The Role of Federation in Identity Management

August 19, 2008

Andrew Latham
Solutions Architect – Identity Management

The Role of Federation in Identity Management

Agenda

- Federation Backgrounder
- Federation in Identity Management
- OpenSSO
- CAUDIT

By 2009, outsourced application hosting services and SaaS providers that do not support identity federation will lose at least 25% of their business to service providers that do support federation.

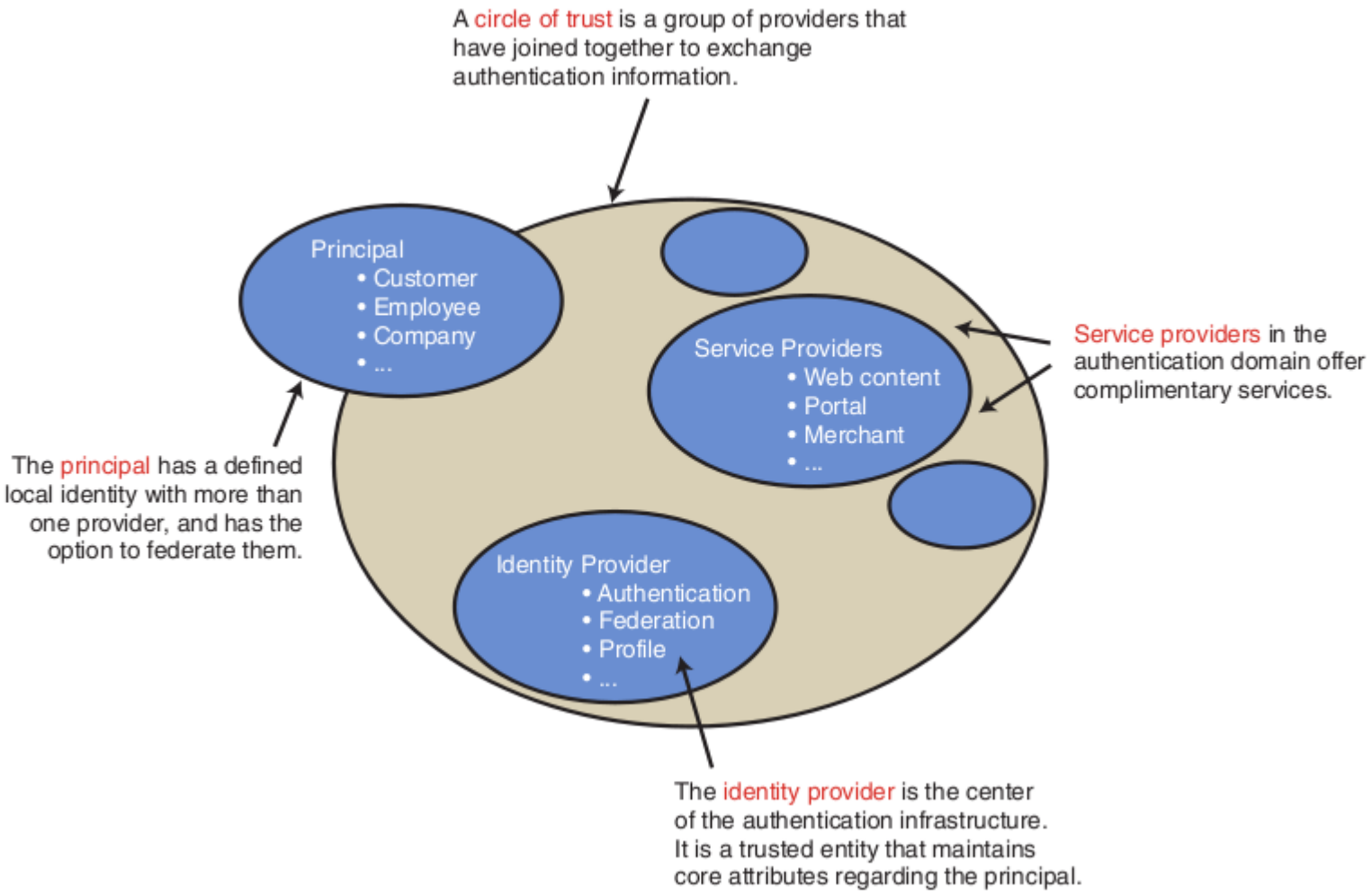
Gartner Predicts 2008: Mobility and Outsourcing are Changing Secure Business Enablement

