Towards an Open Identity Infrastructure with OpenSSO

RMLL
Nantes
July 10 2009

Fulup Ar Foll
Master Architect
fulup@sun.com

Towards an Open Identity Infrastructure with OpenSSO

- OpenSSO Overview
  - *Integration with open source and beyond*
- Integrating further – what's new
  - *SaaS integration – Google*
  - *Fedlet for .Net*
  - *Fine Grained Authorization*
  - *Secure RESTful web services*
- Call to action - Participate!

What is OpenSSO?

Sun OpenSSO

- Web Single Sign-On
- Access Control
- Federation
  - *SAML 2.0*
  - *WS-Federation*
- Web Services
  - *ID-WSF*
  - *WS-**
  - *SOAP*
  - *REST*

OpenSSO Facts

- 1000+ project members at **opensso.org**
- 125 committers (~25% external to Sun)
- Deployments all over the world

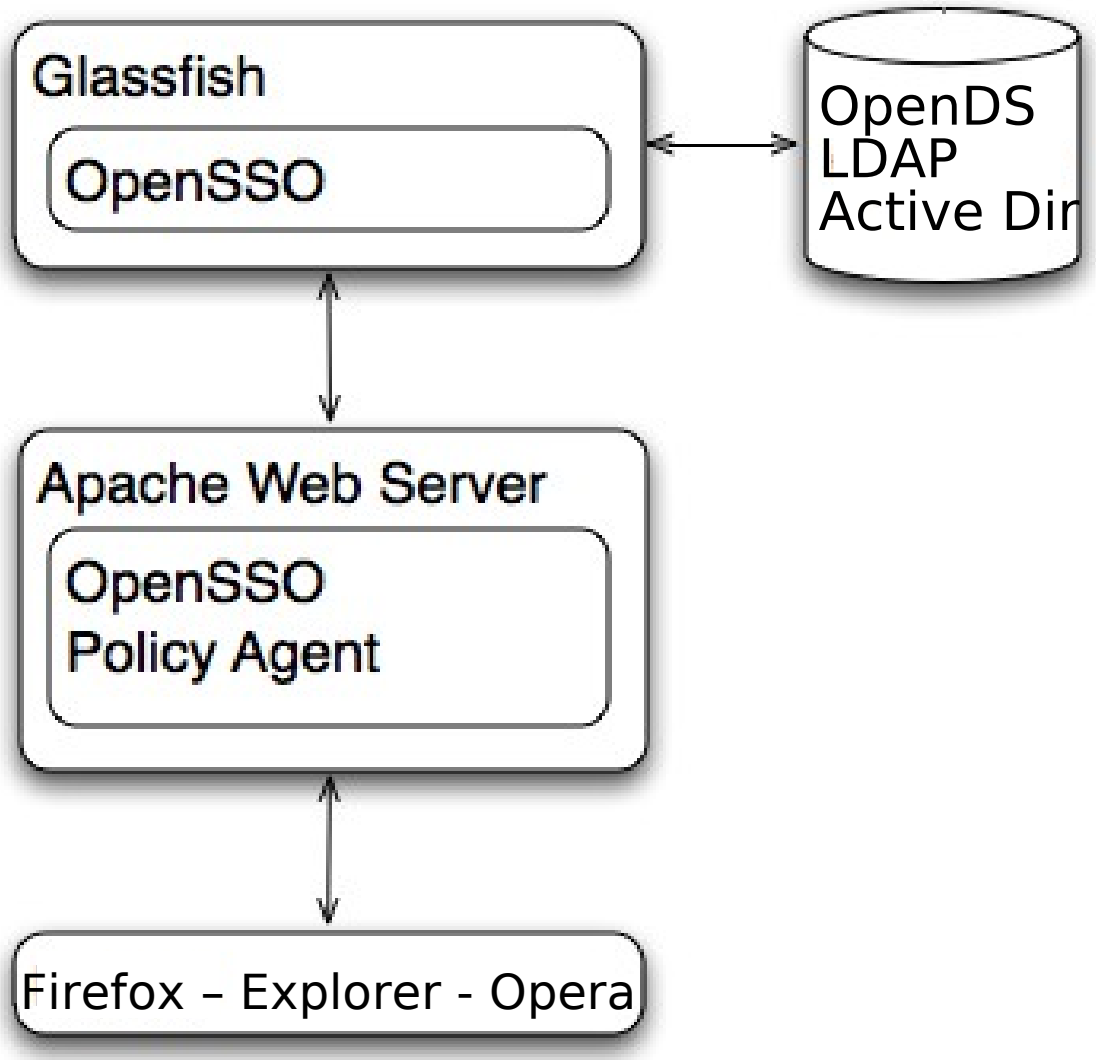
OpenSSO/Identity Community Days

- 1.0 – March 2009
  - *New York City, USA (Community One East)*
- 2.0 – May 2009
  - *Munich, Germany (European Identity Conference)*
- 3.0 – June 2009
  - *San Francisco, USA (Community One West)*
- Sun engineers, community meet, talk, present
- 'Unconference' format

OpenSSO Options

- OpenSSO Enterprise
  - *Delivered every 12 – 15 months*
  - *Long term support – hot patches/service packs*
- OpenSSO Express
  - *Delivered every 3 months*
  - *Medium term support - Fixes in the trunk*
- OpenSSO Periodic Builds
  - *Binaries built every 2-3 days*
  - *Community support*
- CVS :-)

An Open Identity Infrastructure



Software as a Service Integration

- Google Apps
  - *Single sign-on from an identity provider in your enterprise*
    - *Users log in with their enterprise credentials*
  - *Single sign-on handshake between identity provider and Google*
    - *SAML 2.0 protocol*
  - *Valeo (France) in production since May 2009*
    - *Replacing Lotus Domino for 32,000 users*
- What's New
  - *Easy set up for SSO to Google Apps*
    - *Just provide your domain name, cut and paste the rest*

Fedlet for .Net

- Existing Fedlet is a smash hit
  - *Federation-enables small service providers*
  - *Java JAR file and configuration*
  - *http://tinyurl.com/fedlet*
- Next step: .Net version
  - *Same features and functionality as Java version*
