SAP Cloud Identity Services - Identity Authentication

Solution Overview

January 2022

PUBLIC

THE BEST RUN SAP®

Agenda

Introduction

Technologies and capabilities

Further information

Appendix

SAP Identity Management and Access Governance Solutions

Overview

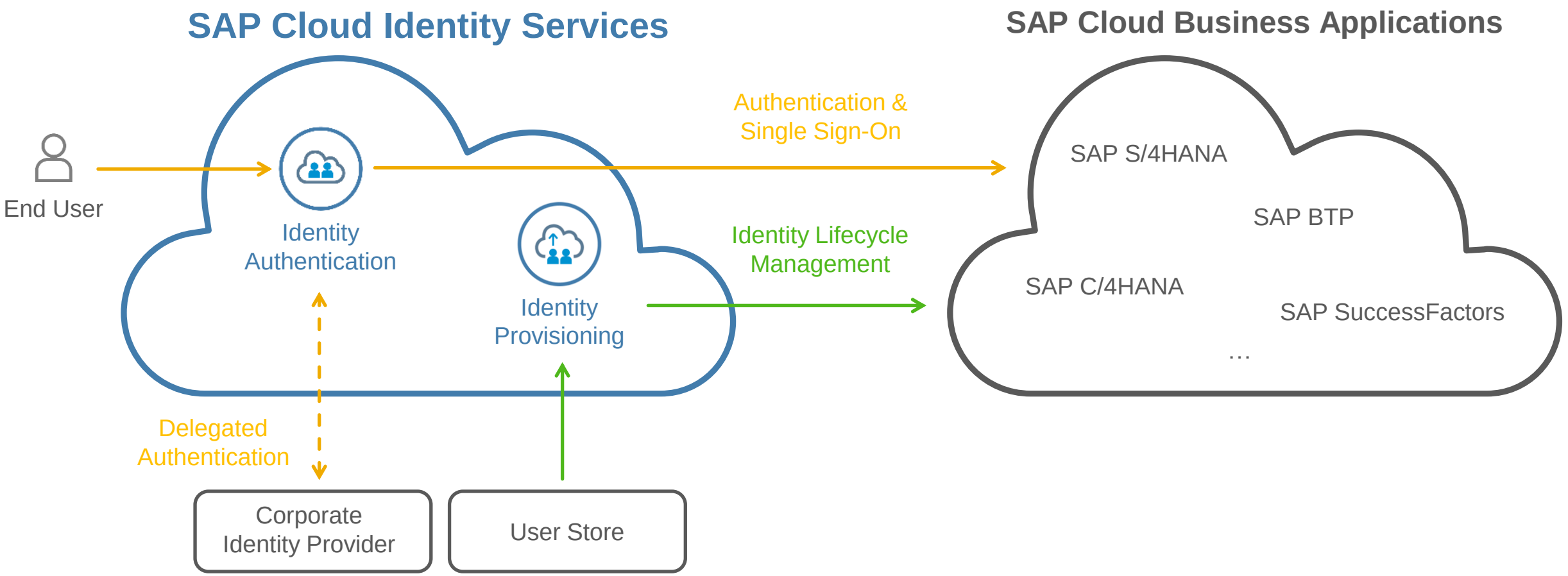
Identity Management	Governance, Risk & Compliance	Authentication & Single Sign-On
Identity Provisioning	SAP Cloud Identity Access Governance	**Identity Authentication**
SAP Identity Management	SAP Access Control	SAP Single Sign-On

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

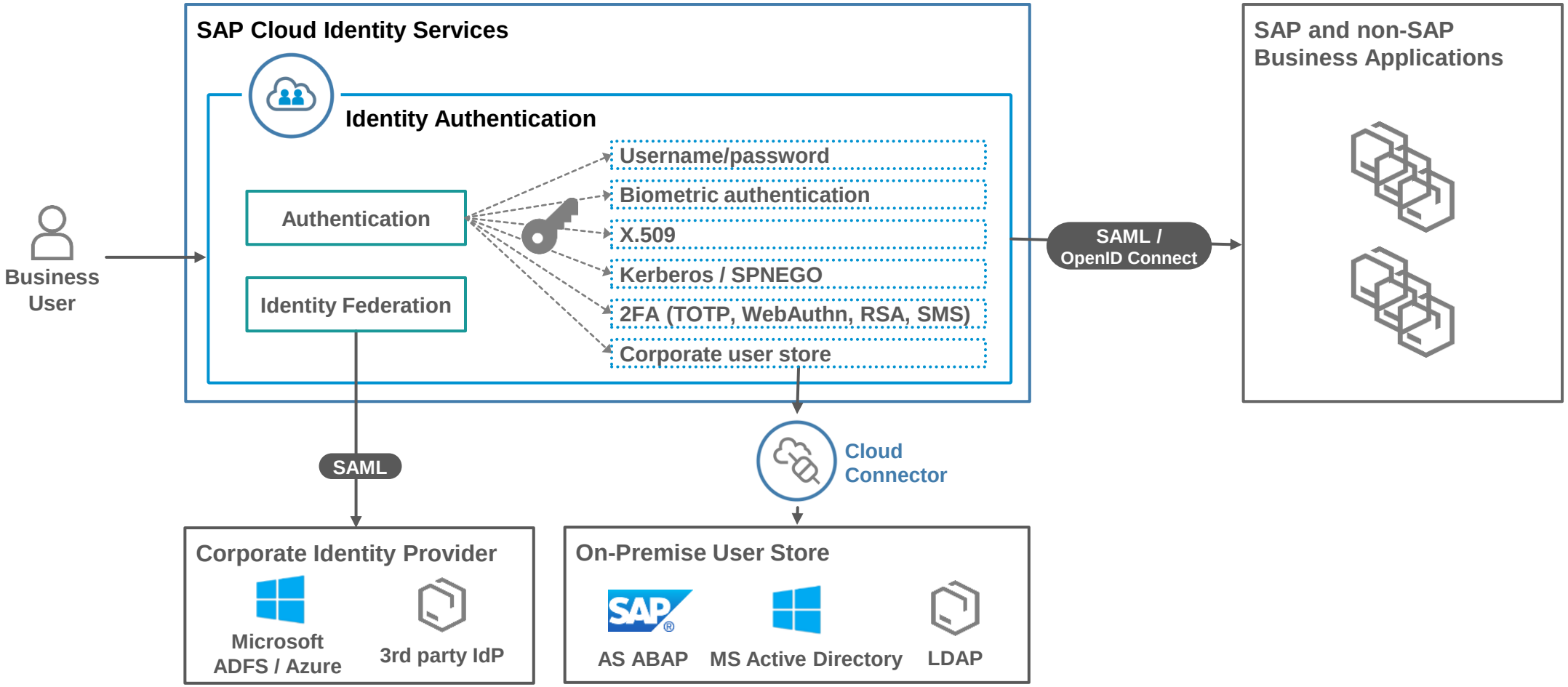
SAP Cloud Identity Services - Identity Authentication enables single sign-on for SAP’s cloud-based business applications, with two usage options

