
# WELCOME TO JAVAPOLIS

JAVAPOLIS '07

10 - 14 DECEMBER ▪ ANTWERP ▪ BELGIUM

JavaPolis '07
10 - 14 December ▪ Antwerp ▪ Belgium

# OpenSSO

Pat Patterson
Federation Architect
Sun Microsystems

Sun microsystems

# Overall Presentation Goal

Learn about the OpenSSO project, its relationship to Sun's Federated Access Manager 8.0 product and how to use it in your next web app

# Speaker's Qualifications

- Pat Patterson is...
  - A Federation Architect at Sun Microsystems
  - The 'community guy' for OpenSSO
  - One of Sun's reps at the Liberty Alliance
  - A speaker for Sun on identity and federation
  - A blogger, covering identity, federation and single malt scotch whisky

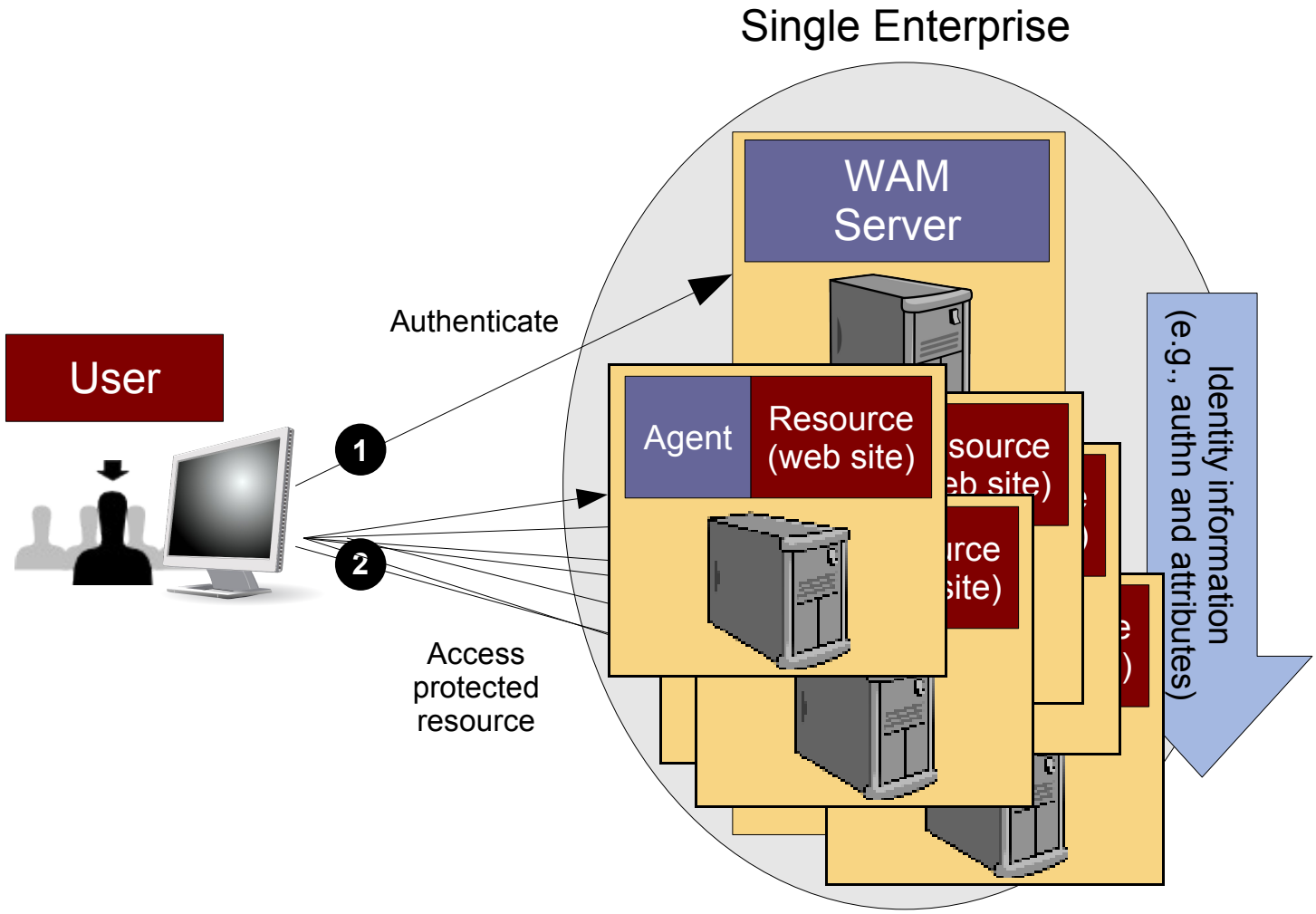
# Mandatory Extravagant Claim

OpenSSO is the Apache Web Server of web access management.

