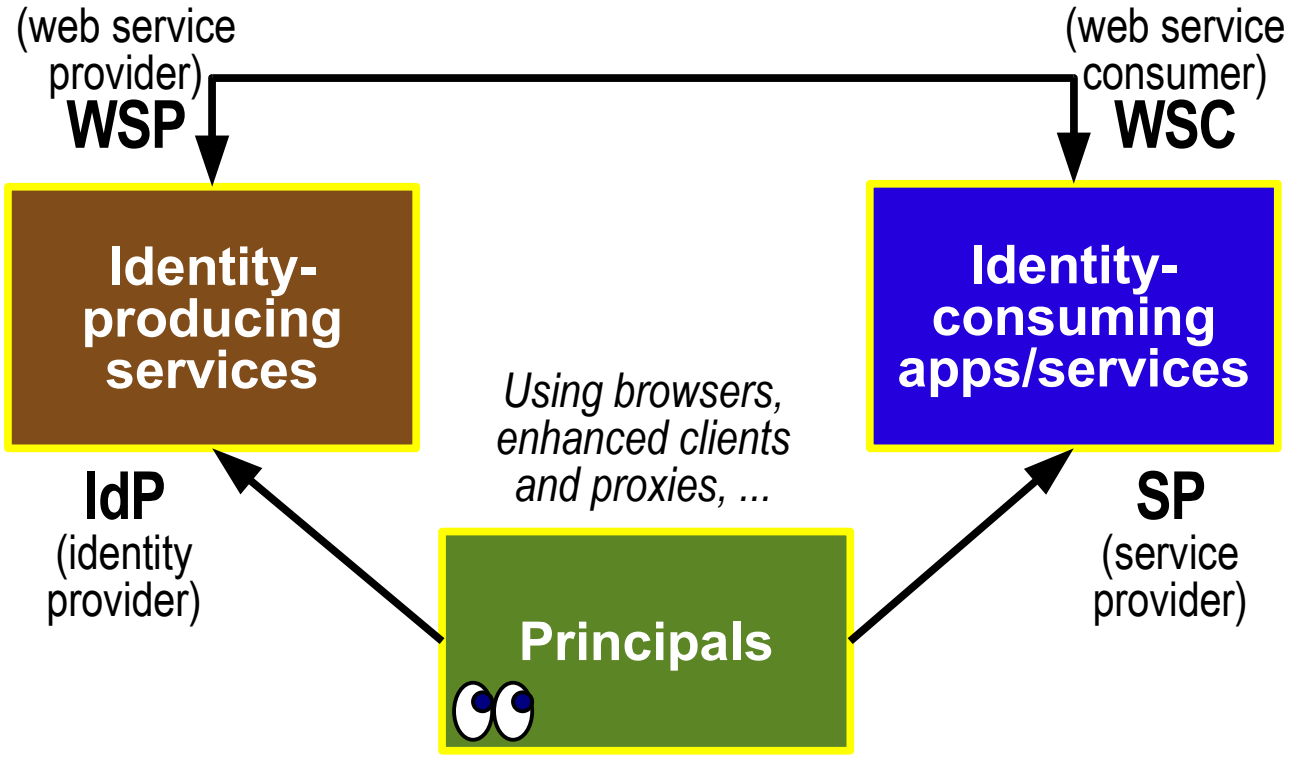
Illustrates Single (sometimes better to call it Simplified) Sign-On with Liberty protocols

See http://blogs.sun.com/roller/resources/superpat/FederationManagerLibertySSODemo_viewlet_swf.html

http://blogs.sun.com/roller/resources/superpat/FederationMa

What's Happening?

- Terminology comes from SAML and Liberty



Some Federation/SSO Use Cases

- Parent checking child's timetable
- Delegating ability to file income tax return
- Government employee access to external service
- Sub-contractor access to parts of government intranet
  - e.g., road builder needs to apply for road closure

