



Open Source Identity Integration with OpenSSO

July 4th, 2008

Pat Patterson
Federation Architect

pat.patterson@sun.com

blogs.sun.com/superpat



Agenda

- Web Access Management
 - > The Problem
 - > The Solution
 - > How Does It Work?
- Federation
 - > Single Sign-On Beyond a Single Enterprise
 - > How Does It Work?
- OpenSSO
 - > Project Overview

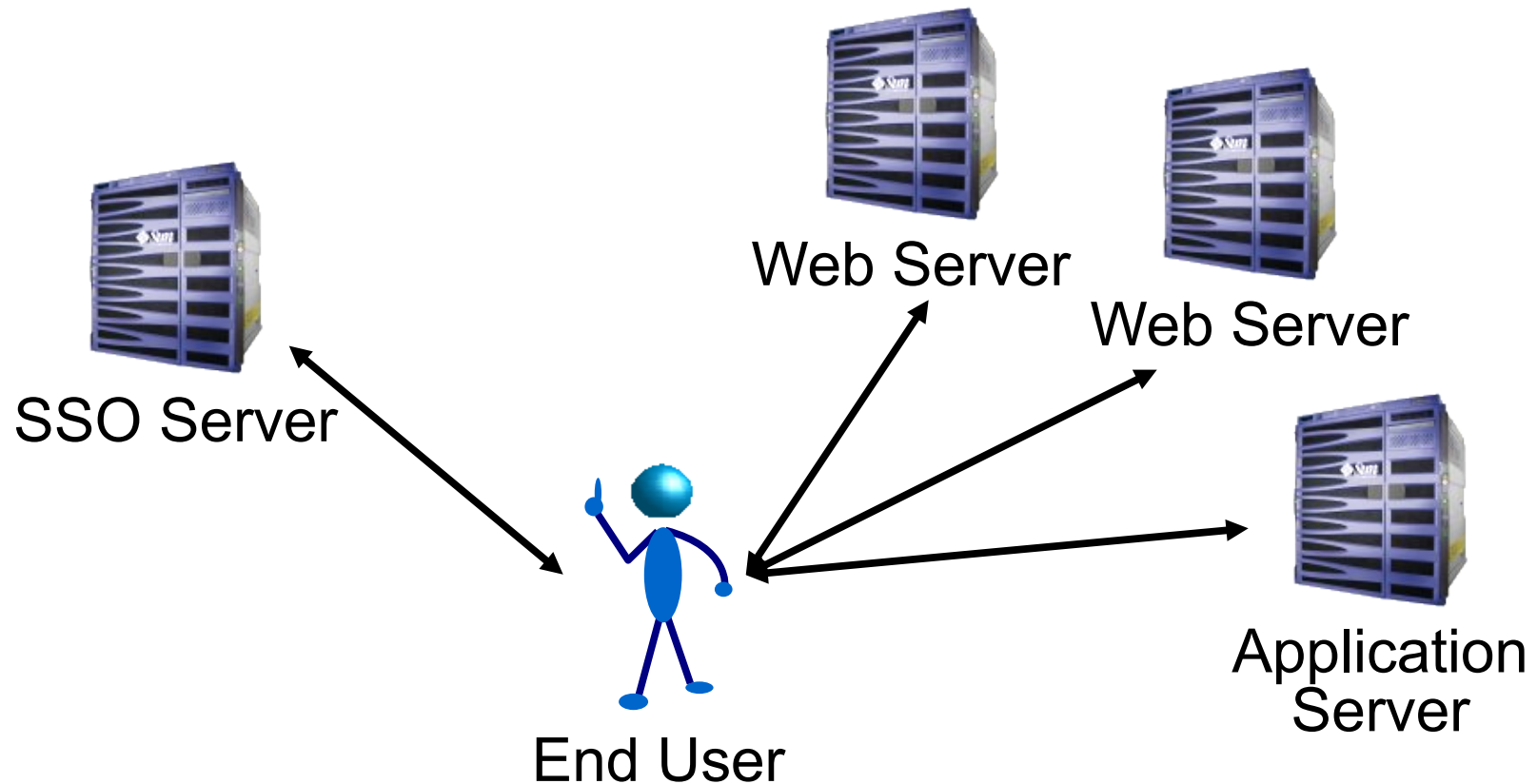
Typical Problems

- “Every application wants me to log in!”
- “I have too many passwords – my monitor is covered in Post-its!”
- “We're implementing Sarbanes-Oxley – we need to control access to applications!”
- “We need to access outsourced functions!”
- “Our partners need to access our applications!”

