



# SAP Cloud Identity Services - Identity Authentication Solution Overview

January 2022

PUBLIC

# Agenda

Introduction

Technologies and capabilities

Further information

Appendix

# SAP Identity Management and Access Governance Solutions

## Overview

### Identity Management

Identity Provisioning

SAP Identity Management

### Governance, Risk & Compliance

SAP Cloud Identity Access Governance

SAP Access Control

### Authentication & Single Sign-On

**Identity Authentication**

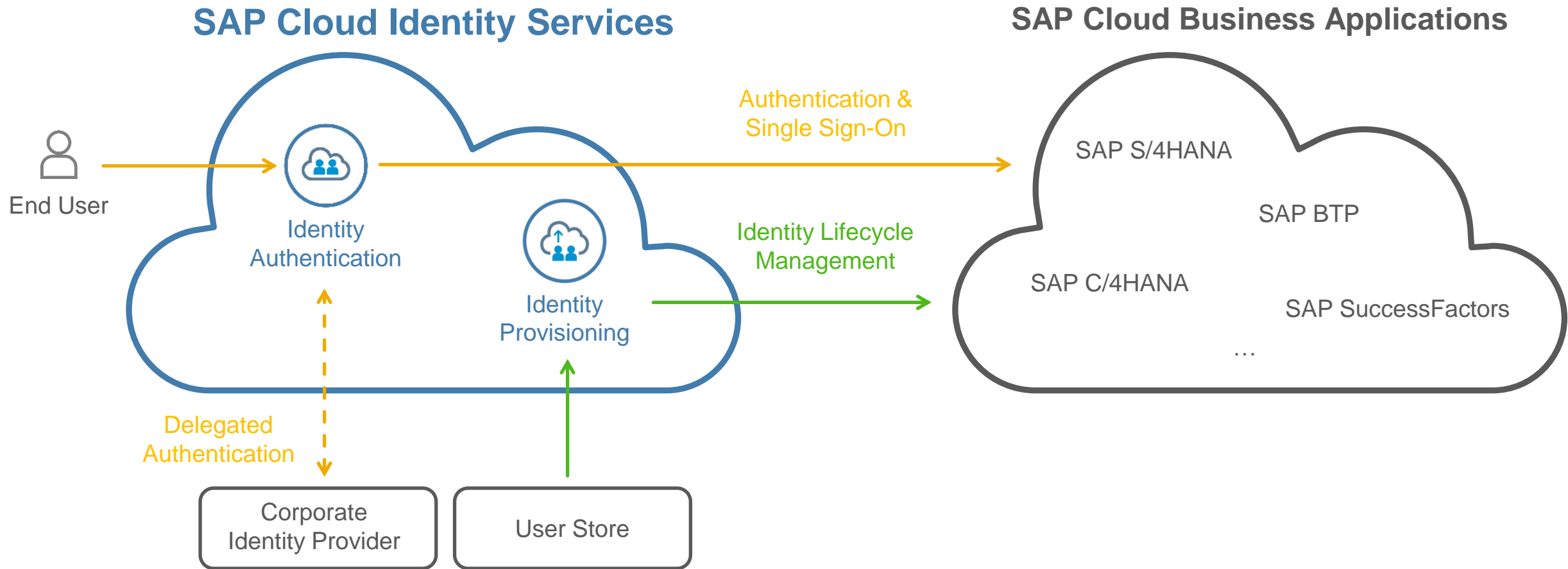
SAP Single Sign-On

**Setting the stage**

**Accessing the applications**

# SAP Cloud Identity Services

## Overview



# Technologies **and capabilities**





# SAP Cloud Identity Services - Identity Authentication

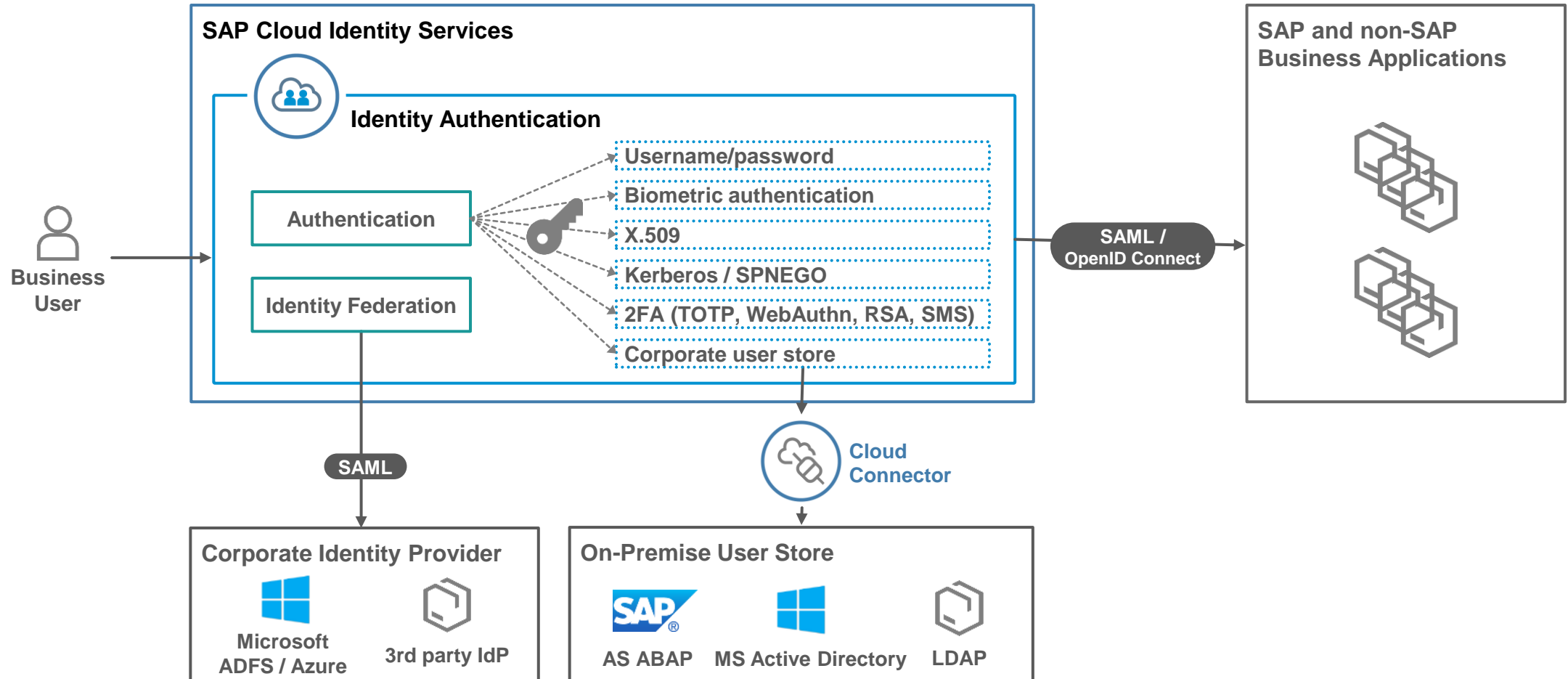
Identity provider for SAP's cloud-based business applications

SAP Cloud Identity Services - Identity Authentication enables single sign-on for SAP's cloud-based business applications, with two usage options

1. As IdP proxy for a seamless, flexible integration with customers' existing IAM infrastructure
  - Simple central configuration
  - Flexible configuration options
  
2. As the landscape-wide identity provider
  - Secure authentication with multiple factors
  - User management and self-services
  - Pre-configured trust configuration