Common Uses for Federated Identity

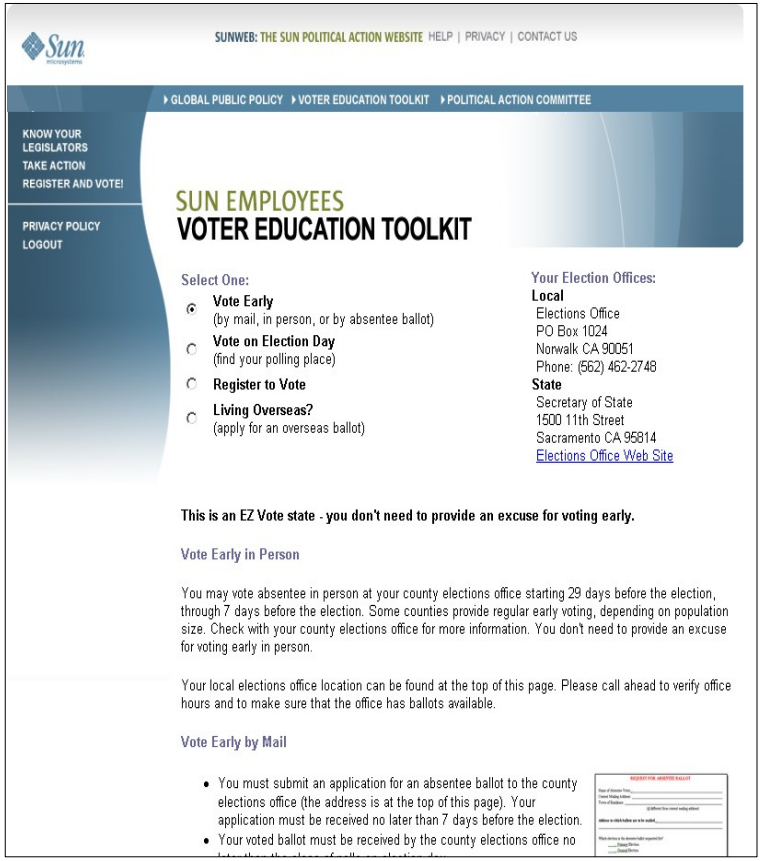
- Employee-facing applications that have been outsourced
- Circle of Trust – free flow for customers between related websites
- Partner/Supplier facing applications-leverage partner/supplier as IDP
- Government mandated “separate” environments
- Internal, “hard to consolidate” environments

Some Deployments

- Norway's Education Sector – implementing identity management with SAML 2.0 http://www.feide.no/index.en.html
- BIPAC/Sun – implemented Liberty specifications for US-based Sun employee anonymous access to BIPAC resources
- Norwegian government citizen portal to enable citizens to reach services such as applying for health card or driver license, apply for child support, calendar service for important dates, ... http://www.projectliberty.org/resources/presentations/myPage_
- Financial services vendors such as American Express and Fidelity Investments
- Fuller list of deployments at http://www.projectliberty.org/about/marketadoption.php

BIPAC Deployment

- Example: US Public Policy application provided by BIPAC
- General Content – candidates, legislation related to Sun's business, voting assistance
- Restricted Content – PAC Contributions
- Before Liberty – biz barriers from data-sharing concerns



Liberty solved key business issues related to authentication and PII!

