



# The Next Generation of Single Sign-On for SAP GUI

Christian Cohrs, SAP SE  
March 21<sup>st</sup> 2024

Public



# Legal disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. This presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has 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's strategy and possible future developments, products, and platforms, directions, and functionality are all subject to change and may be changed by SAP 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. 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 noninfringement. This document is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP's willful misconduct or gross negligence.

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.

For all recent and planned innovations, potential data protection and privacy features include simplified deletion of personal data, reporting of personal data to an identified data subject, restricted access to personal data, masking of personal data, read access logging to special categories of personal data, change logging of personal data, and consent management mechanisms.

# Agenda

Product overview

Technologies and capabilities

Summary

Q&A

# Single Sign-On – Benefits

## Security

Stronger authentication with one secure password, optionally with additional factors

Eliminates need for password reminders on post-it notes

All passwords kept in one protected, central place

## Cost efficiency

Efficiency gains as users only need to remember one password

Higher productivity due to reduced efforts for manual authentication, password reset, and helpdesk interaction

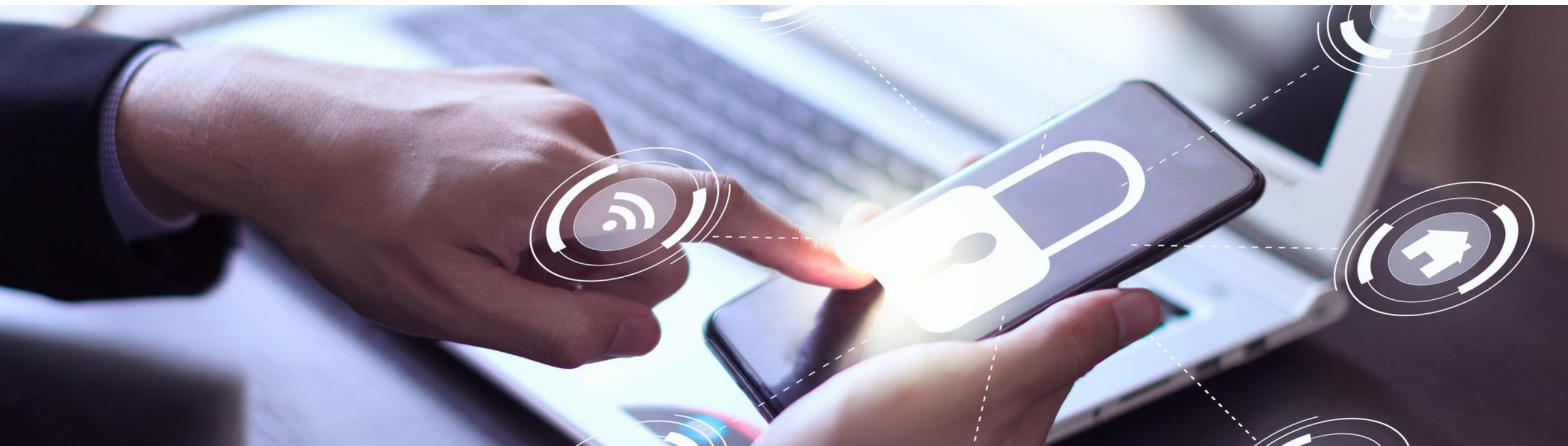
## Simplicity

No more need to provision, protect, and reset passwords across many systems

No longer requires management of password policies across many systems

Lean product, fast implementation project, quick ROI

# Product overview



# SAP Secure Login Service for SAP GUI

SAP Secure Login Service for SAP GUI provides stronger authentication and single sign-on for business applications.

It integrates with central authentication solutions such as an identity provider..

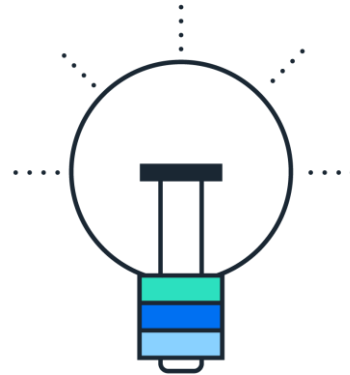
- eliminating the need for multiple passwords
- increasing end-user productivity
- protecting business data with stronger authentication methods.





# Why do we need a dedicated solution for single sign-on in SAP GUI?

## SAP Secure Login Service for SAP GUI enables single sign-on for SAP GUI desktop clients



**SAP GUI for HTML** is based on web technologies including HTTP. Therefore, single sign-on for SAP GUI for HTML can be implemented with an identity provider. SAP Secure Login Service for SAP GUI is not required.

**SAP GUI for Windows** and **SAP GUI for Java** rely on an SAP-specific protocol to communicate with the SAP NetWeaver Application Server ABAP. This protocol is not HTTP-based, so it does not support single sign-on technologies such as SAML or OpenID Connect.

