Agenda

1. **Typical Authentication and SSO Scenarios in SOA**
2. Windows Integration Authentication using Kerberos with SAP NetWeaver
3. Authentication with SAML
4. Single Sign-On using SAML Token Profile
5. Outlook
Secure authentication or SSO of users accessing enterprise resources

Authorize user access to enterprise system resources with user’s own role and permission assignments

Audit user access to enterprise system resources

Access Management and the User Authentication Lifecycle in SOA

Initial User Authentication or SSO to Portal or Desktop application

User Identity Propagation for Service Call
Single Sign-On

Single Sign-On (SSO)

- User authenticates once against a security system
- User is then seamlessly authenticated to access other systems
- Authentication against other applications is transparent for the user

Identity Management for SSO

- Synchronization, provisioning or mapping of user identities for SSO
- User identities for SSO must match to avoid unintended “user impersonations”
- Central user identity management to avoid redundant user information

Mainstream Integrated Authentication and SSO Solutions in SAP NetWeaver

- X.509 Client Certificates and PKIs
- Windows Integrated Authentication and Kerberos
- SAP Logon Tickets and Trusted Systems
- SAML Assertions with Trusted Systems
- Header Variables
- Custom – JAAS or GSS-API v2 based integration
Standardizing End to End SSO Scenarios on SAML

**Initial User Authentication**
- Any Supported Solution
  - e.g. SPNego for Windows integrated authentication

**SSO for Web browser applications**
- SAML Browser/Artifact Profile

**SSO for Web Services**
- WSS SAML Token Profile

1. **Integrated User Authentication against Portal**
   - Any Supported Solution e.g. SPNego for Windows integrated authentication
   - SAML Browser/Artifact Profile

2. **SSO with SAML Browser Artifact**
   - Synchronize User Identities for SSO with SAP NetWeaver Identity Management or User Mapping

3. **Access to Resource with WSS SAML Token Profile**
   - SAML Identity Provider
   - SAP NetWeaver Portal or CE 7.1
   - Web Service Provider
   - SAP NetWeaver AS ABAP
   - Web Service Consumer
   - SAP NetWeaver AS ABAP
Agenda

1. Typical Authentication and SSO Scenarios in SOA
2. Windows Integration Authentication using Kerberos with SAP NetWeaver
3. Authentication with SAML
4. Single Sign-On using SAML Token Profile
5. Outlook
In this Section:
Focus on Windows Integrated Authentication

The Big Picture

IBM/Lotus applications
Microsoft based applications
HR
WebDynpro
IdM
other SAP Systems

UME (Web AS Java)

SSO
SAP NetWeaver Portal
IdM / LDAP Directory

Create and modify users
Use as user repository
Synchronize user data
Use as user repository

Microsoft Active Directory and Windows Domain
Kerberos for User Authentication in SAP NetWeaver – SSO Process

1. Initial logon in Domain
2. Call Portal URL
3. Error 401
   Req. Kerberos Ticket
4. Kerberos Ticket Request
5. Kerberos Ticket Response
6. Forward Kerberos Ticket
7. Ticket verification and user ID resolution
8. Username
9. Resource

Authenticate once to Domain

SSO Access to Information Content Available from Portal Server iViews

Intranet  CRM
Business Apps  BI
Collaborate  Other…
Enabling User Authentication with Kerberos on the SAP NetWeaver Portal: SPNegoLoginModule

Integrated User Authentication from Browser to SAP NetWeaver AS Java/Portal by natively leveraging Microsoft Windows credentials (Kerberos) for authentication

Prerequisites
- Microsoft Windows domain

Authentication of users is delegated to the Windows Domain Controller
1. User authenticates against Windows domain on his or her workstation
2. On portal access user’s browser sends Kerberos Session Ticket to SAP NetWeaver AS Java or Portal
3. UME of AS Java/Portal resolves user id from User Principal Name in Windows Domain
4. Further user interactions with Portal and backend systems in iViews with SSO tickets