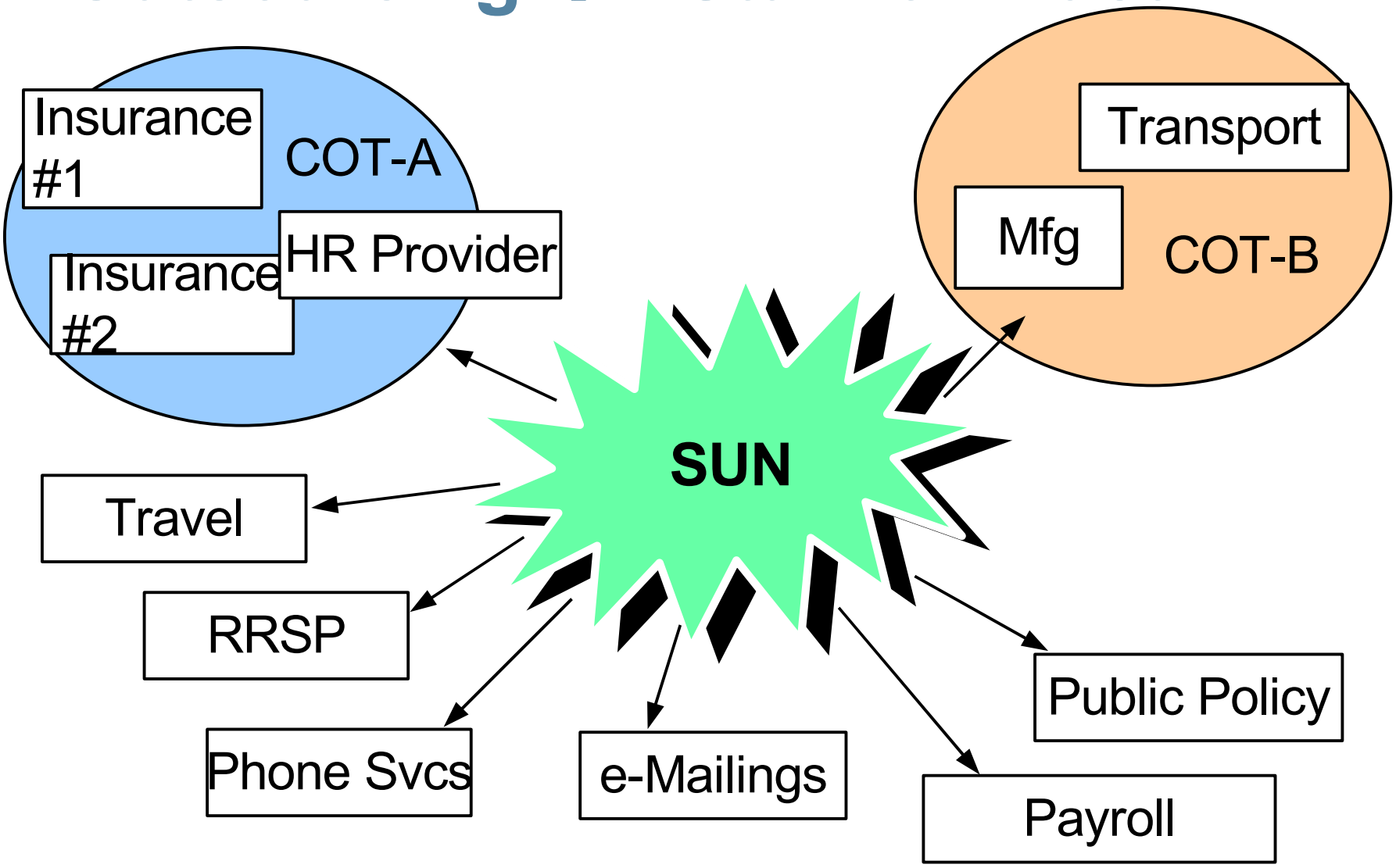
Implementing BIPAC Deployment

- Good first deployment – no personally identifiable information transferred
- Less sensitive than several outsourced operations
- Issues around account creation
  - Self registration – not as easy for users, and they might use internal IDs and passwords
  - Bulk registration – do this initially offline and eventually replace with Liberty provisioning, easiest for users
- Issues around account deletion, if user leaves company
  - Keep account? Remove account? Answer depends...
- Issues around logout
  - Should all sessions be terminated if user logs out of intranet?
  - Should there be a global logout button?
  - No one correct answer, need to discuss options

Other Issues to Think About

- Where to put privacy notices about moving to the SP site
  - For many cases, such as enterprise, no consent form necessary
  - Bulk registration means no registration page
  - IdP has the login page, not the SP, with SSO
  - Good solution is to put a link on the SP site
- SP monitors SP infrastructure
- IdP monitors IdP infrastructure
- Support
  - Users may forget SP IDs and passwords
  - Need system to help with that if non-SSO login ability required
  - Needs to be anonymous in this case