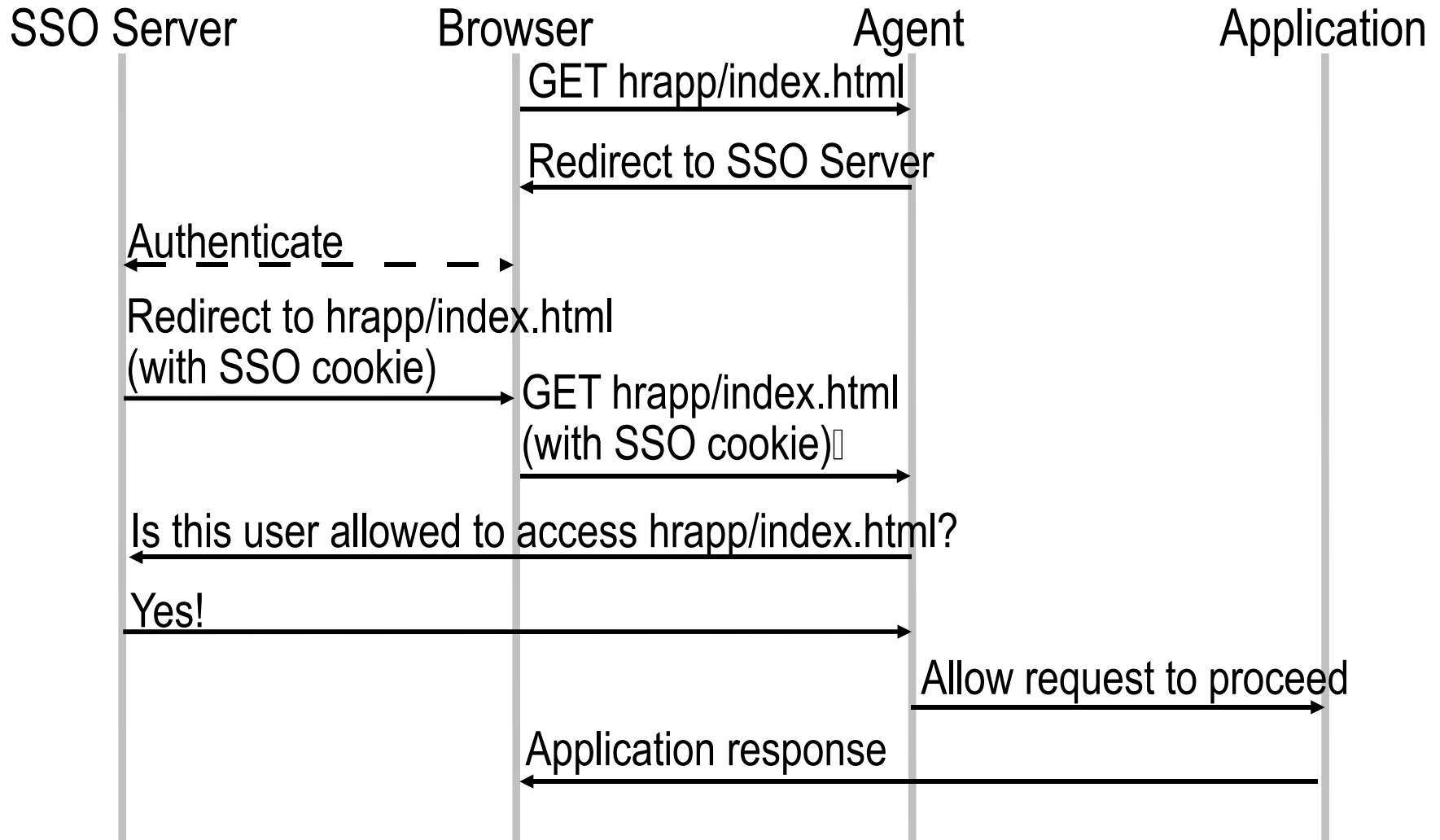
Web Access Management

- Simplest scenario is within a single organization
- Factor authentication and authorization out of web applications into web access management (WAM) solution
- Can use browser cookies within a DNS domain
- Proxy or Agent architecture implements role-based access control (RBAC)
- Users get single sign-on, IT gets control

Single Sign-On Within an Organization



How It Works



Web Access Management Products

- Sun Java System Access Manager
 - > OpenSSO
- CA (Netegrity) SiteMinder Access Manager
- IBM Tivoli Access Manager
- Oracle (Oblix) Access Manager
- Novell Access Manager
- JA-SIG CAS
- Spring Security (Acegi)
- JOSSO