# What is OpenSSO?

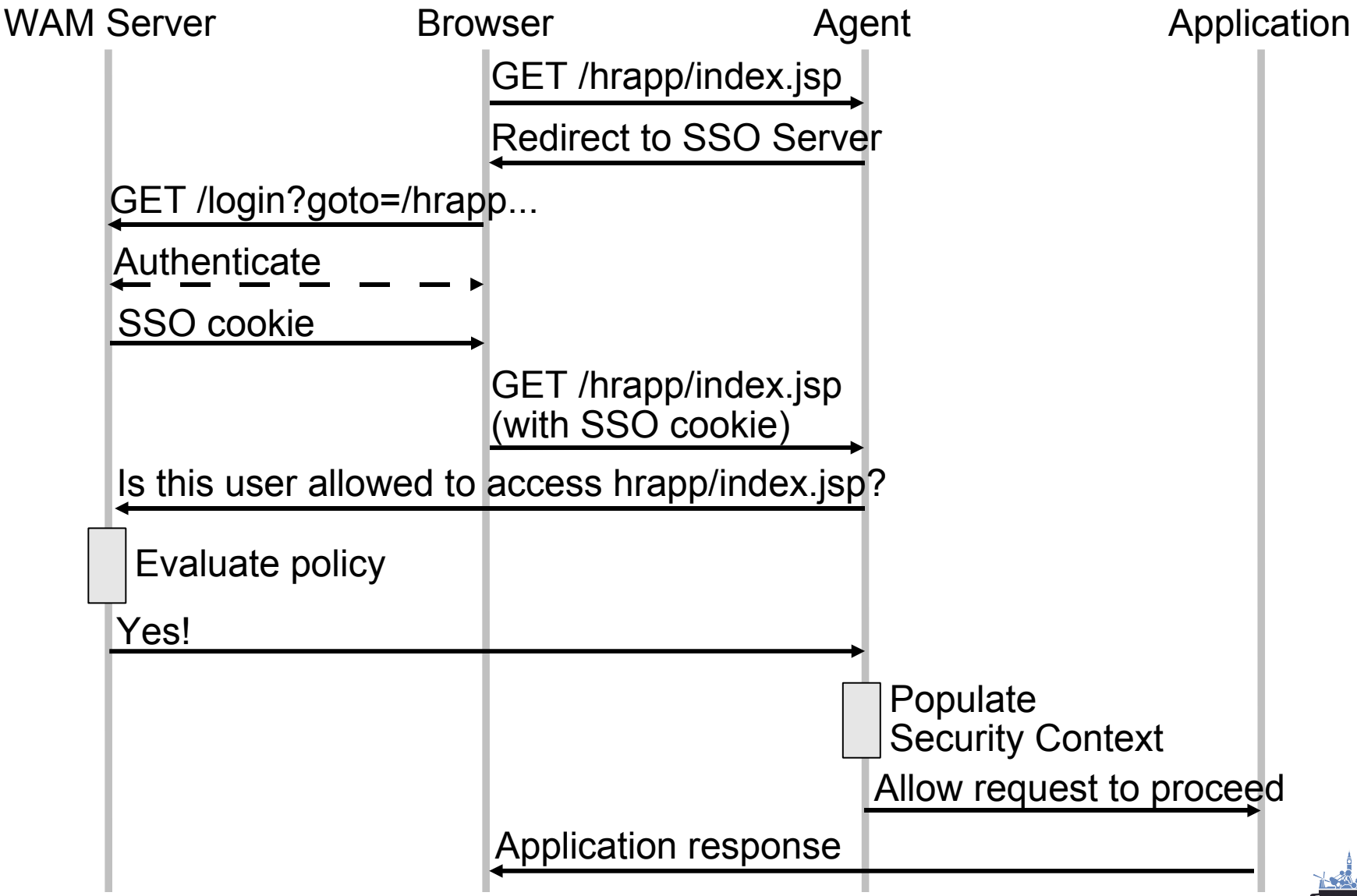
- Sun's open source project implementing web access management, federation, secure web services.
- Based on the shipping product – Sun Java System Access Manager 7.x
- The basis for Sun Java System Federated Access Manager 8.0.
  - Think Glassfish/Application Server 9.x.
- A fully-featured web access management solution that deploys as a single WAR file into the container of your choice.

