SAP Single Sign-On 3.0
International Focus Groups Webinar July 2016
Christian Cohrs
Area Product Owner, SAP SE
Agenda

Overview
Main capabilities and 3.0 news
Summary
SAP Single Sign-On
Market Success

- SAP Single Sign-On has become the Best-Practice for secure authentication
- Around the world
- Across all industries
- From small & medium enterprises to large corporations
- On-Premise & Private Cloud
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 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
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 and mobile scenarios
- 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
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 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
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
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
Secure Login Server as Registration Authority of an existing enterprise PKI

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

SAP NetWeaver Application Server ABAP

Secure Login Server

Provision user certificates
Forward request
Return certificate
Renew server certificates

Enterprise PKI
(ADCS* or CMC** compatible)

Business User

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

Public

*Active Directory Certificate Services
**Certificate management over CMS, RFC 5272
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
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, Android and Windows (universal app)
• 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
SAP Single Sign-On 3.0
Risk-based authentication based on context

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)
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
Get more information

Information
- Overview presentation
- Roadmap
- Release blog
- SAP Single Sign-On community

Features
- Certificate Lifecycle Management training video (part 1, part 2)
- Secure Login Web Client
- Enterprise PKI integration
- Secure Login Server REST API
- SAP Single Sign-On and SAP Mobile Platform

Software
- Download
- Product Availability Matrix

TechEd 2016, planned sessions
- SEC103, Lecture
  Simple Steps Toward Increased Security with the New SAP Single Sign-On 3.0
- SEC163, Hands-On Workshop
  Protect your SAP Landscape with X.509 Certificates Using SAP Single Sign-On
- MOB360, Hands-On Workshop
  Enable SAP Single Sign-On for SAP Fiori Apps
- SEC819, Road Map Q&A, SAP Single Sign-On
No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see http://global12.sap.com/corporate-en/legal/copyright/index.epx for additional trademark information and notices.

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

National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE’s or its affiliated companies’ strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.