OpenSSO in the Clouds

AWSome Atlanta
December 2008

Pat Patterson
Federation Architect
pat.patterson@sun.com

OpenSSO in the Clouds

What is OpenSSO?
    How does it work?

How does OpenSSO fit with cloud computing?
    SaaS – Google/Salesforce.com
    Amazon EC2
    The Fedlet

Call to action - Participate!

What is OpenSSO?

OpenSSO
Open Access . Open Federation

Open Access. Open Federation.

Web Single Sign-On

Access Control

Federation
- SAML 2.0
- WS-Federation

Web Services
- ID-WSF
- WS-*
- SOAP
- REST

OpenSSO Facts

890 project members at **opensso.org**

100 committers, 20 of which are external to Sun

Deployments all over the world

OpenSSO Options

OpenSSO Enterprise 8.0

A community build that has undergone extensive manual and automated testing by Sun Quality Assurance Engineering Team.

Delivered every 12 – 15 months
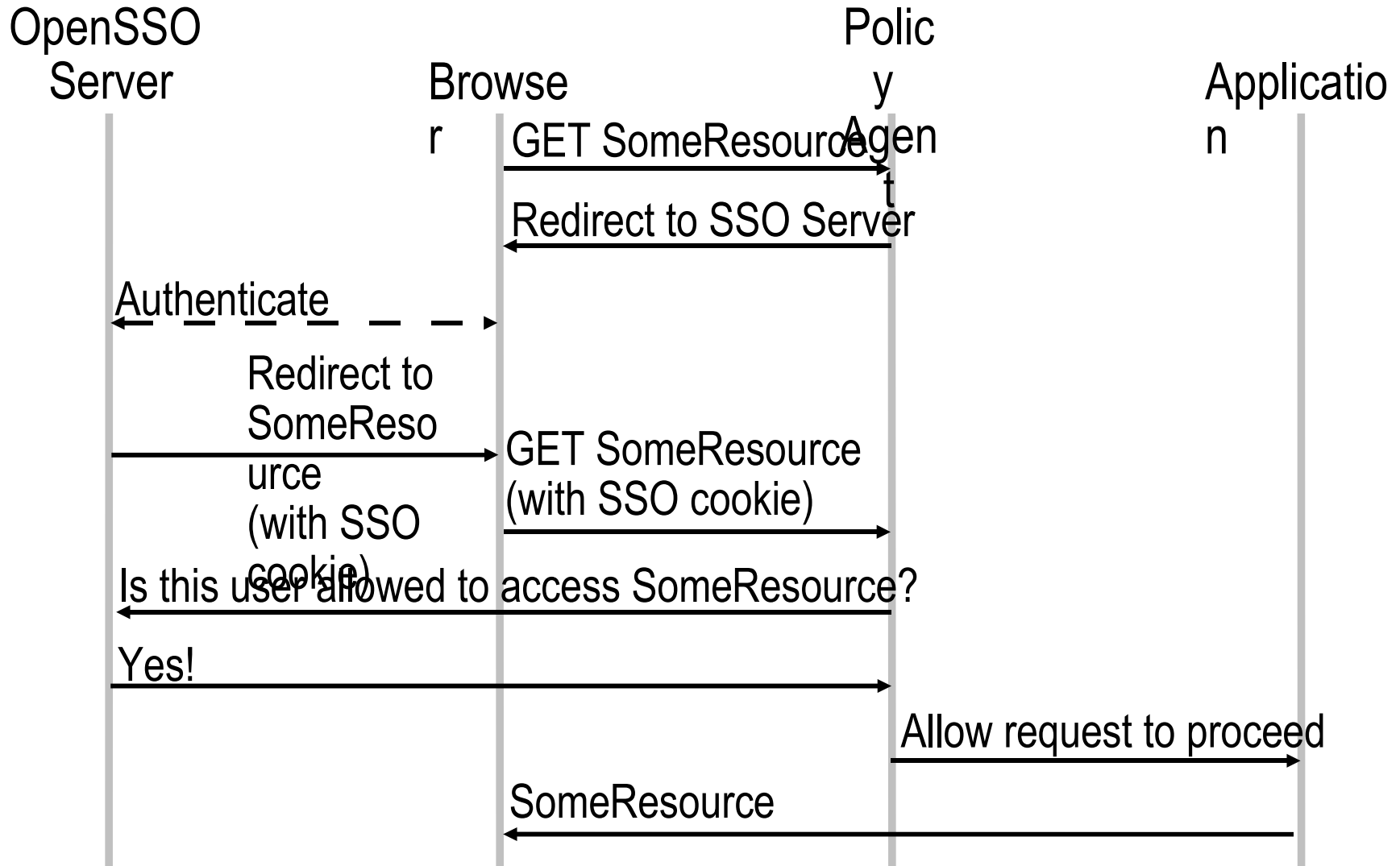
Long term support – hot patches/service packs

OpenSSO Express Builds

A community build that has undergone extensive automated testing and moderate manual testing by Sun's OpenSSO Quality Assurance Engineering Team.