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

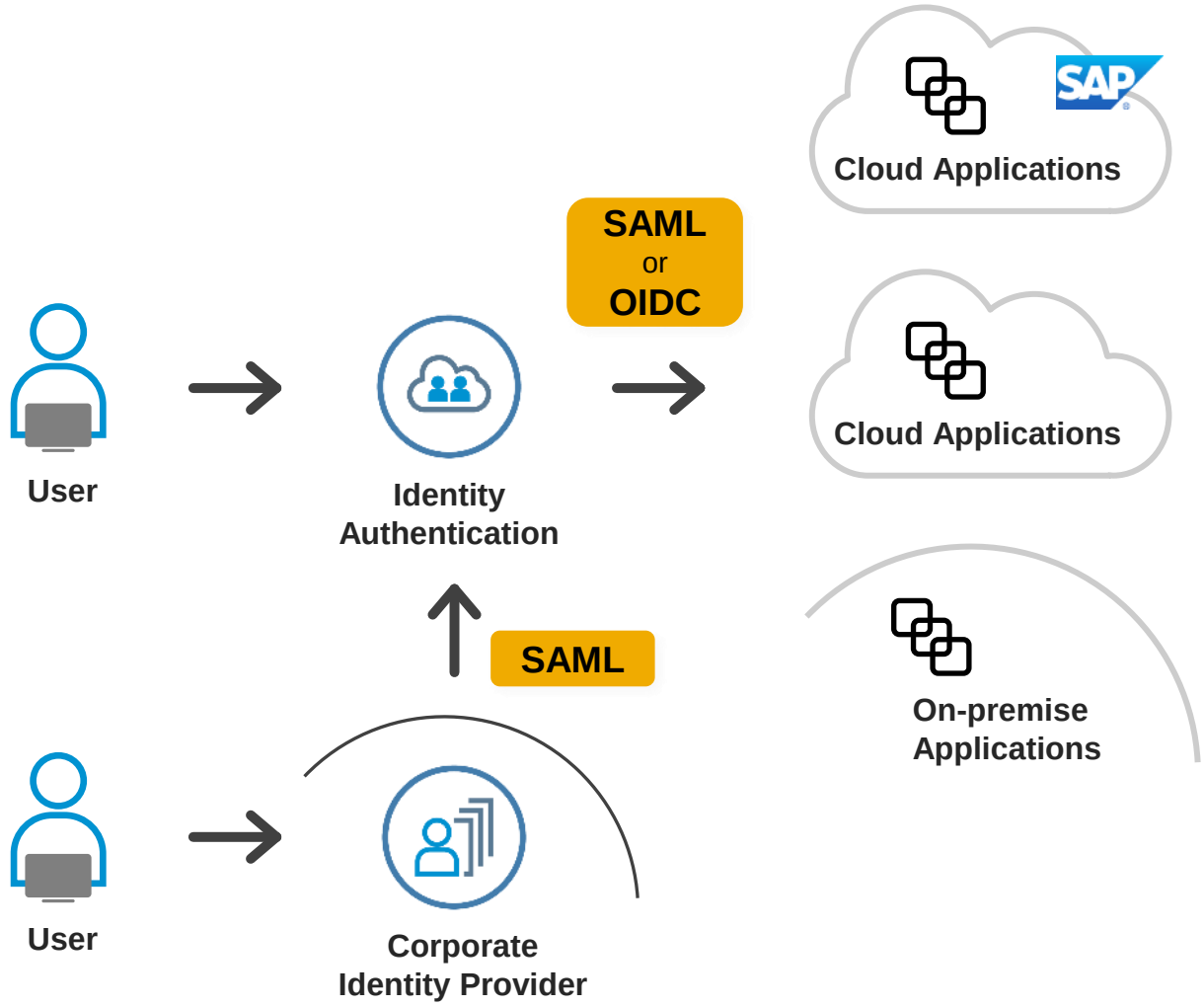


Based on open security standards

Interoperable

with all applications supporting SAML* 2.0 standard

or OpenID Connect (OIDC)



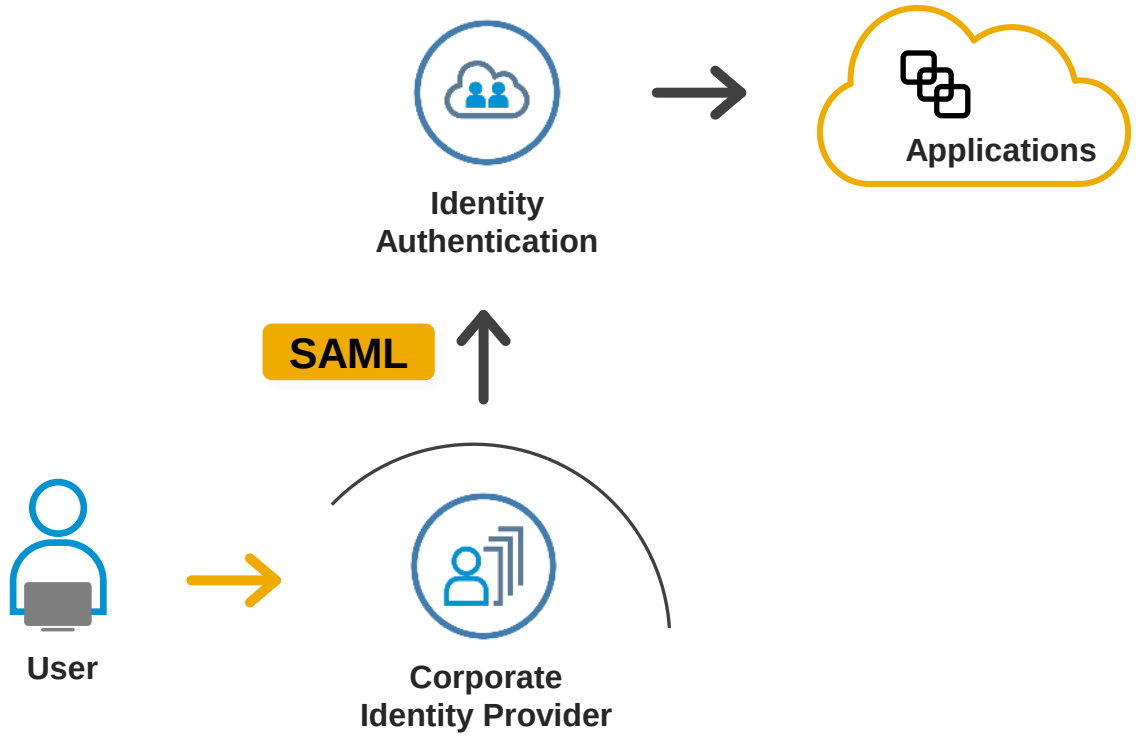
*SAML = Security Assertion Markup Language

