SAP Cloud Identity Services

Discovery Center Mission Overview

December 2023

PUBLIC

About the speaker

Nagesh Caparthy

SAP BTP Onboarding Senior Advisor

Nagesh has 15 years of SAP Experience on multiple topics. He is passionate about customer success and believes the fundamental first step to ensuring that is a successful onboarding.

SAP BTP Onboarding Center | Why and How

Why?

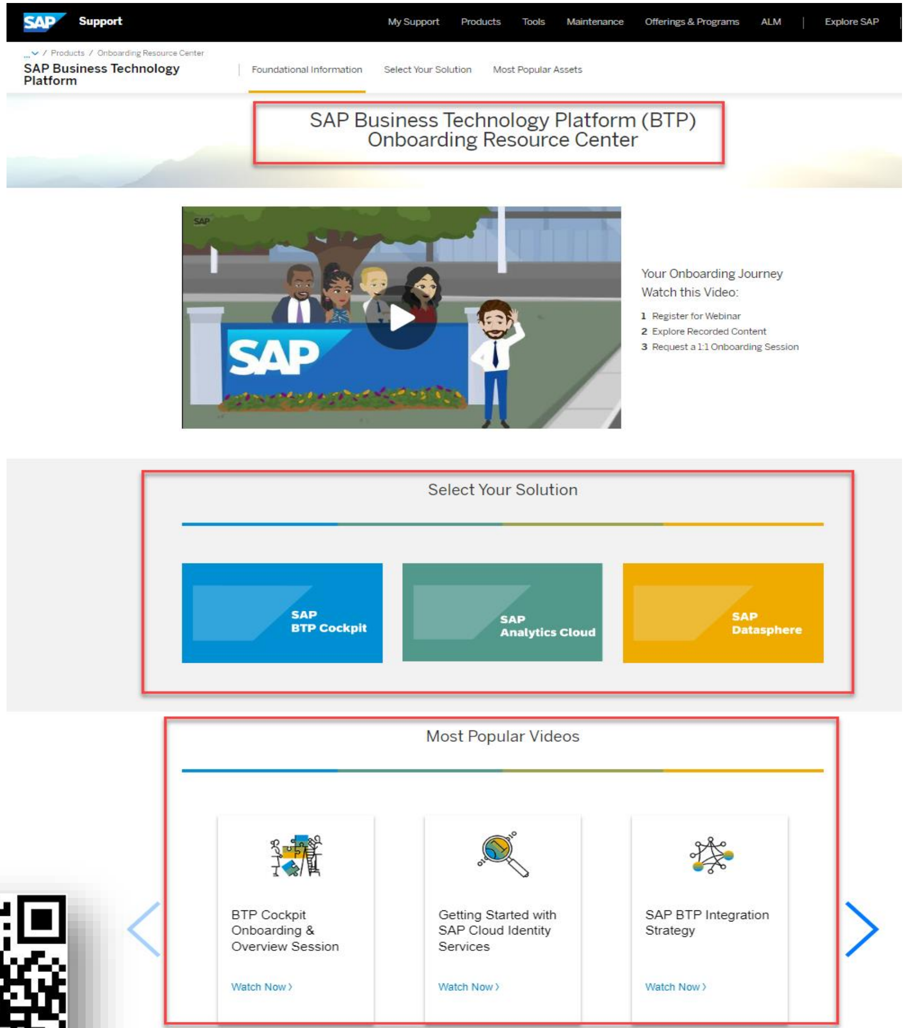
The SAP BTP Onboarding Center understands that getting started on the right path is fundamental to a successful implementation. Our focus as your SAP BTP Onboarding Advisor is to help you by:

- Obtaining access to your services
- Empowering you with proper governance and structure
- Highlighting best practices and things to consider
- Providing helpful assets and resources for self-service guidance

How?

By offering live and on-demand **webinars** to give you the initial overview and demo of your solution and by offering **1:1 engagements** by appointment request**,** where we can focus on your specific use case.