Federation Backgrounder

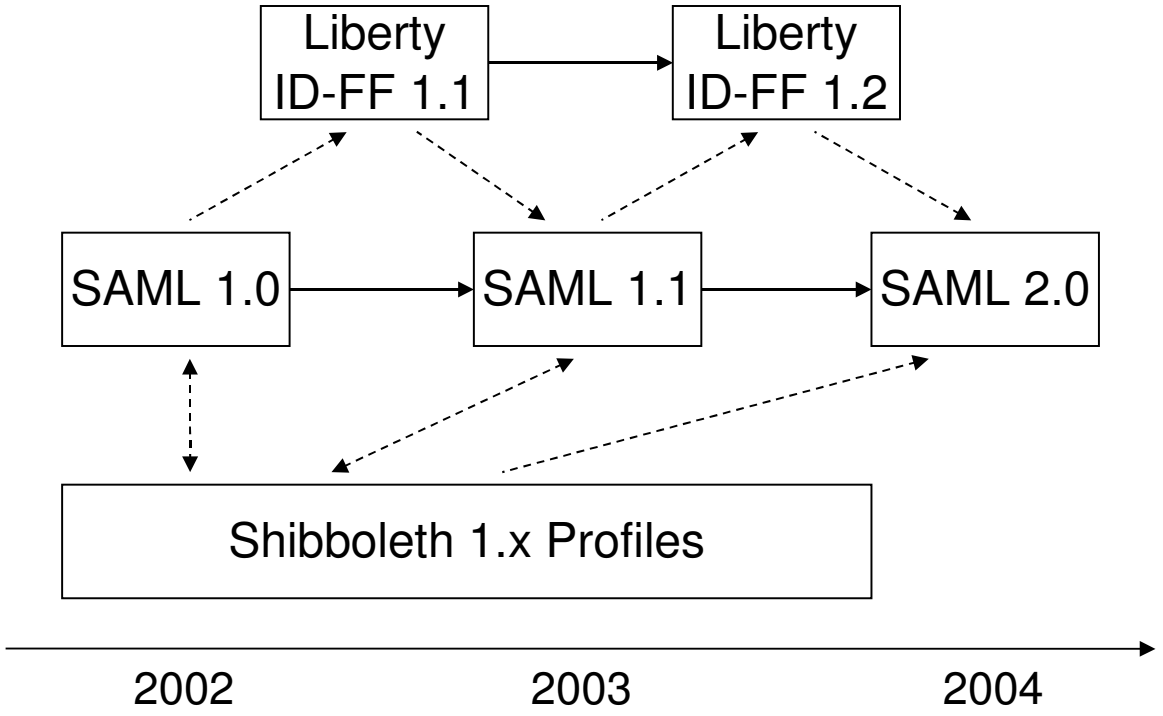
Everybody Knows Your Name

- An integrated technology and trust model where a user's authenticated identity is asserted across security boundaries.
- With respect to the systems participating in the federated infrastructure, “everybody knows your name.”

Circles of Trust



Federation Evolution



SAML

- SAML has become the standard protocol for building federated systems.
- SAML assertions are the building blocks for loosely coupled systems, supporting the passing of secure messages between trusted parties without a need to understand the internal details of each organization.
- Include information about identity, authority,status of keys, and policy claims

Shibboleth

- Help higher education institutions comply with the Family Educational Rights and Privacy Act of 1974 (FERPA). FERPA is a federal law that protects student's education records.
- Emphases access control based on the exchange of user attributes
- Shibboleth enables user privacy (users can control which information is released—in particular, their permanent identity), and supports fine-grained access policies.
- Uses SAML as a foundation for its XML-based messaging framework in support of identity assertions.

Project Liberty

- Each federated domain maps its local identity and security interfaces and formats to the agreed-upon identity-federation standards, **without need to divulge sensitive user or customer data externally**.
- Interoperating domains choose to honor each other's security decisions and trust each other's security assertions, but **always within the context of their respective local policies**.

Project Liberty

- Specifications for federated identity management, single sign-on (SSO), account linking, and global logout in online e-business environments.
- Membership in the Alliance, now more than 170, continues to expand, and includes many end-user organizations, which is unusual in the standards development process.

