Agenda

SAP security products portfolio
Overview SAP Single Sign-On
Single sign-on main scenarios
Capabilities
Summary
SAP Single Sign-On
In the SAP security products portfolio

- **SAP Single Sign-On**: Make it simple for users to do what they are allowed to do.
- **SAP Identity Management**: Know your users and what they can do.
- **SAP Access Control**: Ensure corporate compliance to regulatory requirements.
- **SAP Cloud Identity service**: Manage the identity life-cycle in the cloud.
- **SAP Enterprise Threat Detection**: Counter possible threats and identify attacks.
- **Add-On for Code Vulnerability Analysis**: Find and correct vulnerabilities in customer code.

**Platform Security**
Make sure that SAP solutions run securely.

**SAP HANA Platform**

**SAP NetWeaver Application Server**
Overview
SAP Single Sign-On
Benefits

**Single Sign-On** – authenticate once and subsequently access SAP and non-SAP applications in a **secure** and **user-friendly** way.

**Security** – Improve security measures and meet company and regulatory requirements.

**From Anywhere** – also from **mobile devices**, from outside the corporate network, etc.

**Low Cost** – leverage the benefits of **quick** implementation and **low cost** of ownership.
SAP Single Sign-On
Benefits in detail

**Security**
- Secure authentication with one strong password, optionally with additionally factors
- No more need for password reminders on post-it notes
- All passwords kept in one protected, central place

**Cost saving**
- Efficiency gains for users that only need to remember one password
- Higher productivity due to reduced efforts for manual authentication, password reset, helpdesk interaction,…
- Functions to efficiently set up and manage server-side security capabilities

**Simplicity**
- Lean product, fast implementation project, quick ROI
- No more need to provision, protect and reset passwords across many systems
- No more efforts to manage password policies across many systems
SAP Single Sign-On
Supported authentication modes

**Single sign-on**
- Authenticate once to an authentication server (Active Directory, AS ABAP,..)
- Received security token confirms identity for each subsequent login to business applications

**Multiple sign-on**
- User authenticates each time when accessing a business application
- Authentication is performed against a central authentication server, not the business application itself

**Multi-factor authentication**
- In addition to knowledge of information (password), authentication requires a physical element (possession of mobile phone, RSA SecurID card, etc.)
- Implementation option for both single and multiple sign-on
SAP Single Sign-On

Product description

SAP Single Sign-On provides simple, secure access to IT applications for business users. It offers advanced security capabilities to protect your company data and business applications.

Simple and secure access

- Single sign-on for native SAP clients and web applications
- Single sign-on for mobile devices
- Support for cloud and on-premise landscapes

Secure data communication

- Encryption of data communication for SAP GUI
- Digital signatures
- FIPS 140-2 certification of cryptographic functions

Advanced security capabilities

- Two-factor and risk-based authentication
- Authentication with smart cards or RFID tokens
- Hardware security module support
- Simplified management of backend security capabilities
SAP Single Sign-On 3.0
Continuous innovation on a stable core

Building on a stable core

- SAP released SAP Single Sign-On in 2011 after acquiring the secure login solution, which had been used by SAP internally and by many customers for years.
- Since 2011, we have continuously extended the product, shipping enhancements in support packages.
- The stability of the core and the simplicity of the product remain our key objectives.

SAP Single Sign-On 3.0, a non-disruptive, evolutionary release

- Extending the coverage and integration capabilities towards mobile and cloud.
- Modernization of the X.509 certificate-based scenario, beyond single sign-on.
- Simplified implementation with immediate benefits through close platform integration.
- Continuous improvement of security protocols based on market requirements.
SAP Single Sign-On
From release 2.0 to 3.0

SAP Single Sign-On provides efficient and easy-to-use security capabilities. It is our goal to keep implementation efforts and TCO as low as possible. This includes the update scenario from version 2.0 to 3.0

Compatible functionality set
• Version 3.0 continues to support all capabilities of version 2.0
• The fundamentals of the main scenarios remain unchanged; an implementation started on 2.0 does not need to be repeated or adapted on 3.0

