Biometric Single Sign-on using SAML
Architecture & Design Strategies

Ramesh Nagappan
Java Technology Architect
Sun Microsystems
Ramesh.Nagappan@sun.com

Setting Expectations
What you can take away!

- Understand the importance of Single Sign-On (SSO) and its role in enterprise IT applications.
- Get introduced to SAML standard for enabling SSO with Biometric authentication.
- Understand the Architecture and Strategies for implementing Biometric SSO using SAML.
- How to build Multifactor SSO using Biometrics in enterprise IT applications.
Agenda

• The State of the Industry
  > CIO Headaches
  > Identity Management - Promises
  > Single Sign-on : SAML to the rescue
  > Biometric SSO – Development Challenges

• The role of SAML in Biometric SSO
  > Anatomy of SAML
  > SAML use cases
  > How it works

• Biometric SSO: Architecture & strategies
  > Tools of the Trade
  > Implementation Strategies
  > Multi-factor SSO using Biometrics

Information is Everywhere
Growing Exponentially – Thanks to Internet and Open Standards
Web based Application Proliferation

Multiple Sign-on Authentication Silos
Leads to application extensibility dead-ends!
The Promise of Identity Management

Why it is important?

- Standardized platform to manage identity lifecycle supporting multiple and heterogeneous resources.
- Single sign-on (SSO) access to disparate resources within an enterprise and beyond organizational boundaries.
  > SSO and Cross-domain SSO based authentication and authorization
  > Enhance security with Multi-factor based strong authentication
  > Extend access to trusted partnerships via Federated SSO over Internet
- Centralized or distributed policy enforcement
- Auditing and reporting of authentication and authorization events
- Provisioning and De-provisioning users on-demand

Identity Management is Key to a Successful Security Strategy

Single Sign-on: In reality

Single sign-on offers Consistent User experience & Enhanced Security
Allow access to disparate resources with Strong authentication
Enabling Biometric SSO: Challenges

Common implementation challenges?

• How to enable biometric callbacks in Web based applications.
  > Representing Device callbacks without using client-side dependencies.
  > How to ensure confidentiality and integrity of biometric samples in transit.

• How to identify and verify the client origin host and requests.
  > Identifying spoofed clients, message replay, session hijacks.

• How to manage users sessions, idle time and logout.
  > Managing user sessions and monitoring for session timeouts.
  > Performing single log-out across multiple resources without residue.

• How to initiate Multi-factor authentication and share state?

• How to avoid multiple sign-on among multiple applications.
  > Propagating security context with trust boundaries and avoid re-authentication.

• How to perform biometric enrollment using a Web environment.

Introducing SAML

Overview

• Security Assertions Markup Language

• Open XML Standard protocol for exchanging authentication and authorization information.
  > OASIS approved Industry-standard.
  > Designed for SSO, Multi-domain SSO and Federation.
  > SAML 2.0 allow use of SAML in devices, support session management in Web applications.

• Promotes Interoperability among Identity Providers and Service providers.
  > Authentication Provider Independence.

• SAML is used by other industry-standards – Liberty Alliance, OASIS WS-Security and Shibboleth.
SAML Adoption

How is SAML being used today?

• Web Single sign-on (SSO)
  > SAML enables SSO through exchanging authentication and authorization assertions.
  > SSO can be part of single or multiple autonomous domains.

• Federated Identity
  > Establish Federated Identity sharing between trusted partners.

• Attribute-Based Authorizations
  > Communicate Identity information about a subject from Web site to another.

• Securing Web Services
  > SAML assertions can be used within SOAP Messages.
  > OASIS WS-Security TC has defined a SAML Profile to support use of SAML.

Anatomy of SAML

Core components

• SAML Assertions
  > A set of one or more statements made by a SAML Authority/Identity provider.

• SAML Protocols
  > Define Request/Response protocols to support exchanging assertions.
  > Ex. Authentication Request, Single Logout

• SAML Bindings
  > Defines how SAML can be communicated using standard protocols. (ex. HTTP, SOAP)

• SAML Profiles
  > Defines the usage of SAML for an application.
  > Ex. Web Browser SSO Profile
Anatomy of SAML... contd.

Environment specific components

- SAML Metadata
  - Defines how a SAML entity describe its configuration data.

