Agenda

SAP NetWeaver Single Sign-On: Solution overview
- Key benefits of single sign-on
- Solution positioning

Identity Provider and Security Token Service

Secure Login
- SSO using Kerberos authentication
- SSO using X.509 certificate authentication
- Secure Store & Forward (SSF) integration
- Strong authentication

Enterprise Single Sign-On

Secure communication channel
SAP NetWeaver Single Sign-On
Solution overview
SAP offers a complete suite of compliance, governance, identity management, and single sign-on solutions.
SAP NetWeaver Single Sign-On
Single sign-on and secure communication channels

Secure Communication Channel
- Encryption of communication channel
- Integrity
- Compliance
- Confidentiality

SSO
- Improved security
- Reduction of password-related helpdesk calls
- Improved user productivity
- Alternative user authentication
SAP NetWeaver Single Sign-On
Key capabilities

- Single sign-on for SAP GUI for Windows, SAP GUI for Java, Web applications
- Integration capabilities (Microsoft Active Directory Server; Microsoft Certificate Store)
- Strong encryption of communication channels between client and SAP application server
- Single sign-on for legacy systems
- Support of additional authentication methods (Radius, smart cards)

This presentation and SAP’s strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. 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.
Positioning of SAP NetWeaver Identity Management and SAP NetWeaver Single Sign-On

**SAP NetWeaver Identity Management**
- User and Role Management
- Provisioning
- Identity Center
- Virtual Directory Server
- Identity Services
- Integration with SAP Business Objects
- Access Control
- Identity Provider & Security Token Service

**SAP NetWeaver Single Sign-On**
- Federation with Identity Provider / Security Token Service
- Standards-based Single Sign-On to SAP Windows GUI, SAP and non-SAP web-based applications (Kerberos, X.509, SAML)
- Digital Signatures (hardware crypto tokens)
- Re-authentication
- Strong authentication: Radius (e.g., OTP tokens), smart cards, etc
- Enterprise Single Sign-On
- Web Access Management (via EBS with CA)

**Secure Communication Channels**
- Encryption of communication between client and application server
- Secure default installation for every SAP system

Encryption of communication channels between SAP servers and all SAP GUIs
- Secure default installation for every SAP system (encrypted channels)

Heterogeneous, cross-company identity management and variable, standards-based, multi-method authentication and single sign-on
- Integration: Deploy users, roles, systems as well as authentication and SSO configurations with one click in provisioning
- Secure and standards-based connectivity and integration enhancements of business processes
# SAP NetWeaver Single Sign-On: Solution components

## SAP NetWeaver Single Sign-On

<table>
<thead>
<tr>
<th>Module</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity Federation</strong></td>
<td>Web-based and web service-based authentication, SSO and identity federation with Identity Provider (IDP) and Security Token Service (STS) via SAML 2.0</td>
</tr>
<tr>
<td><strong>Secure Login</strong></td>
<td>Cross-company domain SSO, heterogeneity, interoperability</td>
</tr>
<tr>
<td><strong>Enterprise Single Sign-On</strong></td>
<td>Standards-based single sign-on to SAP Windows GUI, as well as SAP and non-SAP web-based applications (Kerberos, X.509)</td>
</tr>
<tr>
<td></td>
<td>Digital signatures for integrity</td>
</tr>
<tr>
<td></td>
<td>Strong authentication and re-authentication for business-critical applications</td>
</tr>
<tr>
<td><strong>Web Access Management</strong></td>
<td>Enterprise SSO to legacy applications requiring user ID/password authentication (terminal server, ftp, databases etc)</td>
</tr>
<tr>
<td><strong>Secure Communication Channels</strong></td>
<td>Encryption of communication channels between SAP client and application server</td>
</tr>
<tr>
<td><strong>Available free of charge</strong></td>
<td>Based on SNC and Kerberos</td>
</tr>
<tr>
<td><strong>Partner API</strong></td>
<td>Encryption only</td>
</tr>
<tr>
<td><strong>No single sign-on</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Endorsed Business Solution (EBS) with CA SiteMinder product**

**Policy-based authentication and authorization to web applications**

**XACML-based, policy-enforced access**
Solution in detail:
Identity federation
What is Identity Federation?

Identity federation allows the transfer of identity information across (company) domain boundaries.