Comparison of Approaches

- **Liberty** - A user passes identity to the target, and then worries about the target's privacy policy. To comply with privacy, targets have significant regulatory requirements. The user has no control, and no responsibility.
  - "we know who you are, albeit in two different but federated contexts"
- **Shibboleth** - Users release the attributes to the target that are appropriate and necessary. If the attributes are personally identifiable, the user decides whether to release them. The user has control, along with commensurate responsibility.
  - "we may not know who you are but we'll find out enough about you to make a policy decision"

OpenID

- Establishes trust “Like” SAML
- No prior arrangement required
- Not Enterprise-class - User-Centric
- Rapidly becoming the basis for low-assurance authentication on the Internet.
- Allows for noncoordinated growth of clients, providers, and RPs.
- RPs don’t need to establish trust relationships with providers in a coordinated fashion;

Federation in Identity Management

Interoperability Challenges

- Remembering separate passwords for every single application
- Authenticating users' identities across organizational boundaries (and often having to deal with multiple types of identity information for a single user in the process)
- The federated solution:
  - An SSO that provides access across applications in multiple domains
  - Portability of identity information across security domains
  - Leveraging of trust relationships to accept that a user has already been authenticated by a trusted partner

Information Security Challenges

- Applying security policies across multiple organizations
- Keeping private information private from a multitude of sources

- The federated solution:
  - A framework for interoperability in which a user is authenticated only once, but can be authorized as appropriate at the service provider
  - Implementation of the latest standards and technologies to provide sound security policies and strengthen authentication credentials,
  - Clear user control over which external partners can link to a company's identities, and what personal attributes are provided

Cost Control

- Managing identities on an unprecedented scale without incurring untenable infrastructure costs
- Reducing costs by making authentication and authorization portable and reusable across large provider networks in which identities may be owned by external partners

- The federated solution:
  - The ability to accept a trusted partner's authentication of a user's credentials, while efficiently mapping authorizations to those trusted credentials
  - Automation of identity management tasks to eliminate costs for manual processes