- Authentication Context
  - Defines the type and strengths of authentication requirements.
  - What authentication processes are enforced before issuing the assertion.
    (Ex. Using Multi-factor authentication)

SAML Assertions

SAML Assertions are statements issued by a SAML Authority

- Authentication Assertion
  - SAML statement that represents a successful authentication performed on a subject (Service requestor).

- Authorization Decision Assertion
  - It represents an authorization decision that subject is allowed to access a requested resource.
  - Ex. Ramesh Nagappan is permitted to speak at BC 2006.

- Attribute Assertion
  - It identifies the attributes of a subject, especially additional data intended for the service provider.
  - Ex. Ramesh Nagappan works for Sun Microsystems.
Anatomy of SAML Message

```xml
<saml:Assertion
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0"
    IssueInstant="2006-08-01T17:50:50.000Z">
    <!-- Digital signature of the issuer -->
    <ds:Signature>...</ds:Signature>
    <saml:Subject>
        <saml:NameID
            format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">
            xyz000181
        </saml:NameID>
    </saml:Subject>
    <saml:AuthnStatement
        AuthnInstant="2006-08-01T17:50:30.000Z"
        SessionIndex="123456">  
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>
                urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
            </saml:AuthnContextClassRef>
        </saml:AuthnContext>
    </saml:AuthnStatement>
</saml:Assertion>
```

SAML Security

How to protect SAML assertions?

- SAML recommends the use of **HTTP over SSL/TLS** for ensuring transport-level security.
  > Prevents MITM attacks on SAML assertions.

- SAML supports **XML Signature and XML Encryption** for ensuring message-level confidentiality and integrity.
  > The SAML constructs can be encrypted and digitally signed before issuing the assertion.
SAML Use Case Scenario

**Single sign-on**

- User
- SAML Compliant
  - Identity Provider
    - (ex. identityprovider.sun.com)
    - SAML Asserting Party
- SAML Aware
  - Service Provider
    - (ex. services.ebay.com)
    - SAML Relying Party
- Authenticate
- Access
  - Protected resource (SAML Assertion)

---

Biometric SSO

**Architecture and Design Strategies**

- **Identity Provider**
  - Makes use of SAML compliant Identity provider to issue SAML assertions.
  - Biometric vendor is configured as an authentication provider.
    - Ex. Java Authentication and Authorization (JAAS) LoginModule for enabling Identity provider Integration.

- **Biometric AuthN**
  - Makes use of SAML enabled Biometric authentication provider to issue SAML assertions.
    - Ex. Use OpenSAML support to issue SAML tokens
Biometric SSO: Tools of the Trade

- **Identity Provider Infrastructure**
  - OASIS SAML 2.0
  - Liberty Phase II
  - JAAS (Java Authentication & Authorization Service)
  - LDAP v3
  - JSR-196 (Authentication Provider for Web Services)

- **Biometric Authentication Infrastructure**
  - JAAS LoginModule
  - OASIS SAML 2.0
  - OASIS SPML 2.0 Adapter

- **Identity Provisioning Infrastructure**
  - OASIS SPML 2.0
  - OASIS WS-BPEL 1.1

---

Biometric SSO: Identity Provider Strategy

Using a SAML compliant Identity Provider

- Biometrics Single/Multi-modal
- Request Access
- Perform Authentication
- Issue SAML Assertion
- [SAML Asserting Authority]
- [SAML Relying Authorities]
Biometric SSO: Bio AuthN Provider Strategy

Using a SAML compliant Biometric Authentication Provider

Multi-factor SSO including Biometrics
Case study with Sun Java System Access Manager and BiObex

[Authentication Providers]
Further References

- **Core Security Patterns**
  > Chris Steel, Ramesh Nagappan & Ray Lai
  > Special focus on Identity Management using Biometrics and Smartcards
  > [www.coresecuritypatterns.com](http://www.coresecuritypatterns.com)

- **OASIS SAML 2.0**
  > [www.oasis-open.org/specs/index.php#samlv2.0](http://www.oasis-open.org/specs/index.php#samlv2.0)

- **Sun Java System Identity Mgmt Suite**

Article: Biometric Authentication for J2EE and Web based Applications