SAML – Behind the Wheel

August 7, 2012

This post is intended to serve as an introduction to SAML: what it is, what it does, and how it does it. Specially, it will provide the details of web based single sign on (SSO) via SAML 2.0 and includes a demonstration via video.

What does SAML stand for?

Security Assertion Markup Language

What is SAML?

The OASIS Security Assertion Markup Language (SAML) standard defines an XML-based framework for describing and exchanging security information between on-line business partners. This security information is expressed in the form of portable SAML assertions that applications working across security domain boundaries can trust. The OASIS SAML standard defines precise syntax and rules for requesting, creating, communicating, and using these SAML assertions.

What are the components of SAML?

- Identity Provider – Authenticates principals and returns assertions to service providers. *
- Service Provider – Provides resources to principals. Authenticates principals by requesting assertions from an identity provider.
- Assertion – Assert that a principal has been authenticated.

A typical assertion from an identity provider might convey information such as “This user is John Doe, he has an email address of john.doe@example.com, and he was authenticated into this system using a password mechanism.”

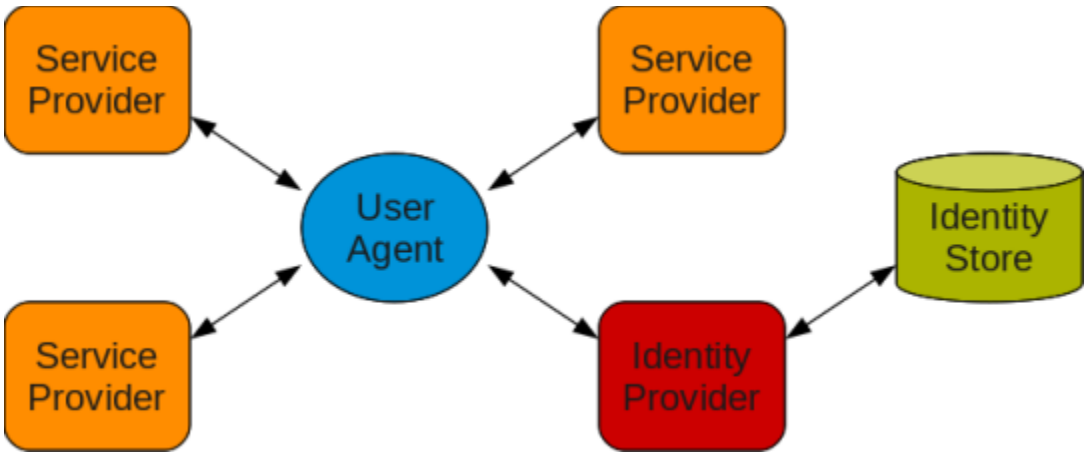
* *SAML does not define how a principal is authenticated against an identity provider.*

What does SAML do?

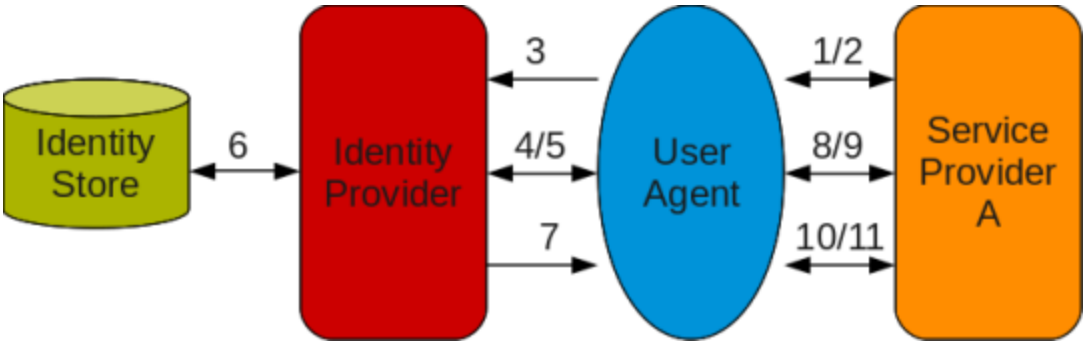
A service provider authenticates a principal by requesting an assertion from an identity provider. The identity provider authenticates the principal, if it has not previously authenticated the principal, and then returns an assertion. The service provider receives the assertion and creates a security context/session for the principal.

What is the process flow?

The following diagram depicts the principal (as a user agent), the identity provider, and multiple service providers in the context of the SAML 2.0 Web Browser SSO Profile.