Extended functionality optional
• Version 3.0 allows customers to extend the coverage of their existing implementation to additional scenarios
• The new capabilities are optional and can be enabled any time

Lean update process
• Updating product components from 2.0 to 3.0 is as easy as a patch
• Versions 2.0 and 3.0 are interoperable: As long as no 3.0 specific functionality is required, components can be updated in any order
Single sign-on main scenarios
SAP Single Sign-On 3.0
Components

Secure Login Client
- Frontend application, managing Kerberos tokens and certificates

Secure Login Server
- Central service providing X.509 certificates

SAP Common Cryptographic Library
- Cryptography and security library for SAP applications
- As of 3.0, this is the only required cryptographic library
- Shipped with SAP Kernel

SSO Authentication Library
- Support for two-factor and risk-based authentication

Identity Provider
- Provides SAML 2.0 assertions for web-based SSO
SAP Single Sign-On 3.0  
Secure, low TCO access to SAP business applications using Kerberos

- Users authenticate to Microsoft Windows domain during desktop login
- Active Directory provides a Kerberos security token that SAP business applications accept as proof of identity
- Supported on desktop systems (Windows, OS X) and mobile devices (iOS) that are part of a Windows domain
- Requires access to the corporate network
- Users need to have an account in an Active Directory
- Very fast implementation, very low TCO, no additional server required
- Single sign-on for AS ABAP and AS Java, covering web-based and desktop clients such as SAP GUI, Business Client, RFC client applications like Analysis for Office, HANA database, Business Intelligence platform, and many more
- Network encryption for SAP GUI and RFC clients using the SNC protocol
**Single sign-on based on the corporate Windows domain**

Secure, low TCO access to SAP business applications using Kerberos

1. User authenticates to Windows domain
2. Active Directory provides Kerberos security token to user
3. User opens a system connection using a native client or browser
4. Kerberos token is forwarded to system using SNC (for SAP GUI and RFC clients) or SPNEGO (for browsers). The Kerberos token is validated offline on the server, no connection to AD required.

**Authentication Scenario**

**Kerberos authentication**

**Microsoft Active Directory**

**SAP NetWeaver Application Server ABAP**

**SAP NetWeaver Application Server Java**

**SAP GUI & RFC (SNC)**

**Browser (SPNEGO)**

**Business User**

**Windows login**

**Start desktop client, app or browser and open connection**
SAP Single Sign-On 3.0
Highly interoperable single sign-on to SAP and non-SAP with X.509 certificates

- Users authenticate to SAP Secure Login Server to retrieve a short-lived X.509 certificate, or re-use available certificates, e.g. from corporate smart cards
- SAP business applications accept the certificate as proof of identity
- Validity of the user certificate (hours, days, weeks) can be configured based on security and usability requirements

- Supported on desktop systems (Windows, OS X) and mobile scenarios (iOS)
- Secure Login Server requires an AS Java to run. If certificates are already available to users, e.g. through smart cards, then no additional server is required.

- Secure Login Server is a lean alternative to introducing a full-blown PKI
- Secure Login Server supports two-factor and risk-based authentication, against different user stores (LDAP, ABAP, ..)
- X.509 certificates are accepted by a broad range of both SAP and 3rd party web applications and clients, including many legacy systems
- Network encryption for SAP GUI and RFC clients using the SNC protocol
Single sign-on using X.509 digital certificates
Highly interoperable single sign-on to SAP and 3rd party applications

Authentication Scenario

1. (*) User authenticates to Secure Login Server. Authentication can be automatic (using e.g. Kerberos) or manual, even based on multiple factors.
2. (*) Secure Login Server returns an X.509 certificate, valid for e.g. a working day
3. User opens a system connection
4. X.509 certificate token is forwarded to system and allows authentication

(*) Steps 1 and 2 are not required if the user is already in possession of a certificate.
Scenario

- Customers that already have an enterprise PKI do not want to establish a second one
- Secure Login Server (SLS) integrates with existing enterprise PKI both for user and server certificates

Benefits

- Certificate signing based on established PKI and security policy
- Storage and revocation processes remain valid
- SAP component integration decoupled, managed inside SLS