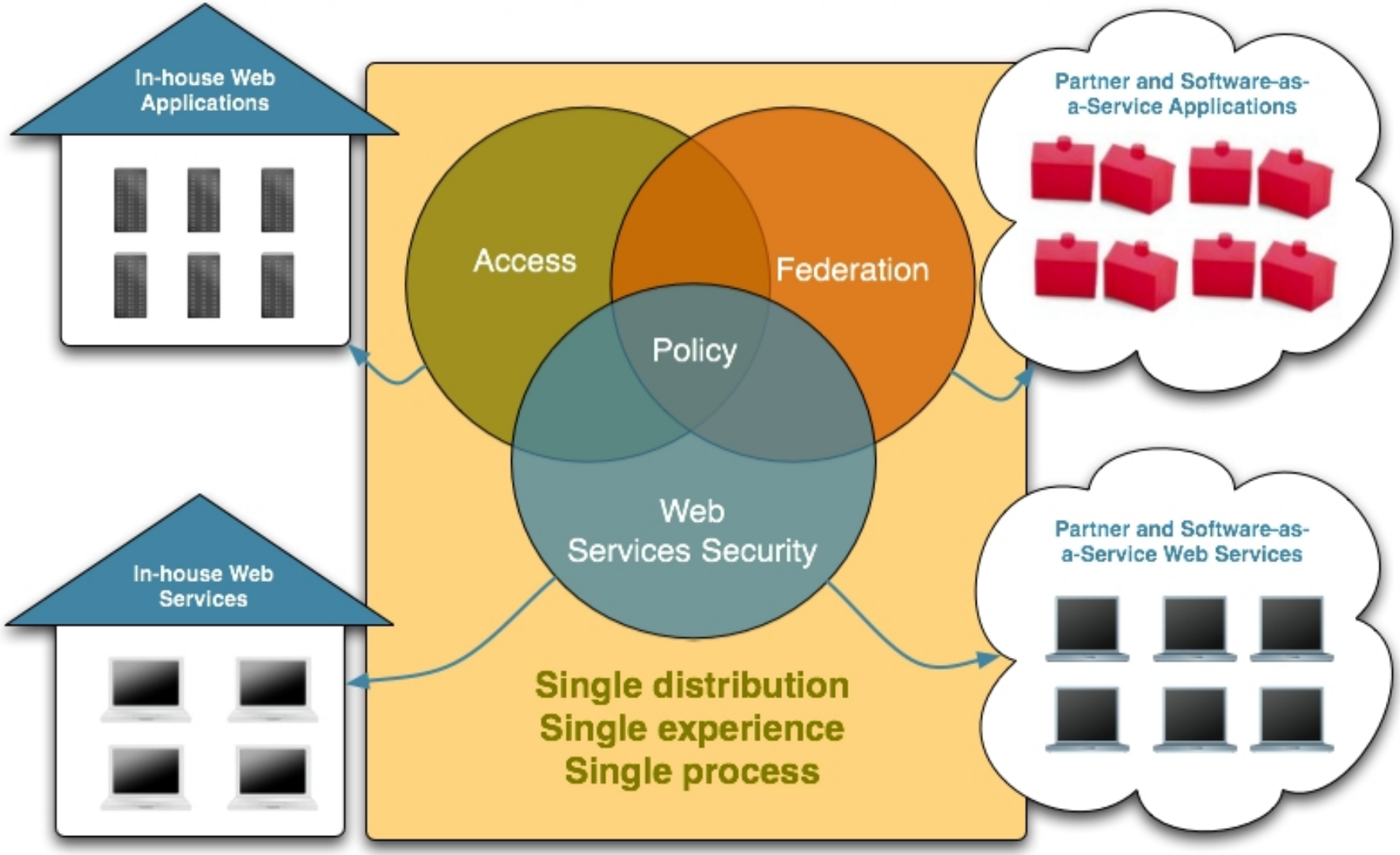
Quality of Service

- Streamlining navigation between internal applications and those hosted by partner
- Securely delivering new services to internal and external users
- The federated solution:
  - SSO for multiple applications hosted in multiple domains
  - Management and authentication of identities where they are owned, enabling new services to be introduced at an accelerated pace

OpenSSO

Sun Federated Access Manager

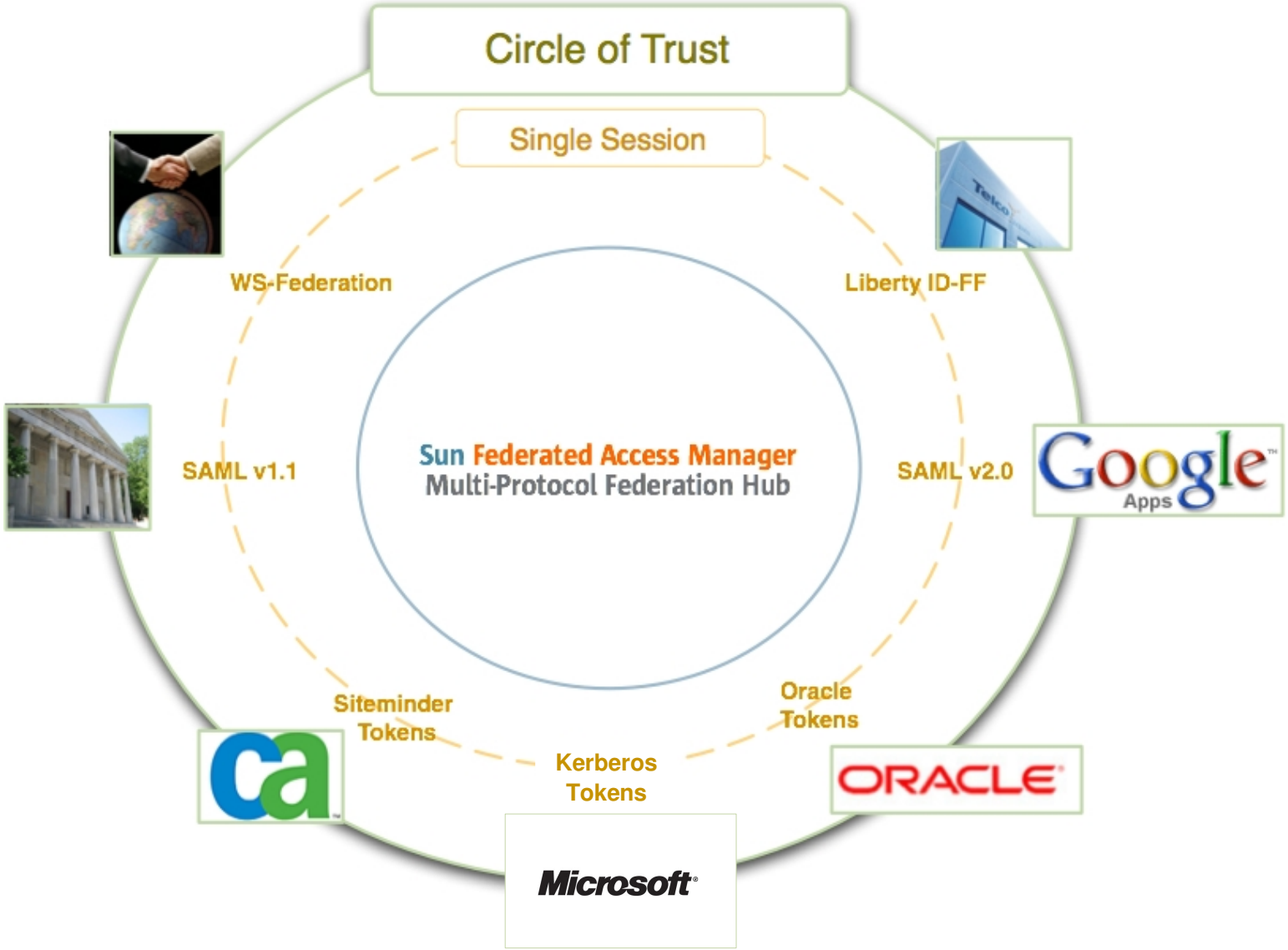
Extend Business Reach and Reduce Security Risk