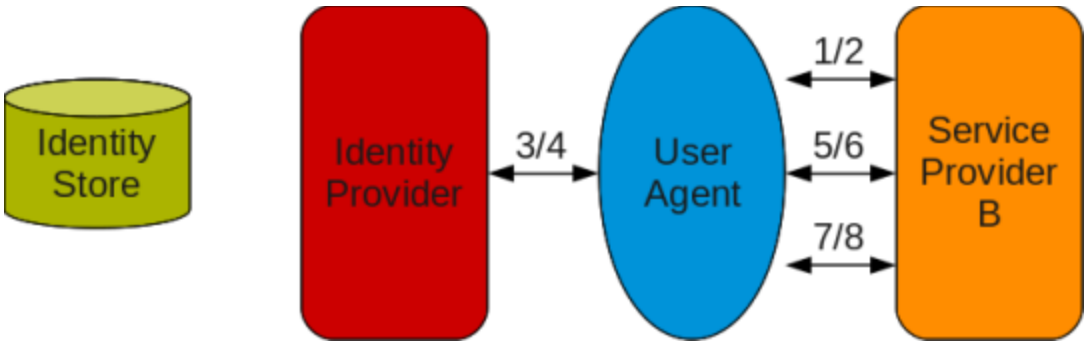
The service provider(s) and the identify provider communicate indirectly via the user agent by using the HTTP redirect and/or HTTP POST bindings. The following diagram depicts the authentication and single sign on process flow using the HTTP redirect binding.



1. The user requests a resource from the service provider.
2. The service provider returns a redirect to the browser (SAML request).
3. The browser is redirected to the identity provider.
4. The identity provider returns an authentication form.
5. The user submits the form to the identity provider.
6. The identity provider authenticates the user.
7. The identity provider returns a redirect to the browser (SAML response).
8. The browser is redirected to the service provider.
9. The service provider returns a redirect to the resource to the browser.
10. The browser is redirected to the resource on the service provider.
11. The service provider returns the resource.

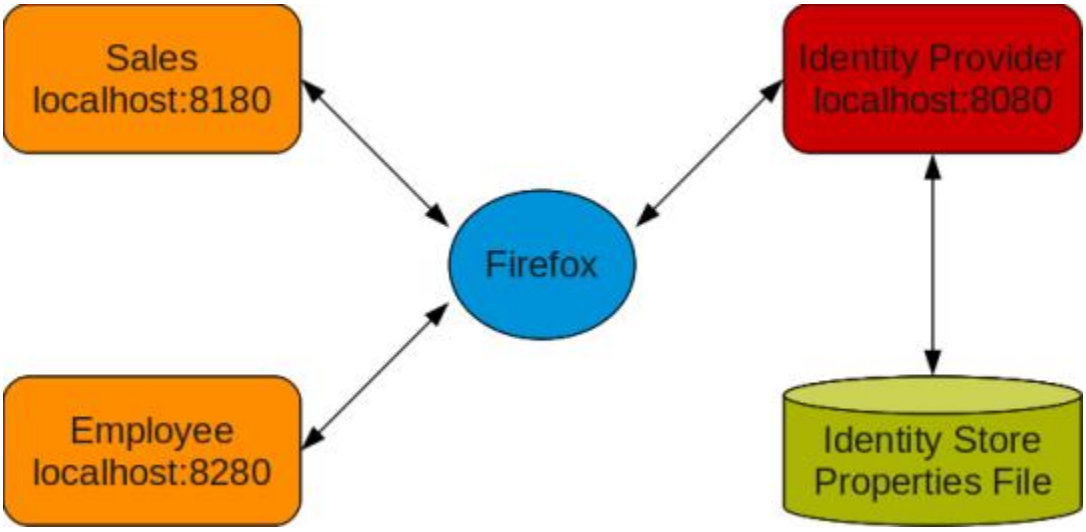
Now that the user has been authenticated, the user can request resources from other service providers without having to authenticate again. The following diagram depicts

the single sign on process flow for an authenticated user requesting a resource from another service provider.



1. The user requests a resource from the service provider.
2. The service provider returns a redirect to the browser (SAML request).
3. The browser is redirected to the identity provider.
4. The identity provider returns a redirect to the browser (SAML response). *Authentication is not necessary because a security context (session) for the user has already been created on the identity provider.*
5. The browser is redirected to the service provider.
6. The service provider returns a direct to the resource to the browser.
7. The browser is redirected to the resource on the service provider.
8. The service provider returns the resource.

Demo



http://videos.videopress.com/0GaV5Wy3/picketlink-saml1_dvd.mp4

This video demonstrates the SAML 2.0 Web Browser SSO Profile and the Single Logout Profile using PicketLink.

The Single Logout Profile undoes the single sign on process. While each service provider has its own security context for the principal, they all share a single *authentication context*. The Single Logout Profile uses the *authentication context* to remove the security context for the principal on the identity provider and on each individual service provider in near real time.

The identity provider and the service providers are running on separate instances of JBoss EAP 5.1 with PicketLink 2.0.1 Final on the same Fedora 16 i686 virtual machine.

Note that SAML 2.0 is fully supported via PicketLink Federation 2.1.1 Final in JBoss EAP 6.