Identity opens the participation age

Open Web Single Sign-On und föderierte SSO

Dr. Rainer Eschrich

Program Manager Identity Management

Sun Microsystems GmbH

Agenda

- The Identity is the Network
- Driving Participation with Identity
- OpenSSO
- Federated SSO
- Q&A

The Online Participation Age

Universities

Collaborative Education Networks, Task Sharing, Research Networks

Developers

Java, Open Source, Standards Development

Students

Blogs, Instant Messaging, Personalized Content on Devices, Social and Study Networking, Online Learning

Government Services

Inter-Agency Collaboration, Library Networks, eGoverment, European Research Programs

Participation Realms

Campus Realm

Service & Control

Collaboration Realm

Share

Hurdles to Participation

Campus Realm

To uncomfortable

- Many services with many logins

Collaboration Realm

To uncomfortable

- Even more services force me to login

Privacy/Regulations

- Who controls the data

Sun Technologies enable Participation

Identity Services

Federated Technology

Open SSO

Federated SSO

Sun microsystems

OpenSS0

Open Source Web Single Sign-On

Dr. Rainer Eschrich

Business Program Manager

Identity Management Practice

What is OpenSSO

- An open source project for Web Single Sign On
- Based on Sun's Acess Manager Product
- Goal:

To Provide the community with a proven, reliable, scalable, standard solution for web based SSO to further adaption of SSO.

OpenSSO Details

- CDDL license: an MPL based, OSI approved license
- Providing source code for basic identity services including:
  - Authentication
  - Single-domain SSO
  - Web and J2EE agents
- Project site live today: http://openSSO.dev.java.net
- Early access code Q4, 2005

Federated SS0

SSO for the collaboration realm

Dr. Rainer Eschrich

Business Program Manager

Identity Management Practice

Driver Bologna Process:
Federated Access to Ressources

"Distributed teaching scenarios" is part of eBologna. Students from different places should be able to cooperate with each other (in distributed projects), to do research projects together (e.g. in Virtual Labs), to participate in special resources offered somewhere else (e.g. taking part in a special seminar offered by a well-know specialist at one of the other universities).

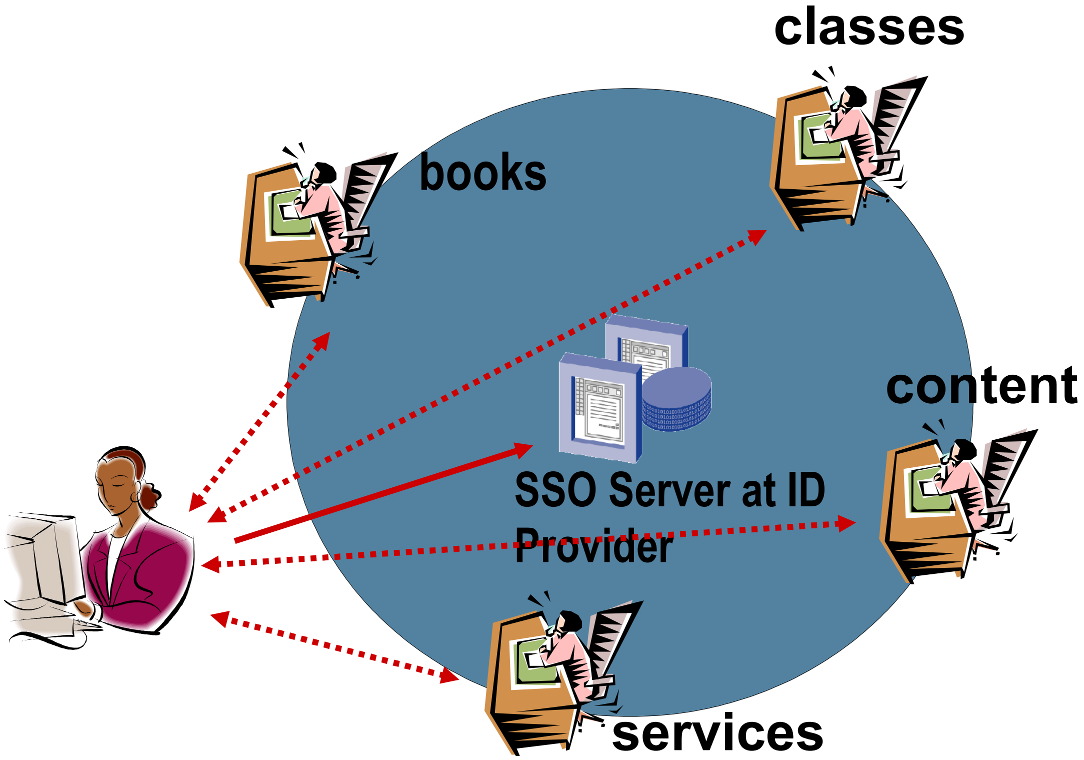
The cooperation should by characterized by "different levels of trusted partnership".