What Makes OpenSSO Unique?

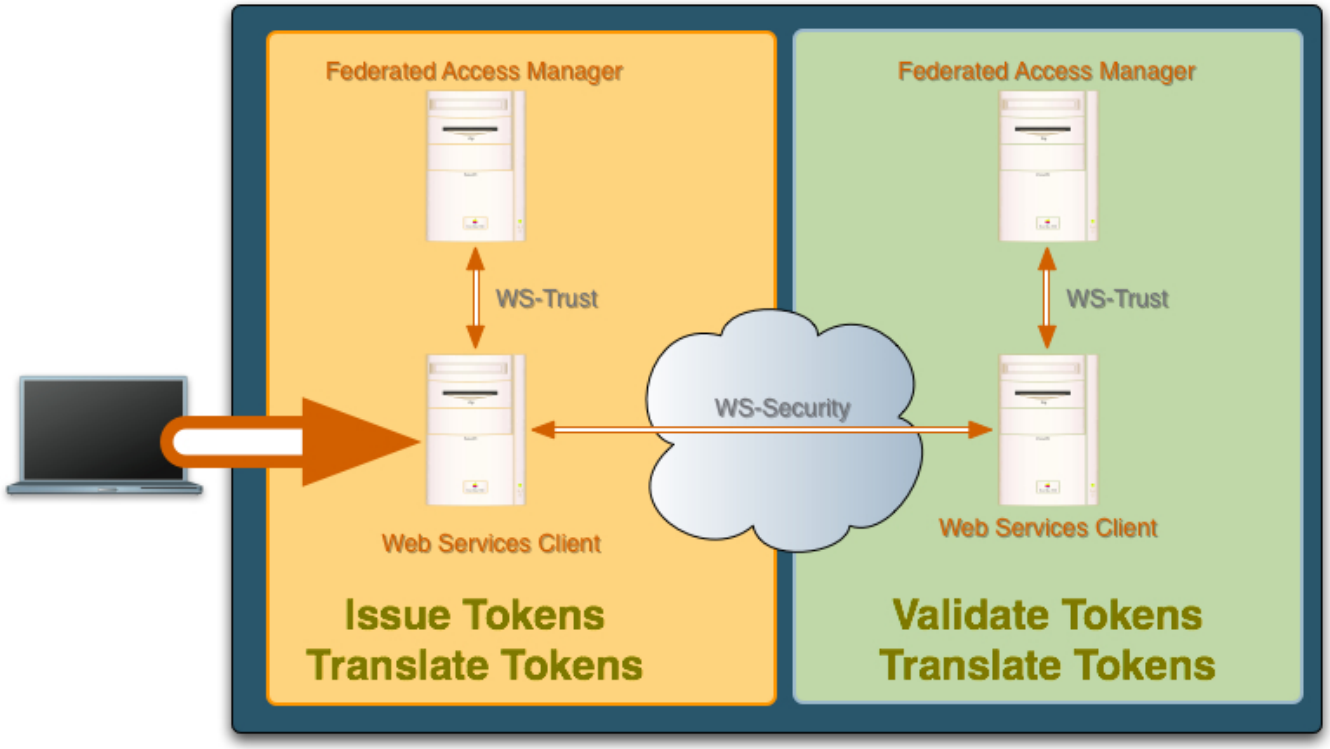
- 100% Java
- The Fedlet
- Virtual Federation
- Multi-Protocol Federation Hub
- Security Token Service
- Identity Services