Typical deployment scenarios
- Intranet scenarios

Active Directory / Windows domain controller

1. Windows domain Logon
2. Browser Sends windows credentials
3. SPNego checks via JVM credentials against DC and UME resolves user id
4. SAP Logon Ticket issued

SAP NetWeaver AS Java / Portal
### JAAS SPNego LoginModule: Authentication

**Flow on the Wire**

---

**Portal Sniffer - Response Headers**

<table>
<thead>
<tr>
<th>ID</th>
<th>Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><strong>HTTP/1.1 401 Unauthorized</strong></td>
</tr>
<tr>
<td></td>
<td>Server: SAP J2EE Engine/6.40</td>
</tr>
<tr>
<td></td>
<td>Content-Type: text/html; charset=utf-8</td>
</tr>
<tr>
<td></td>
<td><strong>WWW-Authenticate: Negotiate</strong></td>
</tr>
<tr>
<td></td>
<td>pragma: no-cache</td>
</tr>
<tr>
<td></td>
<td>cache-control: no-cache</td>
</tr>
<tr>
<td></td>
<td>expires: 0</td>
</tr>
<tr>
<td></td>
<td>Date: Fri, 12 Aug 2005 17:29:21 GMT</td>
</tr>
<tr>
<td></td>
<td>Transfer-Encoding: chunked</td>
</tr>
</tbody>
</table>
SPNego Use Cases

SPNego can see application for authentication in many scenarios

- SAP NetWeaver Portal in intranet
- SAP NetWeaver Portal in intranet + external access with SSO tickets or SAML to Portal applications:
  - Web Dynpro applications
  - ABAP applications, e.g. SAP BW web reports, BSP pages,…
  - Integrated ITS (as of 6.40 onwards)
- Duet scenario for service-based access and SSO to SAP NetWeaver applications
- …and others

Security considerations

- In the JVM 1.4.x versions, Kerberos tokens are only 56-bit encrypted
- Good passwords for the J2EE user account in AD are important for the security of the solution
- The Kerberos Key Table represents the J2EE engine’s identity; Malicious users who obtain the Key Table can setup a phishing site by impersonating the J2EE engine
  - Generate the Key Table with encryption type DES-CBC-MD5; do not use DES-CBC-CRC
  - Keep the Key Table file in a safe place. Allow only <SID>adm and SAPService<SID> to access the Key Table
- In a high security environment, change the service user’s password (and the Key Table) periodically
Available scenarios:
- DB, ADS, multiple ADS as data source
- SUN JDK
- IBM JDK

Launch the Wizard using: http://<server>:<port>/spnego

SPNEGO Configuration Wizard

Step 1 of 4: Prerequisites

- Service user is created and configured in Active Directory
- UME configuration includes SPNego specific settings

Information

1. Create a new user on your domain controller.
   a. Enable the "Password Never Expires" option for this user.
   b. Enable the "Use DES encryption" option for this user.

   We recommend that you use the naming convention j2ee.<SID> for the sAMAccountName attribute of this user.

2. Associate Service Principal Names (SPNs) with the created services user.

   For every DNS name you use to access the Java AS add SPN to the service user account.

   setspn -a HTTP:portal.customer.de j2ee.<SID>
   setspn -a HTTP:alias.customer.de j2ee.<SID>

Close
### SPNEGO Configuration Wizard

**Step 2 of 4: Kerberos Realm**

<table>
<thead>
<tr>
<th>Kerberos Realm</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSCTSC.SAP.CORP</td>
<td></td>
</tr>
</tbody>
</table>

**Realm Configuration**

**KDCs (Key Distribution Centers)**

<table>
<thead>
<tr>
<th>KDC Host</th>
<th>KDC Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSCTSCDC1</td>
<td>88</td>
</tr>
</tbody>
</table>

**KPH (Kerberos Principal Name)**

- **Service User Name**: j2EE-F26-MSCTSC040@MSCTSC.SAP.CORP
- **Service User Password**: ********
- **LDAP Host**: 389
- **LDAP Port**: 389