# The Basic Use Case for Web Single Sign-On



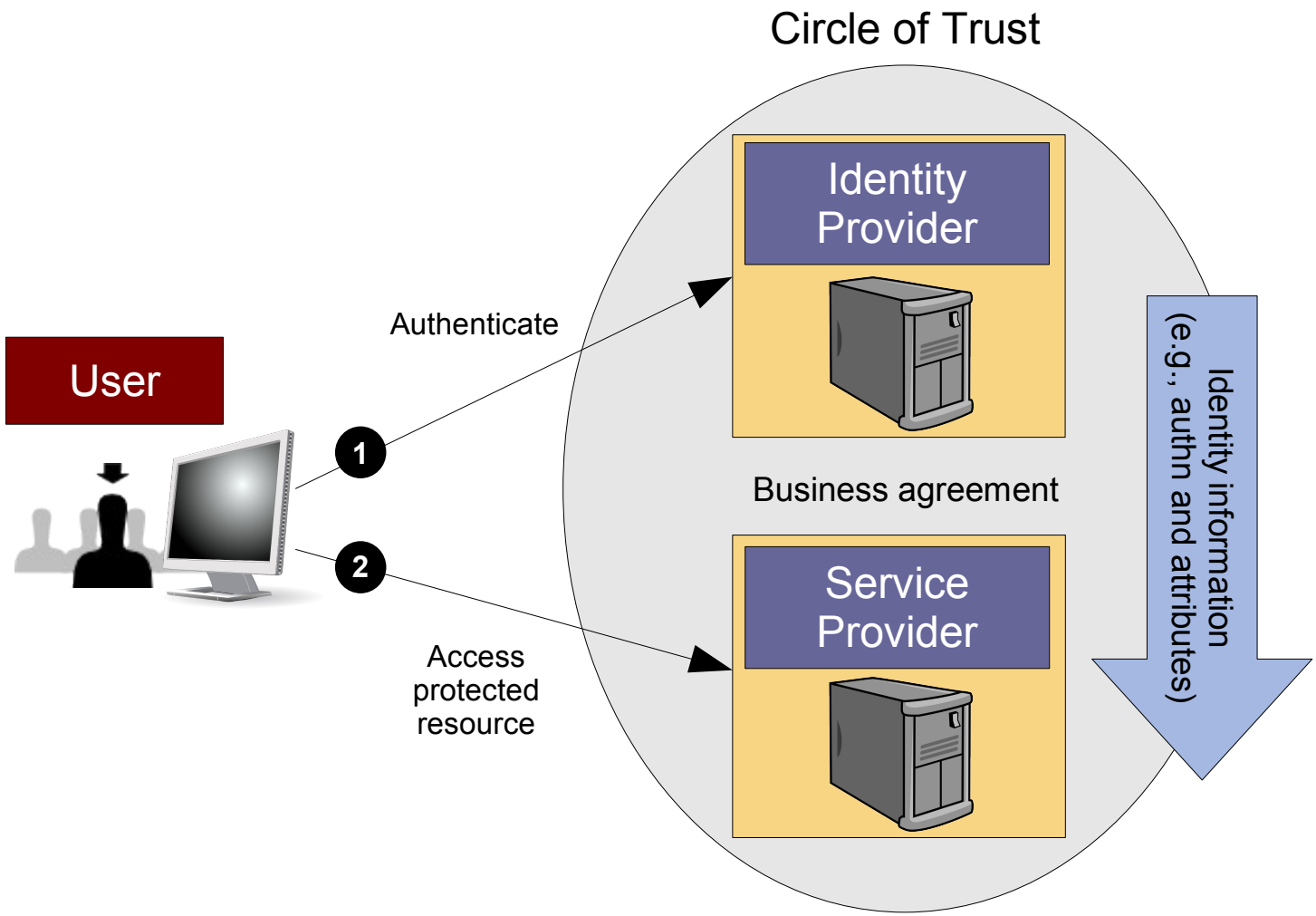

JAVAPOLIS

# How it works

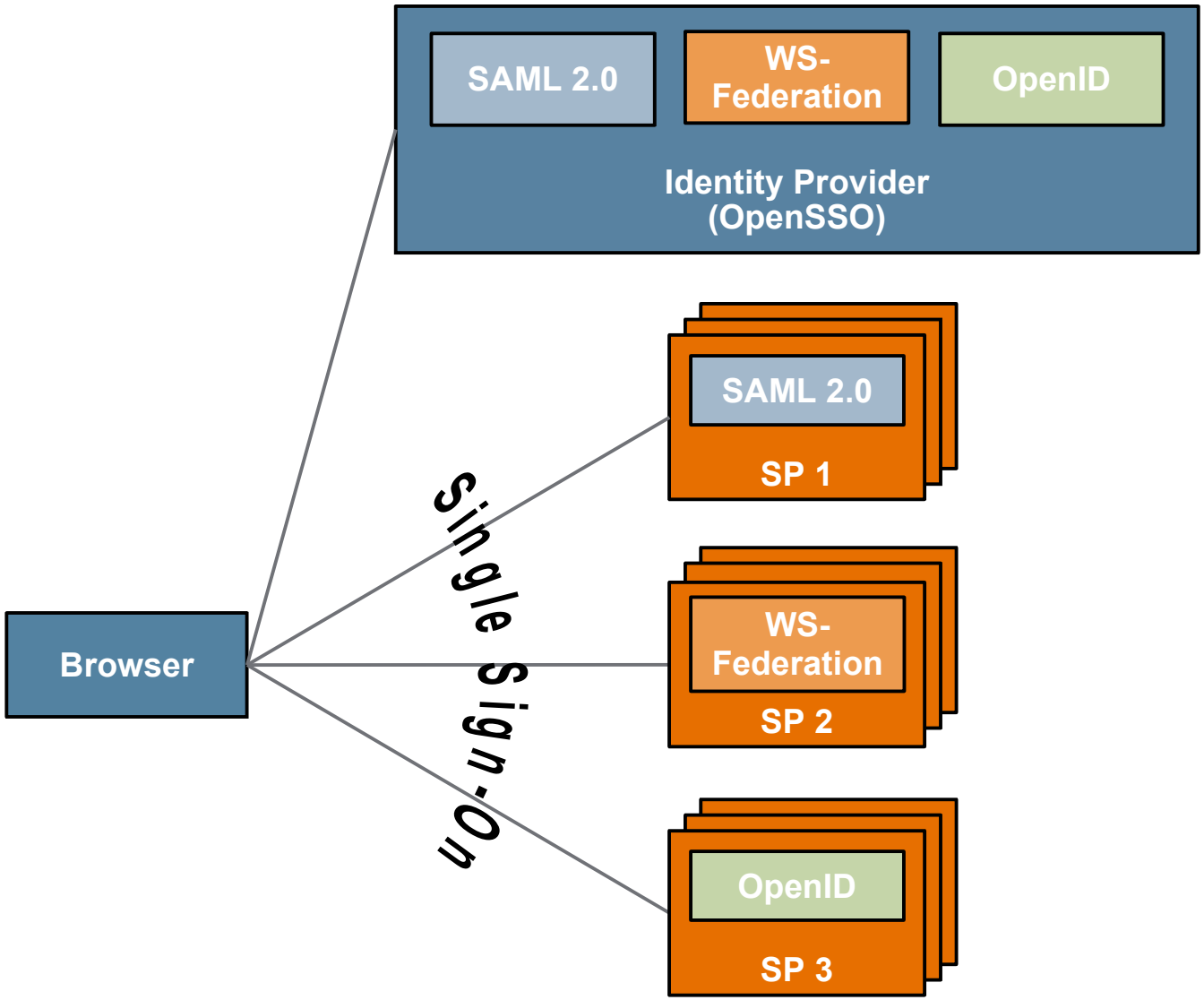



JAVAPOLIS

# SSO Between Enterprises



# Multi-Protocol Federation Hub



# Why Is This Important To You?

- Web Applications:
  - Factor out authentication
    - If your web application is invoked, you know who the user is
  - Factor out course-grained authorization
    - If your web application is invoked, you know that the user is supposed to be there
  - Leverage the infrastructure for fine-grained authorization
    - `if ( request.isUserInRole(ADMIN_ROLE) ) {`
      `...`
  - Focus on your app, not AuthN/AuthZ!