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

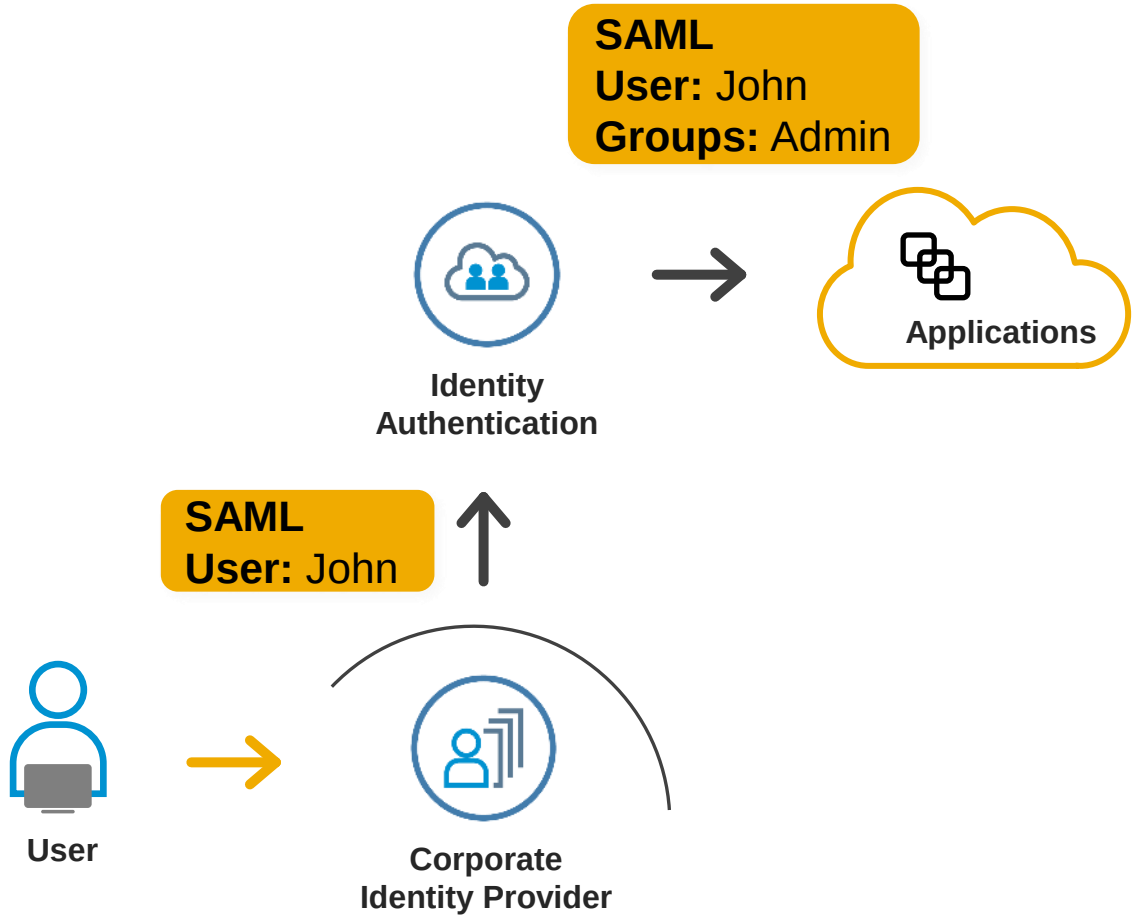


Delegated authentication

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

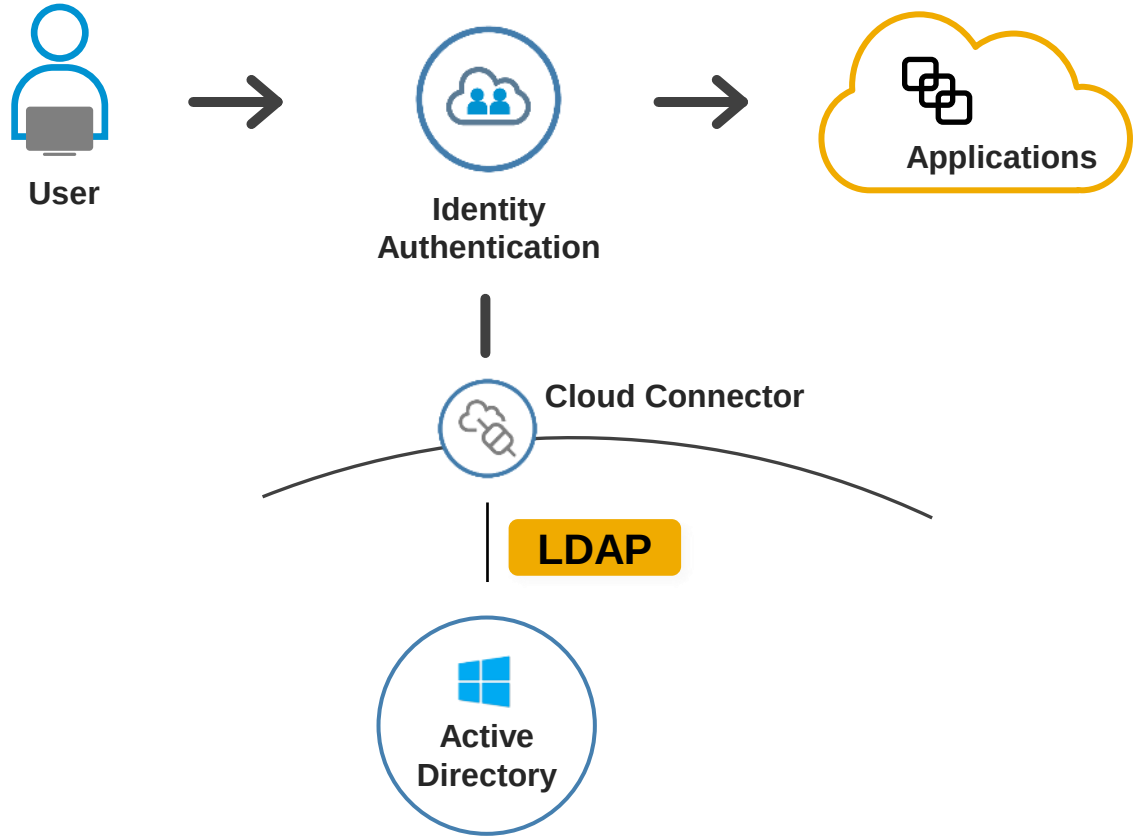


Delegated authentication

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



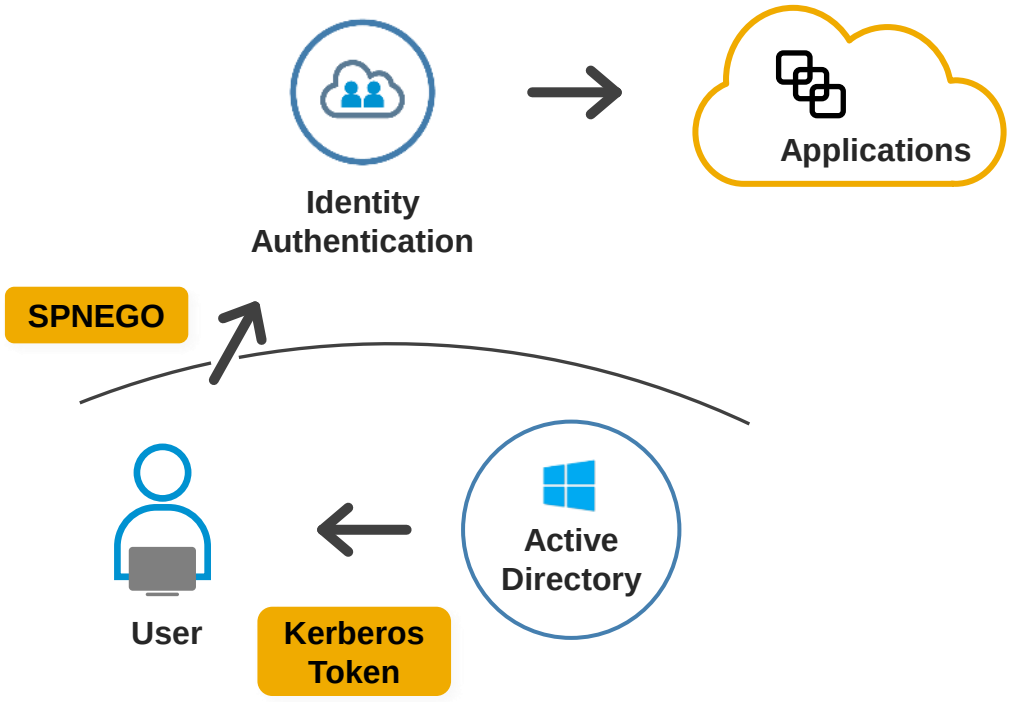
* requires AS Java + SAP Single Sign-On (which enables SCIM interface)

Delegated authentication

Re-use of Windows Domain Authentication (SPNEGO)

SPNEGO* authentication

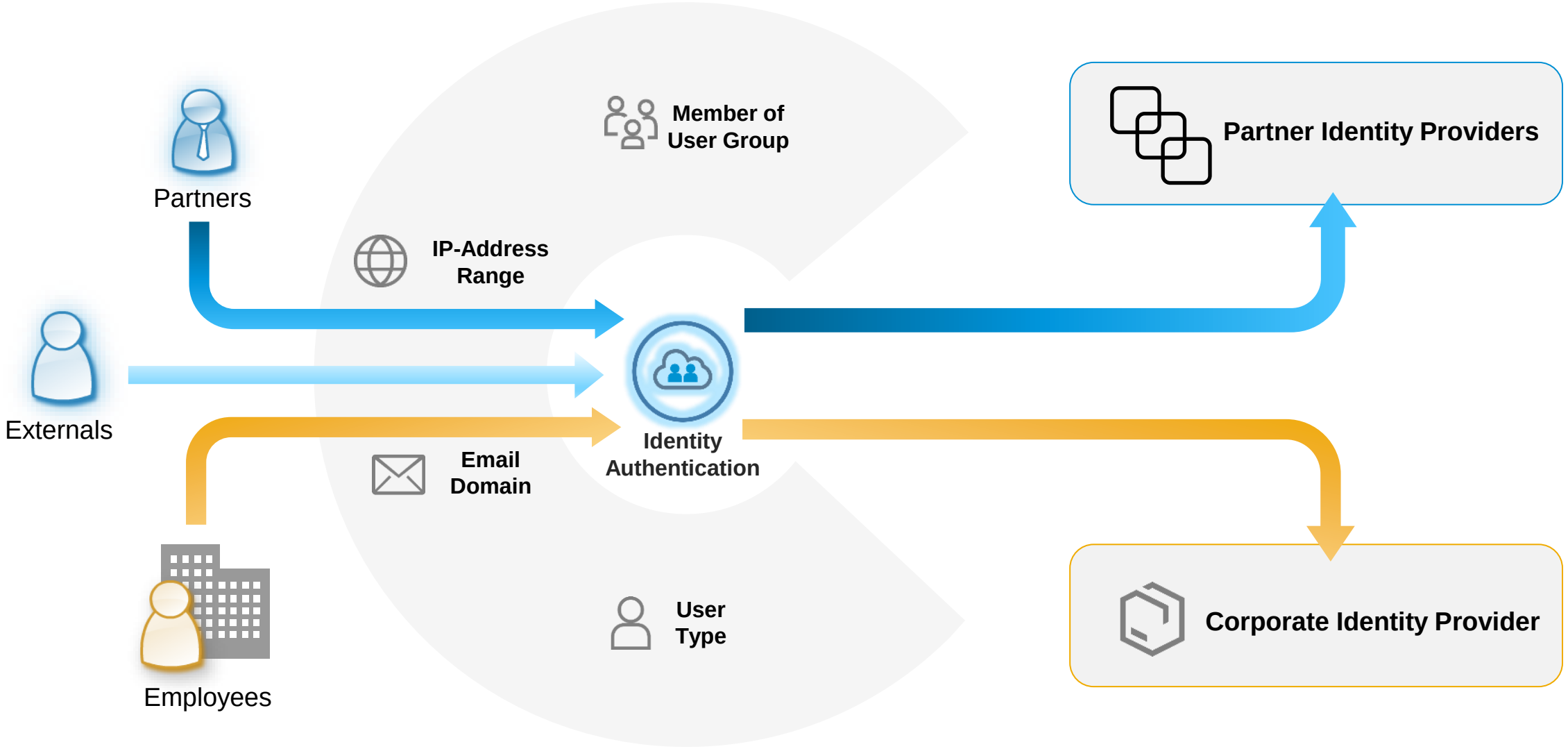
- Users authenticated with Microsoft Active Directory enjoy single sign-on to cloud applications without re-authentication
- Reuse of existing corporate identity infrastructure
- Secure authentication and SSO for cloud and on-premise web applications