Multi-Protocol Hub



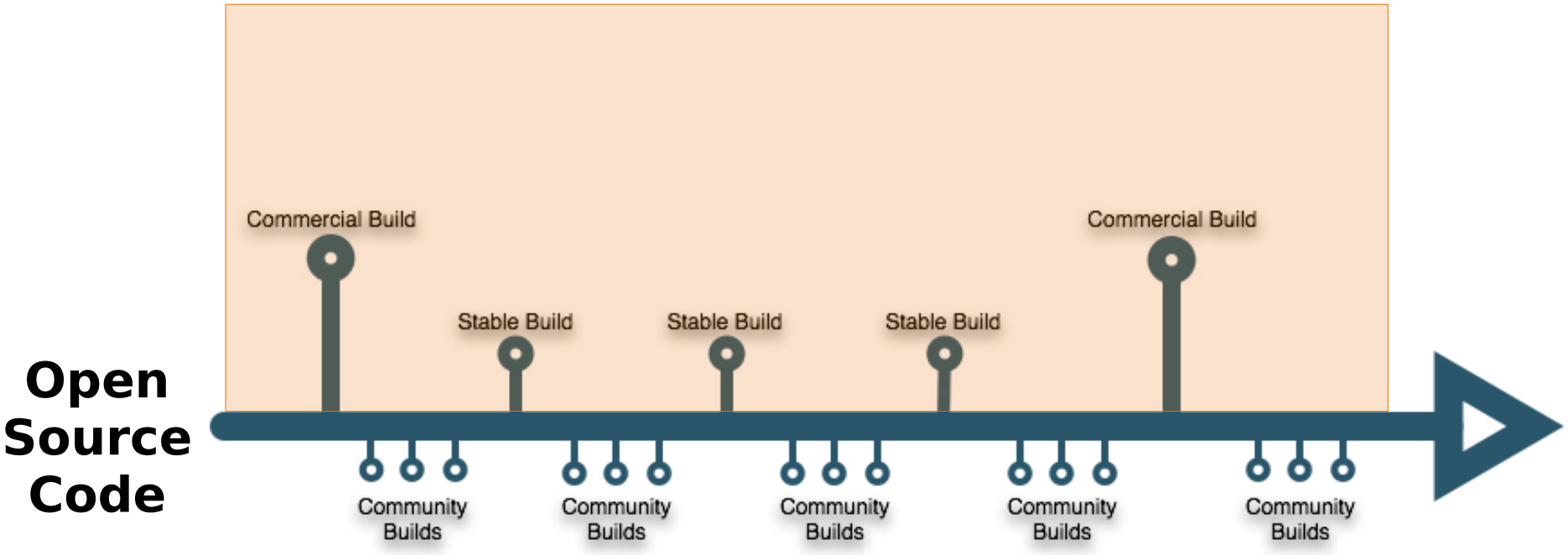
Security Token Service

Centralize Management & Translation of Web Service Tokens



Validate, issue and translate standards-based tokens and proprietary tokens including Oracle Access Manager & CA Siteminder tokens

New Model



New model supports commercial builds and stable builds. Customers will have ability to adopt new features upon availability.

OpenSSO Support Model:

How it Works

- Sun will issue patches and hot-fixes for Sun Access Manager commercial builds only.
- To receive a fix or enhancement for an OpenSSO Stable Build a customer must upgrade to the next stable build that contains that fix or enhancement.
- Sun will support the two most recent OpenSSO stable builds.
- Issues, bugs and/or RFEs are submitted via the same support channel as all other Sun products.