# SSO technologies for SAP GUI desktop clients

SNC supports two types of security tokens for single sign-on

- **X.509 certificates**
- **Kerberos**

Customers can configure either one of these token types or even both to be accepted by the ABAP backend.

Browser-based technologies such as SAML or OpenID Connect are not supported natively and require the SAP Secure Login Service to “translate” the token into an X.509 certificate





# Comparison with SAP Single Sign-On solution

**SAP Single Sign-On** is the best-practice solution for stronger authentication and single sign-on in on-premise landscapes.

**SAP Secure Login Service for SAP GUI** builds on top of the successful concepts of SAP Single Sign-On and offers them in a cloud-oriented way.



**SAP Single Sign-On**



**SAP Secure Login  
Service for SAP GUI**

# Comparison with SAP Single Sign-On solution



## SAP Single Sign-On

Relies for capabilities such as multi-factor authentication on SAP NetWeaver Application Server Java, which will go out of mainstream maintenance end of 2027.



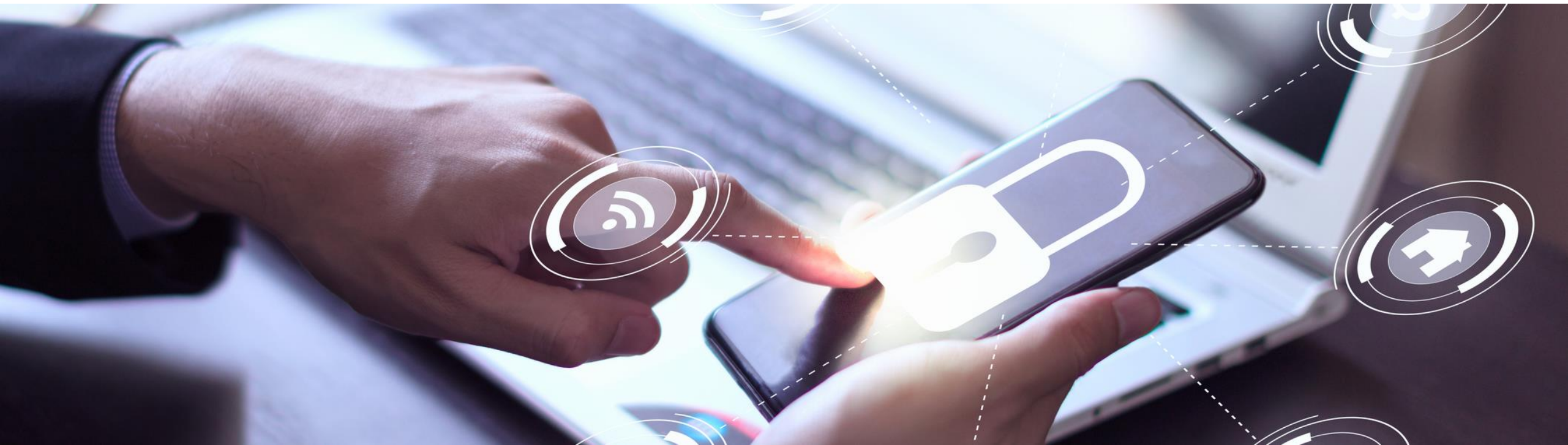
## SAP Secure Login Service for SAP GUI

Does not rely on SAP NetWeaver AS Java, using a cloud service instead.