*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

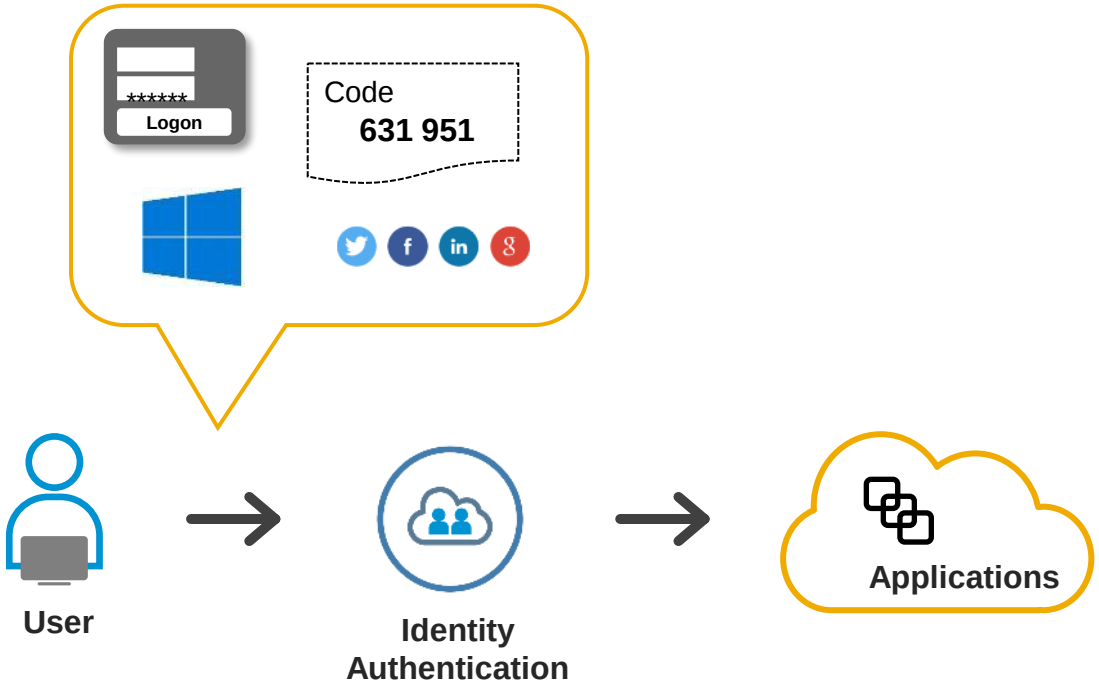
- Use of Kerberos token for single sign-on

Two-factor authentication

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

Delegated logon

- Social IdPs
- Corporate IdP

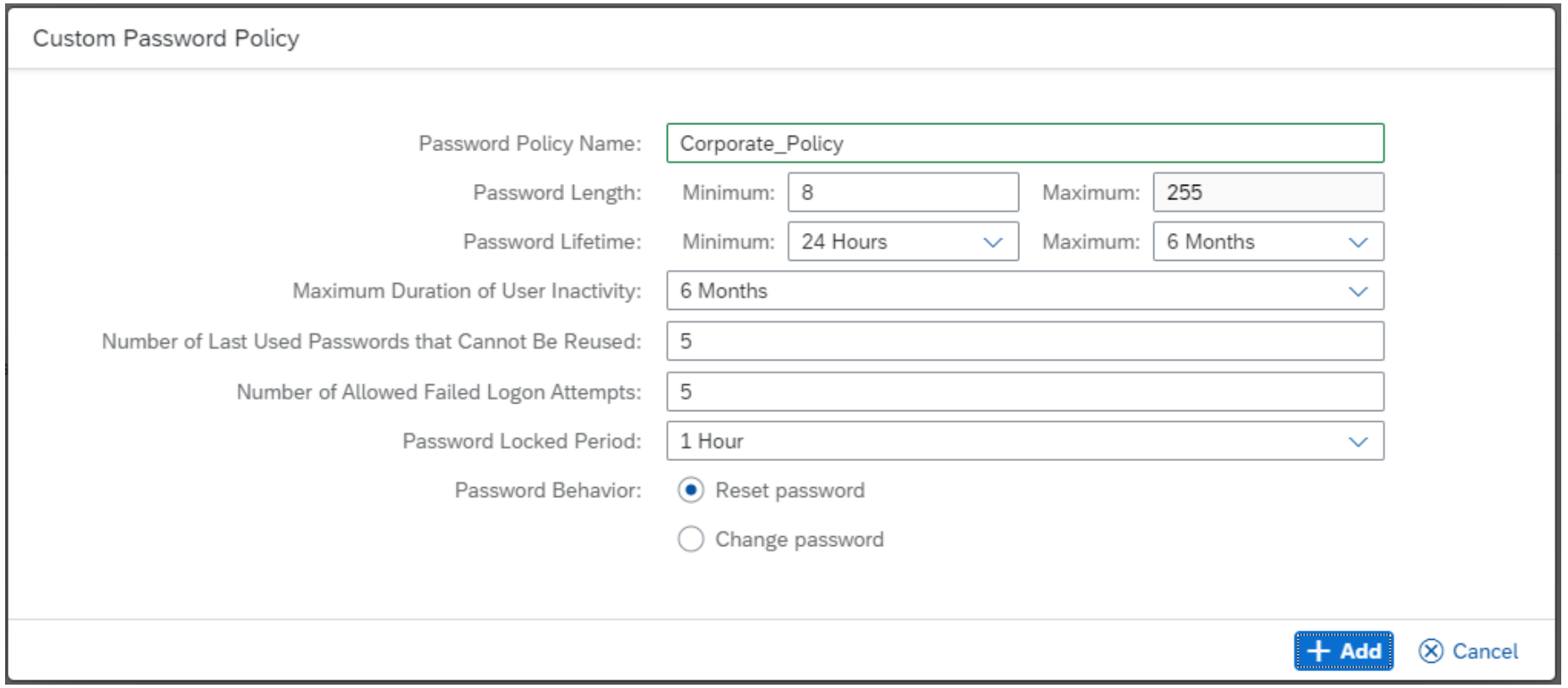


*Radius support enabled upon request

**SMS requires the license of Sinch Authentication 365

Custom password policies

Administrator can configure custom password policies:



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)