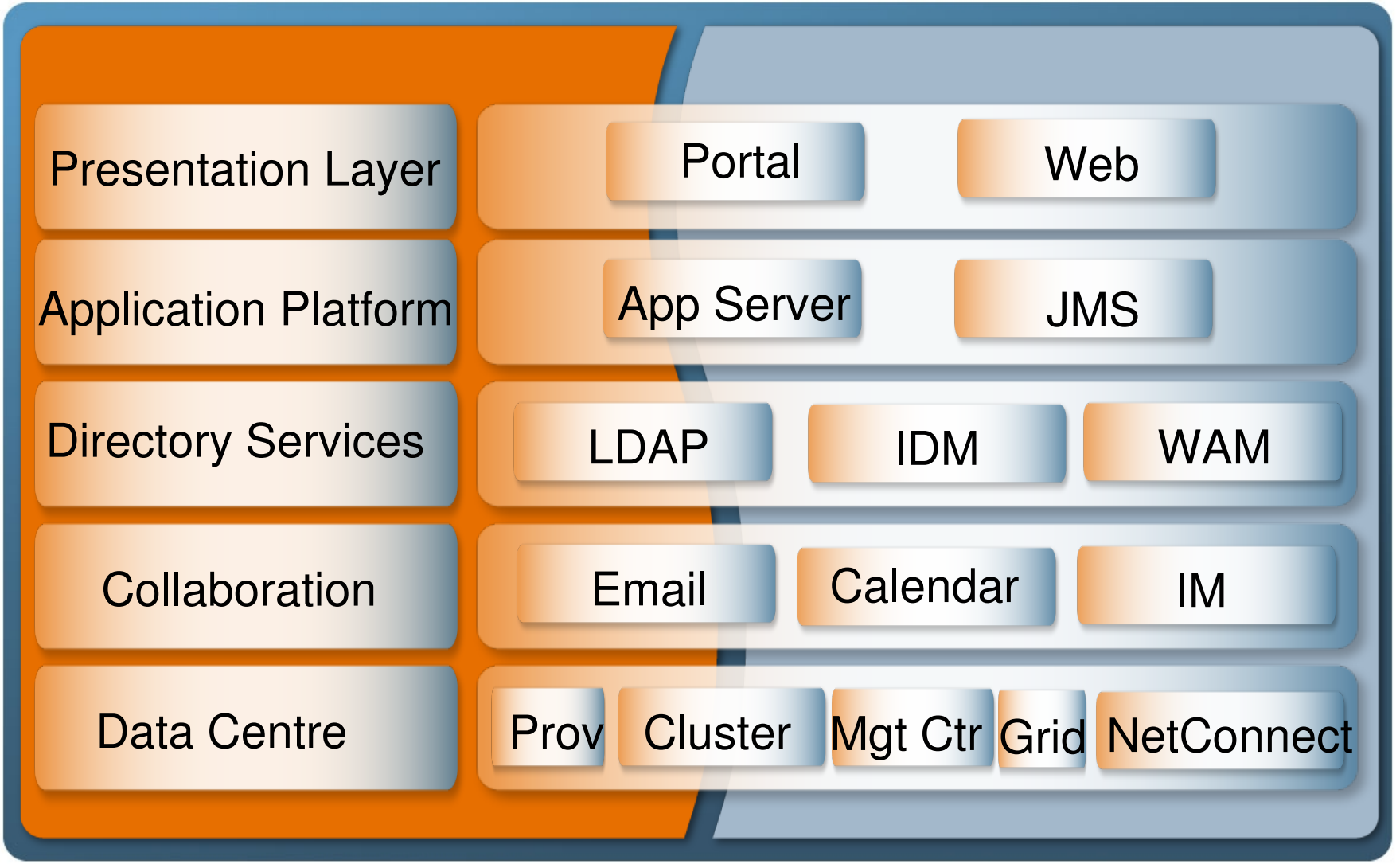
Learn More . . .

http://www.opensso.org

http://www.sun.com/identity/federation

CAUDIT

The Sun CAUDIT stack



Thank You

andrew.latham@sun.com