- Federation enables users to work across domains securely and seamlessly.
- It creates cross-company single sign-on scenarios and reduces the user administration effort by re-using identity information from one domain for user authentication in other domains.
- Identity federation is based on open industry standards to guarantee maximum interoperability.
- SAP provides identity federation capabilities in SAP NetWeaver Identity Management through the Identity Provider (IDP) and the Security Token Service (STS).
- Both options are based on SAML 2.0 (Security Assertion Markup Language); in addition, the STS supports X.509 certificates.
Single sign-on and identity federation using SAML for web applications and services

Identity federation and single sign-on via SAML 2.0 in heterogeneous landscapes

- Single sign-on for Web-based applications and services
- Support of cross-company business processes
- Extensible identity information model
- Based on open SAML standard
- Successful participation in Liberty Alliance and Kantara interop tests 2009 and 2011
Identity Provider: Web browser-based SSO

In a single sign-on environment, a number of systems which provide services to the end user (Service Providers) trust the one system which administrates the end user’s identity (Identity Provider).

Web users who are trying to access such a Service Provider system with their Web browser will be redirected to the Identity Provider. Once a user is authenticated by the Identity Provider, the user can access any of those service providers without re-authenticating.

Web Browser-based single sign-on is user-centric.
SAP support for Web browser-based SSO

IdP/STS can be installed as a component via SAP NetWeaver Identity Management or SAP NetWeaver Single Sign-On.
Security Token Service: Web service-based SSO

For Web services-based SSO, a Security Token Service (STS) is used. The STS is a Web service that enables you to use single sign-on (SSO) in heterogeneous system landscapes.

The STS acts as a token broker. It supports a number of authentication methods from a Web service consumer and can convert these tokens into a security token that a Web service provider can use. The STS supports X.509, SAML 1.1, and SAML 2.0 tokens.

Just as with SAML 2.0 for Web browser-based access, the SAML 2.0 assertion can transport profile and authorization attributes to the target Web service provider.

Web service-based single sign-on is system-centric.
SAP support for Web service-based SSO

SAP NetWeaver Identity Management 7.2
- Identity Center
- Virtual Directory Server
- SAML 2.0 IdP
- STS

Min. Java 7.0 SP 14

SAP NetWeaver Single Sign-On 1.0
- E-SSO
- Secure Login
- SAML 2.0 IdP
- STS

Min. Java 7.20

SAML 2.0
- WS Consumer
  - AS ABAP 7.02 / 7.30
  - No AS Java

SAML 2.0
- WS Provider
  - AS ABAP 7.02 / 7.01
  - No AS Java
Solution in Detail:
Secure Login
What is Secure Login?

Secure Login allows re-using an initial user authentication, such as a Kerberos ticket or SAP system authentication, for subsequent log-ins to connected systems within an enterprise IT landscape.

- Secure Login offers flexibility regarding the initial authentication mechanism.
- The solution offers a standards-based (X.509) SSO technology, but does not require the implementation of a full-blown, costly Public-Key Infrastructure (PKI).
- It combines maximum security, such as re-authentication, with ease of use and minimum implementation requirements.
Secure Login: Platform availability

<table>
<thead>
<tr>
<th></th>
<th>Internet Browser 32-Bit</th>
<th>Internet Browser 64-Bit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Microsoft Internet Explorer 7</td>
<td>Microsoft Internet Explorer 8</td>
</tr>
<tr>
<td>SL Web Client (SAP GUI SNC)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SL Web Client (Certificate Store Support)</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Mozilla Firefox 64Bit is not available (Status May 2011)
Single sign-on with Secure Login via Kerberos

1. User authenticated via Microsoft Active Directory
2. Request security token
3. Security token
4. Authenticate via security token

- Authentication through standardized security tokens based on Kerberos
- Low implementation effort
- Tight integration between SAP GUI, Windows client and Windows Active Directory
- Strong encryption and single sign-on to standard Windows GUI
Single sign-on with Secure Login via X.509 certificates

1. Start SAP GUI
2. Call the SAP Business Suite Login Server
3. Validate the user's credentials
4. Create a certificate
5. Authenticate via certificate