# Identity Authentication & Federation

## SAP Cloud Identity Services

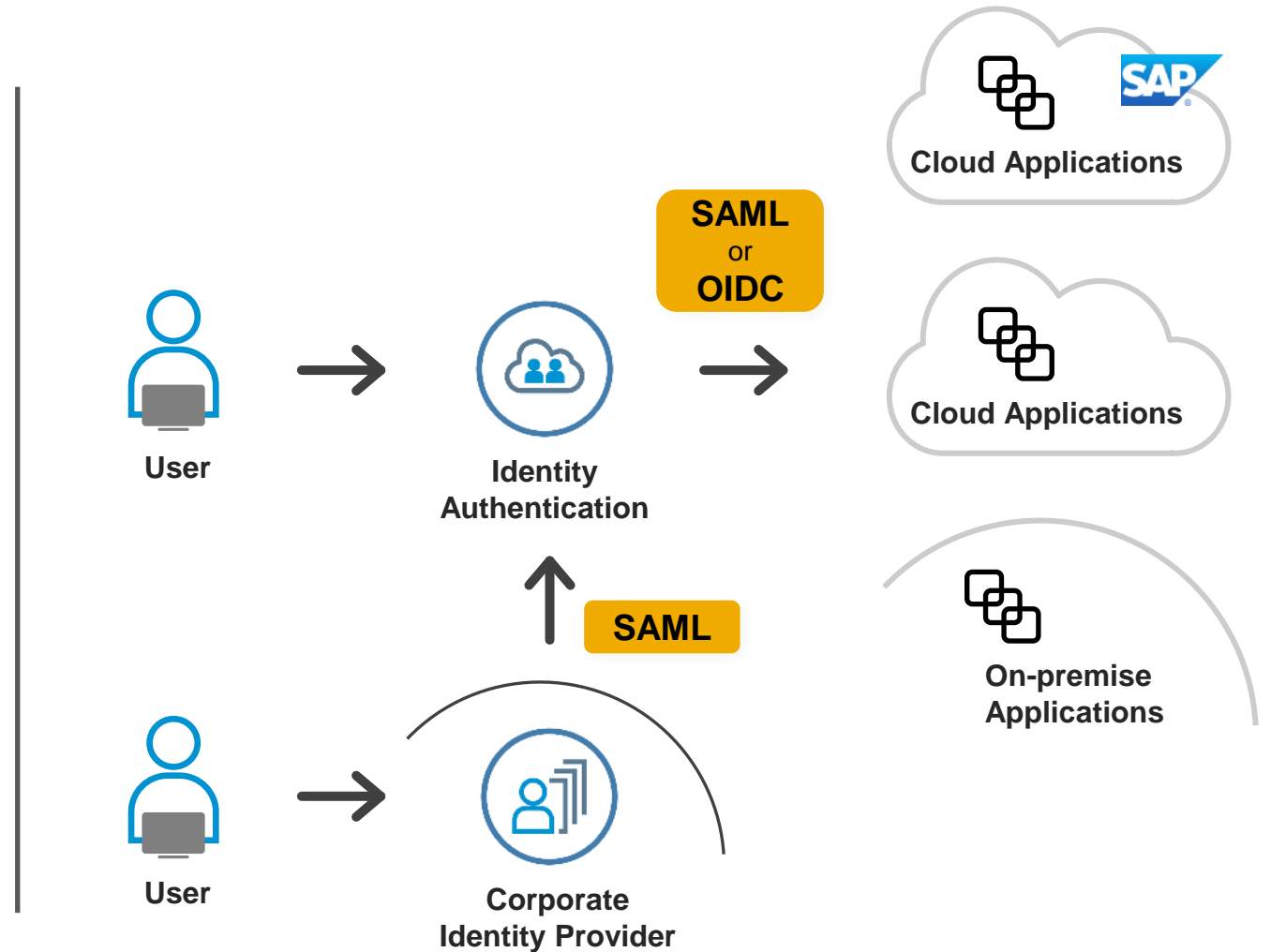


# Based on open security standards

## Interoperable

with all applications supporting SAML\* 2.0 standard

or OpenID Connect (OIDC)



\*SAML = Security Assertion Markup Language

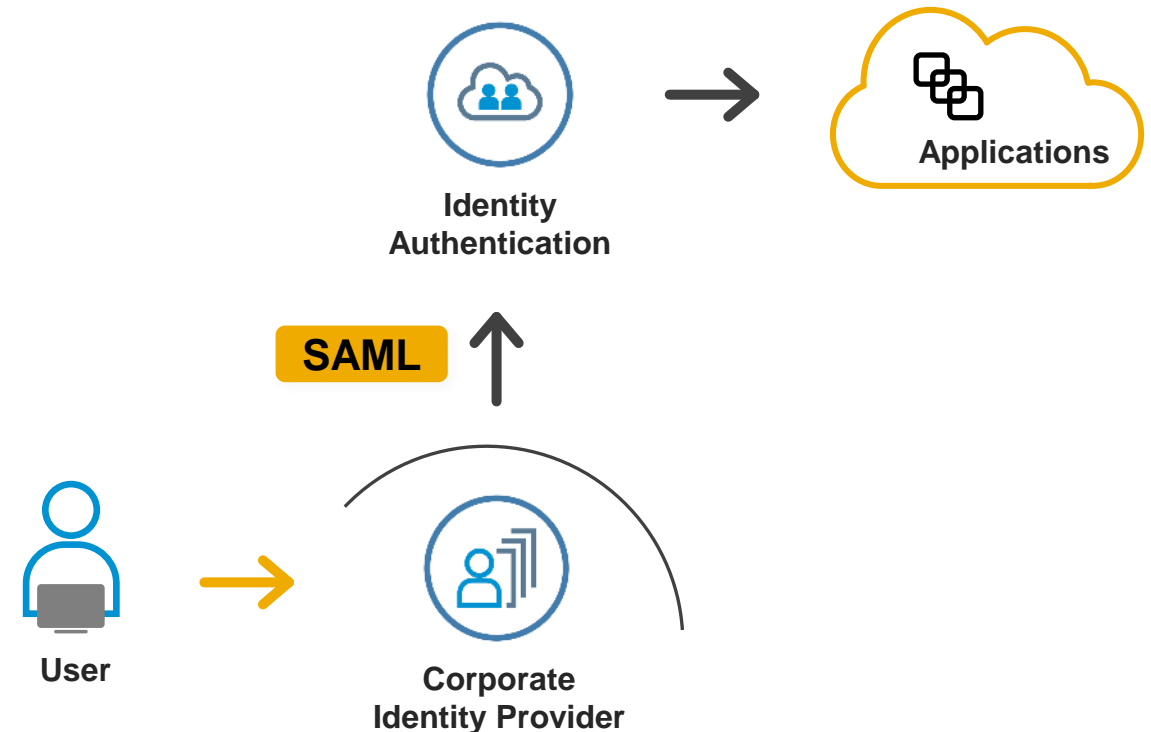


# Delegated authentication

Identity Authentication as a proxy to a corporate identity provider (IdP)

## Identity provider proxy

- Authentication is delegated to corporate identity provider login
- Reuse of existing single sign-on infrastructure
- Easy and secure authentication for employee scenarios
- Federation based on the SAML 2.0 standard
- System applications supported as well

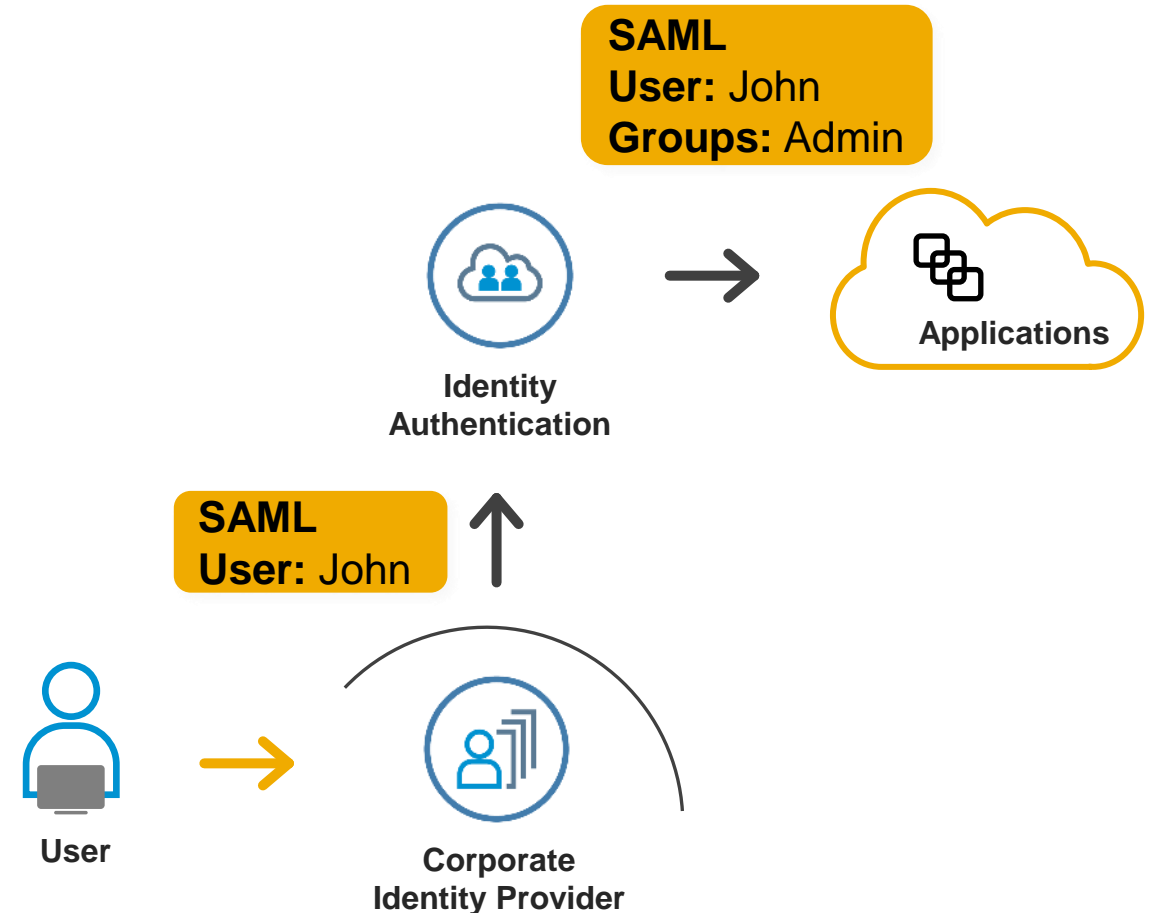


# Delegated authentication

Federation, proxy or both?