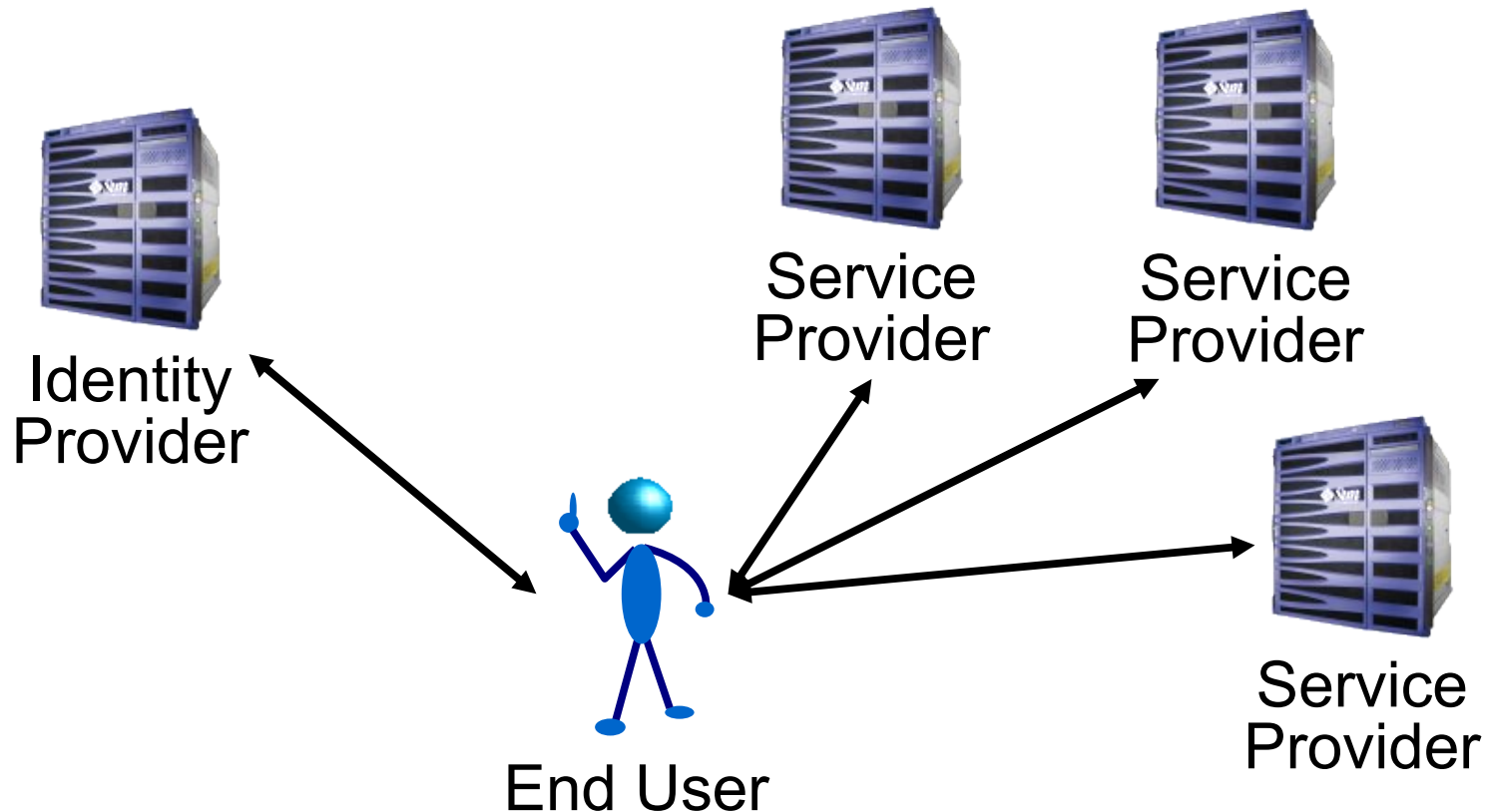
Typical Problems

- ~~“Every application wants me to log in!”~~
- ~~“I have too many passwords – my monitor is covered in Post-its!”~~
- ~~“We’re implementing Sarbanes-Oxley – we need to control access to applications!”~~
- “We need to access outsourced functions!”
- “Our partners need to access our applications!”