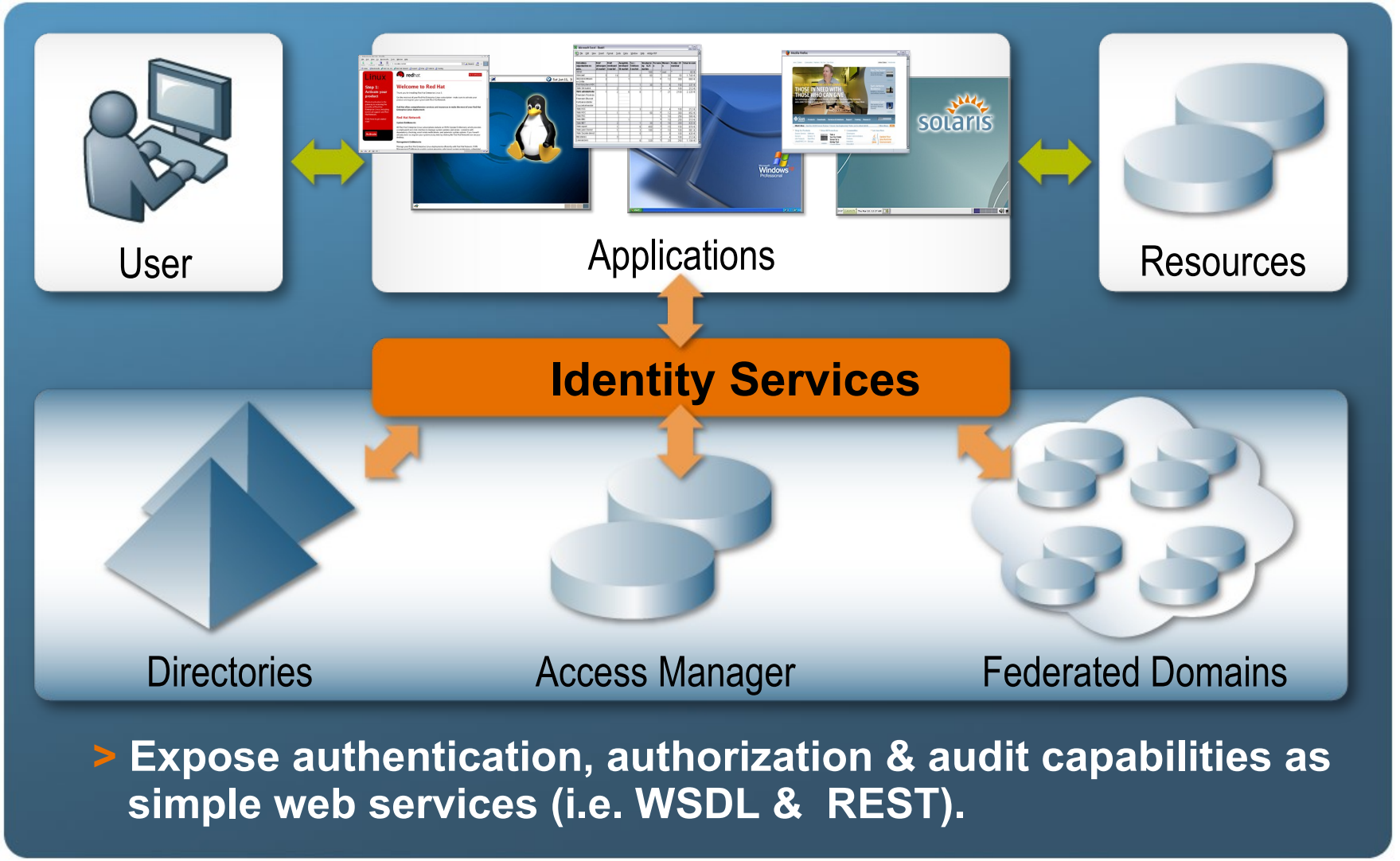
# Web Services – Three Models

- “Just do the identity stuff for me!”
  - JSR 196 plug-ins
- “Make it easy for me to do identity”
  - Identity Services
    - Authentication
    - Authorization
    - Attributes
- “I want the all the bells and whistles!”
  - Liberty Alliance Identity Web Services Framework (ID-WSF)
  - WS-*

# JSR 196

- Java Authentication Service Provider Interface for Containers
- Final release 10 Oct 2007
- “A standard interface by which authentication modules may be integrated with containers and such that these modules may establish the authentication identities used by containers”
- “JAAS for network messages”

# Identity Services




> **Expose authentication, authorization & audit capabilities as simple web services (i.e. WSDL & REST).**

# Identity Services Code Sample

```
...
IdentityServicesImplService service =
    new IdentityServicesImplService();
IdentityServicesImpl port =
    service.getIdentityServicesImplPort();

String uri = "realm=/";
Token subject =
    port.authenticate(username, password, uri);

// Successfully authenticated

if (port.authorize(uri, action, subject)) {
    // Do one thing
} else {
    // Do another
}
```

# ID-WSF

- 'Bootstrap' from SAML single sign-on
- Authentication Service
- Discovery Service
- People Service
- Template for more services

# WS-*

- Security Token Service
  - Issue, validate tokens
  - Support brokered trust models
    - Decompose many-to-many trust into multiple one-to-many
  - Integration with Microsoft WCF (aka Indigo)

# Where Can I Use This?

**OS Platforms**
- Sun Solaris 8, 9, and 10 for SPARC
- Sun Solaris 9 and 10 for x64/x86
- Red Hat Enterprise Linux AS/ES 3
- Red Hat Enterprise Linux AS/ES 4
- Windows 2000 Advanced Server, Data Center Server version SP4 on x86
- Windows 2003 Standard (32 and 64-bit versions), Enterprise (32 and 64-bit versions), Data Center Server (32-bit version) on x86 and x64 based systems
- Windows XP Professional SP2 on x86 based systems
- HP-UX 11i v1 64-bit on PA-RISC 2.0

**Supported Standards**
- Java Authentication & Authorization Service
- Kerberos
- Liberty Identity Federation Framework
- Liberty Identity Web Services Framework
- Lightweight Directory Access Protocol
- Security Assertion Markup Language
- SOAP
- Secure Sockets Layer
- WS-I Basic Security Profile tokens
- XML Digital Signature

**Web Containers**
- Sun Java System Web Server
- Sun Java System Application Server
- BEA WebLogic
- IBM WebSphere Application Server
- JBoss Application Server
- Apache Tomcat

**Policy Agents**
- Apache Web Server
- IBM HTTP Server
- Microsoft Internet Information Services
- Sun Java System Web Server
- Sun Java System Web Proxy
- Apache Tomcat
- BEA WebLogic Application Server
- JBoss Application Server
- IBM WebSphere Application Server
- IBM WebSphere Portal
- Oracle Application Server
- Sun Java System Application Server
- Lotus Domino
- Oracle
- PeopleSoft
- SAP
- Siebel

# OpenSSO Momentum

- In just 1 year...
  - 500+ project members at opensso.org
  - ~60 total committers
  - ~10 external committers
  - 1M+ LoC (excluding blanks and comments)
  - Consistently in Top 10* java.net projects by mail traffic
    - * of over 3000 projects

OpenSSO
Open Access . Open Federation

# OpenSSO Deployments

- Production deployments
  - **openid.sun.com**
    - OpenID for Sun employees
  - **www.audi.co.uk**
    - 250,000 customer profiles
  - **www.ssocircle.com**
    - SAML 2.0 to Google, OpenID, client certificate authentication