*S: Active Directory Certificate Services  
**CMC: Certificate management over CMS, RFC 5272
SAP Single Sign-On 3.0
Extension scenarios based on Secure Login Server and X.509 certificates

- **Instant user identification based on RFID token**
  (Radio Frequency Identification)
  - Warehouse and production scenarios where efficient authentication is key
  - Kiosk/terminal computers shared among teams
  - Simple configuration using Microsoft Active Directory to validate identities
  - Support for PC/SC and WaveID RFID reader devices

- **Single sign-on for terminal sessions** (Secure Shell, putty)
  - Secure Login Client can be configured to run as a secure shell agent
  - Locally stored X.509 certificates and keys can be used for authentication
  - Security enhancement for administrative tasks, particularly for cloud scenarios
SAP Single Sign-On 3.0
Enhancements for SSO based on Kerberos and X.509 certificates

- **Encryption Only Mode: Data privacy, always**

  - Enables network encryption for SNC even if a user-specific security token is not available or not configured

  - Allows customers to protect data communication immediately during an implementation project, before user-specific configuration is in place

  - Data privacy still ensured if the end user’s security token is temporarily unavailable, for example if the user loses the smart card holding the certificate
The security capabilities of the SAP NetWeaver Application Server ABAP are often based on certificates. When customers have a security policy that defines a short certificate validity, certificates expire on a regular basis and need to be updated. Certificate lifecycle management helps manage the renewal of certificates, reduces manual efforts, and prevents downtime.

**Process**
- Trust relationship between AS ABAP and Secure Login Server is configured once
- AS ABAP subsequently checks in regular intervals for expiring certificates and automatically renews them

**Benefits**
- No more manual steps required
- SAP-supported solution
- Mitigate risk of unexpected downtime

**Latest enhancements**
- Command line tool that automates the certificate renewal for all components using file-based PSEs
- Automated central roll-out of trusted root certificates to facilitate the transition from self-signed certificates to a PKI-based approach
- Secure Login Server can act as Registration Authority of an existing enterprise PKI
SAP Single Sign-On 3.0

Identity federation and single sign-on for cross-organizational scenarios with SAML

- Users authenticate to the SAP Identity Provider to retrieve a Security Assertion Markup Language (SAML) assertion
- SAP web applications accept the assertion as proof of identity
- The assertion definition is very flexible and supports the easy mapping of attributes between different systems, allowing loosely coupled integration across organizations
- Supported by browser-based applications on desktop systems and mobile devices
- SAP Identity Provider requires an AS Java to run
- SAP Identity Provider supports two-factor and risk-based authentication, against different user stores (LDAP, ABAP, ..)
- SAML assertions are accepted by a broad range of both SAP and 3rd party web applications
- SAML assertions enable single sign-on during the lifetime of the browser session
Single sign-on using Security Assertion Markup Language (SAML)
Identity federation and single sign-on for cross-organizational scenarios

**Authentication Scenario**

1. The user opens a connection to the business system, which is configured as a SAML Service Provider
2. The business system redirects the browser to the IdP
3. User authenticates to IdP, either automatically (using e.g. SPNEGO) or manual, even based on multiple factors
4. IdP establishes a security session, returns a SAML assertion, and redirects the browser back to the SP
5. User is authenticated
Single sign-on based on SAP Authenticator
Lean solution for single sign-on on mobile devices

- Users authenticate once to the authentication server to store a shared secret on their mobile device
- Time-based One-Time Passwords (TOTP) based on the shared secret are passed from SAP Authenticator to the SAP Identity Provider, which enables single sign-on for web-based business applications

- SAP Authenticator is available on mobile devices (iOS, Android)
- SAP Authenticator supports browser-based applications, the SAP Fiori client, and customer-developed mobile apps
- SAP Authenticator-based authentication requires AS Java

- SAP Authenticator can be combined with two-factor and risk-based authentication
- Fast implementation due to automated roll-out of the configuration to mobile devices
- Highly flexible approach with few infrastructure prerequisites
Single sign-on based on SAP Authenticator
Lean solution for single sign-on on mobile devices