- **Enter Principal**
  - **Principal**: j2EE-F26-MSCTSC040@MSCTSC.SAP.CORP
  - **Password**: ********
Includes the test facility for the selected user resolution mode
SPNEG0 Configuration Wizard

Step 4 of 4: Confirmation

Your engine will be configured for the following realms:

Realm: MSCTSC.SAP.CORP
Principal:
  J2EE-F26-MSCTSC040@MSCTSC.SAP.CORP
KDC:
  MSCTSCDCT:88

Summary of configuration for confirmation
Configuration on the browser clients

- Windows integrated authentication must be switched on
- NetWeaver AS host must be explicitly assigned to local intranet
- Automatic logon in intranet zone must be allowed
Summary

SPNego leverages the Kerberos security standard, which is a built-in capability of a Microsoft Windows user desktop environment, to securely authenticate users to SAP NetWeaver AS Java applications.

Prerequisites:
- SAP NetWeaver J2EE 6.40 SP15 or higher
- SAP NetWeaver 7.0 J2EE SP6 or higher
- SAP NetWeaver 7.1 Composition Environment

SPNego enables integrated Windows authentication to the SAP NetWeaver Portal and AS Java:
- Subsequent single sign-on (SSO) to SAP business applications in Portal, AS Java or AS ABAP, displayed in Portal iViews

AS Java Configuration Wizard under application alias /spnego

Useful SAP Notes:
- **968191 – SPNego: Central Note**
- **957666 – Diagtool for Troubleshooting Security Configuration**
Agenda

1. Overview SOA Scenarios
2. Windows Integration Authentication using Kerberos with SAP NetWeaver
3. **Authentication with SAML**
   3.1 Overview of SAML
   3.2 SAML Browser/Artifact Profile
   3.3 Configuration
4. Single Sign-On using SAML Token Profile
5. Outlook
Benefits of Security Assertions Markup Language (SAML)

- **Interoperable security solution** to allow systems integration with great ease and minimal resources.
- SAML can be used **across different security domains** (e.g. In a B2B scenario).
- 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**, which is widely adopted in the industry and vendor independent.
SAML Based Scenarios

1. Authentication
   - SAML Token Profile
   - Web Service Security Standard

2. Access to Resource
   - SAML Browser/Artifact Profile
   - SAML Standard
Security Assertion Markup Language (SAML) Building Blocks

- **Assertions**: statements about a subject. This could be an authentication, attribute information, or authorization permissions.

- **Protocols**: SAML defines request/response protocols for obtaining assertions.

- **Protocol Bindings**: defines how SAML protocols map to transport and messaging protocols, e.g. SAML SOAP Binding.

- **Profiles**: define how assertions, protocols, and bindings are combined for particular use cases.
SAML Assertion

SAML Issuing Authorities produce “Assertions” in response to client requests.

An SAML Assertion can consist of

- **Authentication Statement**: Piece of data that represents an act of authentication performed on a subject (user) by the SAML Issuing Authority

- **Other Statements**: Attribute Statement, Authorization Decision Statement
SAML Request / Response

Request

<samlp:Request
  RequestID="ID563AD51D8FE16A713C4E38C279492DDEDAB65A5A"
  xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol">
  <samlp:AssertionArtifact>AAH7boOW79mDzbpq7B35WtLF4MP0rzC3J3BM16F+g
  mOEluFkAAAAAAA</samlp:AssertionArtifact>
</samlp:Request>

Response

<samlp:Response
  InResponseTo="ID563AD51D8FE16A713C4E38C279492DDEDAB65A5A"
  xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol">
  <samlp:AssertionArtifact>AAH7boOW79mDzbpq7B35WtLF4MP0rzC3J3BM16F+g
  mOEluFkAAAAAAA</samlp:AssertionArtifact>
  <saml:Assertion
    AssertionID="ID9BB9590058FBC303414444F2D8D81C52D91D640B"
    ResponseID="ID67AB48DAFA08159A35AE6B4BAB109D8E0AF063E9"
    Issuer="www.samlssodemo.com">
    <saml:AuthenticationStatement
      AuthenticationMethod="urn:ietf:rfc:1510">
      <saml:Subject>
        <saml:NameIdentifier>SAML_DEST</saml:NameIdentifier>
      </saml:Subject>
    </saml:AuthenticationStatement>
  </saml:Assertion>
</samlp:Response>
Agenda