## Enriching the assertion

- Original assertion from the corporate identity provider is enriched with additional attributes
- Mix of attribute values coming from the corporate IdP and the local user store
- Users don't need to exist in local user store
- Enables hybrid scenarios such as authenticate via corporate IdP but manage groups via Identity Authentication



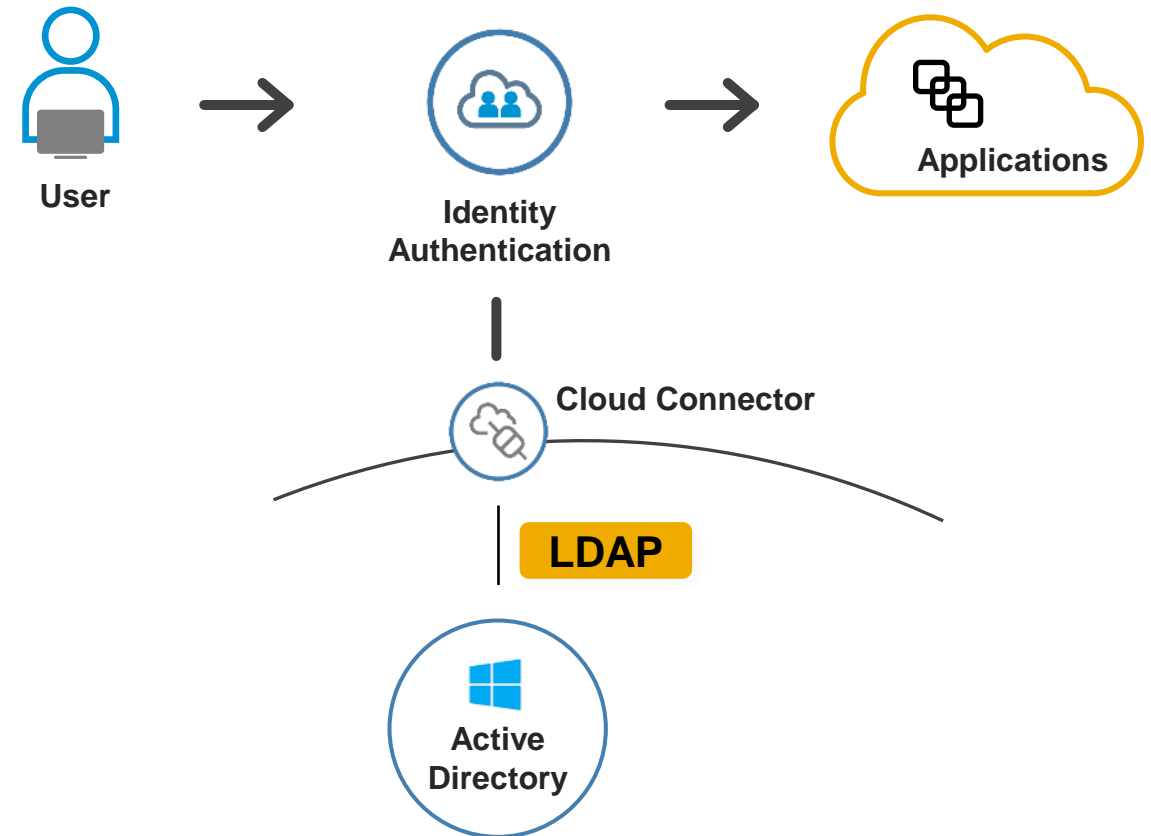
# Delegated authentication

Authentication with an on-premise user store

## On-premise user store

- Users credentials from:
  - Active Directory (through LDAP)
  - AS ABAP (through SCIM\*)
- No user replication to the cloud required
- Internal network ports do not need to be exposed to the Internet
- In addition: usual Identity Authentication product features can be used:
  - UI configuration, policies, two-factor authentication

\* requires AS Java + SAP Single Sign-On (which enables SCIM interface)

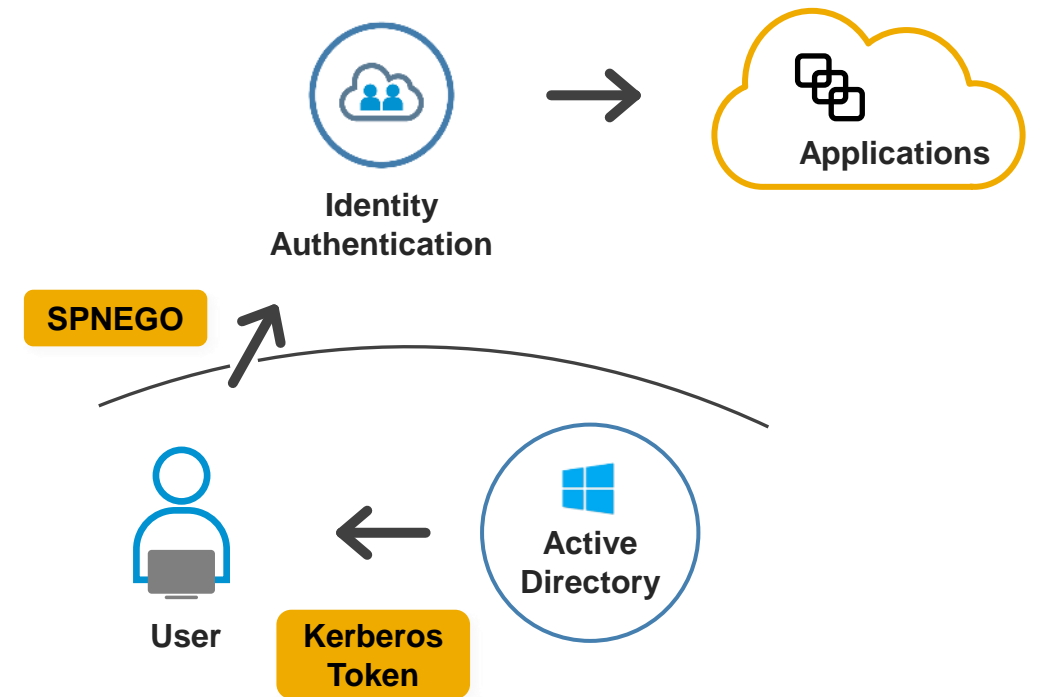


# Delegated authentication

Re-use of Windows Domain Authentication (SPNEGO)

## SPNEGO\* authentication

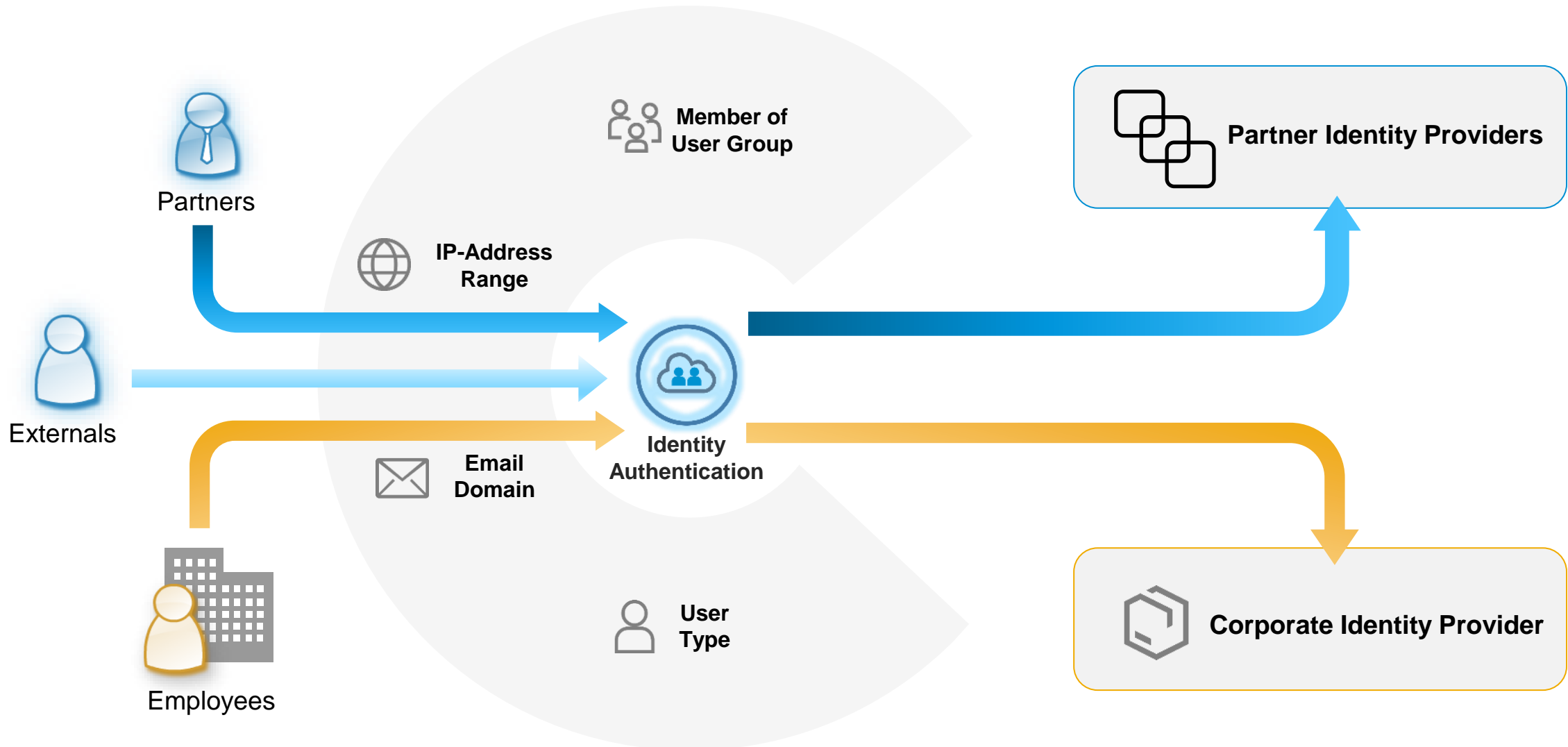
- Users authenticated with Microsoft Active Directory enjoy single sign-on to cloud applications without re-authentication
- Reuse of existing corporate identity infrastructure
- Secure authentication and SSO for cloud and on-premise web applications