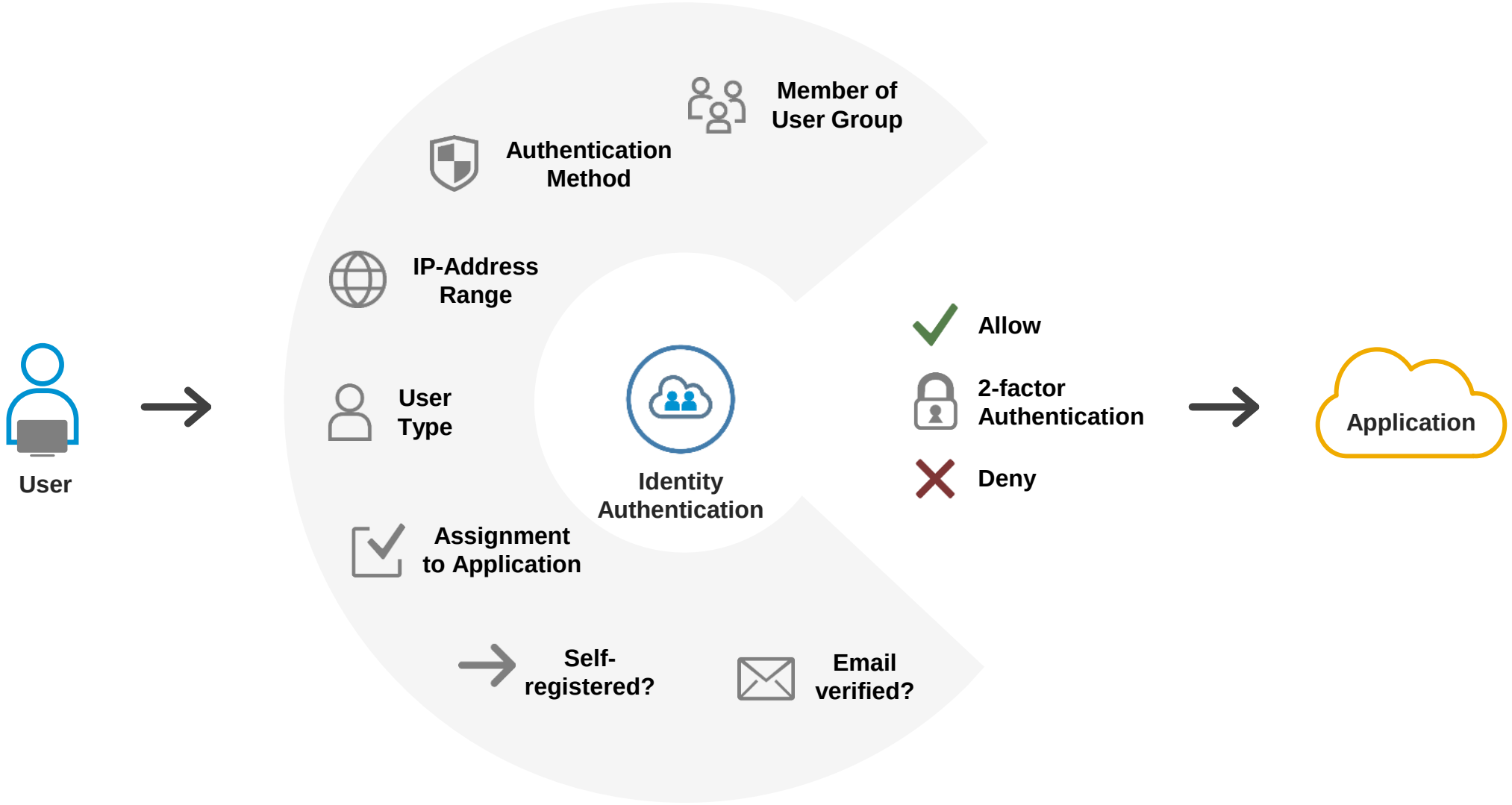
OTP via SMS

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

OTP via RADIUS

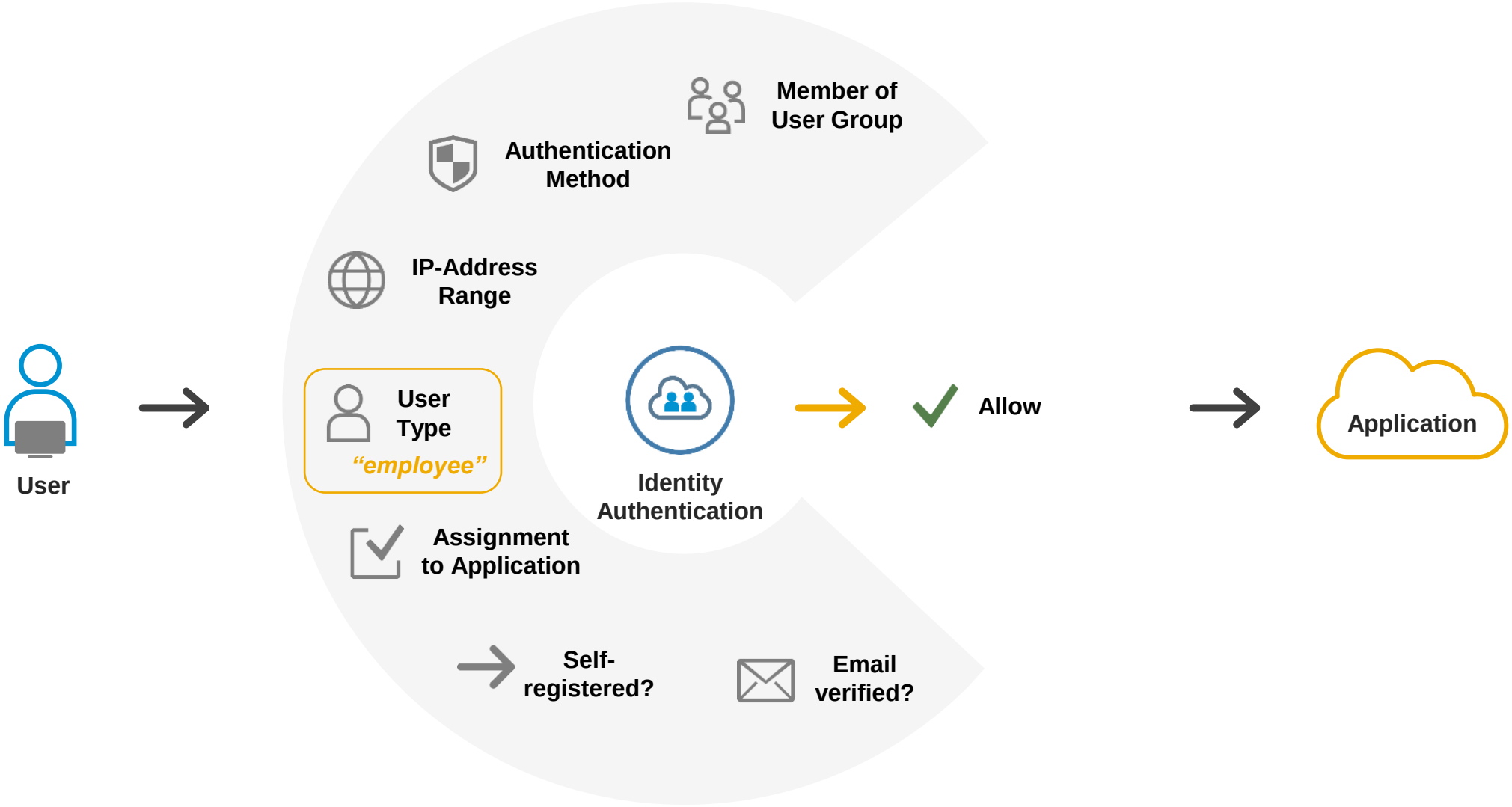
- RADIUS client app to request OTP code
- Code generated by RADIUS server
- Activation upon request