1. Overview SOA Scenarios
2. Windows Integration Authentication using Kerberos with SAP NetWeaver
3. **Authentication with SAML**
   3.1 Overview of SAML
   3.2 SAML Browser/Artifact Profile
   3.3 Configuration
4. Single Sign-On using SAML Token Profile
5. Outlook
SAML – Browser/Artifact Profile for Web SSO

1. Request for a Resource

2. Redirect URL + Artifact

3. SAML Assertion Request

4. SAML Response with Assertion

5. Resource

Initial logon

Source Web Site

SAML Identity Provider

SAML Service

SAML Responder

SAP NW Portal

Destination Web Site

SAML Service Provider

SAML Service

Determine IdP based on SourceID provided with the Artifact

Analyze Assertion

ICF/SAML LoginModule

Authenticate User (User Mapping)

Artifact Receiver

Resource

Redirect

Service Consumer

Create Artifact and Assertion

Determine SAML Artifact Receiver URL

© SAP 2008 Page 27
SAP Landscape

Source Web Site

- SAML Identity Provider
  - SAML Service
  - SAML Responder
- SAP NetWeaver Portal

Destination Web Site

- SAML Service Provider
  - Resource
    - ICF
    - SAP NW ABAP
    - SAML Login Module
    - SAP NW Java
  - SAML Service
    - SAP NW Java
  - Artifact Receiver
    - SAP NW Java

Service Consumer
1. Overview SOA Scenarios
2. Windows Integration Authentication using Kerberos with SAP NetWeaver
3. **Authentication with SAML**
   3.1 Overview of SAML
   3.2 SAML Browser/Artifact Profile
   **3.3 Configuration**
4. Single Sign-On using SAML Token Profile
5. Outlook
Configuration of SAML With NW Portal as Source Site

Prerequisites:

- You have configured SSL

Create a role with the action “SAML Responder” and assign it to the technical user that is used by the Destination Site to get the assertion

Maintain configuration data for the destination sites (SAML outbound partner definition)

Create a system object for the NW AS ABAP and system alias

Maintain Portal Content (e.g. iView)
Maintain Configuration Data for the Destination Sites (SAML Outbound Partner Definition)

NWA: Configuration Management – Infrastructure – Trusted Systems - SAML Browser/Artifact Profile – Outbound Partners
Create a System Object for the NW AS ABAP and System Alias

**Portal:** System Administration – System Configuration
New Property: **SAML Partnername**
New Logon Method value: **SAML Browser/Artifact**
Configuration of SAML With NW AS ABAP as Destination Site

Prerequisites:
- You have configured SSL

Source

get assertion

request

HTTPS

1

2

NW AS Java

RFC

Establishing a Connection between AS ABAP and AS Java (RFC)

Configuring AS Java as a SAML Destination Site (Partner Inbound)

Activating SAML for Resources in the AS ABAP (SAML Login Module)

Mapping SAML Principals to AS ABAP User ID’s (VUSREXTID)

Configuring the Portal as a SAML Source Site
Configuring AS Java as a SAML Destination Site (Partner Inbound)

NWA: Configuration Management – Infrastructure – Trusted Systems - SAML Browser/Artifact Profile – Inbound Partners
Activating SAML for Resources in the AS ABAP (SAML Login Module)

Transaction SICF: Logon Procedure: Alternative Logon Procedure

Logon Procedure: SAML Authentication

Maintain RFC Destination on AS ABAP
Mapping SAML Principals to AS ABAP User ID’s (VUSREXTID)