\*SPNEGO: Simple and Protected GSSAPI Negotiation Mechanism

# Delegated authentication towards multiple identity providers

## Conditional authentication



# Delegated authentication towards multiple identity providers

## IdP-initiated authentication

### Identity Authentication as a proxy to multiple IdPs

- Secure your business network and allow partner users to login via their corporate IdP
- Authentication is initiated by the corporate IdP
- Upon successful authentication, a check for correct user group assignment can be configured (optional)
  - Sync of users from IdPs to groups in Identity Authentication is required





# SAP Cloud Identity Services - Identity Authentication

Value prop for customers with existing IdP

## Authentication

- All SAP cloud applications can offer their users the same authentication mechanisms
- Identity Authentication acts as authentication broker
  - easy separation mechanism for multiple user stores
  - flexible configuration where to validate user's credentials
- Strong authentication: configurable MFA enforcement

## Single Sign-on

- Central SSO endpoint for all SAP Cloud applications
- Choice between SAML and OpenID Connect
- Service provider specific attribute mapping/rewriting and enrichment of assertions by corporate IdP
- Pre-configured or semi-automated trust configuration

## Integrating SAP applications

- Common identity for users
- Unified way for user management
- Data across applications can be correlated (*precondition for central foundation services*)
- Security Token Service for service based SSO (*future scope*)
- Authorization management

## Compliance

- Single audit log for authentication/SSO for all SAP cloud applications

# Authentication options

## Basic authentication

- User ID / email and password

## Biometric authentication

- FIDO2 compatible biometric authentication device

## Client certificates

- X.509

## Re-use of Windows Domain logon

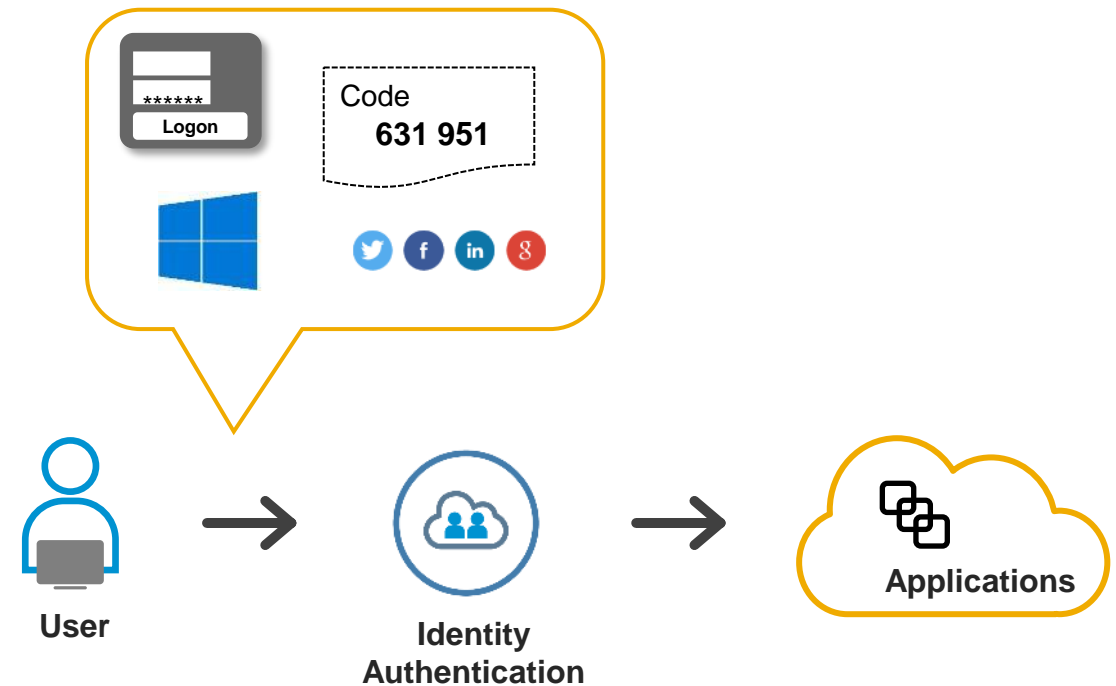
- Use of Kerberos token for single sign-on

## Two-factor authentication

- Second factor via soft-token, WebAuthn, Radius\* or SMS\*\*

## Delegated logon

- Social IdPs
- Corporate IdP



\*Radius support enabled upon request

\*\*SMS requires the license of Sinch Authentication 365

# Custom password policies

Administrator can configure custom password policies:

Custom Password Policy

Password Policy Name:

Corporate\_Policy

Password Length:

Minimum: 8

Maximum: 255

Password Lifetime:

Minimum: 24 Hours

Maximum: 6 Months

Maximum Duration of User Inactivity:

6 Months

Number of Last Used Passwords that Cannot Be Reused:

5

Number of Allowed Failed Logon Attempts:

5

Password Locked Period:

1 Hour

Password Behavior:

☒ Reset password

☐ Change password

+ Add

⊗ Cancel

# Multi-factor authentication options

## Authentication methods for second factor:

- Web authentication with a FIDO2 compliant device
- One-time password (OTP) via authenticator application
- One-time password (OTP) via SMS
- One-time password (OTP) via RADIUS protocol

### Web Authentication

- Biometric secrets (e.g. fingerprint, facial recognition)
- Security hardware key
- [FIDO2](#) compatible

### OTP via authenticator app

- 6-digit OTP generated on mobile device
- SAP Authenticator for iOS or Android
- [RFC 6238](#) compatible app (e.g. authenticator by Google or Microsoft)