Technologically this is given by single-sign on infrastructures realized through portal technologies.

EU FP 6 Ausschreibung, Netlab

The federated identity model

Users connects to service provider and can access all services within the circle of trust.



User:

- must login only once

Universities & Agencies:

- have control over services & content

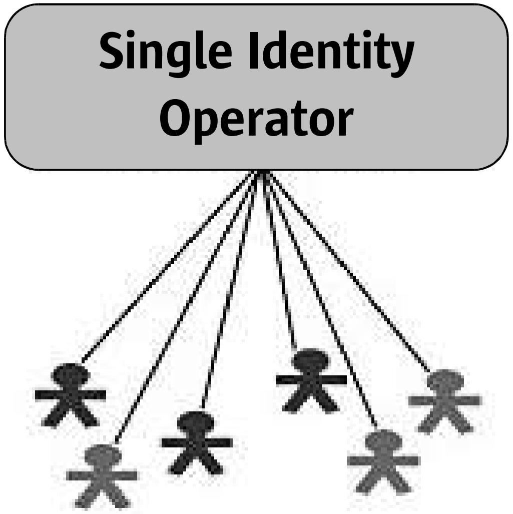
Federation Requirements

Federation Enables Sharing Identity Information Outside the Firewall While Protecting Privacy

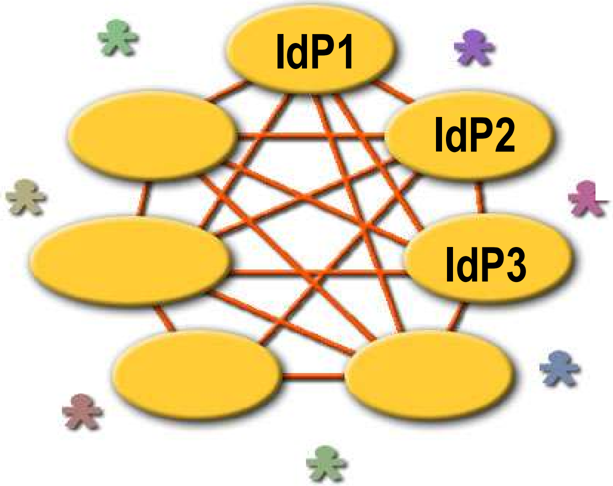
- Federation is necessitated by collaborative research and other inter-institution collaboration
- There are 3 implementation approaches:
  - **The Liberty Alliance Project** – An alliance of more than 150 companies, non-profit and government organizations developing an open standard for federated network identity (http://www.projectliberty.org/)
  - **Shibboleth** – An open source implementation of federated identity information that has gained a lot of momentum in education
  - **WS-F** (Part of WS-*)– A project of Microosft and IBM to create an open standard for federated network identity
- Shibboleth and Liberty are working on interoperability through SAML 2.0, expected in CY'06
- Microsoft & Sun are designing an interoperability framework, expected CY'06