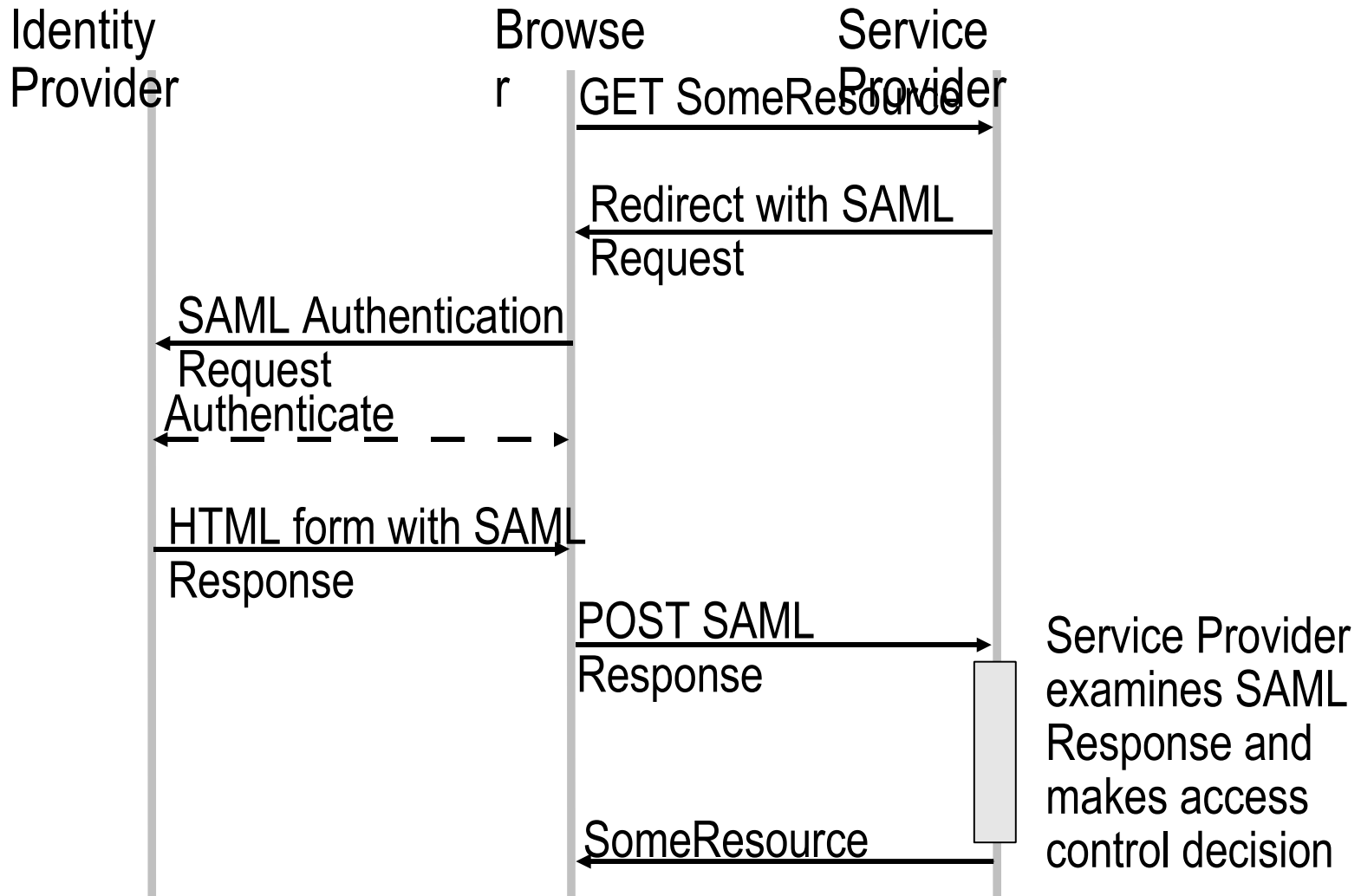Delivered every 3 months

Fixes in the trunk

How It Works – 1: Within the Enterprise

OpenSSO
Server

Browse
r

Polic
y
Agen
t

Applicatio
n

GET SomeResource

Redirect to SSO Server

Authenticate

Redirect to
SomeReso
urce
(with SSO
cookie)

GET SomeResource
(with SSO cookie)

Is this user allowed to access SomeResource?

Yes!

Allow request to proceed

SomeResource

How It Works – 2: Outside the Enterprise

Identity
Provider

Browse
r

Service
Provider

GET SomeResource

Redirect with SAML
Request

SAML Authentication
Request

Authenticate

HTML form with SAML
Response

POST SAML
Response

Service Provider
examines SAML
Response and
makes access
control decision

SomeResource

Software as a Service

Google Apps

 Single sign-on from an identity provider in your enterprise

 Users log in with their enterprise credentials

 SAML 2.0 single sign-on handshake between identity
 provider and Google

Salesforce.com

 Same model, but slight technical differences
 SAML 1.1 rather than SAML 2.0

Let's take a look...

Amazon EC2

Start with OpenSolaris EC2 instance
- Glassfish pre-installed
- Lots more – see http://blogs.sun.com/ec2/

Deploy OpenSSO WAR file
- Web-based configuration
- It. Just. Works.

Configure SAML 2.0 and deploy Fedlet

Next Steps
- Startup script to automagically configure to the environment, instance parameters

The Fedlet

SAML 2.0-enable small service providers

Small (8.5MB) bundle of code and configuration

BIG impact!

Easy to spin up a proof-of-concept:

> Deploy OpenSSO to GlassFish, configure OpenSSO, set up a SAML 2.0 identity provider, create a Fedlet, deploy the Fedlet, single sign-on...
>
> All in less than 5 minutes!

Let's go!

Resources

OpenSSO → http://opensso.org/
http://wiki.opensso.org/

Pat Patterson's Blog → Superpatterns
http://blogs.sun.com/superpat/

Daniel Raskin's Blog → The Smoking Monkey
http://blogs.sun.com/raskin/

Participate!

Join	Download
Sign up at opensso.org	OpenSSO 8.0

Subscribe	Chat
OpenSSO Mailing Lists dev, users, announce	#opensso on freenode.net

Thank You.

Pat Patterson
pat.patterson@sun.com