Authentication Scenario

1. User registers mobile device once with the SAP Authentication Library
2. Shared secret is stored on mobile device once
3. User starts SAP Authenticator on mobile device and opens a link to a web or Fiori client application
4. Access is redirected to the IdP and user is authenticated with OTP
5. IdP establishes a security session, returns a SAML assertion, and redirects the browser to the SP
6. User is authenticated
Capabilities
SAP Single Sign-On 3.0
Integrating cloud and on-premise, browser and native clients

SAP Single Sign-On 3.0 comes with a new version of the Secure Login Web Client, based on a renovated architecture and more integration options

Secure Login Web Client (SLWC)
- The Secure Login Web Client allows a web page to trigger and monitor the certificate enrollment for Secure Login Server profiles
- Using Secure Login Web Client, a business process that is running in a browser session (cloud or on-premise) can trigger a seamless authentication for a native client on the user desktop
- For example, SLWC can accept a SAML 2.0 assertion as security token and in return provision an X.509 certificate for single sign-on of desktop applications such as SAP GUI. This is a major benefit for customers that run a SAML 2.0 Identity Provider or Portal as the central authentication server.

Architecture Renewal
- The previous version of SLWC was based on a Java applet and for some capabilities on an ActiveX control
- The 3.0 version of SLWC no longer depends on Java or ActiveX, relying instead on the Secure Login Client
- As a result, SLWC 3.0 is no longer limited to browsers that (still) support Java applets or even ActiveX, which significantly increases the number of supported browsers
SAP Single Sign-On 3.0
Comprehensive solution for single sign-on on mobile devices

SAP Single Sign-On 3.0 extends the capabilities for mobile single sign-on, covering a broad range of customer scenarios with proven technologies and seamless integration into the existing landscape.

Secure Login Server (SLS)
- X.509 certificates can be provisioned to mobile devices in multiple ways
  - Using the SCEP protocol support of iOS
  - Using the SAP Authenticator app on iOS
  - Calling the new REST API of Secure Login Server from a custom app
- X.509 certificates are highly interoperable and support single sign-on for on-premise and cloud, SAP and non-SAP, app- as well as browser-based applications
- Optionally, customers can integrate Secure Login Server and the SAP Mobile Platform, and benefit from a seamless user experience for mobile applications

Other options
- Kerberos: Kerberos-based single sign-on is only possible on some mobile device types; it does not provide many customization options. On the other hand, it is easy to set up and operate.
- SAML 2.0: SAML assertions provided by the SAP Identity Provider are also supported by mobile web browsers
- SAP Authenticator: One-time password generated by SAP Authenticator require few prerequisites and can be an attractive solution for single sign-on in custom scenarios
SAP Single Sign-On 3.0
FIPS 140-2 certification of the SAP CommonCryptoLib

Component “SAP NW SSO 2.0 Secure Login Library Crypto Kernel” was certified on January 6th, 2015

List entry (Cert# 2308):
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Certificate:

Blog on SAP Community Network:
SAP Single Sign-On 3.0
Enhancements for cryptographic capabilities and security protocols

- **Perfect Forward Secrecy for SNC: Data privacy, now and forever**
  - Based on Elliptic Curve Diffie–Hellman Ephemeral (ECDHE) key exchange
  - Mitigates the risk that compromised keys allow an attacker to decrypt previously recorded session data

- **SSL/TLS support extensions: Higher security**
  - Better protection against protocol downgrade attacks by supporting TLS_FALLBACK_SCSV
Benefits of digital signatures

- Confirm that a document was created by a known sender
- Confirm that a document was not tampered with during transmission
- Provide the means for a binding signature that cannot be denied afterwards

Usage with AS ABAP

- Based on Secure Store & Forward (SSF) interface
- Server-side digital signatures: Supported by the SAP CommonCryptoLib
- SAP Single Sign-On includes support for hardware security modules
- Client-side digital signatures: Supported by Secure Login Client for SAP GUI