Federation Models

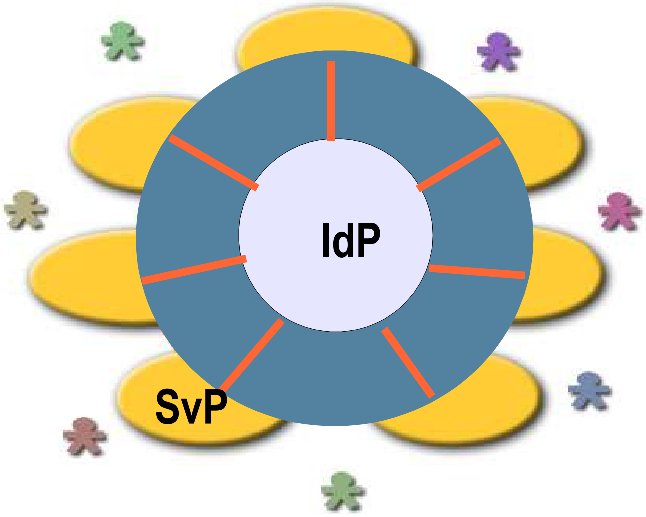
Centralised Model (Passport)



N2N Model (WS-F)



Circle of Trust Model (Liberty)



Liberty Alliance Summary

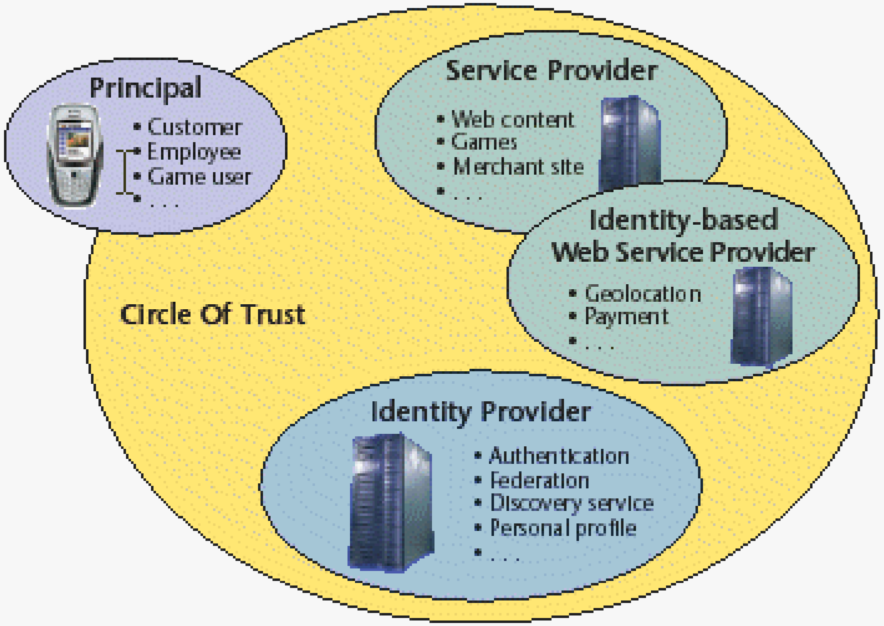
LIBERTY ALLIANCE PROJECT

Founded 2001

- Open group to address business and Public Policy issues:
  - Business guidelines
  - Privacy controls built into the specifications
  - Privacy & security best practices
  - Enable compliance with global privacy legislation and industry regulations (I.e. Article 29, HIPAA)
- Over 150 Members, Over 15 approved products
- Federated Identity and Web services enabling:
  - Interoperability between collaboration partners
  - Device and platform agnostic - Built on open standards
  - Unique conformance program for Identity Management products – more than 30 successful product tests to date
- Over 400 million Liberty enabled identities and services by year end
- Government Standard in France & Norway