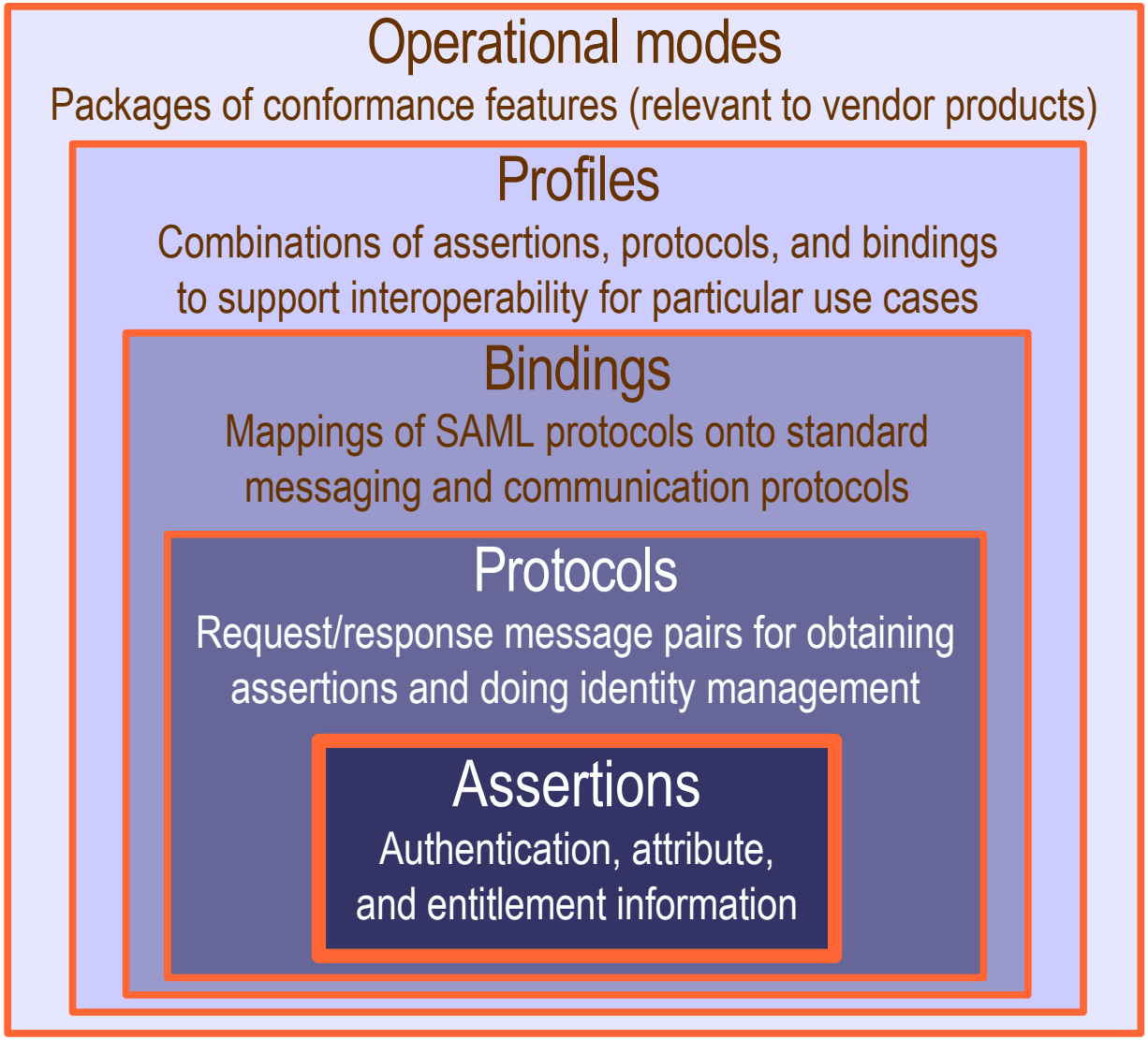
Outsourcing → "Star" of Trust



A Little Bit of Technical Stuff

- What are the underpinnings to all this?
- **SAML –** Security Assertion Markup Language
- Other related standards include
  - **XML Signature:** fine-grained data origin authentication
  - **XML Encryption:** fine-grained confidentiality
  - **XKMS:** key management
  - **XACML:** authorization policy expression and evaluation
  - **WS-Security:** end-to-end secure SOAP messaging
    - Uses security tokens of various types, including SAML