Getting in touch with us is easy! Scan our QR code or contact us while also exploring the various self-help resources we've created and loaded to the [BTP Onboarding Resource Center.](BTP Onboarding Resource Center)



SAP Business Technology Platform (BTP) Onboarding Resource Center

Your Onboarding Journey
Watch this Video:

1 Register for Webinar
2 Explore Recorded Content
3 Request a 1:1 Onboarding Session

Select Your Solution

Most Popular Videos

BTP Cockpit Onboarding & Overview Session

Getting Started with SAP Cloud Identity Services

SAP BTP Integration Strategy

Single Slide Included in BTP L0 & L1

Agenda

Introduction

BTP - Application layer security

SAP Cloud Identity Services - Identity Authentication

SAP Cloud Identity Services - Identity Provisioning

SAP Global User ID – Concept & Implementation

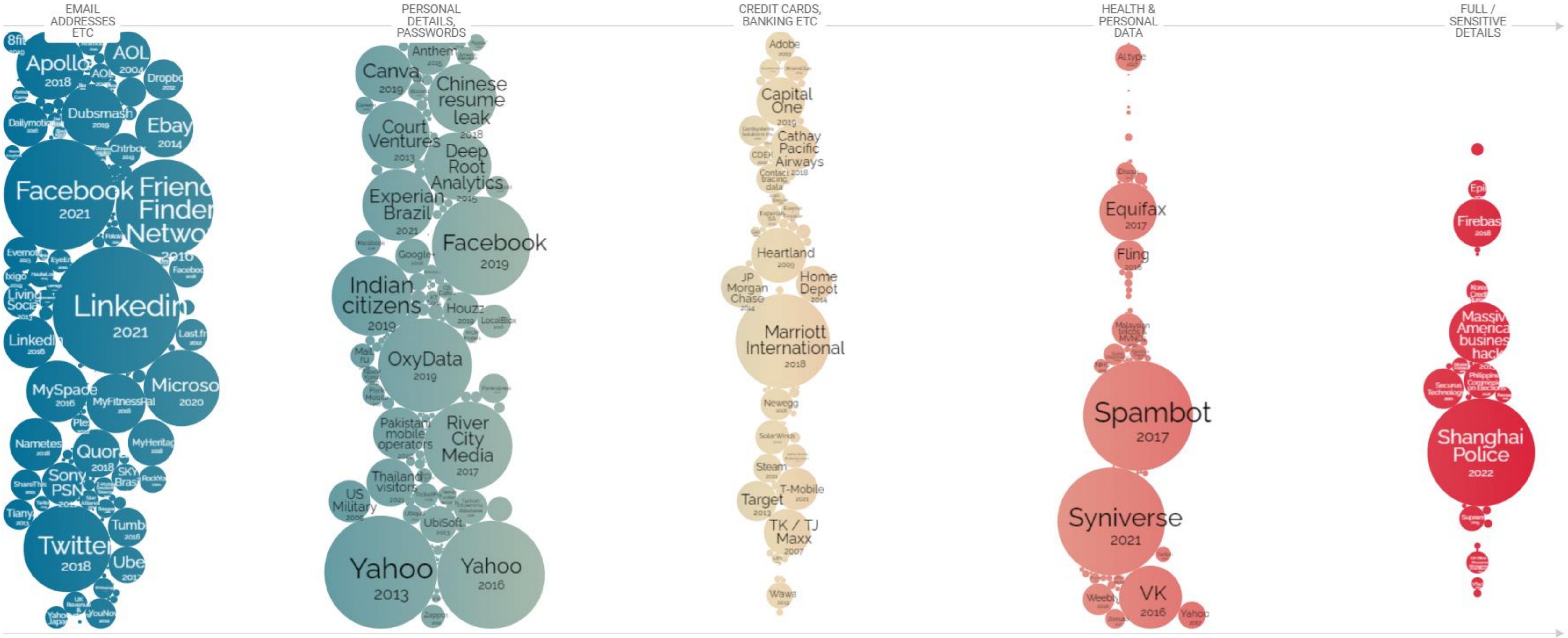
Roadmap

Further information

Appendix

You know the challenge – breaches are increasing

World’s largest data breaches and hacks



Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
Source: https://www.ibm.com/reports/data-breach