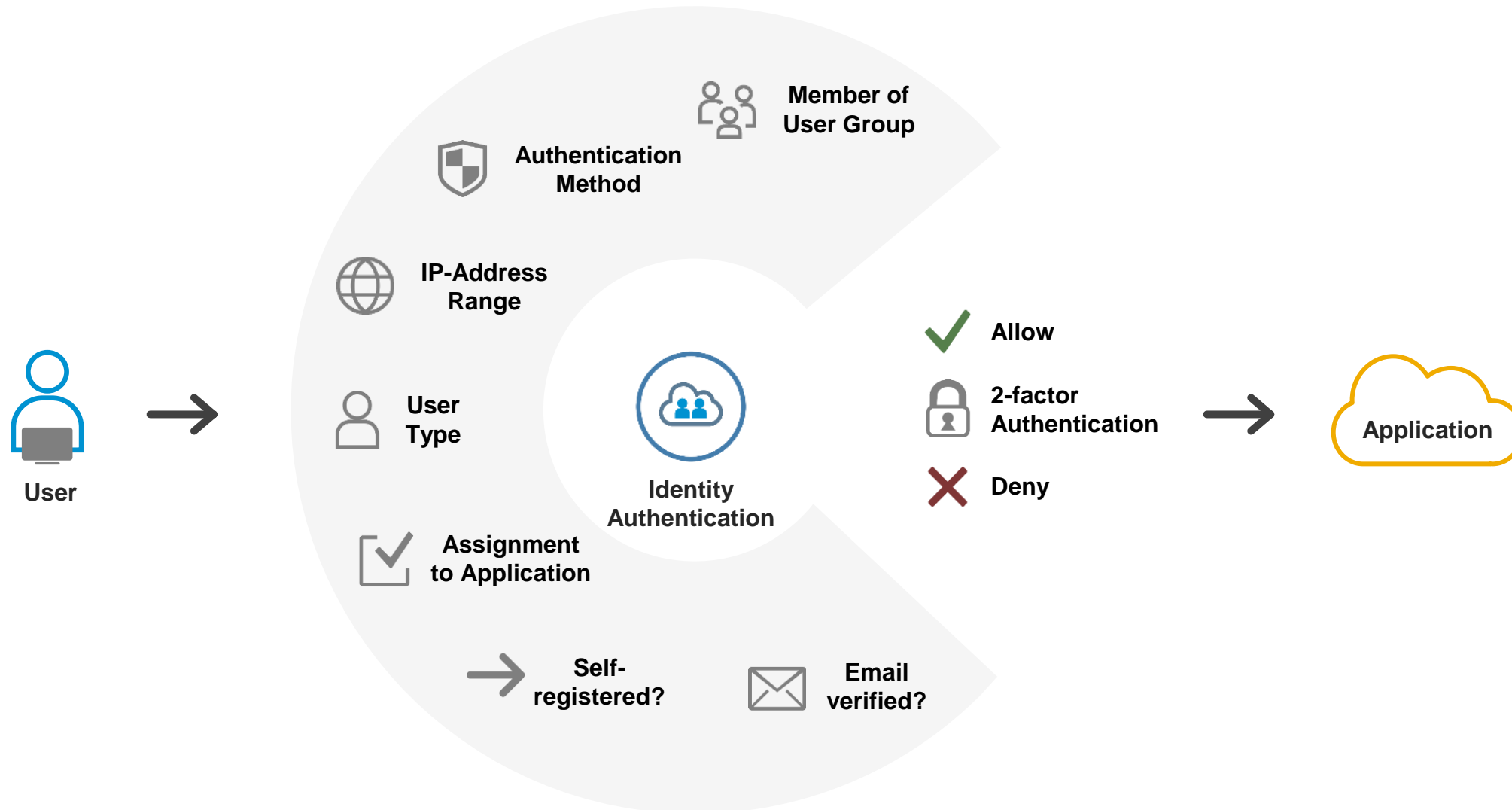
### OTP via SMS

- OTP sent as a text message to mobile phone
- Requires Sinch Authentication 365

### OTP via RADIUS

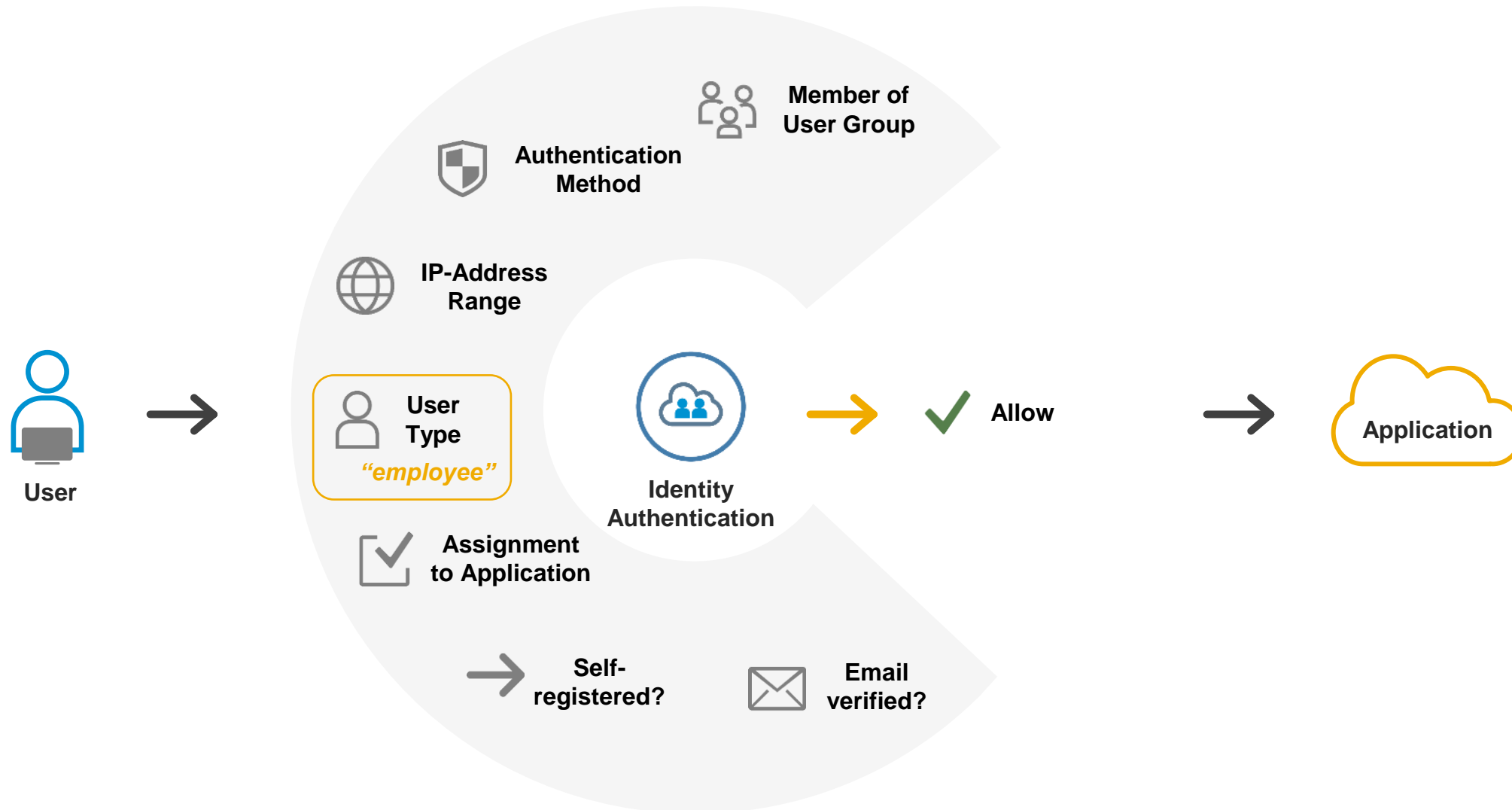
- RADIUS client app to request OTP code
- Code generated by RADIUS server
- Activation upon request

# Control access to the application – risk-based authentication



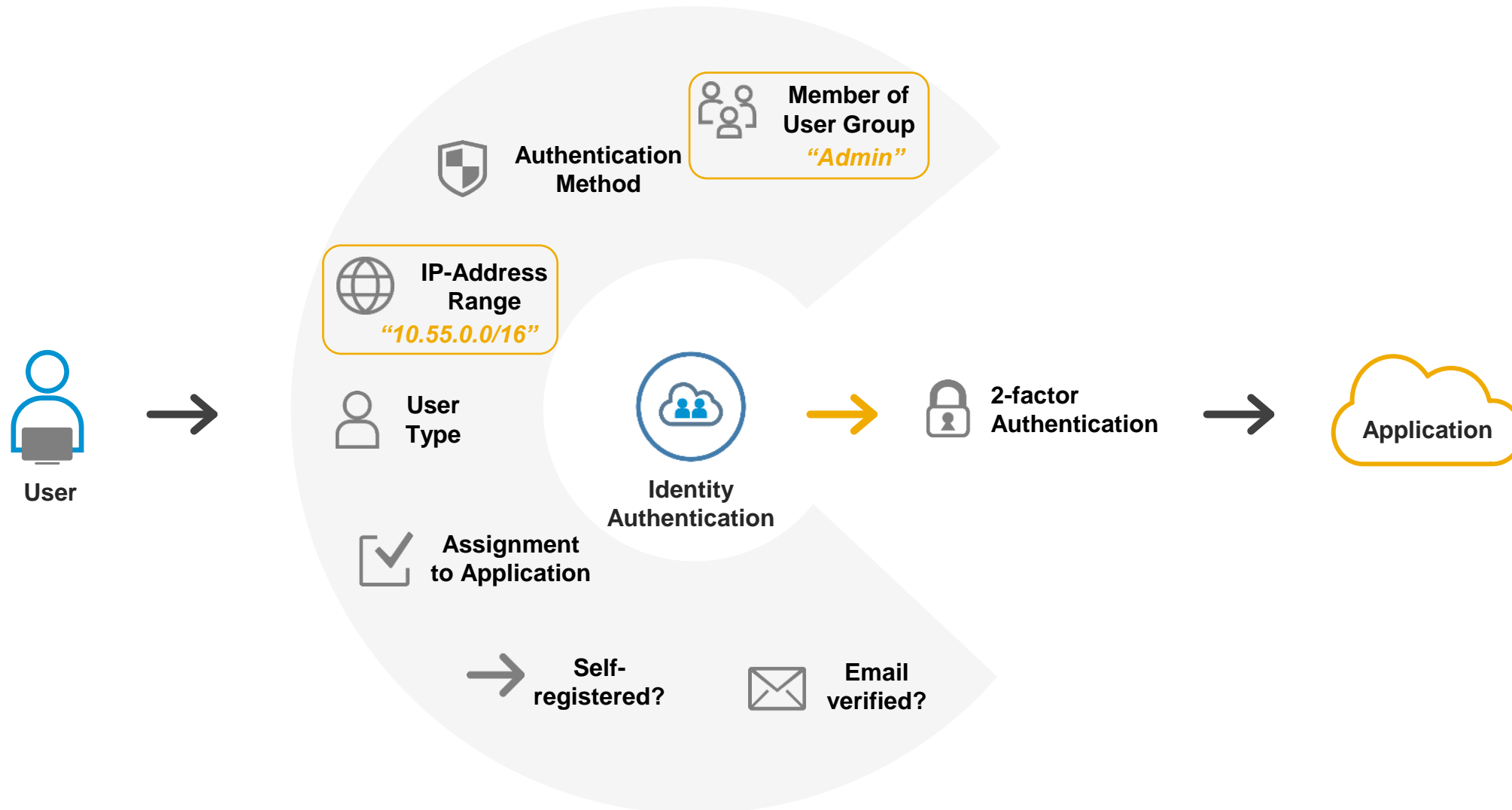
**Supports both local authentication and IdP proxy**

