Biometric Single Sign-on using SAML
Architecture & Design Strategies

Ramesh Nagappan CISSP
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

• 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
Virtual Enterprise
Web based Application Proliferation
Multiple Sign-on: Authentication Silos
The CIO Headaches

- Drive business innovation
- Protect corporate information
- Improve customer experience
- Enable regulatory compliance
- Streamline the IT operations

Information Security, Compliance and User Experience
Security Requires a Delicate Balance

Consistent user experience without sacrificing security

Height of Fences?
Ease of Access?

How much you can balance – Security vs. User experience?
Security and Identity Management
Bringing Together People and Information Security

- Authentication
- Authorization
- Auditing

- Confidentiality
- Integrity
- Availability
The Promise of Identity Management

Why it is important?

- Standardized Platform for managing Identity life-cycle of an organization and its partners
- 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
- Track and audit authentication and authorization events.
- Provisioning and De-provisioning users on-demand
- Compliance Reporting

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 development challenges?

- How to enable Biometric callbacks in Web based applications.
  - Representing device callbacks without client-side dependencies.
  - How to ensure confidentiality and integrity of biometric samples in transit.

- How to identify and verify the client origin host?
  - Identifying spoofed connections, message replay attack and session hijacks.

- How to manage user sessions, idle time and single logout?

- How to initiate authentication and share state within a Multifactor authentication session?

- How to avoid multiple sign-on scenarios?
  - Propagating security context within trust boundaries and avoid re-authentication.

- How to perform biometric enrollment in a registration workflow?
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.
- SAML is used by other industry-standards – Liberty Alliance, OASIS WS-Security and Shibboleth.
SAML Adoption

How is SAML being used?

• Web Single sign-on (SSO)
  > SAML enables SSO through exchanging authentication 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

<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

Authenticate

SAML Compliant Identity Provider
(ex. identityprovider.sun.com)
SAML Asserting Party

Access

Protected resource
(SAML Assertion)

SAML Aware Service Provider
(ex. services.ebay.com)
SAML Relying Party

Authenticate
Biometric SSO
Architecture and Design Strategies

- Makes use of SAML compliant Identity provider to issue SAML assertions.
- Biometric vendor is configured as an authentication provider.

- Makes use of SAML enabled Biometric authentication provider to issue SAML assertions.
  > Ex. OpenSAML support
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)

- **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: IdP Strategy

Using a SAML compliant Identity Provider

Biometrics
Single/Multi-modal

Request Access

SAML Compliant Identity Provider Infrastructure

Perform Authentication

Biometric AuthN Middleware

Issue SAML Assertion

[SAML Asserting Authority]

[SAML Relying Authorities]

J2EE Applications
Directories
Databases
Enterprise Applications
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

BiObex
Certificate Authority w/ OCSP Resp.
LDAP Directory / Oracle Database

Sun Java System Access Manager
- Authentication
- Authorization
- Policies
- User/Role Profiles
- Audit Logs

[SAML Asserting Authority]
[SAML Relying Authority]

Multi-modal Biometrics
Smartcard (CAC/PKCS#15)
Password

Single Sign-on
Multi-Domain SSO
Federated SSO

Perform Authentication Chain

SSL

Databases / Directories
Portal Applications
Enterprise Applications
Desktops

SAML Assertion

[Authentication Providers]

Biometrics Consortium 2006
Further References

- Core Security Patterns
  - Chris Steel, Ramesh Nagappan & Ray Lai
  - Special focus on Identity Management using Biometrics and Smartcards
  - www.coresecuritypatterns.com

- OASIS SAML 2.0
  - www.oasis-open.org/specs/index.php#samlv2.0

- Sun Java System Identity Suite
  - www.sun.com/products/identity/index.jsp

Article: Biometric Authentication for J2EE and Web based Applications
Biometric Single Sign-on using SAML
Architecture and Design Strategies

Ramesh Nagappan
nramesh@post.harvard.edu
www.coresecuritypatterns.com/downloads