- Out-of-the-box generated certificates can be used for SAP GUI and Web applications
- Low entry barrier into X.509 certificate based access
- PKI integration available but not required, short lived X.509 certificates can be generated
- Strong encryption
- Digital signatures via SSF integration

New capabilities

(AD, LDAP, ...)
Strong authentication with Secure Login

1. User authenticated via Microsoft Active Directory
2. Request
3. Security token
4. Authenticate via security token
   - Secure communication

- Authentication via smart card and existing PKI (Microsoft CA)
- PKCS#11 also supported
- Low implementation effort
- Strong encryption
- Multi-factor authentication
Re-authentication with Secure Login

- Re-authentication to secure business-critical transactions
- Possibility to configure the enforcement of an additional authentication step (user re-enters credentials) for critical transactions
Web client: Zero footprint client software

- Provides certificate to SAP GUI and internet browser (SSO enablement)
- Secure connection between SAP GUI and SAP application server
- Support of SAP GUI Java
- No distribution of client software

New capabilities
Digital signatures via SSF API and Secure Login Library

- Digital signatures for legally binding contracts
- Integration with SSF API
- Out of the box support for a set of SAP transactions
- Consistent with SAP SSO mechanisms
- Easy and flexible to implement
- Generation of X.509 certificates and smart card support
Digital signatures – step by step

1. SAP transaction triggers digital signature

2. User authenticates and digital certificate is received

3. User information is transferred

4. SAP application digitally signs document and stores data

Supported out of the box for a set of SAP transactions; additional programming/integration necessary if:

- ABAP programming for other transactions not yet supporting SSF
- Integration of Secure Login Library with client actions
- Hardware support needed
Solution in Detail:
Enterprise Single Sign-On
What is Enterprise Single Sign-On?

Enterprise Single Sign-On (E-SSO) helps users authenticate to multiple non-SAP systems or applications without the need to remember every password or logon dialog. After the end user has successfully authenticated to the E-SSO, further logon procedures to applications running under the system’s control are carried out automatically by E-SSO.

- If you do not have a smart card you can use a soft token to store the credentials.
- E-SSO installs plug-ins (toolbar) for Internet Explorer and/or Firefox to facilitate SSO to protected web sites.
Scope and highlights of Enterprise Single Sign-On

Provides access to:
- Single sign-on to applications that do not support standardized authentication tokens
- Web applications
- Windows applications
- Java applications
- Databases
- Terminal emulators

Highlights:
- Wizard-based
- Automatic and/or drag & drop authentication
Solution in Detail:
Web Access Management

SAP
NetWeaver
Single
Sign-On
Identity Federation
Secure Login
Enterprise SSO
Web Access Mgmt
Secure Communication
What is Web access management?

Web access management controls access to Web resources, providing:

- Authentication management
- Policy-based authorizations
- Auditing and reporting
- Single sign-on

CA SiteMinder Web access management solution is an SAP-endorsed business solution. It complements the security features in the SAP NetWeaver technology platform by controlling user access to SAP applications and helping securely deliver essential information to millions of employees, partners, suppliers and customers.
Endorsed Business Solution for Web Access Management: CA SiteMinder

CA SiteMinder for WAM to SAP NetWeaver Application Server

- Extends web-based single sign-on to SAP NetWeaver Application Server systems to offer Web Access Management
- Offers policy-based authentication and authorization in web environments
- Integration via certification against SAP standard APIs for JAAS login modules
- Successful, long-term partnership between SAP and CA
Solution in Detail:
Secure Communication Channel

- SAP NetWeaver
- Single Sign-On
- Secure Login
- Identity Federation
- Enterprise SSO
- Web Access Mgmt
- Secure Communication
What is a secure communication channel?

A secure communication channel uses an encryption algorithm to render the transmitted data unreadable during transport, protecting the information passing through the channel.

SAP offers free encryption libraries for the communication between SAP Application Servers and between SAP Clients and Servers (based on the SNC interface and Kerberos technology, planned to be available in October / November 2011).

A secure communication channel provides:
- Compliance
- Integrity
- Confidentiality
Securing the communication channel between client and standard Windows GUI

- Included in SAP NetWeaver license
- Encryption between SAP client and application server
- Based on SNC and Kerberos
- Encryption of communication channel only
- No single sign-on
- Planned to be available with SP1 around Oct/Nov 2011 as part of the GUI installation