# Control access to the application





# Control access to the application



# Protecting self-registration with Google reCAPTCHA / phone verification

## Access protection for applications

- Protect the registration to applications from spam and abuse
- Prevent bots from automated fake user registrations to your websites
- Further information
  - [Google reCAPTCHA](#)
  - [Phone verification](#)

The image displays three overlapping screenshots of a web application's registration process:

- Registration Form:** A form titled "Registration" with the sub-header "Tell Us About Yourself". It includes input fields for First Name (Peter), Last Name (Miller), E-Mail (peter.miller@velotics.com), and Phone (+1 234 5678 90). Below this is a "Set Password" section with fields for Password and Re-Enter Password, both marked as required and showing green checkmarks.
- Verify Your Telephone Number:** A modal dialog box titled "Verify Your Telephone Number". It contains a blue information box stating: "You can change your telephone number. Please type: +(country code) followed by the area code without the leading zero, followed by the subscriber number. Example: +(XXX) XXX XXXXXXXX". Below this, it says: "The Document Center application requires telephone verification. We have sent a code to your telephone number. Please enter the code you have received and choose Continue." There are input fields for Telephone (+1234567890) and Code, with a "Required" label. At the bottom are "New Code" and "Continue" buttons.
- reCAPTCHA Challenge:** A screenshot of a reCAPTCHA challenge. It asks the user to "Select all squares with vehicles" and provides a grid of images. A "SKIP" button is visible at the bottom right of the challenge area.

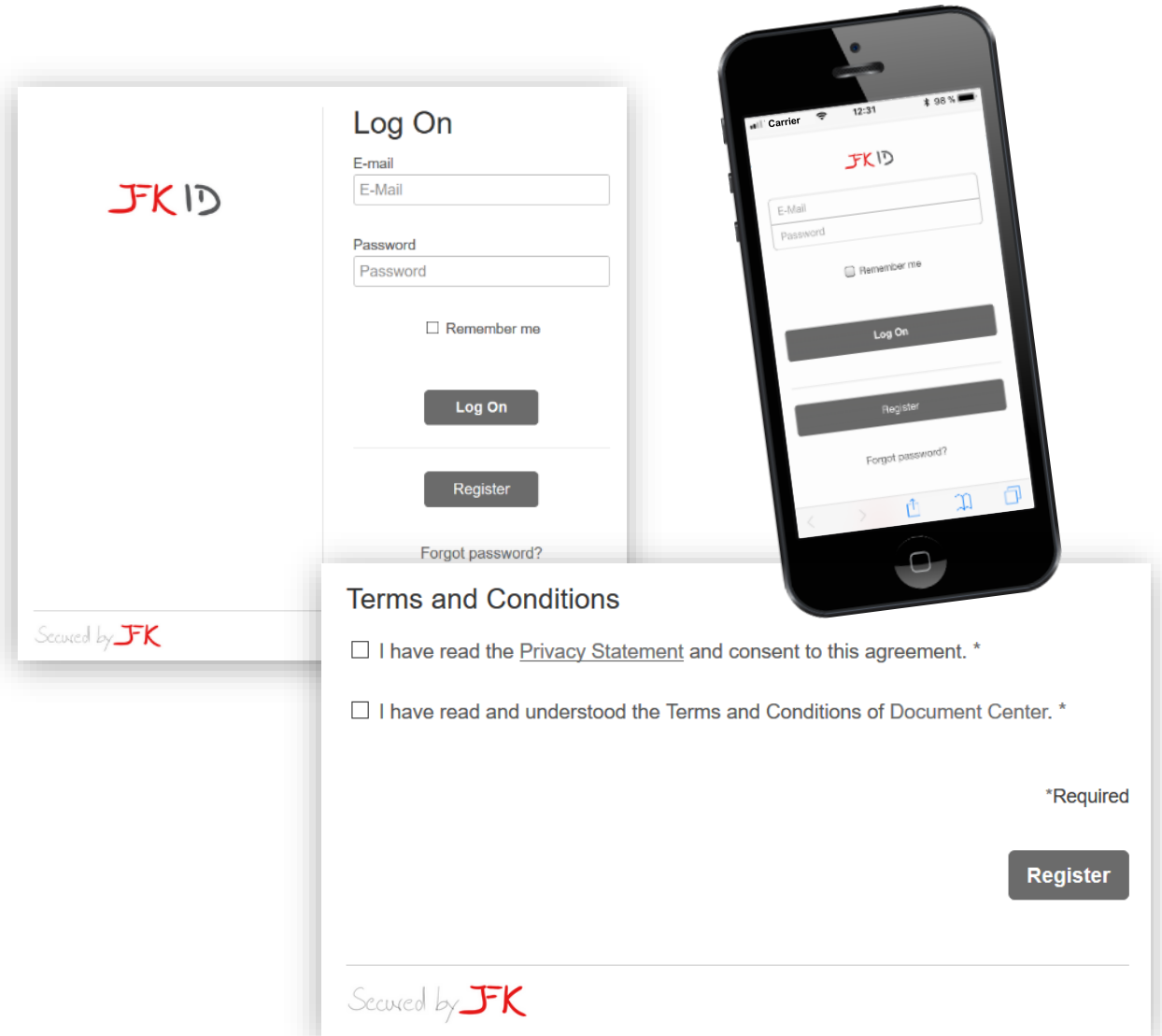
# Branding and customization

## Customization features

- Company logo
- Application name and logo
- Color style
- Full customization via CSS
- Terms of use & privacy policy, incl. IdP proxy
- Adjust UI texts via API
- Email templates