SAML Components



Authentication context
Detailed data on types and strengths of authentication

Metadata
Configuration data for assertion-exchanging parties

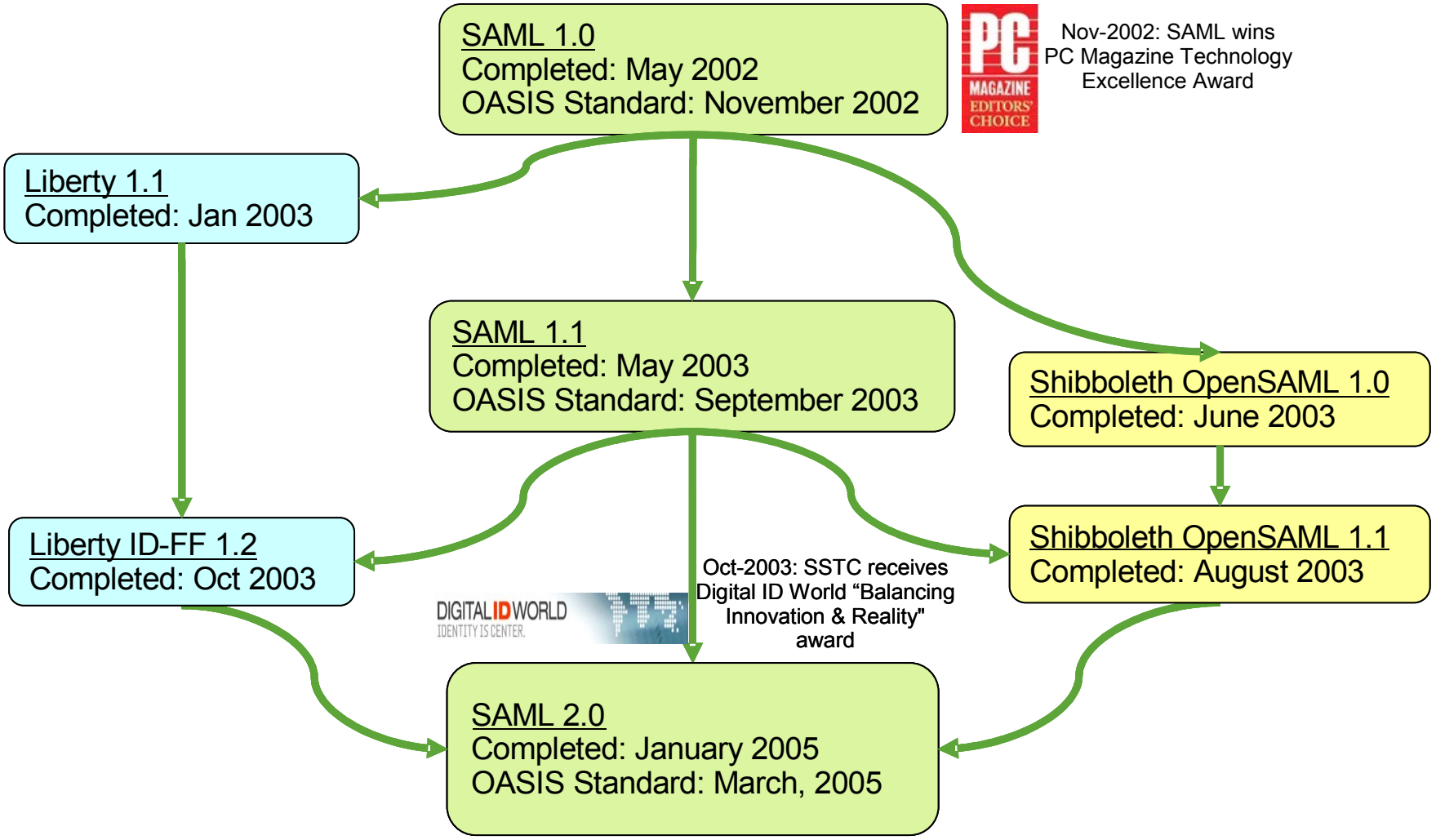
SAML Assertions (the core)

- An **assertion** is a declaration of fact (according to someone)
- SAML assertions contain one or more statements about a subject:
  - Authentication statement: **"Sam authenticated with a smartcard PKI certificate at 9:07am today"**
  - Attribute statement (which itself can contain multiple attributes): **"Sam is a faculty member in the department of Physics"**
  - Authorization decision statement (now deprecated)
  - Your own customized statements...
- Assertions can be digitally signed

SAML Protocols

- Go hand-in-hand with assertions
- Agreement which assertions are needed
- Agreement how they're defined in the message
- Definitions of things such as
  - Logout
  - Authentication request
  - Assertion query
  - Name identifier
- The SOAP Binding defines how the message is communicated (usually SOAP or HTTP)

Where did SAML Come From?



Shibboleth

- An umbrella of activities around federated authentication and access management managed by Internet2 and its international partners
- Includes specifications (currently based on SAML 1.1) and software/APIs
- Moving towards SAML 2.0 for both specifications and software (OpenSAML), both expected this year
- Added useful concepts to SAML 2
  - Pseudonymity
- Can be used by itself
- Often used in multi-federation scenario
- Level of formalism and trust may vary according to needs of SP

Identity Services

- A service that presents external interface to some aspect of my online identity
- Typically exposed as a SOAP-based web service
- Allows for greater control of my identity by reducing duplication throughout the network
- Increases privacy because fewer personal information items are released, e.g.:
  - An “Inbox” service might allow me to receive "permission-based" marketing without releasing my email address
  - A “Payment” service would allow payments to be made without releasing my credit card number

User-Centric Identity Service Demo

Shows how Liberty protocols can be used in products shipping today to solve identity issues in a way that incorporates user control and user consent.