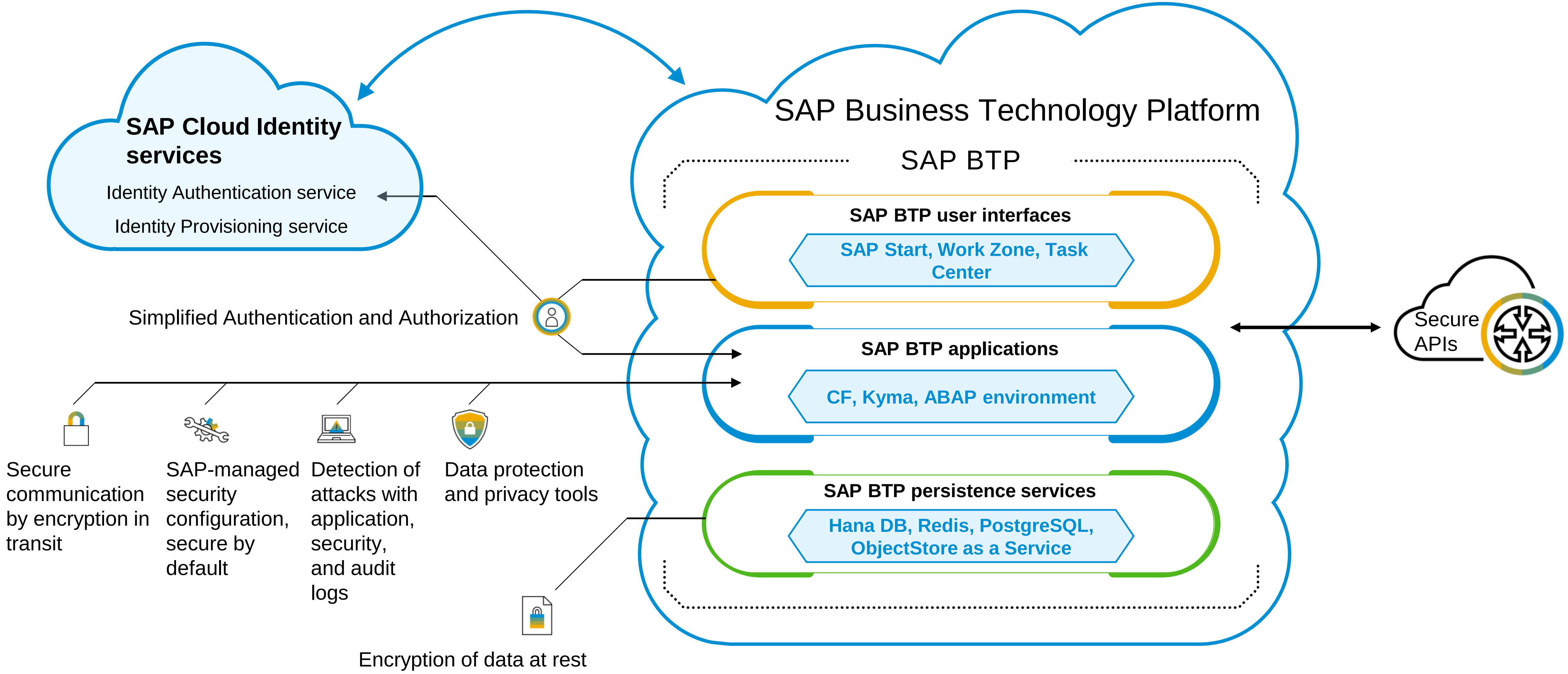
Security Operations Map

Organization	Awareness	Security Governance	Risk Management	
Process	Regulatory Process Compliance	Data Privacy & Protection	Audit & Fraud Management	
Application	User & Identity Management	Authentication & Single Sign-On	Roles & Authorizations	Custom Code Security
System	Security Hardening	Secure SAP Code	Security Monitoring & Forensics	
Environment	Network Security	Operating System & Database Security	Client Security	