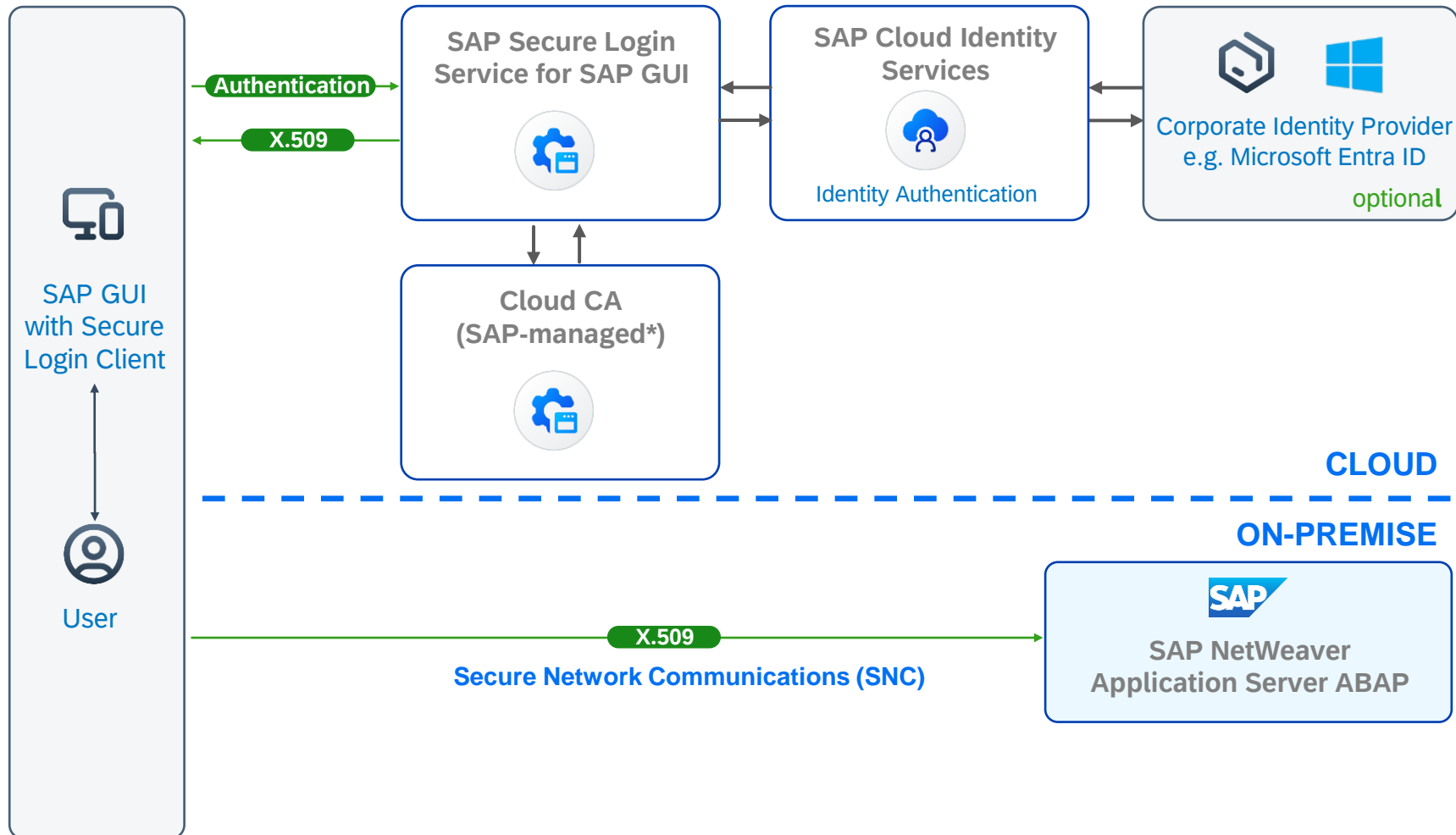
Focusses on an easy integration with cloud-based identity providers.

Is available as a cloud subscription, in line with how customers want to license their software today.

# Technologies and capabilities



# Single sign-on based on X.509 certificates – Process flow



1. User opens a SAP GUI connection
2. Secure Login Client (SLC) redirects user to the identity provider logon page
3. User authenticates to Identity Authentication Service
4. Optionally, authentication can be delegated to a corporate IdP (such as Azure AD)
5. After successful authentication, SAP-managed\* Cloud CA issues an X.509 certificate
6. SAP Secure Login Service returns the X.509 certificate, valid for one day, to SLC
7. X.509 certificate token is used for authenticating the SAP GUI user to the ABAP system

\* Support for customer-managed Cloud CA's is a roadmap topic

# Secure handling of the Certificate and Private Key

## Enrollment

- Secure Login Client creates a new private key and starts the certificate enrollment based on a secure authentication
- After authentication to the identity provider, SAP Secure Login Service provisions a short-lived X.509 certificate with the validity between 1 and 24 hours (configurable, default is 12 hours)

## Storage

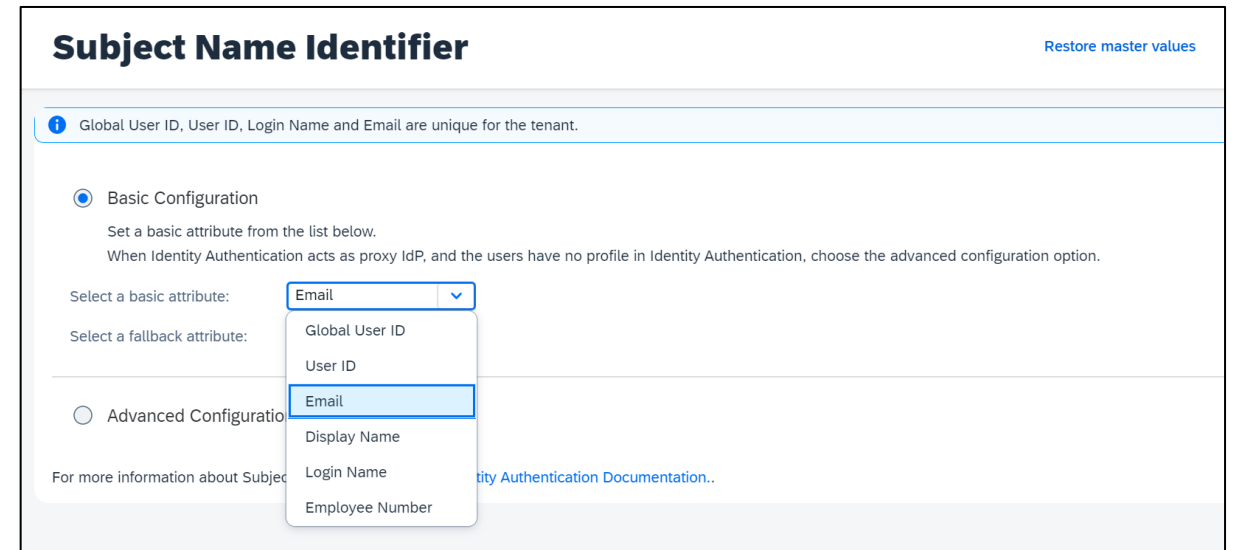
- Secure Login Client stores the private key and certificate in the protected storage of the operating system, Windows Certificate Store or Apple macOS keychain
- The private key is stored as non-exportable
- The private key and certificate are removed when the certificate expires or when the Secure Login Client is closed