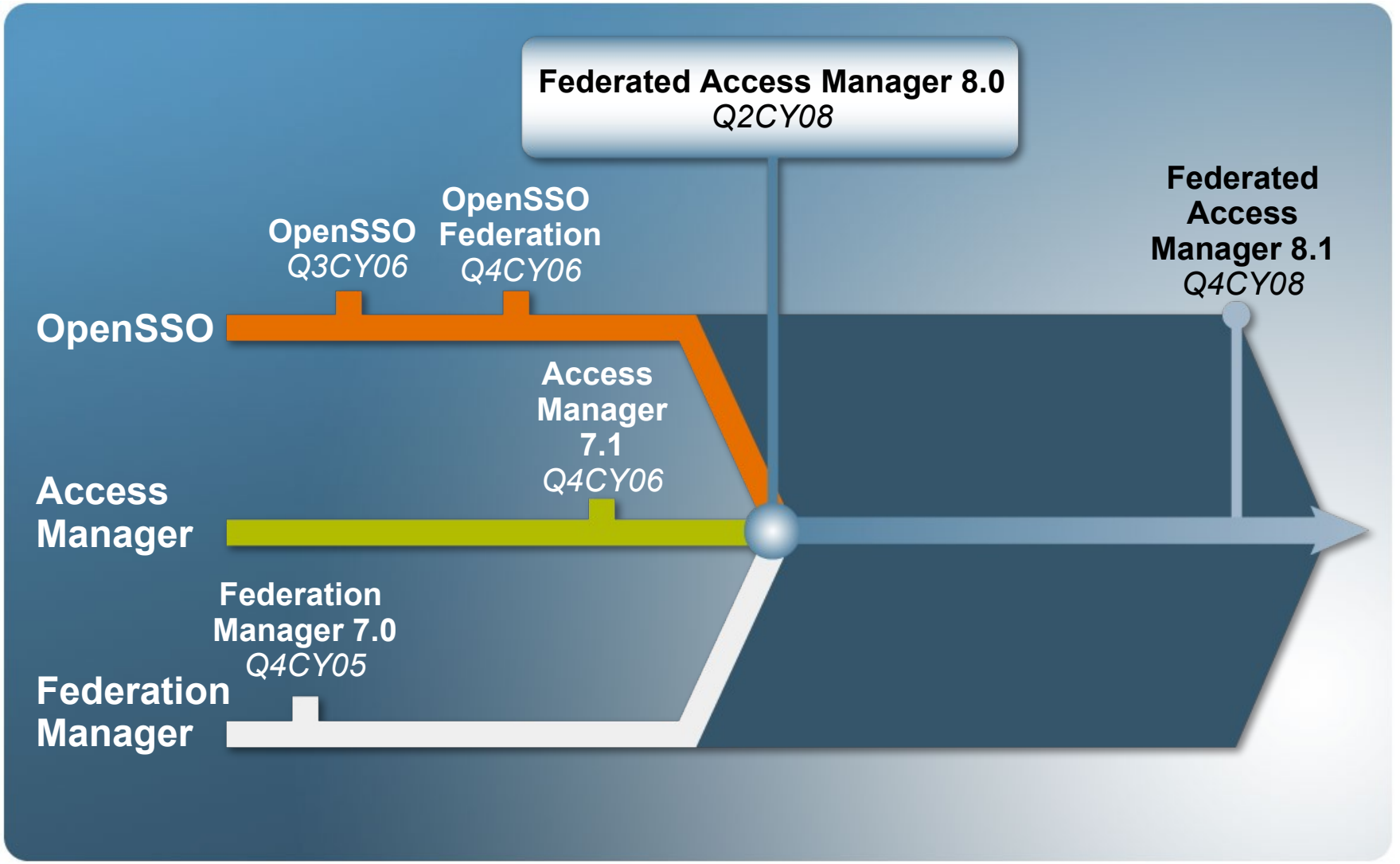
# OpenSSO & Federated Access Manager 8.0