SAP BTP - Application layer security

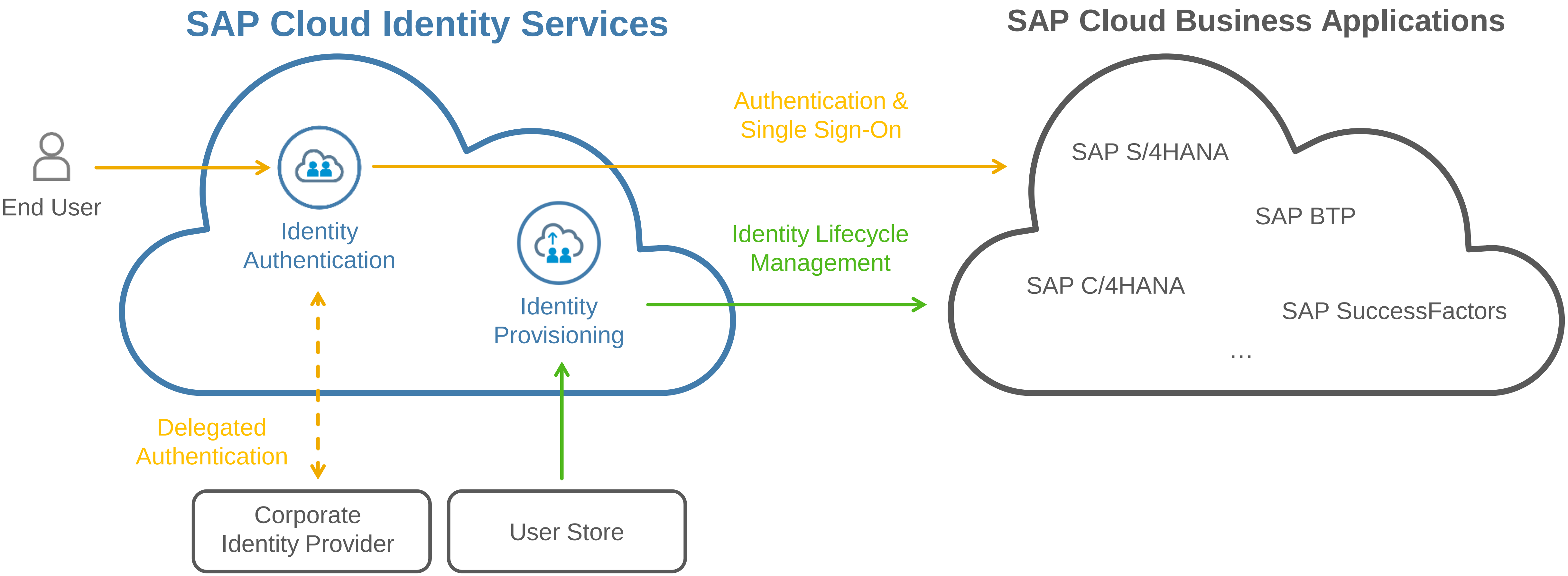
Build securely

Security solutions and features


SAP Cloud Identity services
Identity Authentication service
Identity Provisioning service
Simplified Authentication and Authorization
SAP Business Technology Platform
SAP BTP
SAP BTP user interfaces
SAP Start, Work Zone, Task Center
SAP BTP applications
CF, Kyma, ABAP environment
SAP BTP persistence services
Hana DB, Redis, PostgreSQL, ObjectStore as a Service
Secure APIs
Secure communication by encryption in transit
SAP-managed security configuration, secure by default
Detection of attacks with application, security, and audit logs
Data protection and privacy tools
Encryption of data at rest

