Agenda

SAP security portfolio
Overview SAP Single Sign-On
Single sign-on main scenarios
Capabilities
Summary
SAP security portfolio
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.
- SAP HANA Platform
- SAP NetWeaver Application Server
Overview SAP Single Sign-On
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** – from your **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**
- With just one password to remember, a strong password policy is finally feasible
- No more need for password reminders on post-it notes
- All passwords kept in one protected, central place

**Reduce costs**
- Efficiency gains for users that only need to remember one password
- Higher productivity due to reduced efforts for manual authentication, password reset, helpdesk interaction,…

**Simplicity**
- Lean product, fast implementation project, quick ROI
- No more efforts 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.)
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 security functions

Advanced security capabilities
- Two-factor authentication
- Risk-based authentication using access policies
- RFID-based authentication
- Hardware security module support
Single sign-on main scenarios
SAP Single Sign-On
Components

Secure Login Client
• Client application
• Manages security tokens (Kerberos tokens, X.509 certificates)

Secure Login Server
• Central service on SAP NetWeaver AS Java
• Provides X.509 certificates to users and application servers

SAP Common Cryptographic Library (f.k.a. Secure Login Library)
• Cryptography and security library for SAP applications

Identity Provider
• Central service on SAP NetWeaver AS Java
• Provides SAML 2.0 assertions for Web-based SSO
Single sign-on based on the Windows domain authentication
Secure, low TCO access to SAP business applications using Kerberos

- Users authenticate to Microsoft Active Directory during Windows 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, Windows Mobile) 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 web applications on AS ABAP and AS Java, 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 is available based on SNC
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.
Single sign-on using X.509 digital certificates
Highly interoperable single sign-on to SAP and 3rd party applications

- Users authenticate to SAP Secure Login Server to retrieve a short-lived X.509 certificate, or reuse already 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)
- 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 is available based on SNC
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.
Single sign-on using X.509 digital certificates
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 Secure Shell (SSH, putty)**
  - Secure Login Client can be configured to run as an SSH agent
  - X.509 certificates and keys that are stored locally can be used for authentication in SSH terminal sessions
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.

**Registration of SAP NetWeaver AS ABAP with Secure Login Server**
- Administrator establishes trust relationship between AS ABAP and Secure Login Server
- Administrator configures the corresponding Secure Login Server profile for each relevant certificate

**Automated renewal of certificates**
- Scheduled ABAP report checks the local AS ABAP for certificates that are about to expire
- ABAP report retrieves renewed certificate from Secure Login Server and installs it

**Benefits**
- No more manual steps required
- SAP supported solution
- Mitigate risk of unexpected downtime
Single sign-on using Security Assertion Markup Language (SAML)
Identity federation and single sign-on for cross organizational scenarios

- Users authenticate to the SAP Identity Provider to retrieve a 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.

**Business User**

Start browser and open connection

Create SAML assertion and redirect back to Service Provider

Business application server redirects browser to the Identity Provider

SAML-based authentication

Service Provider (SP), e.g. SAP NetWeaver Application Server ABAP or Java

SAP Identity Provider (IdP) on AS Java
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 the 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 little 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
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:
Latest enhancements in version 8.4.38*

- Significant performance increase on all major platforms
  - RSA, AES, SHA-2
- Perfect Forward Secrecy for TLS
  - Ephemeral key agreement
  - Elliptic curve Diffie-Hellman key exchange
- Elliptic curves P-224, P-256, P-384, P-521
- TLS 1.2 cipher suites in Galois Counter Mode (GCM)
- New command “sapgenpse tlsinfo” to help configure cipher suite profile parameters for TLS

Previous support**

- Hash algorithms: SHA-2, ..
- Signature algorithms: DSA, PKCS #1 v 2.1 RSA PSS, ..
- Key exchange algorithms: Diffie-Hellman, ElGamal, PKCS #1 v 2.1 RSA OAEP, ..
- Block cipher algorithms: AES 256bit, ..

* See SAP Note 2181733 for details
** See SAP Note 2004653 for complete list

** Copyright 2016 SAP SE or an SAP affiliate company. All rights reserved. **
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
Single sign-on 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
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 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)
SAP Single Sign-On
Limit business functionality based on context

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
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 out there, she can enforce encrypted communication as described in SAP Note 1690662
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
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.
Summary

SAP Single Sign-On offers a suite of security capabilities, for SAP as well as non-SAP applications

It offers

- Investment protection
- Flexibility
- Single sign-on for heterogeneous system landscapes

What are the main business drivers?

- Protect business, reputation and trust
- Lower password related costs
- Simplicity and agility
Get more information

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