## Usage

- The certificate only gives access to applications that are explicitly configured to accept it
  - The application needs to trust the Certificate Authority
  - The application needs to accept the Distinguished Name (DN) in the certificate. In an ABAP-based system (SAP ECC, SAP S/4HANA), this requires the mapping of the DN to an SAP user account

# Certificate format: Configuration of the Common Name

- The Common Name is configured by the customer
- By default, the Subject Name Identifier coming from the identity provider is taken as the Common Name
- Identity Authentication Service and other identity providers offer various configuration options for the Subject Name Identifier
- Customers can also explicitly configure the Common Name in Identity Authentication Service



**Subject Name Identifier** [Restore master values](#)

**i** Global User ID, User ID, Login Name and Email are unique for the tenant.

Basic Configuration  
Set a basic attribute from the list below.  
When Identity Authentication acts as proxy IdP, and the users have no profile in Identity Authentication, choose the advanced configuration option.

Select a basic attribute:

Select a fallback attribute:

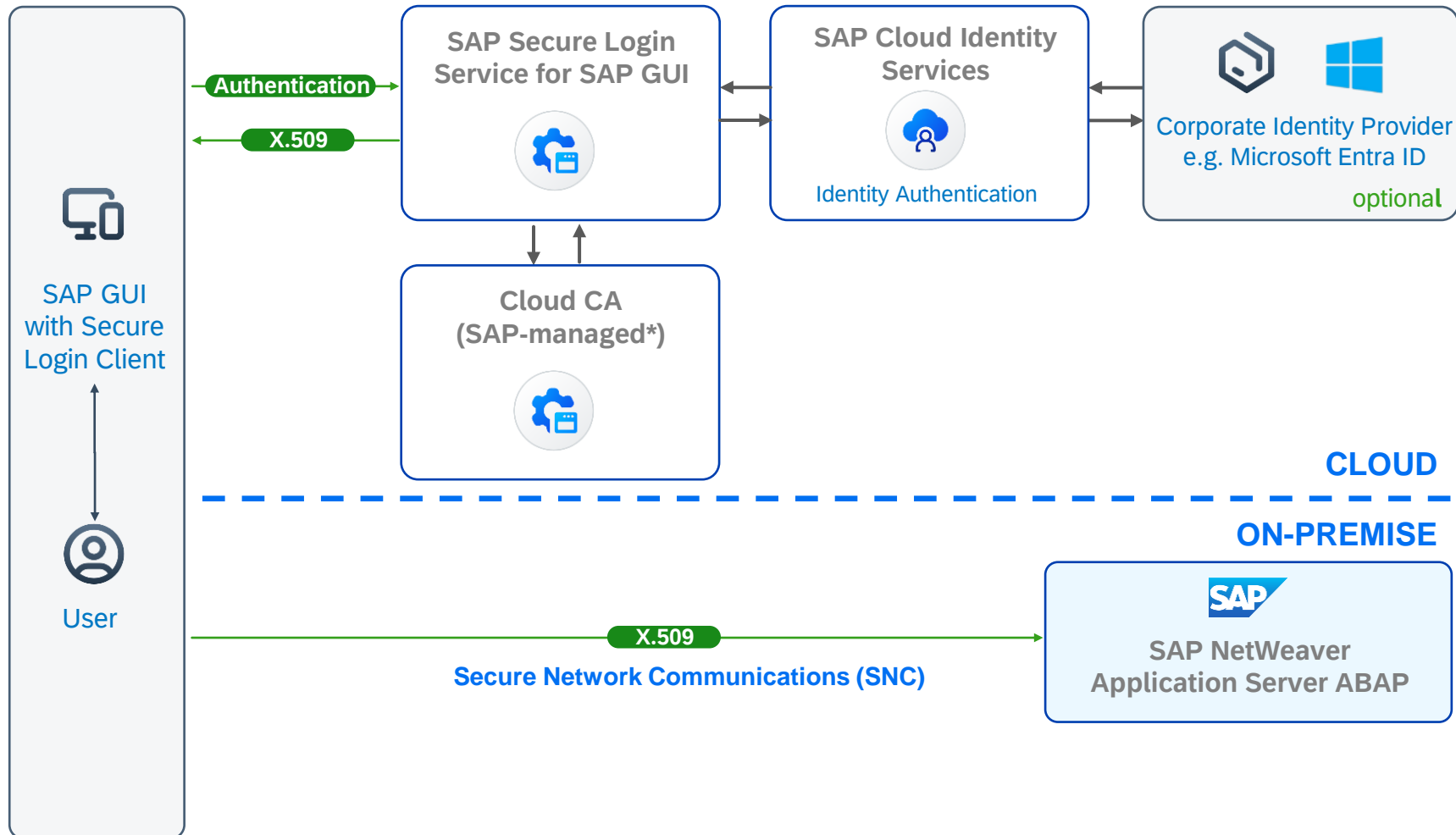
Advanced Configuration

For more information about Subject Name Identifier, see [Identity Authentication Documentation..](#)

Global User ID  
User ID  
Email  
Display Name  
Login Name  
Employee Number



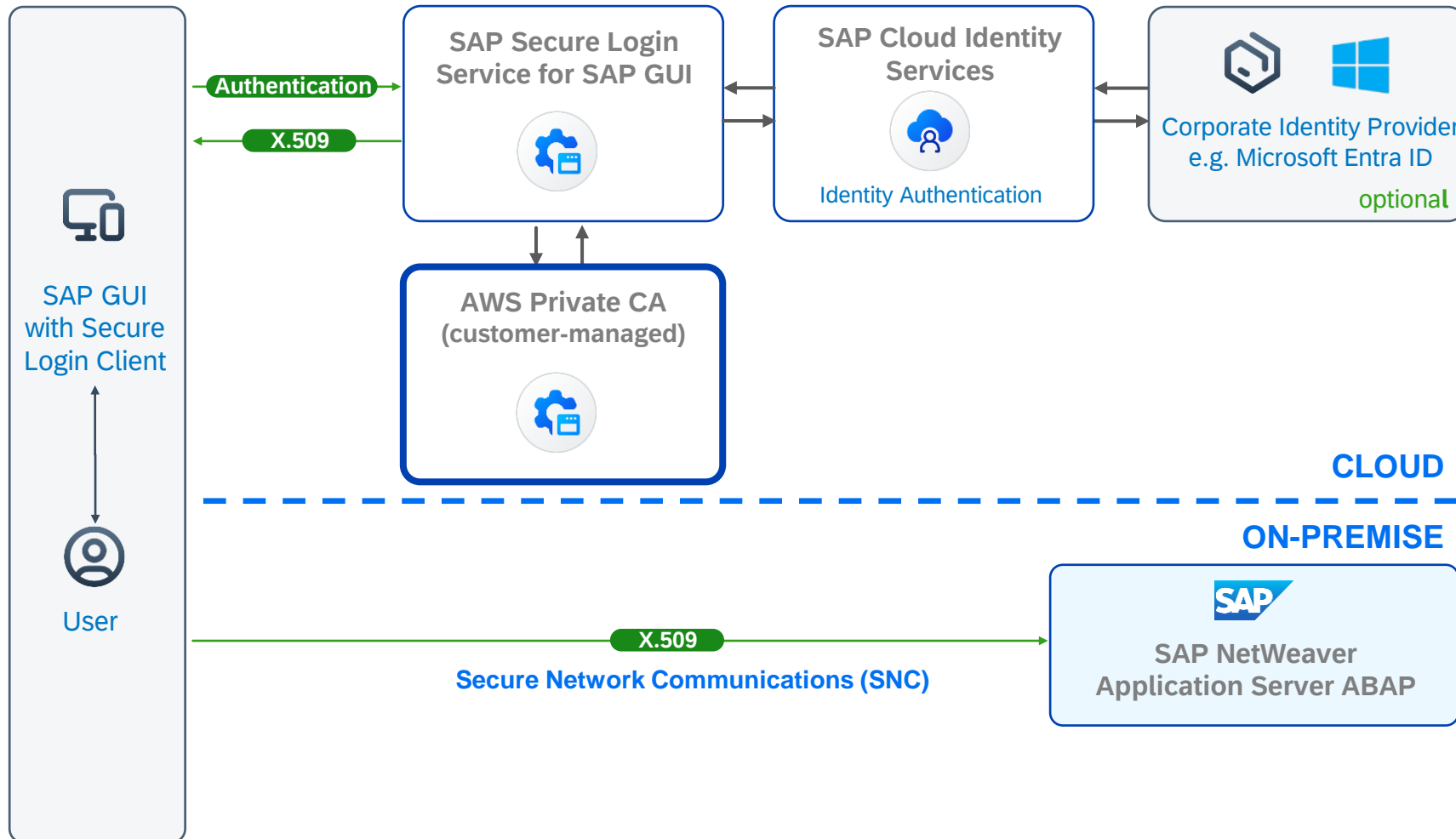
# Single sign-on based on X.509 certificates – Process flow