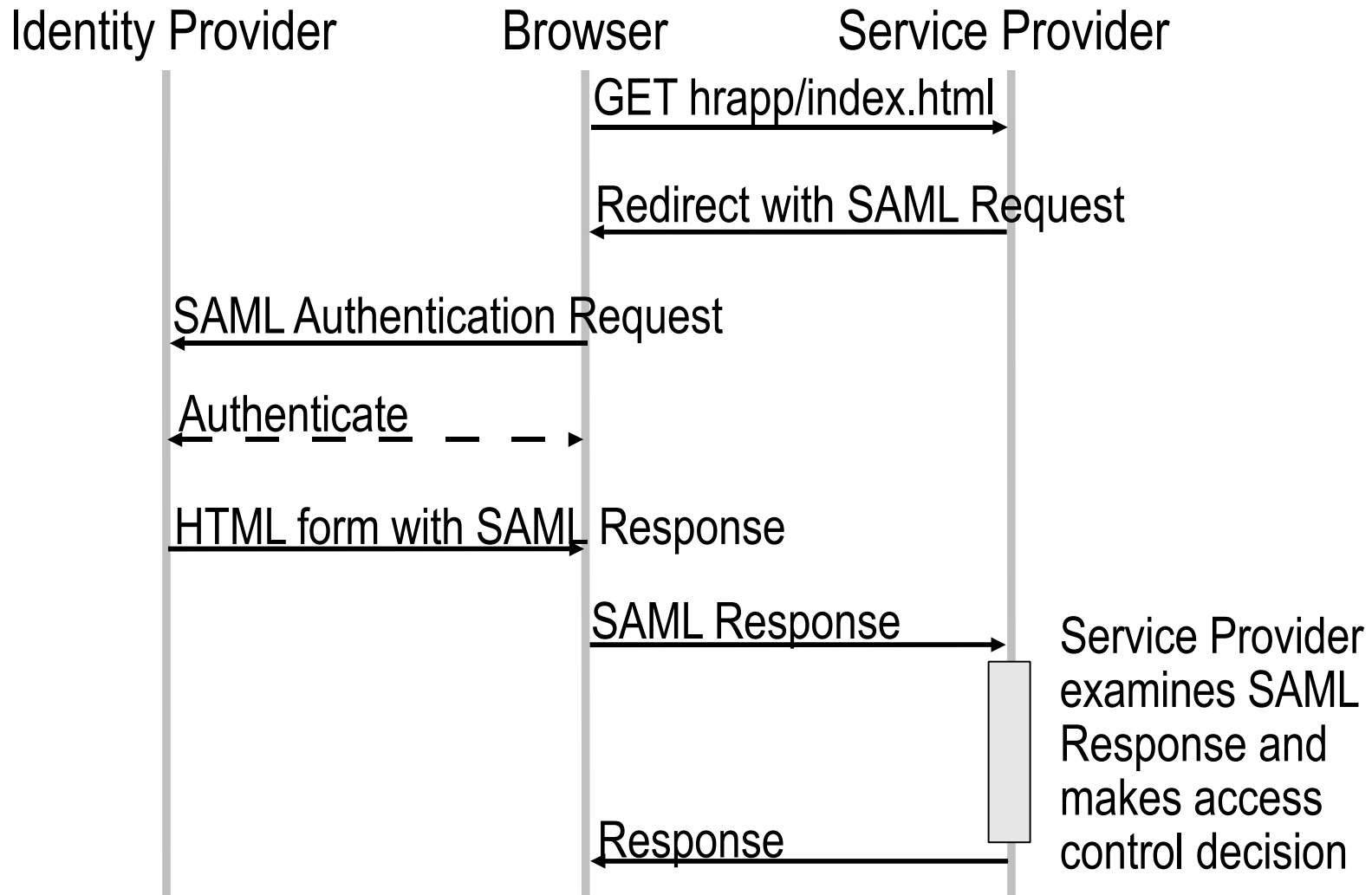
Single Sign-on *between* Organizations

- Cookies no longer work
 - > Need a more sophisticated protocol
- Can't mandate single vendor solution
 - > Need standards for interoperability

SSO Across Organizations



SAML 2.0 SSO Basics



SAML 2.0 Assertion

(Abbreviated!)

```
<Assertion Version="2.0" ID="..." IssueInstant="2007-11-06T16:42:28Z">
  <Issuer>https://pat-pattersons-computer.local:8181/</Issuer>
  <Signature>...</Signature>
  <saml:Subject>
    <saml:NameID Format="urn:oasis:...:persistent" ...>
      ZG00Z3JWP9yduIQ1zFJbVVGHLQ9M
    </saml:NameID>
    <saml:SubjectConfirmation Method="urn:oasis:...:bearer">
      <saml:SubjectConfirmationData .../>
    </saml:SubjectConfirmation>
  </saml:Subject>
  <saml:Conditions
    NotBefore="2007-11-06T16:42:28Z"
    NotOnOrAfter="2007-11-06T16:52:28Z">
    <saml:AudienceRestriction>
      <saml:Audience>
        https://pat-pattersons-computer.local/example-pat/
      </saml:Audience>
    </saml:AudienceRestriction>
  </saml:Conditions>
  <saml:AuthnStatement AuthnInstant="2007-11-06T16:42:28Z" ...>
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>
        urn:oasis:...:PasswordProtectedTransport
      </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
</saml:Assertion>
```

