1. Authentication and Authorization

2. Web Services and Security

3. Web Services and Change Management

4. Summary
Business Roles and Privileges

Business Roles
- Represent the business tasks of an employee
- Are usually defined as part of a business process
- Can be set up in hierarchies
- Are a combination of privileges and/or other business roles
- Are usually assigned to end users

Privileges
- Represent the access information or technical authorizations (like ABAP authorization roles, UME roles, Portal roles, AD groups, …)
- Are system specific
- Can span internal and external systems
Role Definition and Provisioning

Role Definition (design, 1-time)
- Read system access information (roles, groups, authorizations, …) from target systems
- Define a business role hierarchy
- Assign technical roles to business roles
- Develop rules for role assignments

Provisioning (regularly)
- Assign or remove roles to/from people
  - manually through Workflow or automatically, e.g. HR-driven/event-driven
- Automatic adjustment of master data and assignments of technical authorizations in target systems

Connectors:
- ABAP (BAPI from 4.6c onwards)
- Java (SPML from SAP NetWeaver 04 onwards)
- Non SAP (MS ADS, LDAP, … and others)
- Connector API in Java
Enterprise Services – Authentication and Single Sign-On

Authentication can occur with solutions that are available with:

- the transport (HTTP protocol)
- the message (SOAP protocol)

Message level mechanisms build on transport level

⇒ authentication levels not mutually exclusive

Authentication solutions supported by SAP NetWeaver:

Service Consumer Application

Service Transport Level
- User ID and Password
- X.509 Client Certificates
- Logon Tickets

Service Message Level
- WSS Username Token Profiles
- WSS X.509 Certificate Token Profiles
- WSS SAML Token Profiles*

*support with SAP NetWeaver CE and PI 7.1.
Down ported to SAP NetWeaver AS ABAP 7.0 SP14 and higher
Security Assertion Markup Language (SAML)

SAML is an established OASIS standard to provide open, standard-based and interoperable Single Sign-On in heterogeneous landscapes.

SAML is a security protocol for
- Encoding authentication (and authorization) information in XML “Assertions”
- Verifying authentication against a SAML assertion authority – source site
- Exchanging authentication information in a request/response fashion

SAML provides Single Sign-On after an initial authentication
- Comparable to SAP Logon Tickets but not cookie based

For secure message exchange SAML uses standard security protocols like SSL, TLS and XML signatures.

Support for SAML is strategic within SAP and will be continuously enhanced.
Benefits of Security Assertions Markup Language (SAML)

- Interoperable security solution to allow systems integration with great ease and minimal resources
- SAML is a protocol for encoding security related information (assertions) into XML and exchanging this information in a request/response fashion
- Provides standard based mechanisms to exchange security information using SOAP, HTTP(s)
- SAML is an OASIS standard
SAML authorities produce “assertions” in response to client requests.

An assertion can consist of

- Authentication Statement:
  - piece of data that represents an act of authentication performed on a subject (user) by the authority
- Authorization Statement
- Attribute Statement
SAML Based Single Sign-On Scenarios

Web Browser based SSO
- SAML Browser/Artifact Profile
- SAML Standard

Web Service based SSO
- SAML Token Profile
- Web Service Security Standard
SAML Token Profiles: Sender Vouches Subject Scenario

Underlies Principal Propagation with Process Integration 7.1

How it works:

Enables access to provider-side resources via consumer side user context in message in an interoperable way

User access to service verified by consumer system with a SAML assertion
Secure Propagation of User Identity

Goal

- Enforce user-based access control for distributed application processes
- Audit user access in service provider backend
- Securely pass the identity of a user in a system-to-system service call

Solutions supporting secure Service Client to Service Provider identity propagation:

- SAP service consumers:
  - Logon Tickets
- Heterogeneous system landscapes:
  - WSS SAML Token Profiles
1. Authentication and Authorization – Identity Management

2. Web Services and Security

3. Web Services and Change Management

4. Summary
The SOAP protocol on its own does not provide any security mechanisms for
- Message Integrity & Confidentiality
- Authentication
- Non Repudiation of origin or receipt

But: SOAP can be extended to provide additional features

Up to the year 2002, best practice was to secure Web Services using Secure Sockets Layer (SSL)

But SSL provides transport – not application-level security
- SOAP Messages secured point-to-point, not end-to-end
- Messages stored unencrypted in files or databases at intermediaries
- not independent of underlying transport protocol

WS-Security submitted to standards body (OASIS) in Sept 2002 and approved as an OASIS Standard in April 2004
WS-Security in SAP NetWeaver Core Concepts

- **Security Templates** describe the security (i.e. Signature) used to protect the message (*What* will be protected). They define common security best practice scenarios.

- **Security Profiles** define the runtime configuration of a Service or Consumer (Proxy) based on a Security Template (*How* will the message be protected).

- One profile may be assigned to multiple operations - that is, when the same certificate is to be used for an XML Signature, or different profiles of the same template are used for operations with different XML Signatures.
WS Security in SAP NetWeaver
Extended message level security options for Web Services

Message authentication
- Username token profiles
- X.509 certificate token profiles
- SAML token profiles

Message guarantees
- XML signatures
- XML encryption
- Web Service Reliable Messaging

Message security configuration
- WS Security Policy
- WS Trust

SOAP Envelope

SOAP Header
- WS-Security Header

SOAP Body
- Security Token
- Timestamp
- Signature
- Encrypted Key + Data
Point to Point Service Consumption – Simplified Example

**System security**
- Service destination to provider
- Exchange system certificates with provider
- Setup transport security (SSL) - optional

**Application security**
- Define web access authentication configuration (in ticket policy configuration)
- Authorization check with UME

**Service security**
- Acquired from WS Security Policy definitions in WSDL
- Create new LP ⇒ must sync with SEI

**System security**
- Exchange system certificates with Consumer
- Setup Service User / User Mapping (ABAP / Portal)
- Setup secure communication (SSL) - optional

**Application security**
- Role based authorization check

**Service security**
- Authentication requirements in SEI
- Service guarantees in SEI
  - Confidentiality (SSL / XML enc)
  - Integrity (XML Sign)
  - WS-Reliable Messaging and fault reports
  - Secure Conversation (with SSL for bootstrap)
- Setup service call via proxy
Mediated consumption via Process Integration

7.1

Service call through Process Integration provides for value added services
- Single point for service provisioning from various providers
- Service Routing, BPM and Mapping
- Connectivity to backend systems
- Asynchronous service capabilities
- XML schema validation for protecting message contents against misuse
- ...