More information on SAP Help Portal and SAP Service Marketplace

- Digital Signing with Secure Store and Forward (SSF)
- Digital Client Signature
- Digital Signatures (SSF) with a Hardware Security Module
- SAP Note 1973271 - Secure Login Library 2.0 HSM Configuration for SSF
SAP Single Sign-On 3.0
Support for new SAP clients

SAP user interface integration
Combines beautiful user interfaces with great usability
Support new SAP clients out of the box
• SAP Fiori
• SAP NetWeaver Business Client
• SAP Screen Personas
SAP Single Sign-On 3.0
Two-factor authentication

**Authentication requires two means of identification**
- Knowledge of a password
- Possession of a physical device, such as a cell phone

**Options for the second factor**
- SAP Authenticator mobile app
  - Generates one-time passwords ([RFC 6238](https://tools.ietf.org/html/rfc6238) compatible)
  - Available for iOS and Android
- One-time password sent using SMS
- One-time password sent using e-mail
- RSA / RADIUS

**Usage scenarios**
- Recommended for scenarios with special security requirements
- Web and SAP GUI applications
Risk-based authentication

- Risk-based enforcement of stronger authentication
- Example: User access from outside the corporate network ➔ Two-factor authentication is required

- Evaluate context such as IP address, user roles, device,…
- Accept access, deny access or enforce 2FA
- Return SSO token (SAML or X.509)
Risk-based authorization handling

- Relies on SAP Identity Provider, using SAML 2.0
- Access policy information added to SAML assertion after authentication
- On AS Java, dynamic reduction of available roles based on access policy. See SAP note 2151025.
- On AS ABAP, access policy information available in security session. See SAP note 2057832.

Including access policy information from SAP IdP

SAML assertion

Check access policy and handle access restrictions

- Temporarily reduce user roles and authorizations for session on AS Java
- Extend customer exits in applications on AS ABAP to allow risk-based authorization checks, e.g. for admin tasks or data download
SAP Single Sign-On 3.0
Guided SNC configuration on AS ABAP using the SNC Wizard
Platform security
Support for eliminating unencrypted SAP GUI / RFC access to AS ABAP

Situation
• It is often a compliance requirement to only allow encrypted communication to SAP systems
• As documented in SAP Note 1690662, unencrypted communication can be blocked
• Enabling this setting may be a risk for business continuity if SAP Single Sign-On was not yet configured on all clients, as some people may lose access to the system

Solution
• Unencrypted access to the backend can be recorded in the Security Audit Log, as documented in SAP Note 2122578
• Customers can enable the logging function and keep an eye on whether there are still unencrypted connections from certain client machines, which can then be configured to use SAP Single Sign-On
• Once the administrator is reassured that there are no more clients with missing configuration, they can enforce encrypted communication as described in SAP Note 1690662
SAP Single Sign-On 3.0
Hardware security module support

**Store private keys in hardware**
- Protect Secure Login Server Certificate Authority
- Protect private keys for digital signatures (Secure Store and Forward, SSF)
- Performance acceleration

Thales
SafeNet
Summary
Summary

SAP Single Sign-On is SAP’s solution for efficient and secure authentication and data handling

Security
• Secure authentication and FIPS-certified cryptographic functions
• Risk-based authentication and two-factor authentication
• Digital signatures

Productivity
• Single sign-on to SAP and non-SAP applications
• Fast return on investment

Ready for the future
• Based on industry standards such as Kerberos, X.509, SAML
• State-of-the-art security functions
• Cloud and mobile integration
Recommendations

Identify the most critical systems. Which systems contain your most sensitive business information? How many people have access to them? Define your overall single sign-on strategy and start with these critical business systems.

Understand the different modules of SAP Single Sign-On and analyze your system landscape to determine which SSO standards can be used. If your organization does not have the appropriate resources and know-how, involve SAP Consulting or SAP partners.

Passwords are often the weakest link in enterprises. Prevent the usage of passwords by relying on standards such as SAML, X.509 certificates, or Kerberos. SAP Single Sign-On offers solutions for all of these standards.

Once you have implemented single sign-on, start enforcing strong passwords in the related systems. Mid-term strategy: Consider disabling user name/password authentication in critical business systems.
Get more information

http://scn.sap.com/community/community/sso