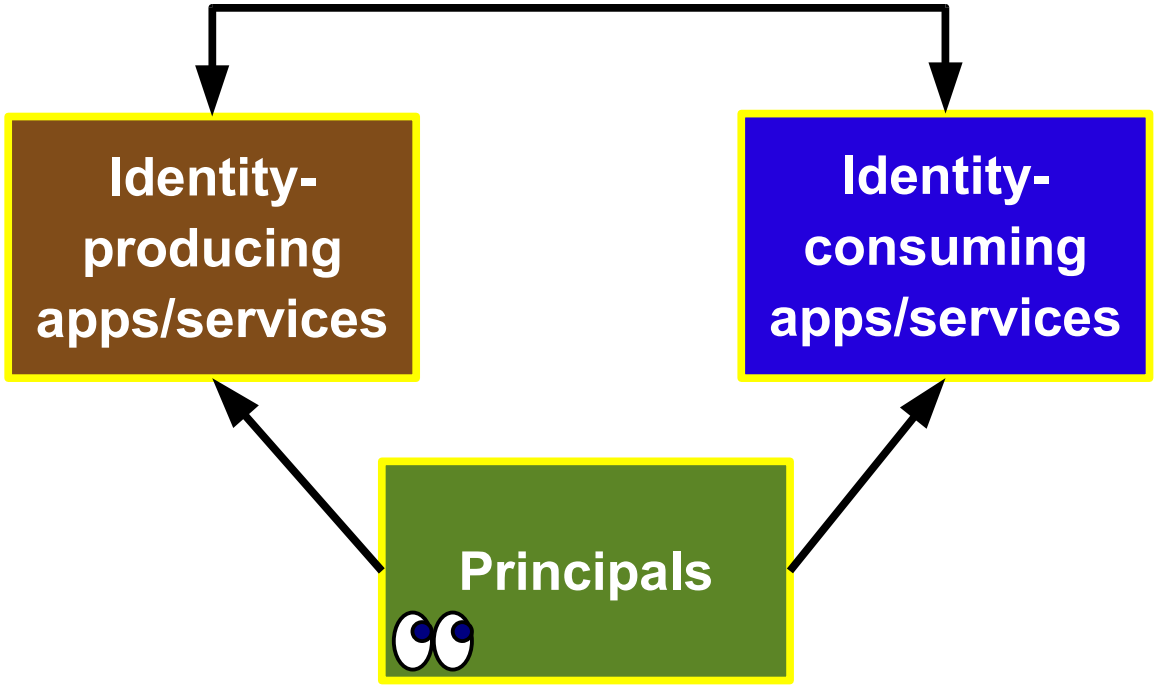
See http://blogs.sun.com/roller/resources/hubertsblog/LotD_viewlet_swf.html

http://blogs.sun.com/roller/resources/hubertsblog/LotD_

Identity in Web Services

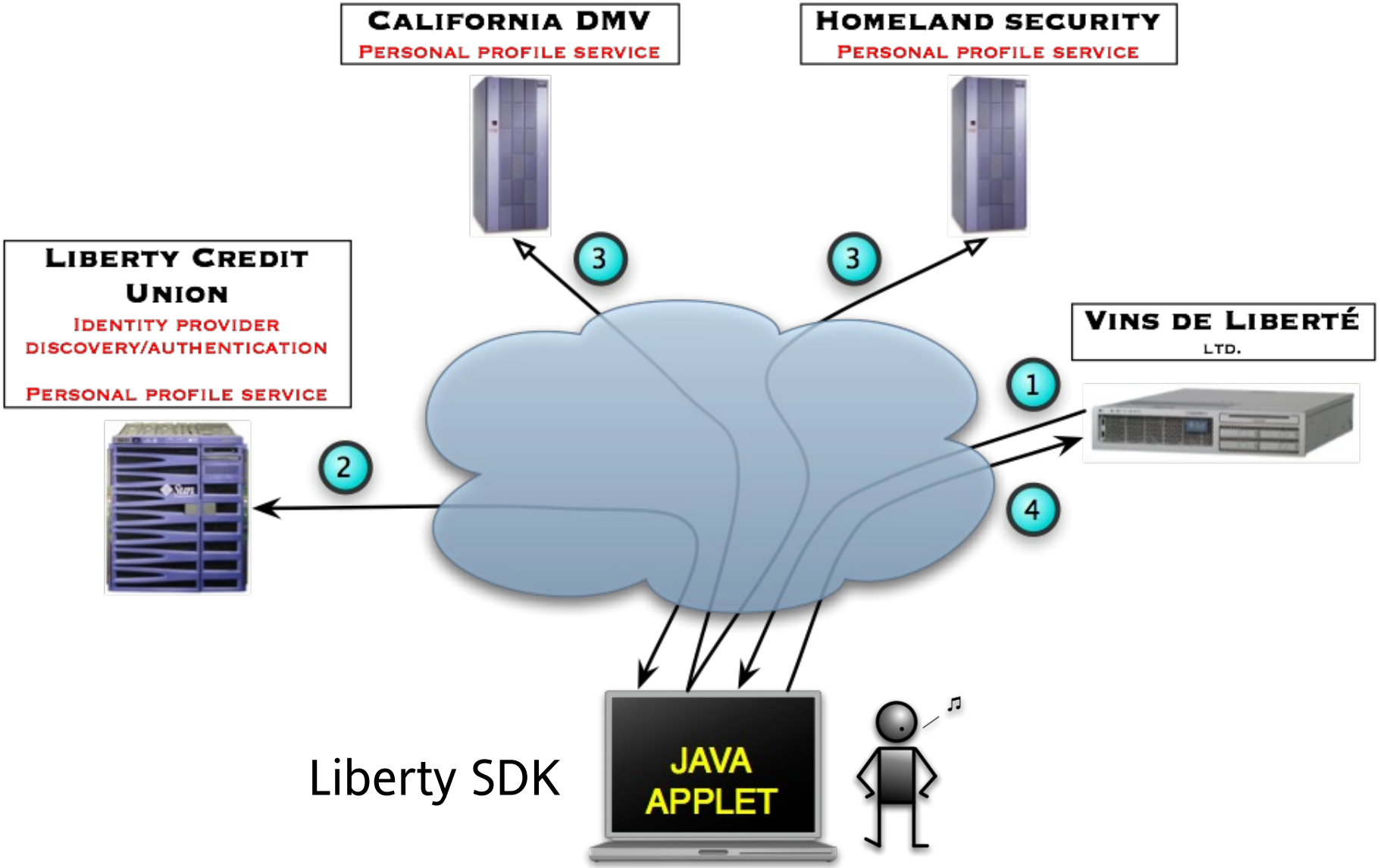
Identity Web Services Framework
- > Focused on application/application interaction