SAML 2.0 Adoption

- Sun, IBM, CA – all the usual suspects, except Microsoft
- OpenSAML (Internet2)
 - > Java, C++
- OpenSSO (Sun)
 - > Java, PHP, Ruby
- SimpleSAMLphp (Feide)
- LASSO (Entr'ouvert)
 - > C/SWIG
- ZXID (Symlabs)
 - > C/SWIG

What is OpenSSO?



OpenSSO
Open Access . Open Federation

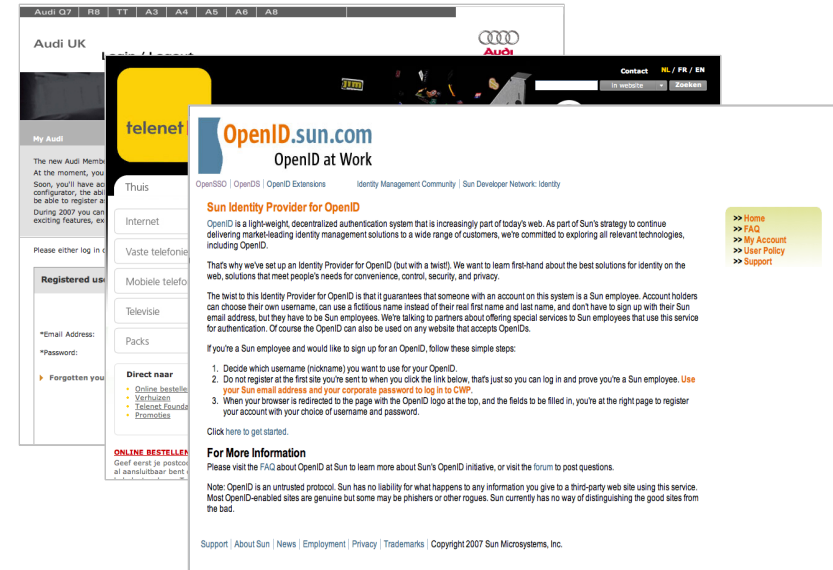
**Open Access.
Open Federation.**

- OpenSSO 1.0 == Federated Access Manager 8.0
- All FAM 8.0 builds available via OpenSSO
- Preview Features
- Provide Feedback
- Review code security

OpenSSO Momentum

OpenSSO
Open Access . Open Federation

- In less than 2 years...
 - > >700 project members at opensso.org
 - > ~15 external committers
 - > Consistently in Top 10* java.net projects by mail traffic
 - * of over 3000 projects
- Production deployments
 - > www.audi.co.uk
 - 250,000 customer profiles
 - > openid.sun.com
 - OpenID for Sun employees
 - > telenet.be
 - Foundation for fine-grained authorization



OpenSSO Extensions

<https://opensso.dev.java.net/public/extensions/>



SAML 2.0

- **PHP** SAML 2.0 SP implementation
 - > Picked up by Feide
- **Ruby** SAML 2.0 SP implementation
- SAML 2.0 ECP test rig

OpenID

- OpenID 1.1 Provider
 - > Deployed at openid.sun.com

Client SDK

- PHP Client SDK implementation

Authentication Modules

- ActivIdentity 4Tress
- Hitachi Finger Vein Biometric
- Information Card (aka CardSpace)

Demo

Deploy and Configure OpenSSO
Create an Identity Provider
SAML-enable a Service Provider...
All in less than 10 minutes!

DEMO

GO!!!

Participez!

Join

Sign up at
opensso.org

Download

OpenSSO 1.0
Build 4

Subscribe

OpenSSO Mailing Lists
dev, users, announce

Chat

#opensso
on
freenode.net

Resources

<https://opensso.dev.java.net/public/extensions/>

OpenSSO

- <http://opensso.org/>
-

OpenSSO Wiki

- <http://wiki.opensso.org/>
-

Pat's Blog

- Superpatterns
 - > <http://blogs.sun.com/superpat/>
-

Daniel Raskin's Blog

- Virtual Daniel
 - > <http://blogs.sun.com/raskin/>



Open Source Identity Integration with OpenSSO

July 4th, 2008

Pat Patterson
Federation Architect

pat.patterson@sun.com

blogs.sun.com/superpat