**Open Access.**
**Open Federation.**

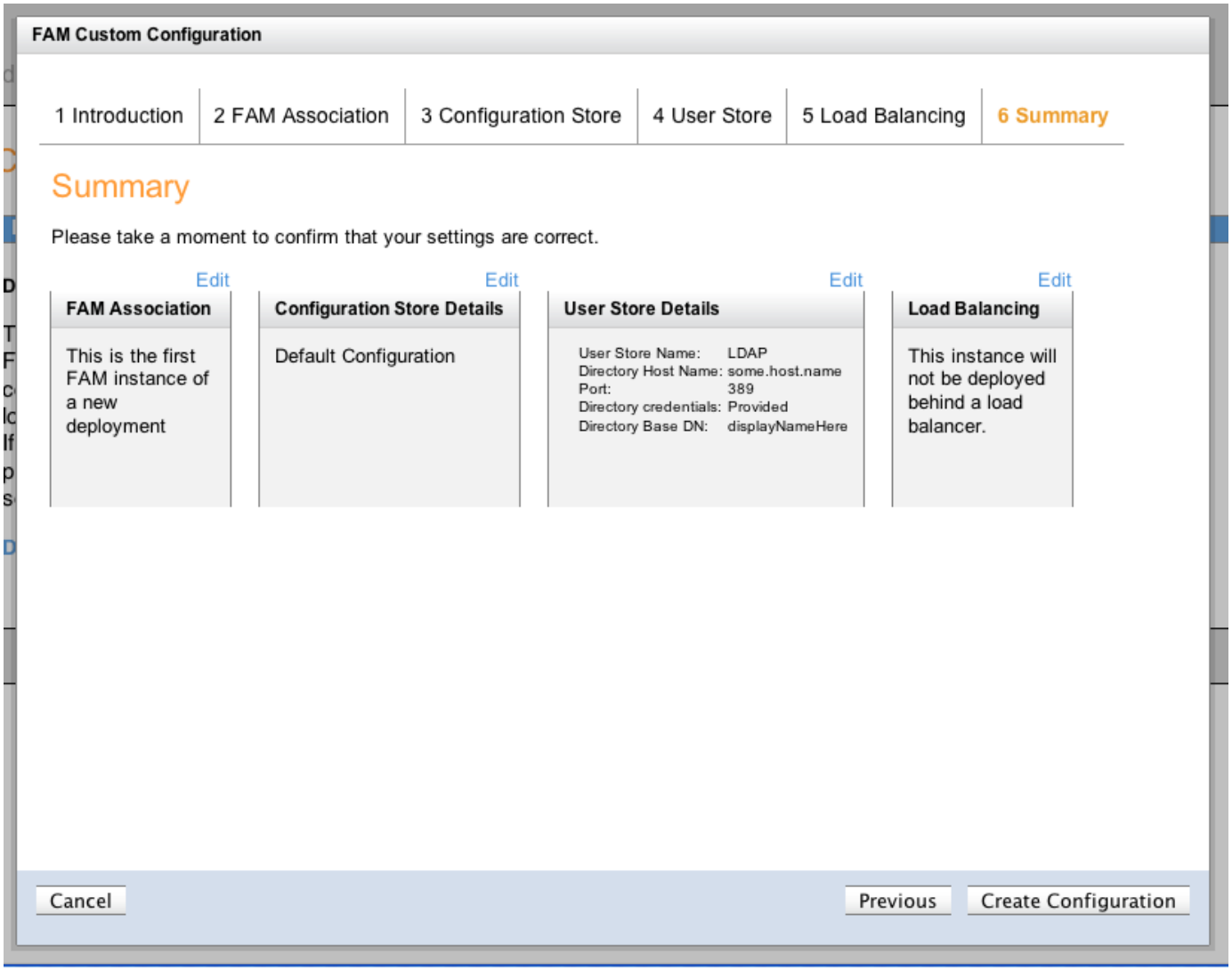
- OpenSSO v1.0 == FAM 8.0
- All FAM 8.0 builds available via OpenSSO
- Preview Features
- Provide Feedback
- Review code security

JAVAPOLIS

# Federated Access Manager Roadmap



# Simplified Configuration




JAVAPOLIS

# OpenSSO v1.0: More Features

**Access Management**

- Centralized Agent Configuration & Deployment
- Centralized Configuration
- XACML Request/Response
- More Application Servers

**Federation**

- WS-Federation 1.1
- Simple Federated Partner Enablement
- Multi-Federation Protocol Hub
- Secure Attribute Exchange
- 3rd Party WAM Interoperability

# OpenSSO v1.0 More Features

**Identity Services**

- Authentication as a service
- Authorization as a service
- Audit Log as a service
- Attribute Query as a service
- Secure Trust Authority
- Web Services Security Plug-ins
- SDK for Securing Web Services