1. User opens a SAP GUI connection
2. Secure Login Client (SLC) redirects user to the identity provider logon page
3. User authenticates to Identity Authentication Service
4. Optionally, authentication can be delegated to a corporate IdP (such as Azure AD)
5. After successful authentication, SAP-managed\* Cloud CA issues an X.509 certificate
6. SAP Secure Login Service returns the X.509 certificate, valid for one day, to SLC
7. X.509 certificate token is used for authenticating the SAP GUI user to the ABAP system

\* Support for customer-managed Cloud CA's is a roadmap topic

# Released today: Support for AWS Private Certificate Authority



1. User opens a SAP GUI connection
2. Secure Login Client (SLC) redirects user to the identity provider logon page
3. User authenticates to Identity Authentication Service
4. Optionally, authentication can be delegated to a corporate IdP (such as Azure AD)
5. After successful authentication, **AWS Private CA** issues an X.509 certificate
6. SAP Secure Login Service returns the X.509 certificate, valid for one day, to SLC
7. X.509 certificate token is used for authenticating the SAP GUI user to the ABAP system

# Released today: Support for AWS Private Certificate Authority

- New tab “Custom CA” in SAP Secure Login Service administration console
- Configuration for token exchange
- Credentials for accessing AWS
- Identifier of AWS Private CA to be used

The screenshot displays the SAP Secure Login Service administration console. The top navigation bar includes the SAP logo, "Secure Login Service", and a "User Menu" dropdown. Below the navigation bar, there are tabs for "Home", "Subscriber", and "Custom CA". The main content area is titled "Custom CA Configuration" and includes a sub-header "Use this page to configure your Custom CA setup." Below this, it states "Supported Hyperscale- Provider: Amazon Web Services (AWS)". There are two tabs: "OIDC Configuration" (selected) and "Custom CA Configuration".