Control access to the application – risk-based authentication

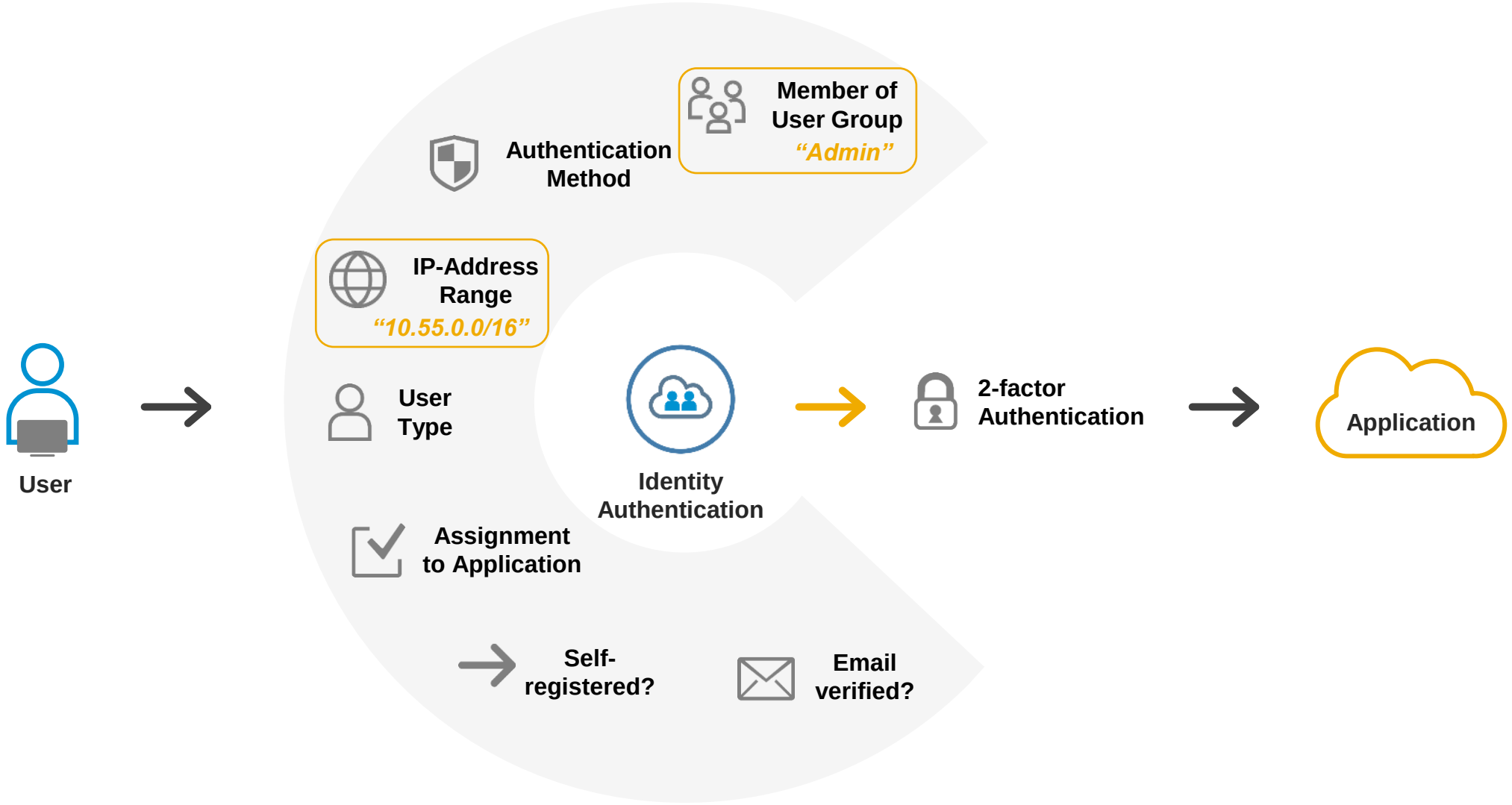


Supports both local authentication and IdP proxy

Control access to the application



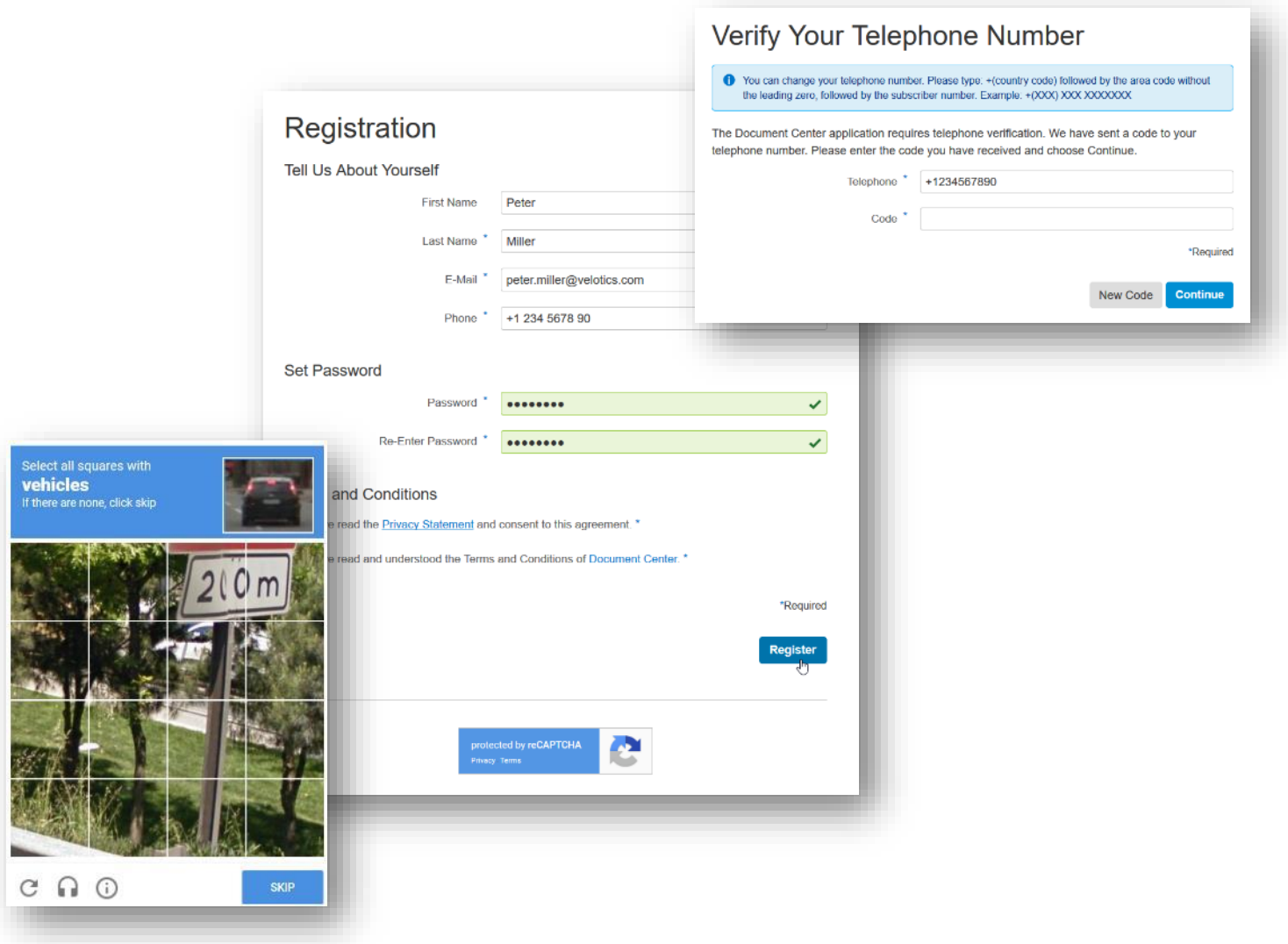
Control access to the application



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



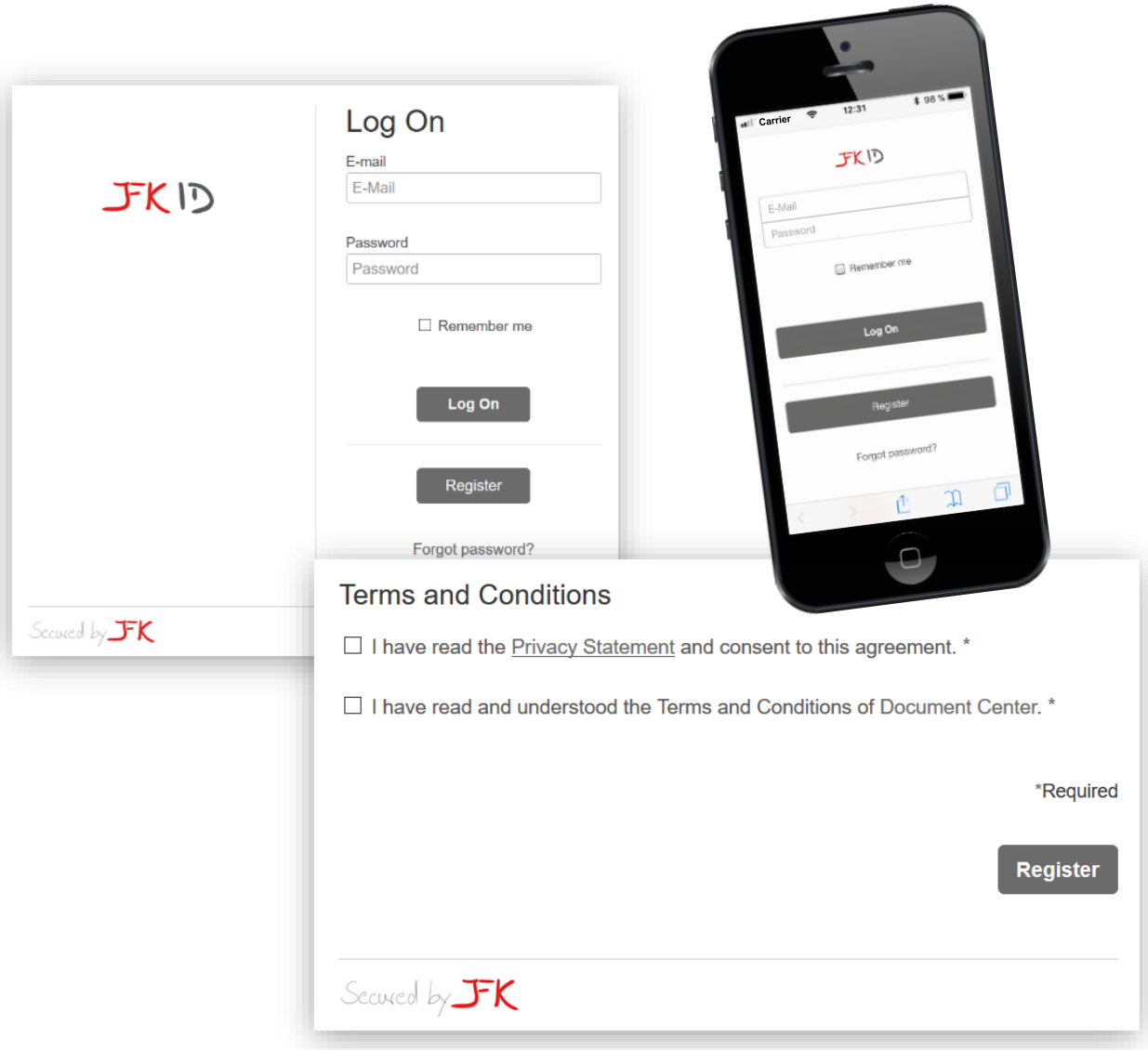
Branding and customization

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