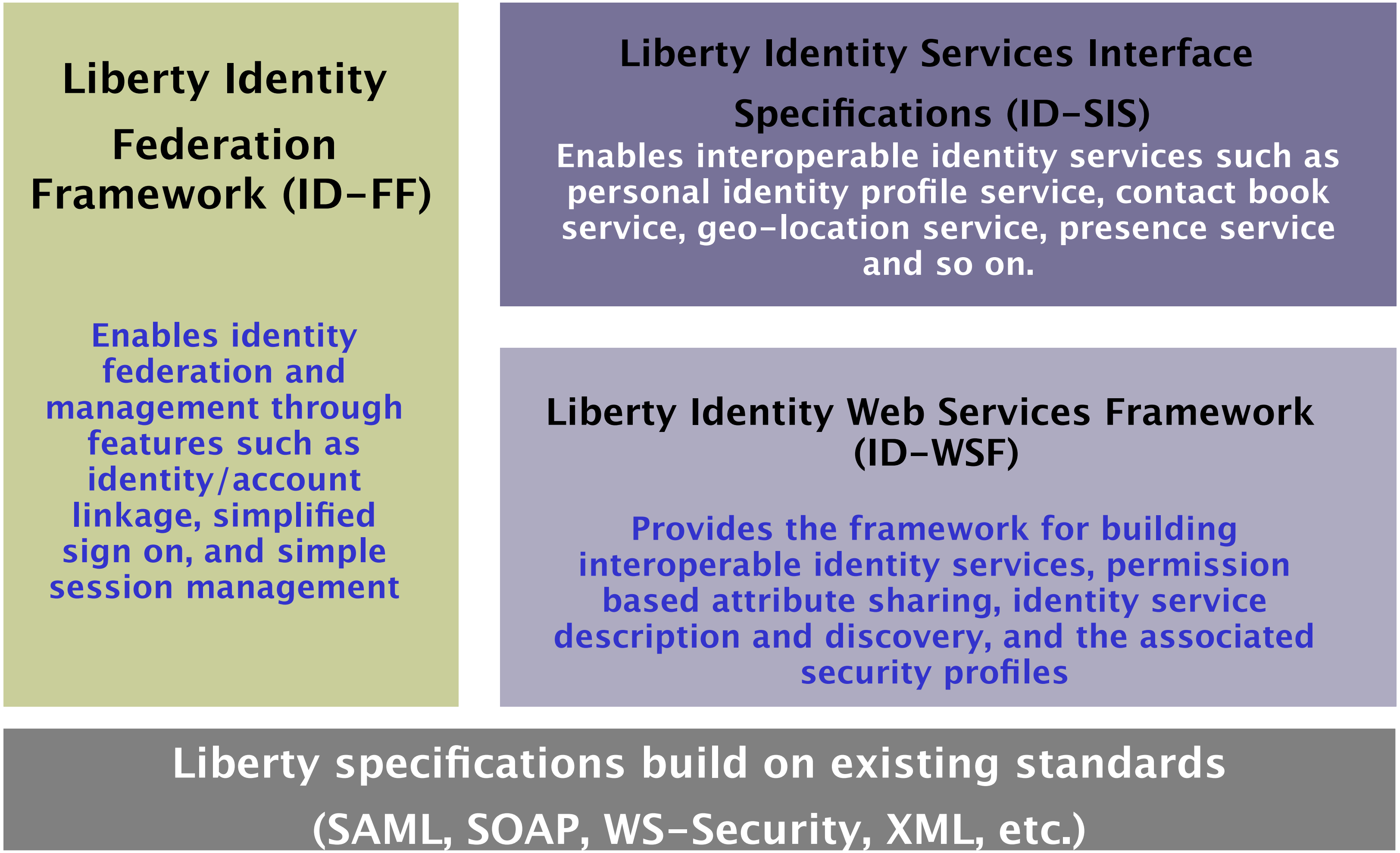
Key Concepts

- **Federation** – The act of establishing a relationship between two entities, an association comprising any number of Service Providers and Identity Providers
- **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
- **SdP,** Service Provider – a instance that needs to knwo abount the principals idenity to deliver services
- **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



Further definitions from the Glossary, found at:
http://www.projectliberty.org/specs/liberty-glossary-v1.3.pdf

Liberty’s Architecture



Liberty Identity Federation Framework (ID-FF)

Enables identity federation and management through features such as identity/account linkage, simplified sign on, and simple session management

Liberty Identity Services Interface Specifications (ID-SIS)

Enables interoperable identity services such as personal identity profile service, contact book service, geo-location service, presence service and so on.