  - *.Net ZIP file and configuration*
  - *http://blogs.sun.com/whalphin/entry/fedlet*
- Try it out – give feedback!

Fine Grained Authorization

- Existing policy engine works well, but was designed for URL's – 'course grained authorization'
  - *Scales to ~ 10,000 policies*
- Demand for fine-grained authorization - entitlements
  - *Scale to ~ 1,000,000 policies*
  - *XACML model*
- Flexible deployment options
  - *Colocate PEP, PDP*
  - *Embed OpenSSO*

RESTful Identity Services in OpenSSO

- Evolution of previous, RPC-style approach
  - *Goal – provide easy access to OpenSSO identity services from any programming language (previous APIs were Java/C only)*
  - *SOAP and 'REST-like'*
    - *SOAP emphasised*
    - *REST-like actually used by most developers*

First Generation of Services

Authentication

Verification of user credentials

```
POST .../authenticate?
username=demo&password=demo
```

Authorization

Permission for user to access protected resource

```
GET .../authorize?token=aaa&
resource=bbb&action=ccc...
```

Attributes

Obtain attributes of users

```
GET .../attributes?
token=aaa&attributes_names=cn
```

Audit log

Perform log & audit operations

```
POST .../log?appid=aaa&
subjectid=bbb=cn&logname=...
```

OpenSSO REST simple security

- Authen/Authorization of callers to REST URLs
  - *Course-grained policy enforcement based on URL*
- Fine-grained authorization within the application logic
  - *Examples: access to attributes, ability to log, etc.*
- Session established & maintained after authentication
  - *SSOToken: random string usually stored as cookie*
- SSOToken passed in each request
  - *As either cookie or query parameter*
- Key parameters passed as query parameters

Pros for REST simple identity services

- Easy!
- Programming language agnostic
  - *OpenSSO is not restricted to Java and C languages*
- Can build loosely coupled systems
  - *Liferay / WebSynergy*

Cons of using simple identity services

- Need for client SDK?
  - *Caching? How can consumer site cache the authorization decisions, user attributes, etc, from OpenSSO server?*
  - *Maybe a need for SDK.*
- Exceptions?
  - *Mapping of HTTP error codes and passing of error messages.*