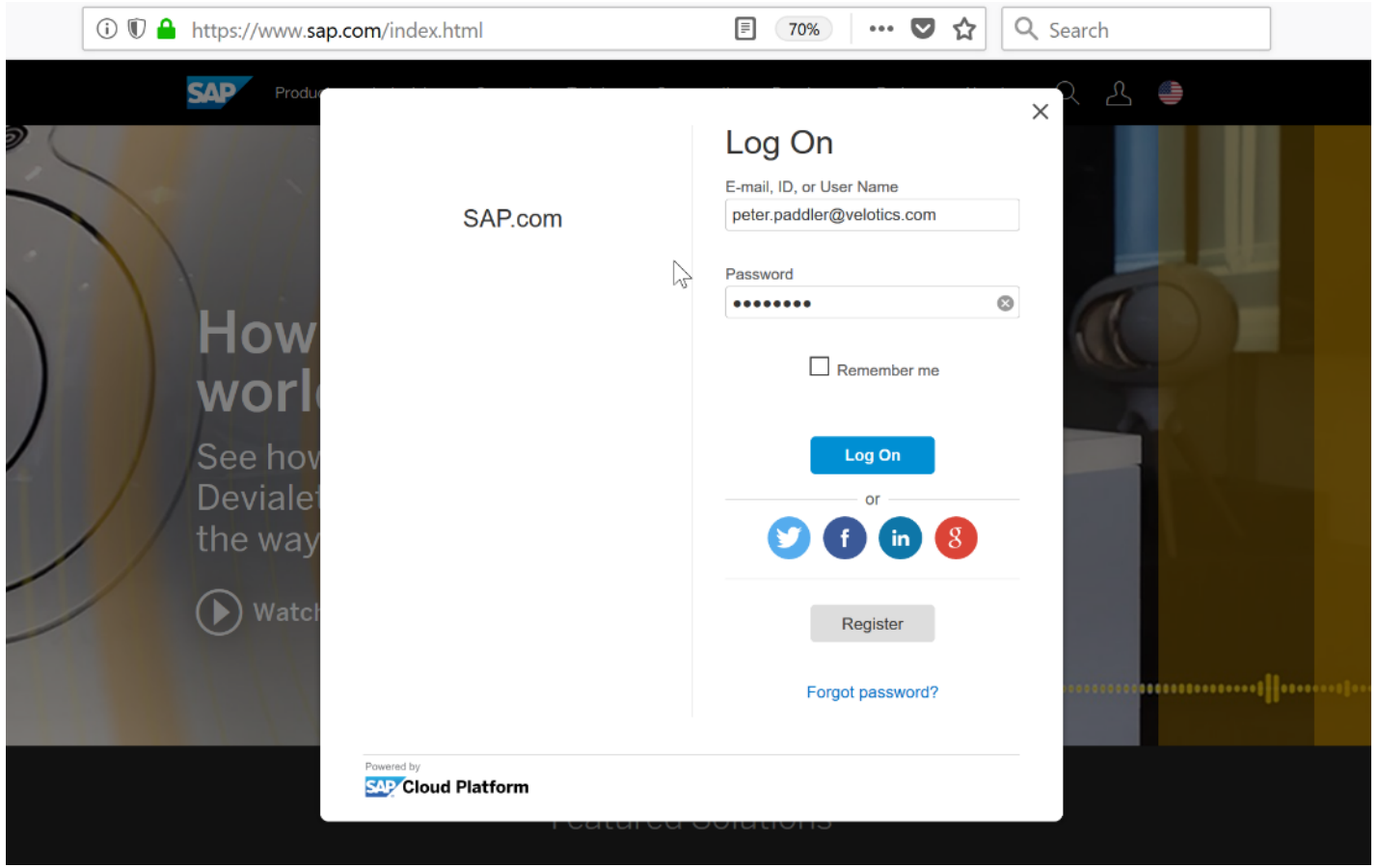
- Responsive UIs
- Multi-language support



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?

Self-registration

Sync through IPS*

CSV-upload

Manual creation

Programmatically through SCIM

* IPS: SAP Cloud Identity Services - Identity Provisioning

User & group management

User administration

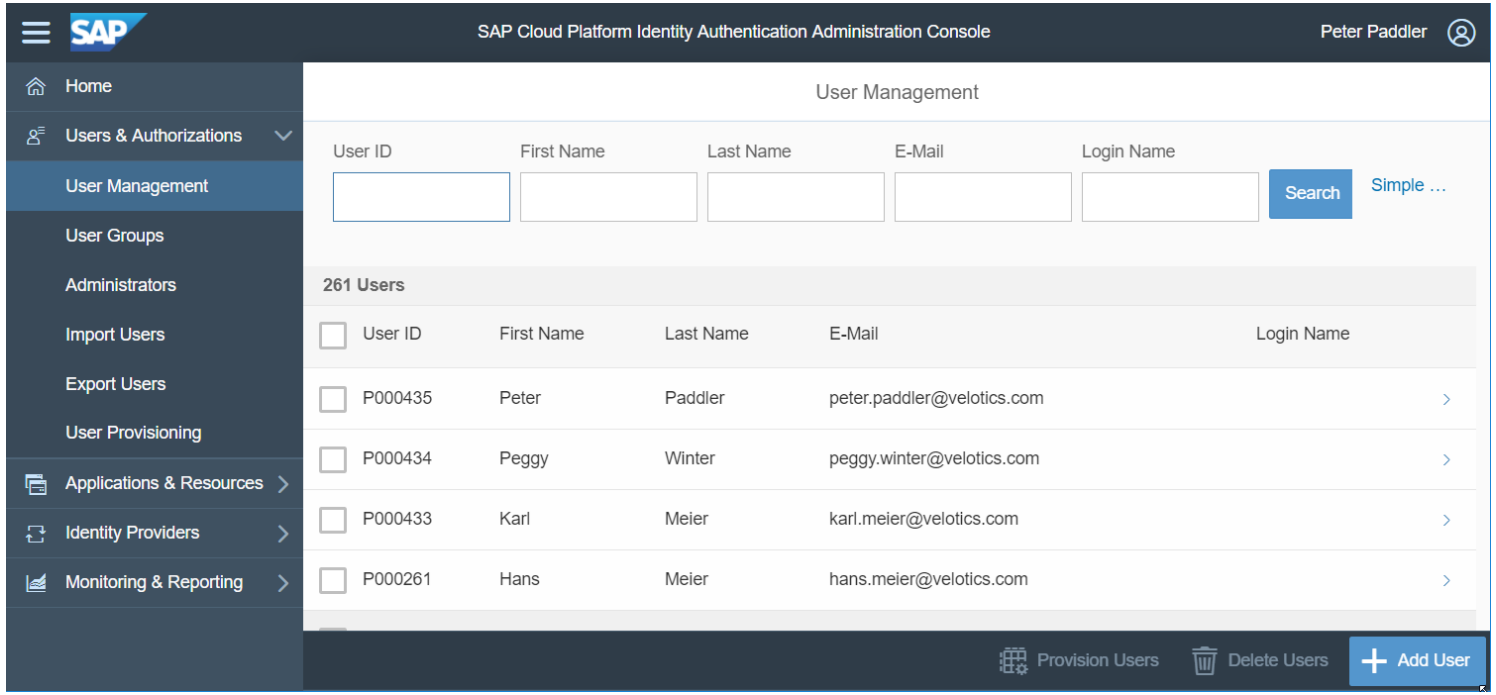
- Web based user management
- User search
- Mass user import/export
- Monitor user access