Transaction SM30: VUSREXTID
New External ID type: SA for SAML NameIdentifier

New Entries: Details of Added Entries

<table>
<thead>
<tr>
<th>External ID type</th>
<th>SA</th>
<th>SAML NameIdentifier (PartnerID.NameQualifier.Name)</th>
</tr>
</thead>
<tbody>
<tr>
<td>External ID</td>
<td>SAML_SOURCE_SITE_CE1: D023939</td>
<td></td>
</tr>
<tr>
<td>Seq. No.</td>
<td>000</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>D023939</td>
<td></td>
</tr>
<tr>
<td>Min. date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activated</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Administration Data

<table>
<thead>
<tr>
<th>Hash value for ext. ID</th>
<th>Length Ext. ID</th>
<th>Created By</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>D023939</td>
</tr>
</tbody>
</table>

Administration Data USREXTIDH

<table>
<thead>
<tr>
<th>Created By</th>
<th>Changed</th>
</tr>
</thead>
<tbody>
<tr>
<td>D023939</td>
<td>04.08.2008 16:15:02</td>
</tr>
</tbody>
</table>
Configuration of SAML With NW AS Java as Destination Site

Prerequisites:
- You have configured SSL

Configuring the Portal as a SAML Source Site

Configuring AS Java as a SAML Destination Site (Partner Inbound)

Adjust login module stack
## Support of SAML Browser/Artifact Profile

### Support for the “SAML Browser/Artifact Profile” as Destination Site

<table>
<thead>
<tr>
<th>Functionality</th>
<th>NW04</th>
<th>NW 7.00</th>
<th>NW &gt;=7.10</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML Browser/Artifact Profile – Java</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SAML Browser/Artifact Profile - ABAP</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
</tbody>
</table>

### Support for the “SAML Browser/Artifact Profile” as Source Site

<table>
<thead>
<tr>
<th>Functionality</th>
<th>NW04</th>
<th>NW 7.00</th>
<th>NW &gt;=7.10</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML Browser/Artifact Profile – SAP NetWeaver Portal</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
</tbody>
</table>
Agenda

1. Overview SOA Scenarios
2. Windows Integration Authentication using Kerberos with SAP NetWeaver
3. Authentication with SAML
4. **Single Sign-On using SAML Token Profile**
   4.1 Overview
   4.2 Configuration
5. Outlook
SAML Based Scenarios

Web Service based SSO
- SAML Token Profile
- Web Service Security Standard

Web Browser based SSO
- SAML Browser/Artifact Profile
- SAML Standard
The OASIS WS-Security Standard extends a SOAP message by one or more **WS-Security Headers** (wsse:Security) which contains security information for each recipient.

This new SOAP Header contains all relevant security metadata to secure a SOAP message, such as:
- **Security Tokens** to carry security information (e.g. user authentication data, X.509 certificates)
- A **Timestamp** to protect against Replay Attacks
- **Signatures** to protect against message tampering*
- **Encrypted Keys** and **Data** to protect confidential information

Single Sign-On is provided by using e.g. SAML Security Tokens

* The act of altering something secretly or improperly
Relationship between WS Security SAML Token Profile and the SAML Standard

WS-Security

Profiles

- SAML Confirmation Methods

Bindings

- Assertions and Protocol
  - SAML Assertions
  - Authentication, Attribute and Authorization Information

SAML Token Profile

SOAP Message Security

Username Token Profile

...
The **SAML Token Profile** defines the use of **SAML Assertions** as **Security Tokens** in the **WS-Security Header**.

The SAML Token is used by the service provider to authenticate the user based on the identity information in the SAML Assertion in incoming requests from service consumers.
Web Services SSO with SAML General Message Exchange

1. Web Service (WS) Consumer authenticates at the Token Issuer (Security Token Service, STS) and requests a SAML Token
2. Token Issuer authenticates the User and issues a SAML Token to the WS Consumer
3. WS Consumer uses the SAML Token for authentication at the WS Provider
4. WS Provider must trust the assertion in the SAML Token to authenticate the WS Consumer and sends back the response

The SAML Token profile addresses two major questions:

- How can the SAML assertions be bound to the SOAP message so that the service provider can be sure that they belong together?
- How can the service provider be sure that the sender of the message is really the subject in the assertion?
**Sender-Vouches**: Basis of trust is the WS Consumer’s certificate

- **Sender-Vouches (SV) Subject Confirmation Method**
  - The WS Consumer cryptographically binds the assertion to the body of the SOAP message by signing both with its private key
  - The WS Provider compares the identity information from the message signature with the subject information in the assertion

- **Holder-of-Key (HoK) Subject Confirmation Method**
  - The assertion holds a key that is used by the WS Consumer to cryptographically bind (sign) the assertion and the body of the SOAP message
  - The WS Provider uses the same key to verify the signature. The subject in the assertion is the party that can demonstrate that it is the holder of the key
Benefits of WS-Security

The Reverse Proxy terminates the SSL connection between WS Consumer and WS Provider.

SSL Only Point-to-Point security

End-to-End security
Example of SAML Token Profile Usage

```xml
<wsse:Security>
  <saml:Assertion AssertionID="SAML_ID" Issuer="www.example.org" />
  <saml:Conditions NotBefore="..." NotOnOrAfter="...">
    <saml:AuthenticationStatement AuthenticationMethod="urn:...:password"
      AuthenticationInstant="2005-03-19T...Z"
      ...
    <saml:Subject>
      <saml:NameIdentifier>MUELLERTHOM2</saml:NameIdentifier>
      <saml:SubjectConfirmation>
        <saml:ConfirmationMethod>
          urn:oasis:names:tc:SAML:1.0:cm:sender-vouches
        </saml:ConfirmationMethod>
        <ds:KeyInfo> ...
      </saml:SubjectConfirmation>
    </saml:Subject>
  </saml:AuthenticationStatement>
  <ds:Signature>
    <ds:SignedInfo>
      ...
      <ds:Reference URI="SAML_ID"> ...
    </ds:SignedInfo>
  </ds:Signature>
</saml:Assertion>
</wsse:Security>
```
Agenda

1. Overview SOA Scenarios
2. Windows Integration Authentication using Kerberos with SAP NetWeaver
3. Authentication with SAML
4. **Single Sign-On using SAML Token Profile**
   4.1 Overview
   4.2 Configuration
5. Outlook
Configuring SAML Trust Connection between ABAP systems

- In the consumer system, start the Trust Manager
- In the system PSE, find the certificate of the consumer system that issues SAML assertions
- Export this system’s certificate
- In the provider system import the consumer system’s certificate

STRUST
Enabling SSO with SAML Token Profile

- Configure a WS service endpoint for providing a Web Service
- Configure a WS port for consuming a Web Service

Maintain User Mapping

SOAMANAGER

SE38 - RSUSREXTID
Configure a WS Service Endpoint for Providing a Web Service

Transaction: **SOAMANAGER** – Application and Scenario Communication – Single Service Administration: **Service** Configuration
Configure a WS Port for Consuming a Web Service

Transaction: **SOAMANAGER** – Application and Scenario Communication – Single Service Administration: **Consumer Proxy** Configuration
Maintain User Mapping

Transaction **SE38 : RSUSREXTID**

Enter Correct SNC Names in Table View VUSREXTID (from SAP R/3 4.5)

<table>
<thead>
<tr>
<th>User</th>
<th>D023539</th>
<th>to</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User group</td>
<td></td>
<td>to</td>
<td></td>
</tr>
<tr>
<td>External ID type</td>
<td>SA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix of External Name</td>
<td>CN=TE1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suffix of External Name</td>
<td>M23/000::</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optional: Name of Issuer</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Only Users Without Ext. Names
- Test Mode
Support of WS Security with the SAP NetWeaver Platform

Support for the “**SAML-Token Profile**” for Web Services

<table>
<thead>
<tr>
<th>Functionality</th>
<th>NW04</th>
<th>NW 7.00</th>
<th>NW &gt;=7.10</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSS SAML Token Profile - Java</td>
<td>-</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>WSS SAML Token Profile - ABAP</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Support for the “**XML Signature/ XML Encryption**” for Web Services