## Product features

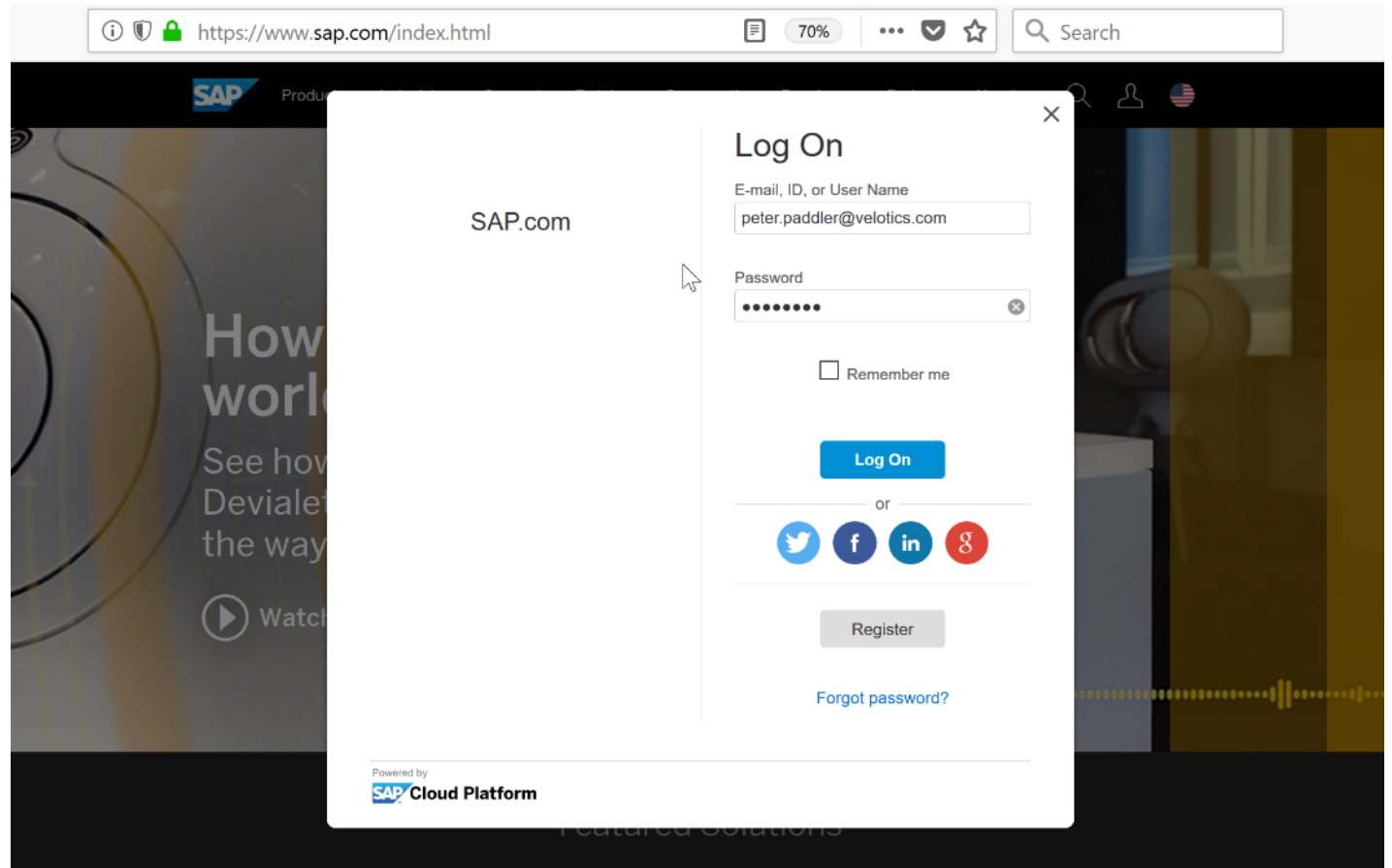
- Responsive UIs
- Multi-language support



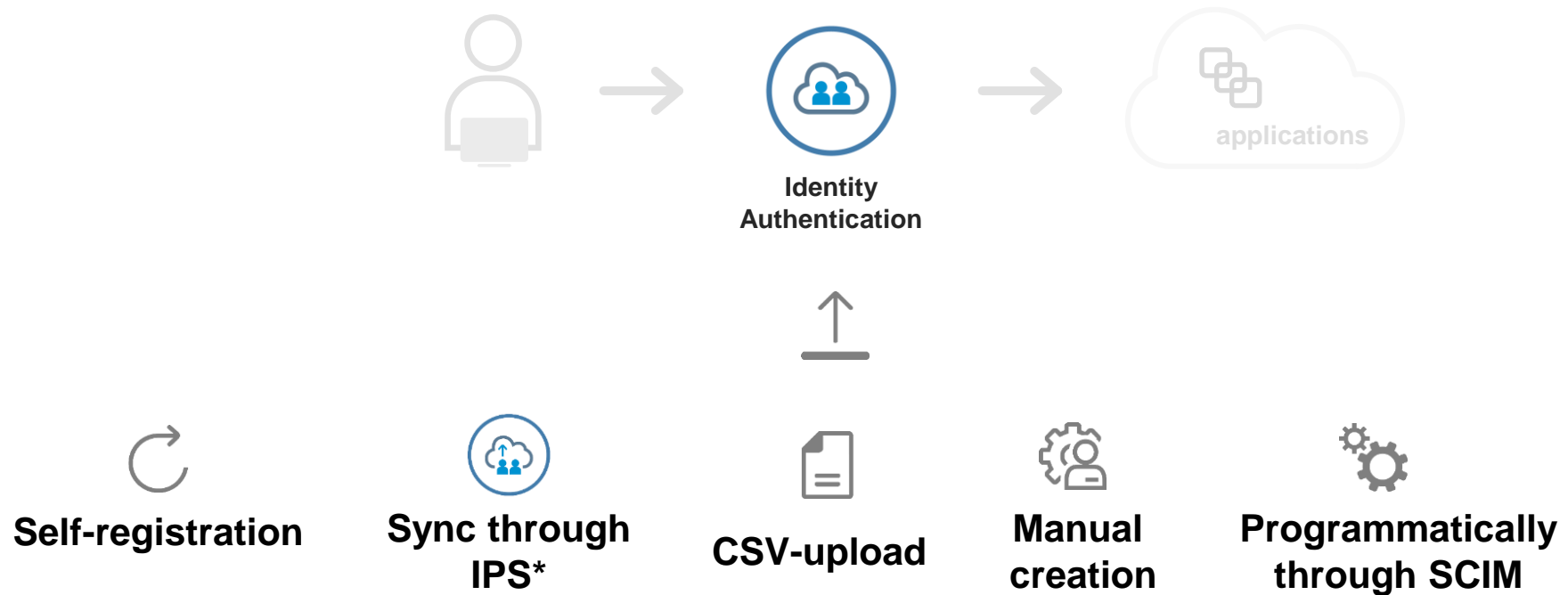
# Logon overlays in customer applications

**Logon screen as an overlay**  
(compared to a browser redirect to navigate away from application)

- Can programmatically be integrated by the application
- Out-of-the-box integration for SAP Cloud Portal



# How can users be created?



\* IPS: SAP Cloud Identity Services - Identity Provisioning

# User & group management

## User administration

- Web based user management
- User search
- Mass user import/export
- Monitor user access

## User groups administration

- Define user groups
- Assign users to groups

## Integration

- Programmatic integration via SCIM REST APIs

The screenshot displays the SAP Cloud Platform Identity Authentication Administration Console. The left sidebar contains a navigation menu with options: Home, Users & Authorizations (expanded), User Management (selected), User Groups, Administrators, Import Users, Export Users, User Provisioning, Applications & Resources, Identity Providers, and Monitoring & Reporting. The main content area is titled 'User Management' and features a search bar with fields for User ID, First Name, Last Name, E-Mail, and Login Name, followed by a 'Search' button and a 'Simple ...' link. Below the search bar, a table lists 261 users. The table has columns for checkboxes, User ID, First Name, Last Name, E-Mail, and Login Name. The first four users listed are:

	User ID	First Name	Last Name	E-Mail	Login Name
<input type="checkbox"/>	P000435	Peter	Paddler	peter.paddler@velotics.com	>
<input type="checkbox"/>	P000434	Peggy	Winter	peggy.winter@velotics.com	>
<input type="checkbox"/>	P000433	Karl	Meier	karl.meier@velotics.com	>
<input type="checkbox"/>	P000261	Hans	Meier	hans.meier@velotics.com	>

At the bottom right of the console, there are three buttons: 'Provision Users' (with a plus icon), 'Delete Users' (with a trash icon), and 'Add User' (with a plus icon).



# Further **information**



# Where to find more information

## Security software

<https://community.sap.com/topics/security>

## SAP Cloud Identity Services - Identity Authentication

<https://community.sap.com/topics/cloud-identity-services/identity-authentication>





# Appendix



# Product strategy for IAM & CIAM

General direction

*SAP Cloud Identity Services - Identity Authentication service and SAP Customer Identity are complementary side-by-side solutions:*

- **Identity Authentication service addresses mainly B2E-scenarios** with focus on employee and contractor users
- **SAP Customer Identity addresses mainly B2C-scenarios and B2B-scenarios** with focus on consumer (end customers and businesses) and prospect-users

Integration between the two products for authentication can be established by delegating authentication requests to the 'other' IdP.