User groups administration

- Define user groups
- Assign users to groups

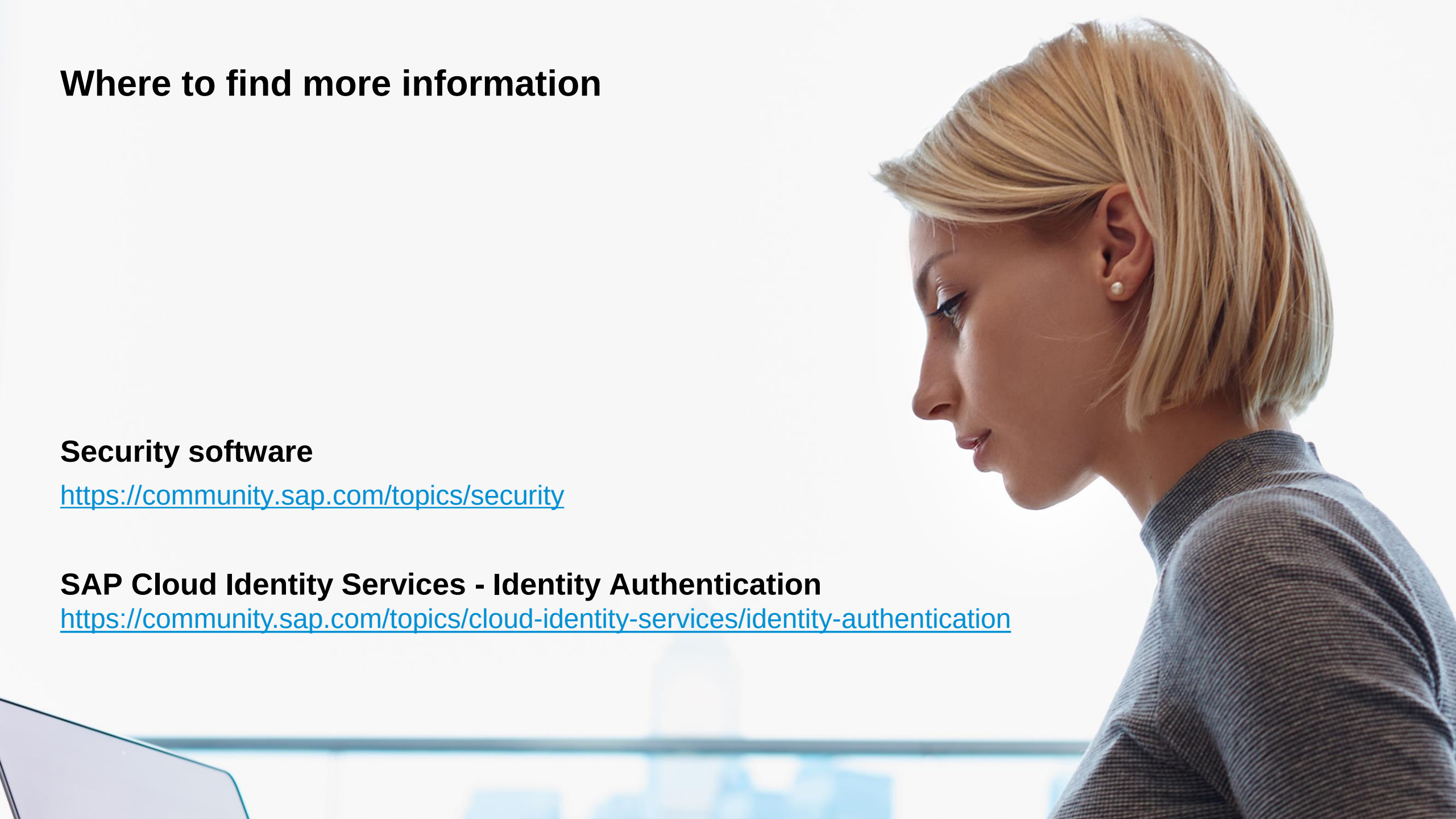
Integration

- Programmatic integration via SCIM REST APIs



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.

IAM - Identity Access Management
CIAM - Customer Identity Access Management

Product strategy for IAM & CIAM

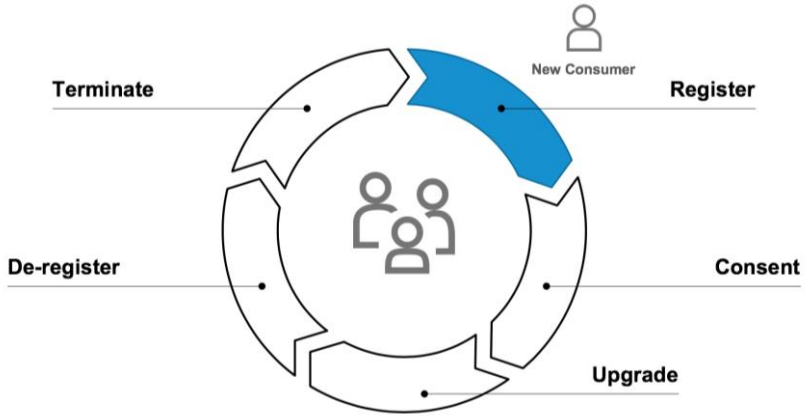
Focus areas

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’)



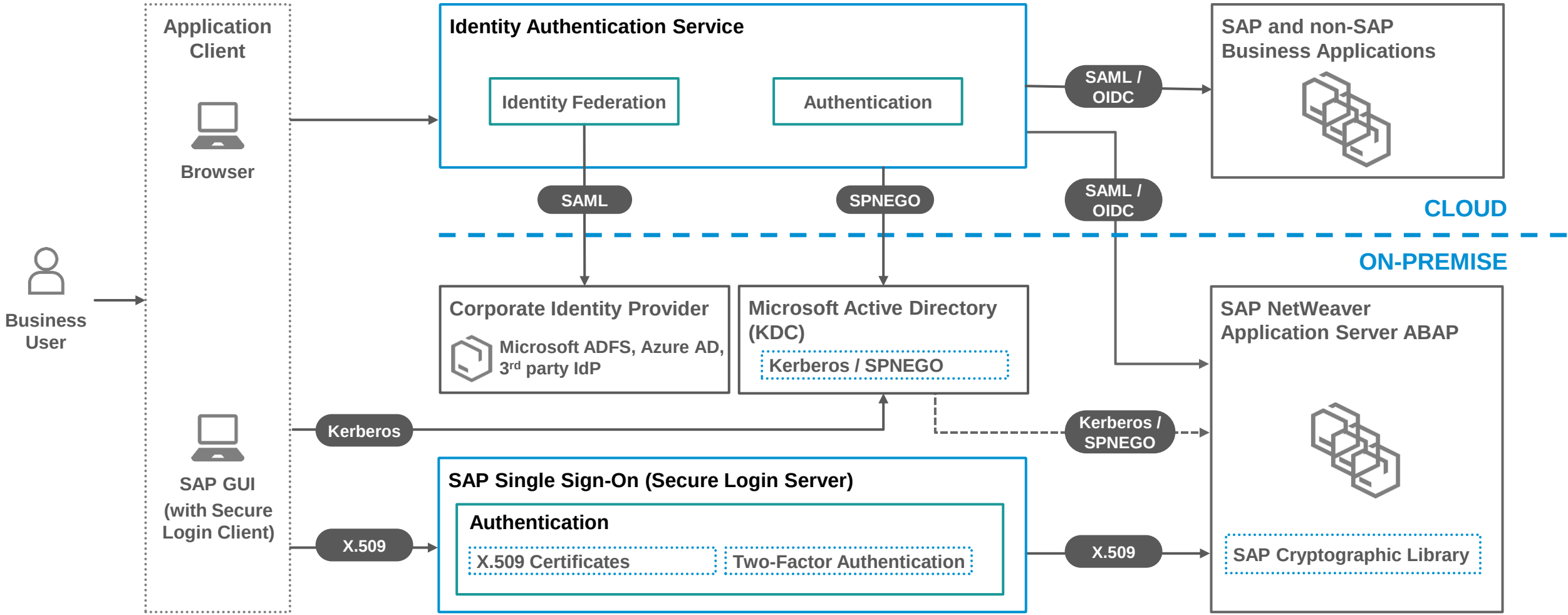
Secure authentication and single sign-on

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
SAP Single Sign-On	• Kerberos/ SPNEGO • X.509 certificates • SAML	• Browser • Desktop clients	• Employee	• Risk-based authentication • Digital signatures • Certificate lifecycle management	• On-premise • Some capabilities require SAP AS Java • Some capabilities require a desktop client
SAP Cloud Identity Services - Identity Authentication	• SAML • SPNEGO • X.509 certificates • Social IdP	• Browser	• Employee • Partner	• Self-registration • User management • Branding • Risk-based authentication	• Cloud subscription • Run by SAP • Zero footprint on desktop

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

Follow us

www.sap.com/contactsap

THE BEST RUN SAP®

SAP folgen auf

www.sap.com/germany/contactsap

THE BEST RUN SAP®