Service Interface Specifications
- > Define specific identity-based services



SAML 2.0
- > Focused on human/application interaction
- > Authentication basis

Overview



Liberty SDK

Simple for the Service Provider

- The Applet could be a well known platform extension
- The Service Provider (SP) only needs to specify the requested data

```
<applet name="bridge" archive="dist/LibertyApplet.jar"
  code="com/sun/research/liberty/LibertyBridge.class" width="1"
  height="1">
    <param name="ClickURL" value="ConfirmAddress.html" />
    <param name="Attributes" value="legalname, age" />
</applet>
```

Benefits to the User

The user is in control

- Controls what data is provided to SP
- Controls who provides that data
- The user's interaction with IdP/Discovery Service is local to the desktop
- The Service Provider only gets the information the user choses to supply

Benefits for the Service Provider

- Obtains reliable data
- Reassure the customer about privacy issues
- Form-filling is an efficient way to minimize the impact on existing deployments
  - Since the applet has the data it can fill out the form automatically
  - SP doesn't have the data it doesn't need – helps with privacy concerns
  - The SP does not need to care as much about the underlying framework being used

Services Used

- Authentication Service
  - Authenticates Principals and provides appropriate credentials for accessing systems (analogous to IdP in ID-FF)
  - Uses SAML to communicate identity information
- Discovery Service
  - Registry for Identity-based services (e.g., find the bank)
  - Web service providers register the services they provide (may be multiple providers)
- Data Services Template
  - Provides an extensible framework to produce new Identity-based Services above the protocol stack, allowing interoperability
  - Defines guidelines, common XML attributes and data types to build different services

Other Interesting Services

- Geo-location
  - identify a person's location, at the user's request, to provide services like weather, news
- Presence
  - share presence information, such as whether the user is online, offline, on the phone or in a meeting
- People
  - allows individuals to store, maintain, and categorize online relationships
- Contact Book
  - allows a Principal to manage contacts for private and business acquaintances, friends, family members

Some Deployments of Identity Web Services

Finland Board of Taxes

Created Identity Provider (IDP) for on-line tax payment and management of official documents. The initial phase is serving 2.6 million citizens.

http://www.projectliberty.org/about/adoption_egov.php

- **Requirements gathering was finished in May 2005**
- **Call for tenders in June 2005**
- **Selected supplier in August 2005**
- **Project started in September 2005**
- **Phase I, November 2005**
  - SAML 2.0 WebSSO
  - ID-WSF
- **Phase II, January 2006**
  - IDP and authorization
- **Phase III, February 2006**
  - Federation