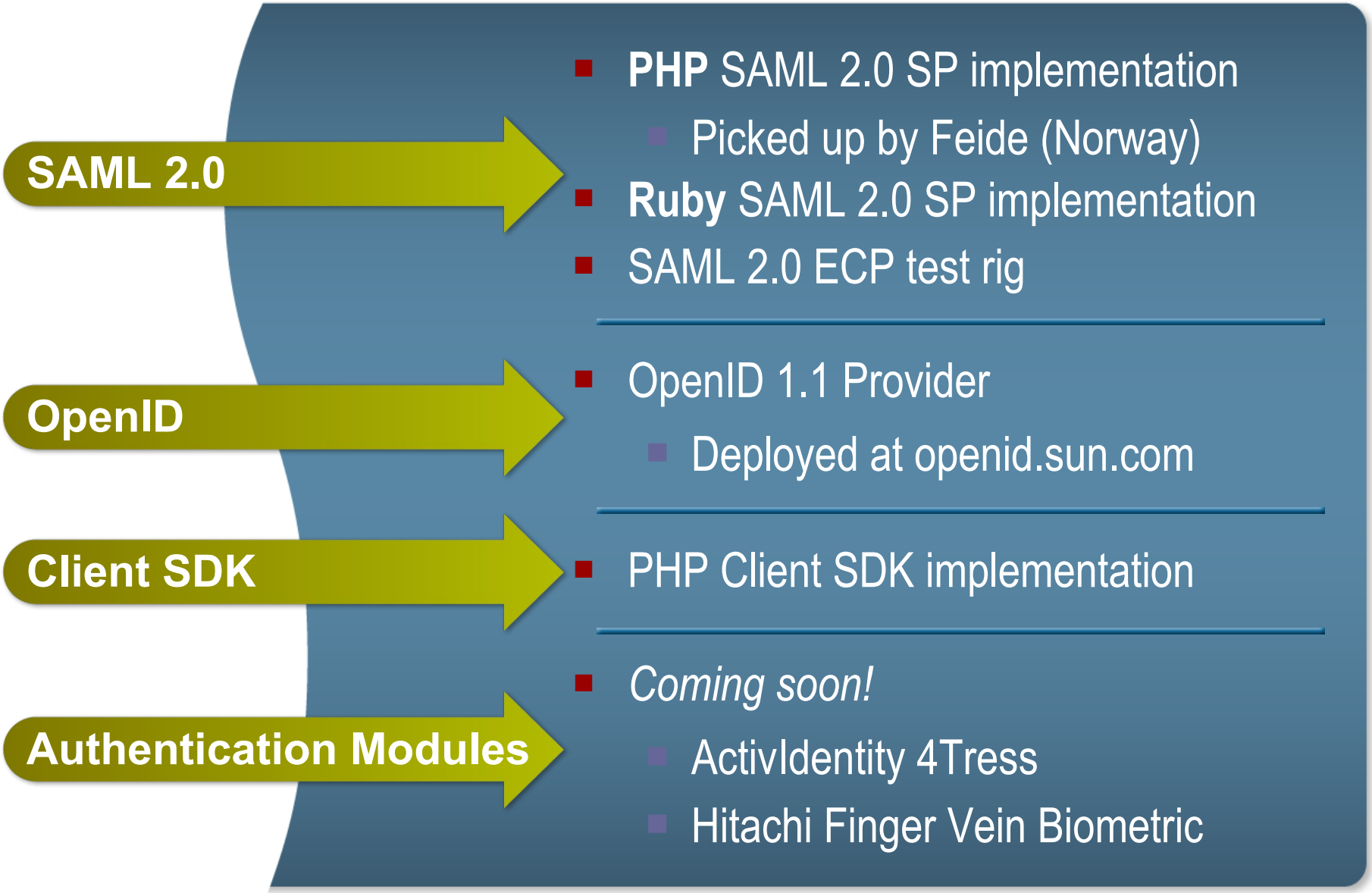
**Interested Yet?**

# Beyond

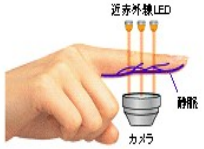
- Fine-Grained Authorization
- Compliance/Auditing
- Dashboard/RSS feeds
- OpenID
- More 3rd Party Interoperability
- More Simplification
- More Workflows

**Stay Tuned. More To Come . . .**

# OpenSSO Extensions

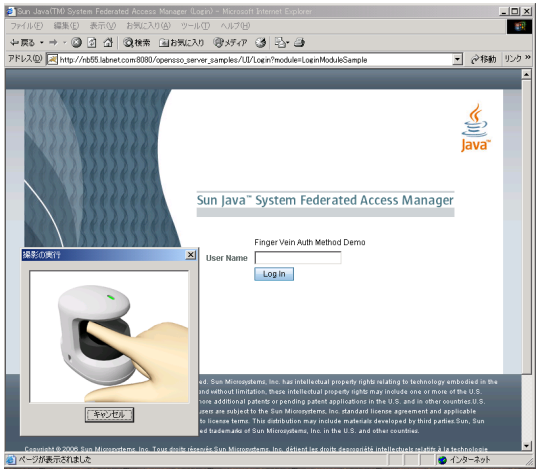


# Hitachi Finger Vein Authentication




●外光に強く高い認証精度

上部のフードにより外光の影響を低減するとともに、近赤外線を指の上から透過させ、下からカメラで読み取る方式を採用し、高い認証精度を実現しました。




**OpenSSO**

- SAML Service
- Logging Service
- Liberty Service
- Session Service
- Policy Service
- SOAP Service
- etc

Protected Applications/ Resources

SOAP

Authentication Service

ASP.NET/IIS

SOAP

Directory Server EE

JAVAPOLIS

JAVAPOLIS '07
10 - 14 DECEMBER ▪ ANTWERP ▪ BELGIUM

# DEMO

SSO Circle:
SAML 2.0 to Google
OpenID to Dopplr

# Resources

**OpenSSO**

- opensso.org

**Pat's Blog**

- Superpatterns
  - blogs.sun.com/superpat/

**Daniel Raskin's Blog**

- Virtual Daniel
  - blogs.sun.com/raskin/

# Participate!

## Join

Sign up at
opensso.org

## Download

AM 7.1 WAR file
FAM 8.0 Build 1

## Subscribe

OpenSSO Mailing Lists
dev, users, announce

## Chat

#opensso
on
freenode.net

JAVAPOLIS '07
10 - 14 DECEMBER ▪ ANTWERP ▪ BELGIUM

# Q&A

View JavaPolis talks @ www.parleys.com

Sun microsystems

JavaPolis '07
10 - 14 December ▪ Antwerp ▪ Belgium

# Thank you for your attention

Sun microsystems