**OIDC Configuration**

Dependency Name for Token Exchange  
sls-custom-ca

Provider URL  
https://sapslsdemo.accounts400.ondemand.com

AWS Audience (aud)  
5f832e31-10f1-4fea

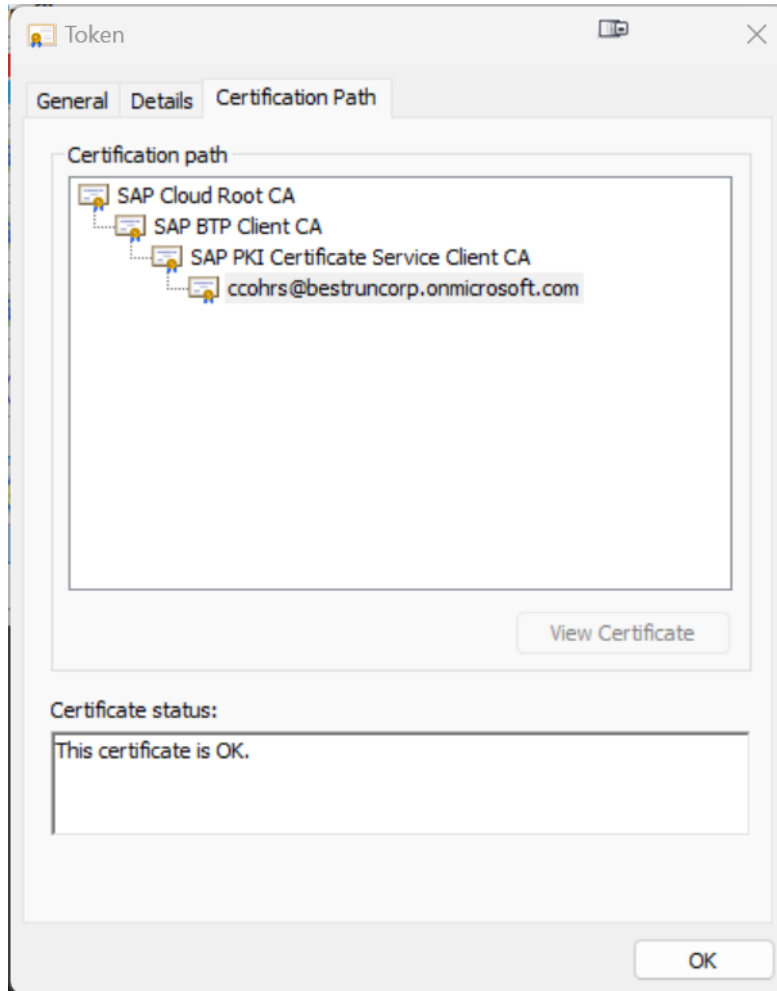
AWS oAudience (oaud)  
39c59d00-2fb4-

**Custom CA Configuration**

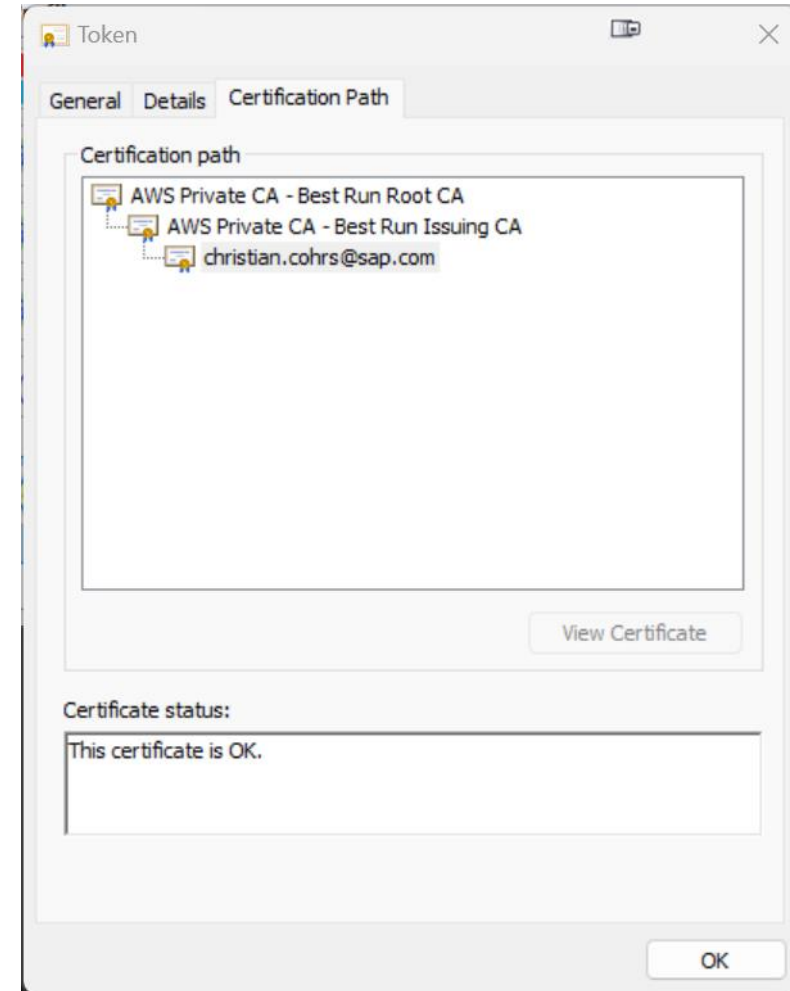
Use the table below to provide the information about your AWS Private CA

Role ARN:	arn:aws:iam:::role/sap-sls-demo_custom-ca
Private CA ARN:	arn:aws:acm-pca:eu-west-1::certificate-authority/56609a21-
Enabled:	<input checked="" type="checkbox"/>

# Released today: Support for AWS Private Certificate Authority



Certificate based on SAP Cloud Root CA



Certificate based on AWS Private CA

This is the current state of planning and may be changed by SAP at any time without notice.