Lessons learned (simple identity services)

- Imperfect RESTful APIs
  - *Current application not easy to convert to URL resources like REST*
- Message authentication
- Requires user presence
- Consumer could masquerade as the user
- Token management
- Still useful
  - *Allow access from any programming language*
  - *A step toward a more RESTful approach*

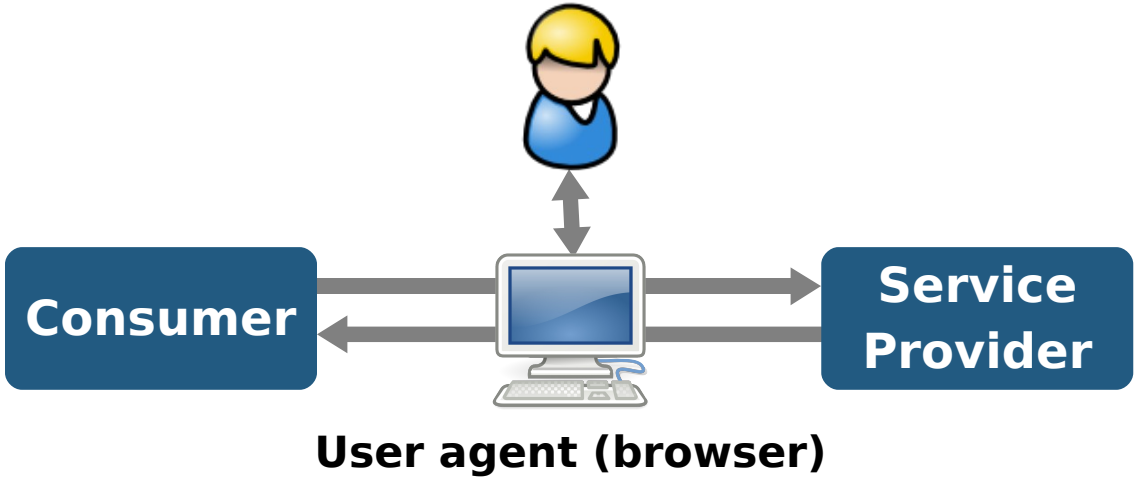
Second Generation of Services

- Still under construction!
- First example is entitlement (fine grained authorization)
  - *Pass in subject, action, resource*
  - *Get back allow/deny*
- Secured by OAuth
  - *Specifically designed to protect RESTful web services*

OAuth overview

- Users securely share their resources in one service with another service **without exposing credentials**.
- Prototypical use case: user shares images from an image gallery with a photo printing service.
- Once user brokers issuance of token, it can be used on an ongoing basis. Think: session keys for consumer applications.
- Provides a very handy consumer authentication capability through the OAuth digital signature.

❶ User brokers issuance of access token



- User introduces service provider to consumer
- Authorization performed through browser redirects
- Standard user authentication with service provider
- Access token is issued to consumer on behalf of user

❷ Consumer accesses resource directly

- Consumer signs requests with access token secret
- Service provider can enforce its own access controls
- Doesn't require constant user presence

Why consider OAuth over others?

- Mashups quickly evolve toward delegation model
- Aligns very well with REST (use of HTTP header)
- More secure than storing credentials everywhere
- Flexible access token management capability
- Already multiple client and server implementations
- Strong community — now an IETF working group

Conclusion

- OpenSSO
  - *provides an open source solution for authentication, authorization and beyond*
  - *integrates with other open source components such as GlassFish and Apache Web Server allowing a completely open source identity infrastructure*
  - *has hundreds of deployments, serving millions of users*
  - *has a thriving open source community*
- Download OpenSSO today!

Resources

OpenSSO
- http://opensso.org/

Pat Patterson's
- http://blogs.sun.com/superpat/

Daniel Raskin's
- http://blogs.sun.com/raskin/

Fulup Ar Foll
- http://www.fridu.org/fulup

Participez!

Join

Sign up at
opensso.org

Download

OpenSSO 8.0
Express Build 7*

Subscribe

OpenSSO Mailing List
users@opensso.dev.java.net

Chat

#opensso
on
freenode.net

Thank You.

Fulup Ar Foll
Master Architect
fulup@sun.com