<table>
<thead>
<tr>
<th>Functionality</th>
<th>NW04</th>
<th>NW 7.00</th>
<th>NW &gt;=7.10</th>
</tr>
</thead>
<tbody>
<tr>
<td>XML Signature/ XML Encryption – Java</td>
<td>-</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>XML Signature/ XML Encryption – ABAP</td>
<td>-</td>
<td>x</td>
<td>X</td>
</tr>
</tbody>
</table>
Agenda

1. Overview SOA Scenarios
2. Windows Integration Authentication using Kerberos with SAP NetWeaver
3. Authentication with SAML
4. Single Sign-On using SAML Token Profile
5. Outlook
### SSO in the SAP NetWeaver Roadmap

<table>
<thead>
<tr>
<th>Role &amp; Authorization Mgmt.</th>
<th>Identity Management</th>
<th>Enterprise SOA and Standards</th>
<th>Security Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meta-roles definition and assignment</td>
<td>Central Identity Management for heterogeneous landscapes</td>
<td>Standards-based principal propagation</td>
<td>Harmonization of security administration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enhanced support for WS-* standards</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Standards-based single sign-on infrastructure (SAML)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identity federation support (SAMLv2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Add. WS-* standards (WS-Sec.Conversation, WS-Trust)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Model driven security management</td>
<td></td>
</tr>
</tbody>
</table>

- **2007/2008**
  - Trust Configuration using X.509 System Certificates
  - Secure Single Sign On and Single Log Out for Trusted Systems in Heterogeneous Landscapes
  - User Mapping, Account Linking and Identity Federation from Authentication Protocols

- **2009**
  - Role management simplification and TCO reduction
  - Business process integrated identity management
  - Centralized policy-based security administration

- **2010 and beyond**
  - Role & Authorization Mgmt.
  - Identity Management
  - Enterprise SOA and Standards
  - Security Management
No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, SAP Business ByDesign, ByDesign, PartnerEdge and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned and associated logos displayed are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

The information in this document is proprietary to SAP. No part of this document may be reproduced, copied, or transmitted in any form or for any purpose without the express prior written permission of SAP AG. This document is a preliminary version and not subject to your license agreement or any other agreement with SAP. This document contains only intended strategies, developments, and functionalities of the SAP® product and is not intended to be binding upon SAP to any particular course of business, product strategy, and/or development. Please note that this document is subject to change and may be changed by SAP at any time without notice. SAP assumes no responsibility for errors or omissions in this document. SAP does not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

SAP shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. This limitation shall not apply in cases of intent or gross negligence.

The statutory liability for personal injury and defective products is not affected. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third-party Web pages nor provide any warranty whatsoever relating to third-party Web pages.

Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP AG nicht gestattet. In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden.

Einige von der SAP AG und deren Vertriebspartnern vertriebene Softwareprodukte können Softwarekomponenten umfassen, die Eigentum anderer Softwarehersteller sind.

SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, SAP Business ByDesign, ByDesign, PartnerEdge und andere in diesem Dokument erwähnte SAP-Produkte und Services sowie die dazugehörigen Logos sind Marken oder eingetragene Marken der SAP AG in Deutschland und in mehreren anderen Ländern weltweit. Alle anderen in diesem Dokument erwähnten Namen von Produkten und Services sowie die damit verbundenen Firmenlogos sind Marken der jeweiligen Unternehmen. Die Angaben im Text sind unverbindlich und dienen lediglich zu Informationszwecken. Produkte können länderspezifische Unterschiede aufweisen.


Die gesetzliche Haftung bei Personenschäden oder Produkthaftung bleibt unberührt. Die Informationen, auf die Sie möglicherweise über die in diesem Material enthaltenen Hotlinks zugreifen, unterliegen nicht dem Einfluss von SAP, und SAP unterstützt nicht die Nutzung von Internetseiten Dritter durch Sie und gibt keinerlei Gewährleistungen oder Zusagen über Internetseiten Dritter ab.

Alle Rechte vorbehalten.