Security options for letting user Bob access to provider:

**Direct Access:**
- User ID/Password (service user based)
- X.509 Certificate (service user based)
- SAML Tokens (propagate end user)
- Logon Ticket (propagate end user)

**Principal Propagation via PI:**
- SAML Token Profile (message)
- Logon Tickets (transport)

Refined access control for brokered access
Security Administration in SAP NetWeaver Administrator

Efficient management of security through integrated interface accessible from a Web browser

Centralized and web based administration of security functionality through integration in SAP NetWeaver Administrator

- Key Storage, Virus Scan, Destinations, Authentication
- Trusted Systems
  - SSO2 Logon Ticket Configuration Wizard
  - SAML Browser Artifact
  - SAML Token Profiles
- Identity Management (User Management Engine user interface)
- Web Service Security configuration management
- Mass Administration for service provisioning
- Remote logging and monitoring administration with Computer Center Management System

Functionality for landscape-based security management with System Landscape Directory functions (continuously enhanced)
Profile/Domain
- Supported Authentication Mechanisms
  - SAML (always possible)
  - Assertion Ticket
  - Username/Password in message

Two runtime configurations on provider and consumer side:

Provider Side
- Consumable via HTTPS
- Supported Authentication Mechanisms: SAML, Assertion Ticket, Username/Password in message

Consumer Side
- Uses HTTPS
- LeaveRequestOverviewService uses service user authentication (Account’s Service User)
- ChangeBankDataService uses SAML authentication
Agenda

1. Authentication and Authorization – Identity Management

2. Web Services and Security

3. Web Services and Change Management

4. Summary
Web Service Change Management and Interoperability

Types of interaction with a Services Registry
- Publish/Unpublish/Update (service provider ↔ service registry)
- Find/Browse/Discover (service consumer/requester ↔ service registry)
- Invoke/Bind (service consumer/requester ↔ service provider)

Challenges
- A WebService is typically consumed by multiple consumer
- Web service that has been running for a while it will most likely change in some regard (e.g. security configuration, bug fixes, or others)

Solution Approach for UDDI 3.x with Subscriptions:
- UDDI version 3 provides the Subscription API Set, which is a mechanism that allows Web service consumers to subscribe to certain search criteria or directly to certain UDDI entities in order to get informed about changes in the registry.
UDDI Notification Mechanisms

Synchronous change tracking

Asynchronous notifications
1. Authentication and Authorization – Identity Management

2. Web Services and Security

3. Web Services and Change Management

4. Summary
# SAP NetWeaver Platform Based Security Solutions:
Integrated infrastructural services for meet requirements of diverse enterprise environments

<table>
<thead>
<tr>
<th>REQUIREMENT</th>
<th>SAP NETWEAVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empower business users</td>
<td>- Delegated user and content administration with centralized Identity Management for landscapes</td>
</tr>
<tr>
<td></td>
<td>- Support for flexible service and user authentication and SSO solutions</td>
</tr>
<tr>
<td>Simplify administration and ensure business continuity with lower TCO</td>
<td>- Integrated security administration in Web-based NetWeaver Administrator</td>
</tr>
<tr>
<td></td>
<td>- SAP NetWeaver Identity Management</td>
</tr>
<tr>
<td></td>
<td>- Standards-based security solutions</td>
</tr>
<tr>
<td>Native support for interoperable and flexible security solutions based on</td>
<td>- JAAS</td>
</tr>
<tr>
<td>open standards</td>
<td>- SAML</td>
</tr>
<tr>
<td></td>
<td>- SPML</td>
</tr>
<tr>
<td></td>
<td>- GSS API</td>
</tr>
<tr>
<td>Security Solutions for Enterprise Service Oriented Architectures and Process</td>
<td>- WS-Security</td>
</tr>
<tr>
<td>Integration</td>
<td>- WS-Secure Conversation</td>
</tr>
<tr>
<td></td>
<td>- WS-Policy and WS-SecurityPolicy</td>
</tr>
<tr>
<td></td>
<td>- WS-Reliable Messaging</td>
</tr>
<tr>
<td>Infrastructure-based protection of SAP NetWeaver applications against</td>
<td>- WS-Security, WS Security Extensions*</td>
</tr>
<tr>
<td>common attacks</td>
<td>- SAML Browser Artifacts and WSS SAML Token Profiles</td>
</tr>
<tr>
<td></td>
<td>- Service Repository and Composites Security</td>
</tr>
<tr>
<td></td>
<td>- Access control and secure key management</td>
</tr>
<tr>
<td></td>
<td>- Virus Scanning interface, Output Encoding, Blacklist filtering, XML Schema Validation with PI 7.1</td>
</tr>
</tbody>
</table>

*support for XML Signatures, Username and Certificate token Certificates. Full support for XML Encryption and SAML Token Profiles with SAP NetWeaver 7.10, down port to SAP NetWeaver 7.0 AS ABAP SP 14 and higher