# Migrating single sign-on from SAP Single Sign-On to SAP Secure Login Service

## SAP Single Sign-On

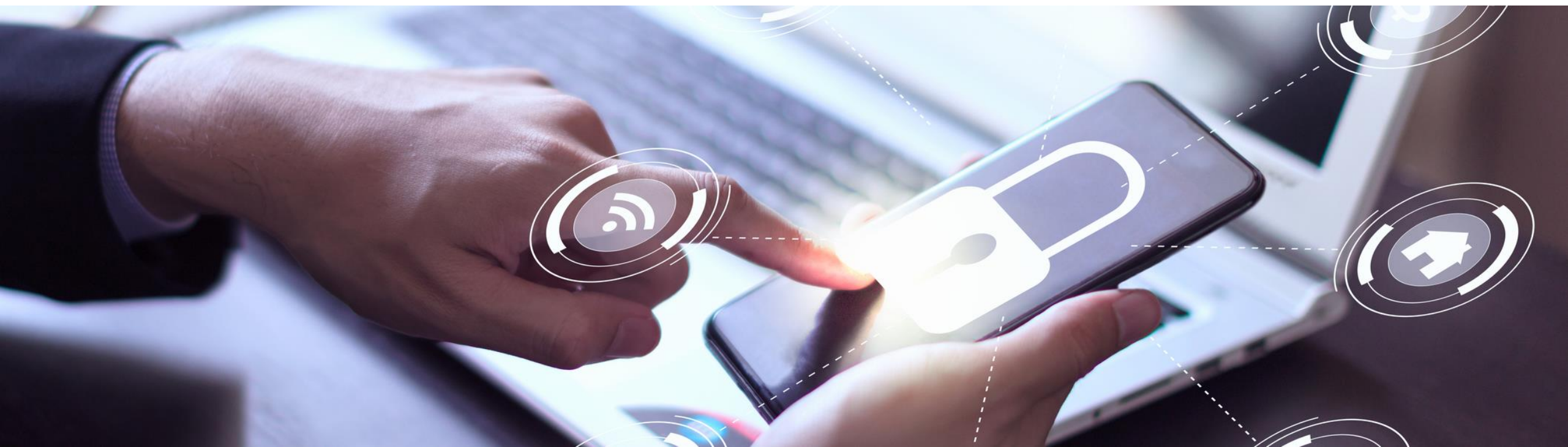
1. SSO with Kerberos
2. SSO with customer-provided X.509 certificates
3. SSO based on X.509 certificate from Secure Login Server, on SAP NetWeaver AS Java



## SAP Secure Login Service

1. No change, existing software and configuration can be reused
2. Same as 1.
3. On-premise server replaced by SAP Secure Login Service plus identity provider
  - SAP NetWeaver AS Java authentication stack replaced with IAS or corporate IdP
  - On-premise Certificate Authority replaced with cloud service
  - On user desktop, new profile in Secure Login Client
  - On SAP NetWeaver AS ABAP, added trust to SAP Cloud Root CA and updated user mappings in SU01

# Summary





# SAP Secure Login Service for SAP GUI

## Simple and more secure access for SAP GUI users

Offer single sign-on based on X.509 certificates or Kerberos technology

Protect business data with stronger authentication methods

Benefit from enhanced user experience and increased productivity

## Integration with existing authentication infrastructure

Integrate with your existing corporate identity provider

Alternatively use Kerberos technology, based on corporate Windows domain

## Fast implementation and low TCO

Rely on a lean cloud service

Achieve short time-to-value without any additional on-premise server components



# Additional information

SAP Product Page

<https://www.sap.com/products/financial-management/secure-login-service-for-gui.html>

SAP Community

<https://community.sap.com/topics/single-sign-on>

Documentation

<https://help.sap.com/sls>

Blog

[SAP GUI MFA with SAP Secure Login Service and Microsoft Entra ID](#)

[Subscribe to our monthly security newsletter](#)



**Q & A**

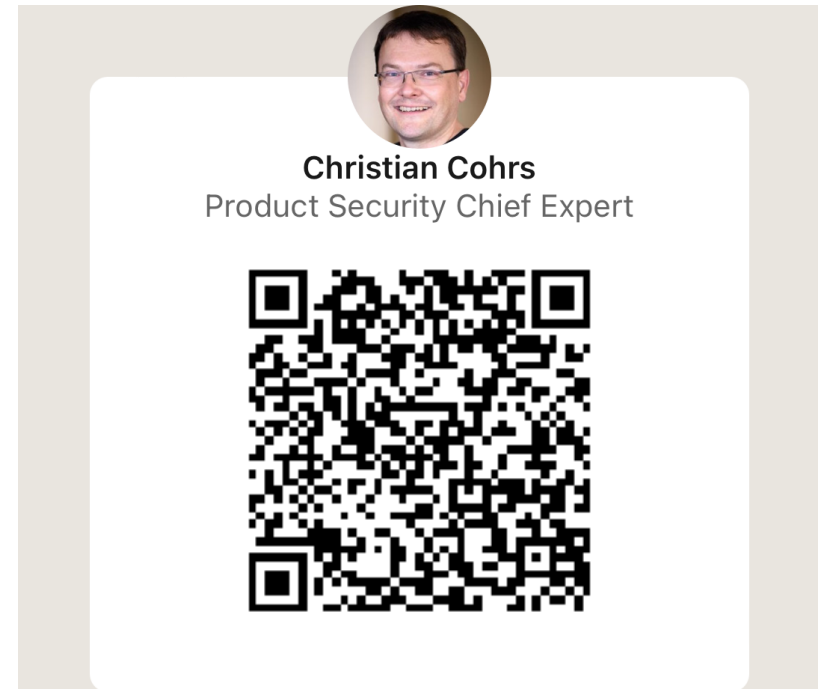


# Thank you.

Contact information:

Christian Cohrs

[christian.cohrs@sap.com](mailto:christian.cohrs@sap.com)



<https://www.linkedin.com/in/christian-cohrs>