Liberty Identity Web Services Framework (ID-WSF)

Provides the framework for building interoperable identity services, permission based attribute sharing, identity service description and discovery, and the associated security profiles

Liberty specifications build on existing standards

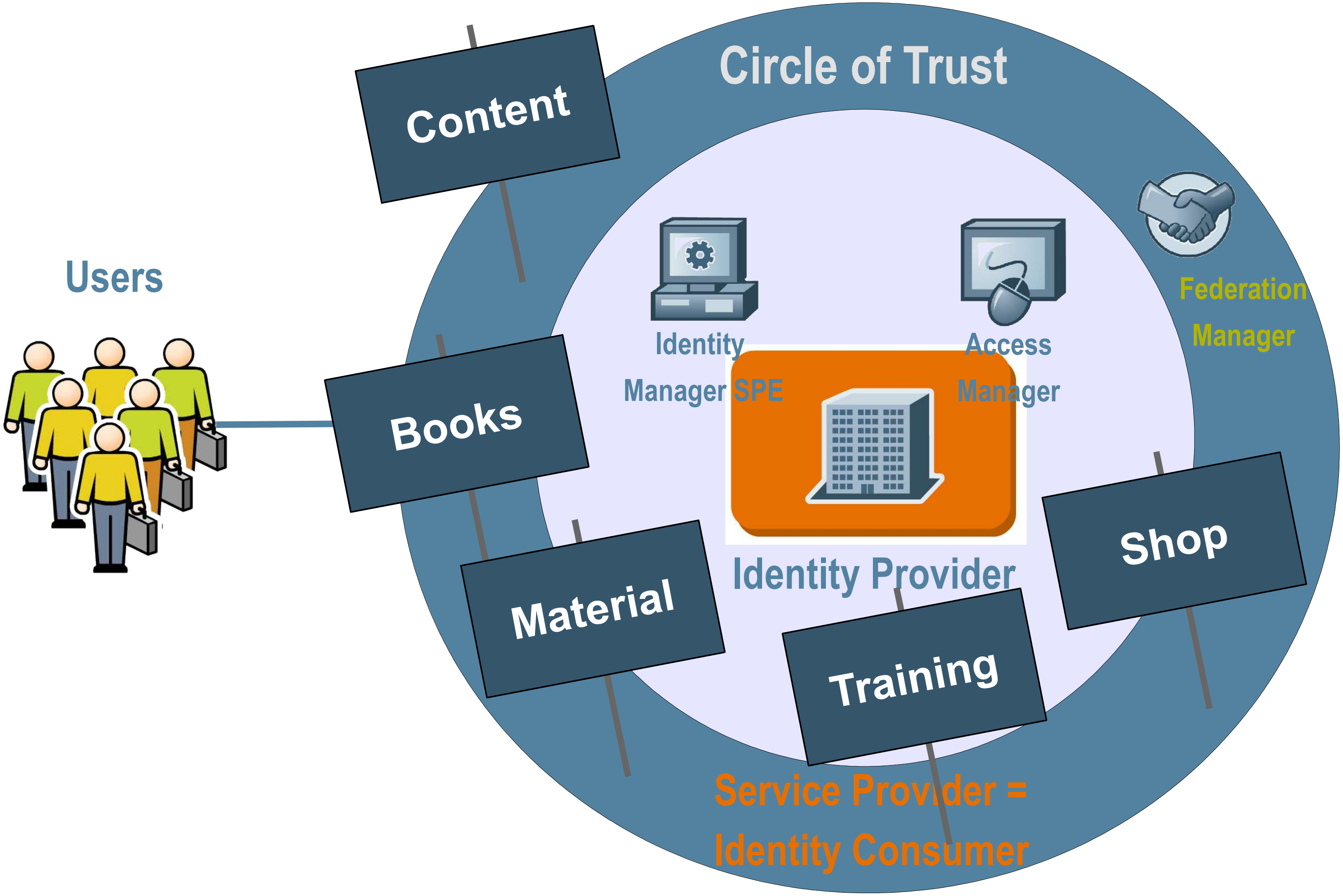
(SAML, SOAP, WS-Security, XML, etc.)