# Product strategy for IAM & CIAM

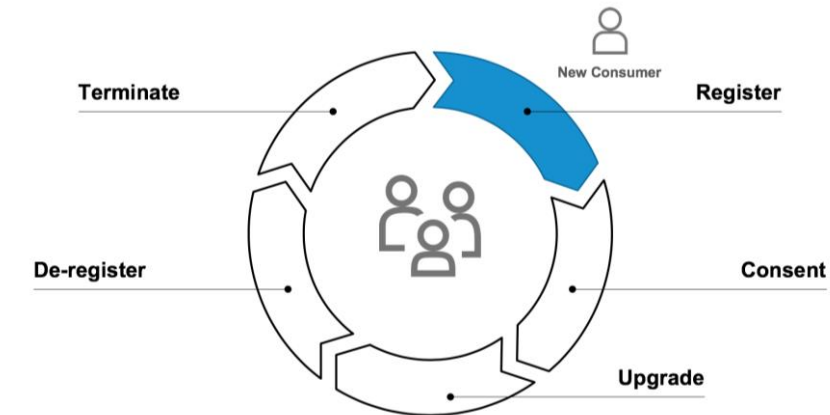
## Focus areas

### SAP Cloud Identity Services - Identity Authentication service

- Integration with a corporate SSO infrastructure / federation capabilities
- Support for various standards to delegate authentication
- Stronger means of authentication (2FA/MFA)
- Support for managed identity lifecycle via IDM solutions

### SAP Customer Identity

- User self-registration scenarios and progressive profiling
- Enterprise consent management
- Integration with social IdPs
- Sophisticated branding capabilities
- Seamless integration of IdP functionality directly into customer's sites ('native integration')



# Secure authentication and single sign-on

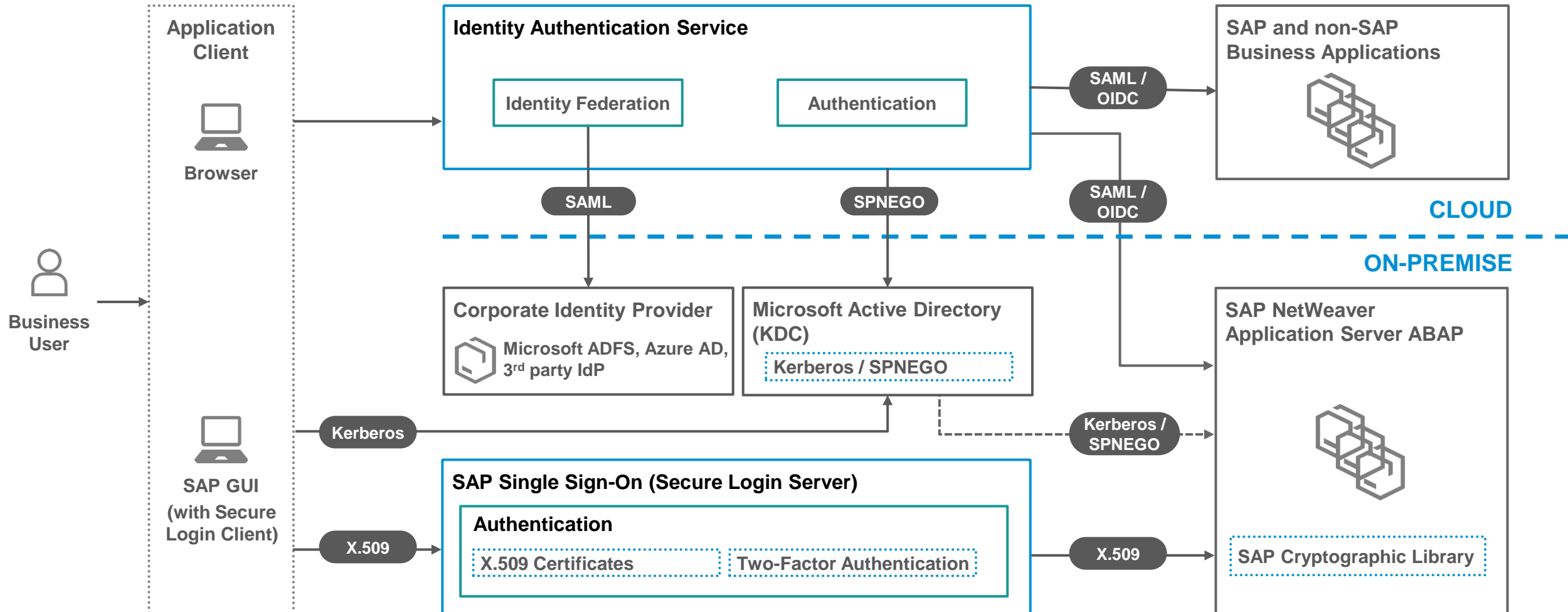
How to decide on the right solution

**SAP Single Sign-On** and **SAP Cloud Identity Services - Identity Authentication** both support secure authentication and single sign-on. While SAP Single Sign-On focuses on employee scenarios, and on-premise, the Identity Authentication service targets cloud applications beyond the corporate user base.

Solution	Supported SSO technologies	Supported clients	User types in focus	Specific capabilities	Consumption model
<b>SAP Single Sign-On</b>	<ul style="list-style-type: none"><li>• Kerberos/SPNEGO</li><li>• X.509 certificates</li><li>• SAML</li></ul>	<ul style="list-style-type: none"><li>• Browser</li><li>• Desktop clients</li></ul>	<ul style="list-style-type: none"><li>• Employee</li></ul>	<ul style="list-style-type: none"><li>• Risk-based authentication</li><li>• Digital signatures</li><li>• Certificate lifecycle management</li></ul>	<ul style="list-style-type: none"><li>• On-premise</li><li>• Some capabilities require SAP AS Java</li><li>• Some capabilities require a desktop client</li></ul>
<b>SAP Cloud Identity Services - Identity Authentication</b>	<ul style="list-style-type: none"><li>• SAML</li><li>• SPNEGO</li><li>• X.509 certificates</li><li>• Social IdP</li></ul>	<ul style="list-style-type: none"><li>• Browser</li></ul>	<ul style="list-style-type: none"><li>• Employee</li><li>• Partner</li></ul>	<ul style="list-style-type: none"><li>• Self-registration</li><li>• User management</li><li>• Branding</li><li>• Risk-based authentication</li></ul>	<ul style="list-style-type: none"><li>• Cloud subscription</li><li>• Run by SAP</li><li>• Zero footprint on desktop</li></ul>



# Authentication and single sign-on in a hybrid system landscape



# Thank you.

Contact information:

**Marko Sommer**

Product Manager

SAP SE

69190 Walldorf, Germany

[marko.sommer@sap.com](mailto:marko.sommer@sap.com)

Follow us



[www.sap.com/contactsap](https://www.sap.com/contactsap)

© 2022 SAP SE or an SAP affiliate company. All rights reserved.

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.

The information contained herein may be changed without prior notice. 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 or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP 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 platforms, 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, and they should not be relied upon in making purchasing decisions.

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. All other product and service names mentioned are the trademarks of their respective companies.

See [www.sap.com/copyright](https://www.sap.com/copyright) for additional trademark information and notices.

SAP folgen auf



[www.sap.com/germany/contactsap](https://www.sap.com/germany/contactsap)

© 2022 SAP SE oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP SE oder ein SAP-Konzernunternehmen nicht gestattet.

In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden. Die von SAP SE oder deren Vertriebsfirmen angebotenen Softwareprodukte können Softwarekomponenten auch anderer Softwarehersteller enthalten. Produkte können länderspezifische Unterschiede aufweisen.

Die vorliegenden Unterlagen werden von der SAP SE oder einem SAP-Konzernunternehmen bereitgestellt und dienen ausschließlich zu Informationszwecken. Die SAP SE oder ihre Konzernunternehmen übernehmen keinerlei Haftung oder Gewährleistung für Fehler oder Unvollständigkeiten in dieser Publikation. Die SAP SE oder ein SAP-Konzernunternehmen steht lediglich für Produkte und Dienstleistungen nach der Maßgabe ein, die in der Vereinbarung über die jeweiligen Produkte und Dienstleistungen ausdrücklich geregelt ist. Keine der hierin enthaltenen Informationen ist als zusätzliche Garantie zu interpretieren.

Insbesondere sind die SAP SE oder ihre Konzernunternehmen in keiner Weise verpflichtet, in dieser Publikation oder einer zugehörigen Präsentation dargestellte Geschäftsabläufe zu verfolgen oder hierin wiedergegebene Funktionen zu entwickeln oder zu veröffentlichen. Diese Publikation oder eine zugehörige Präsentation, die Strategie und etwaige künftige Entwicklungen, Produkte und/oder Plattformen der SAP SE oder ihrer Konzernunternehmen können von der SAP SE oder ihren Konzernunternehmen jederzeit und ohne Angabe von Gründen unangekündigt geändert werden. Die in dieser Publikation enthaltenen Informationen stellen keine Zusage, kein Versprechen und keine rechtliche Verpflichtung zur Lieferung von Material, Code oder Funktionen dar. Sämtliche vorausschauenden Aussagen unterliegen unterschiedlichen Risiken und Unsicherheiten, durch die die tatsächlichen Ergebnisse von den Erwartungen abweichen können. Dem Leser wird empfohlen, diesen vorausschauenden Aussagen kein übertriebenes Vertrauen zu schenken und sich bei Kaufentscheidungen nicht auf sie zu stützen.

SAP und andere in diesem Dokument erwähnte Produkte und Dienstleistungen von SAP sowie die dazugehörigen Logos sind Marken oder eingetragene Marken der SAP SE (oder von einem SAP-Konzernunternehmen) in Deutschland und verschiedenen anderen Ländern weltweit. Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen.

Zusätzliche Informationen zur Marke und Vermerke finden Sie auf der Seite [www.sap.com/corporate/de/legal/copyright.html](https://www.sap.com/corporate/de/legal/copyright.html).