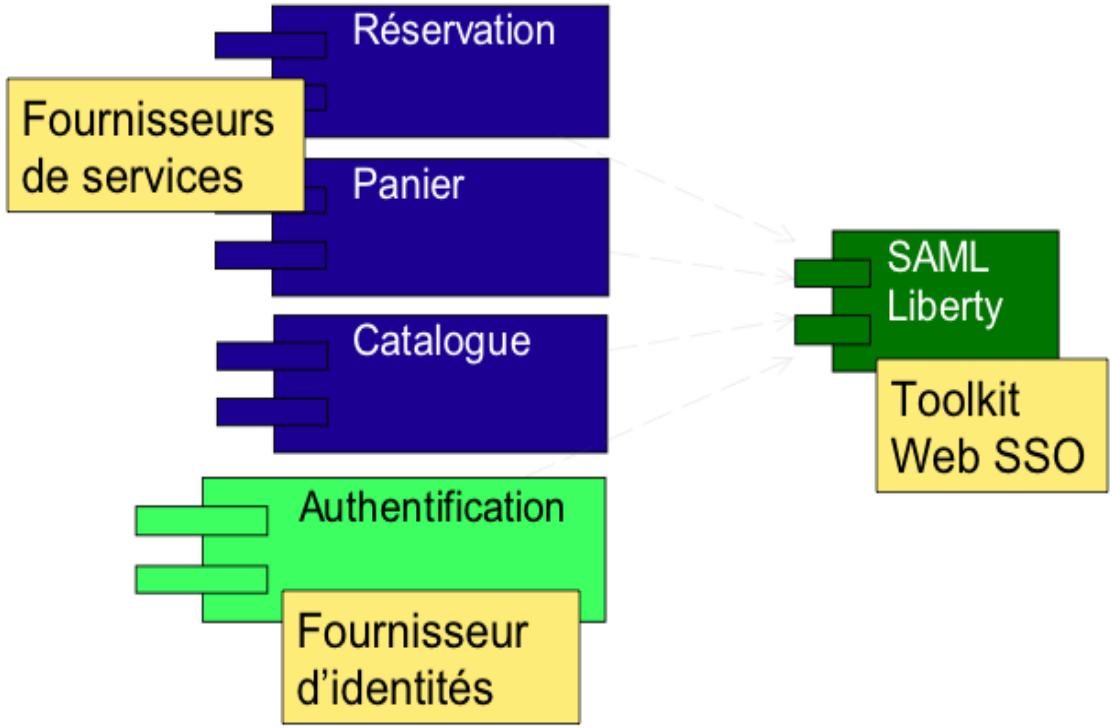
Benefits

- **E-services enables significant cost savings**
  - Every transaction made in office costs 20 – 50 euros and an e-transaction 10 – 50 euro cents
- **Simplified processes**
  - Reduced 5 phases on e-filing
- **New possibilities to arrange e-services**
  - E.g. e-filing straight from Pay-roll –system instead of Tax portal web site
- **Life-cycle management (e.g. changes in management, users, mergers etc.)**
- **Reliable roles and authorization (audit-trail)**

French National Library

Library account management and authorization. The project is serving 20,000 accounts and 6,000 authorizations per day.

http://www.projectliberty.org/about/adoption_egov.php



Deployment (4 man months):

- 3 developers
- 2 test engineers
- 2 system engineers
- 2 architects

Summary

- Liberty specifications are being widely deployed to meet business needs for identity management in a secure way that takes into account the need for privacy
- Increasing amounts of information available to help people implement and deploy the systems they need to meet their particular needs
- Most identity management vendors now support SAML 2.0
- An increasing number of vendor products support various other Liberty specifications
- Convergence between Shibboleth and SAML 2.0 is good news for the education community

Resources

- Liberty tutorial at http://projectliberty.org/resources/LibertyTechnologyTutorial.pdf
- Flash version of SSO demo at http://blogs.sun.com/roller/resources/superpat/FederationManagerLibertySSODemo_viewlet_swf.html
- Flash version of user-centric Liberty demo at http://blogs.sun.com/roller/resources/hubertsblog/LotD_viewlet_swf.html
- Info on Shibboleth at http://shibboleth.internet2.edu/ and http://www.opensaml.org
- Liberty Alliance Deployment list at http://www.projectliberty.org/about/marketadoption.php
- BIPAC deployment: see http://www.idealliance.org/proceedings/xml05/abstracts/paper154.HT
- Federation concepts: http://www.xmlgrrl.com/maler-fed-id/maler-fed-id-notes-5jan2006.pdf

QUESTIONS?

Lauren Wood
lauren.wood@sun.com