Sun's Leadership in Federation

- Catalyst for Liberty Alliance Project
  - Co-founder in Sept 2001
  - First to implement Liberty specifications in product
  - First to be have product certified as “Liberty Interoperable”
- Leader in development of SAML
  - OASIS SSTC Chair
  - Drove standards convergence of Liberty ID-FF 1.1 and SAML
  - Demonstrating leadership through SAML interop events
- Strong and ongoing investment and executive commitment throughout company

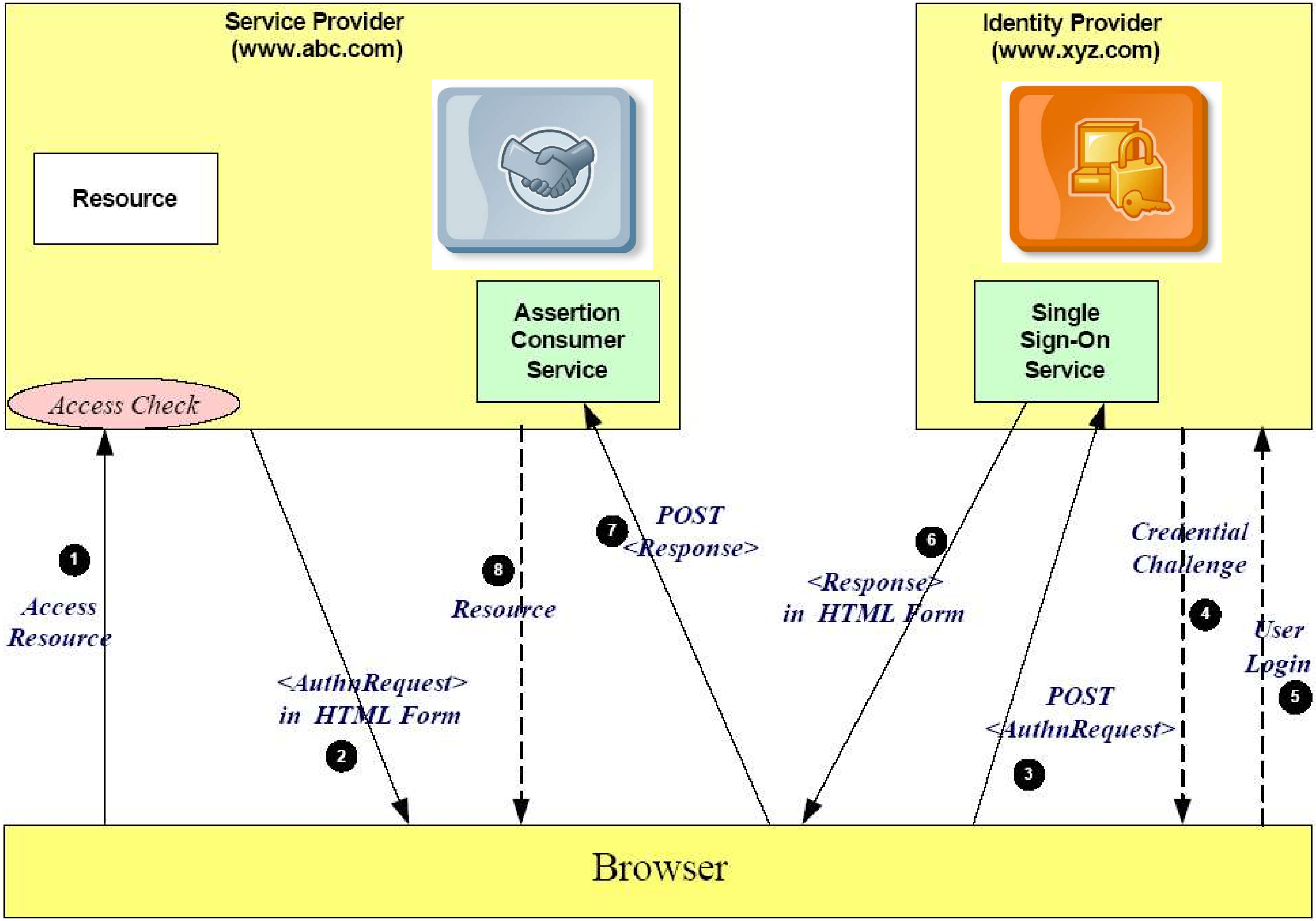
Sun's Federated Technology

Aligning participants for the participation age



Liberty Web Single-Sign-On

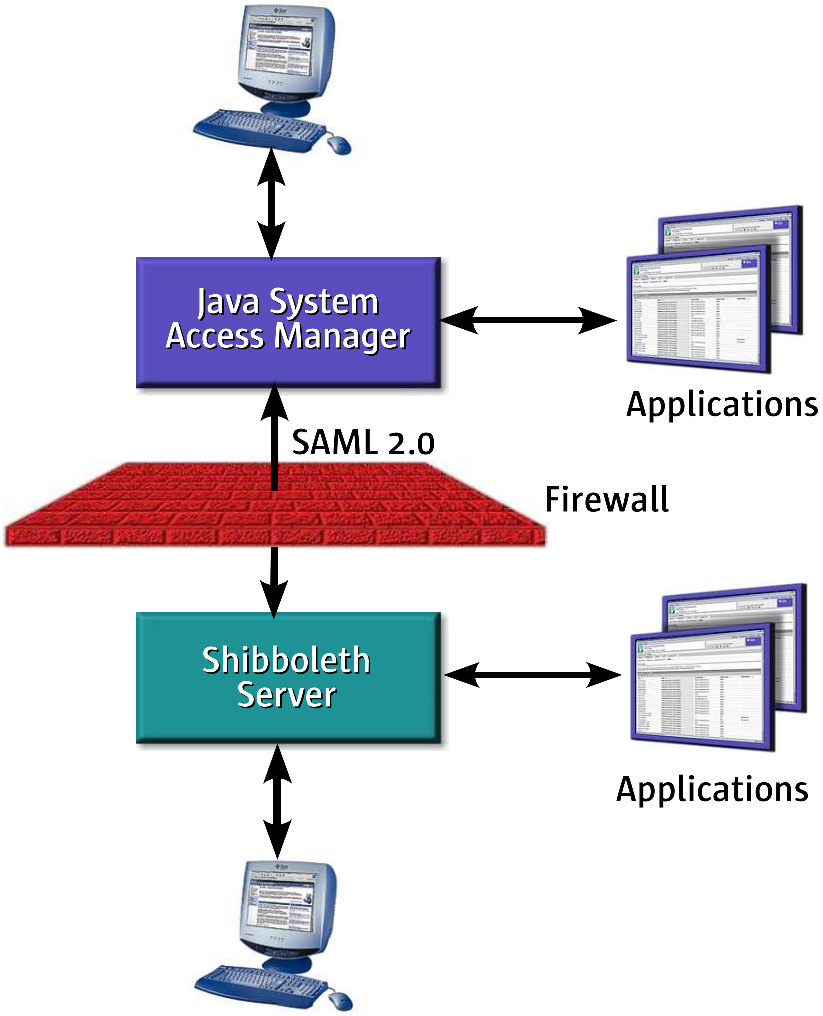
Browser Post Flow, SP initiated



Interoperability of Sun's Technology & Shibboleth

Standards-based Approach Allows Integration With Shibboleth

- AM & FM already support federation using Liberty specification (using SAML)
- Interoperability with Shibboleth through SAML 2.0 (Shibboleth expected to support SAML 2.0 in calendar Q2-06)



Sun's Product Line Landscape

OpenSSO

Developer

- Authentication
- Single-domain SSO
- Web & J2EE Agents

Access Manager

Intranet

- Policy Management
- Policy Enforcement
- Federation (IdP)
- Identity Web Services

Federation Manager

Extranet

- Federation (SP)
- Identity Web Services

The Network is the Computer.
Identity is the Network.

Questions?

Dr. Rainer Eschrich

rainer.eschrich@sun.com