SAP Cloud Identity Services

Overview


SAP Cloud Identity Services
SAP Cloud Business Applications
End User
Identity Authentication
Identity Provisioning
Authentication & Single Sign-On
Identity Lifecycle Management
Delegated Authentication
Corporate Identity Provider
User Store
SAP S/4HANA
SAP BTP
SAP C/4HANA
SAP SuccessFactors
…

SAP Cloud Identity Services

Identity Authentication

SAP Cloud Identity Services - Identity Authentication

Identity provider for SAP’s cloud-based business applications

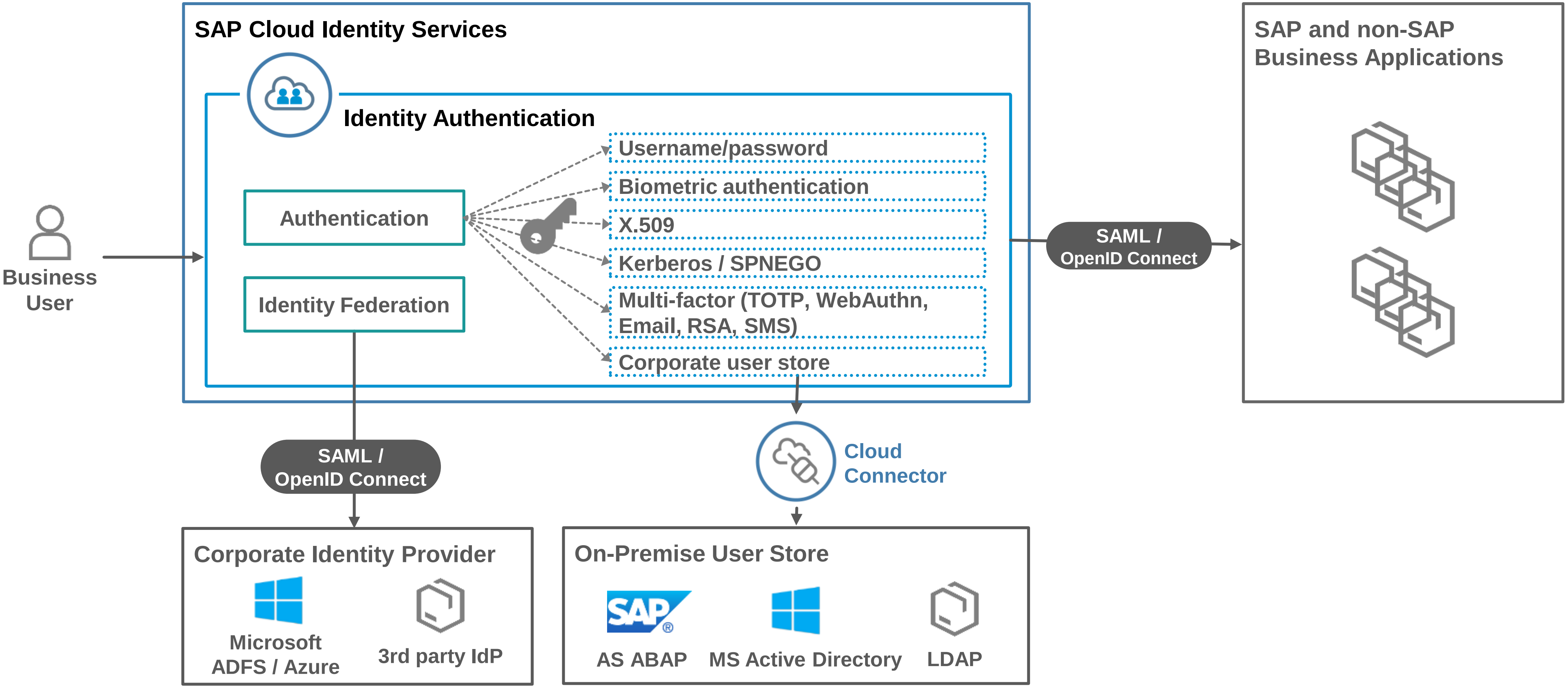
SAP Cloud Identity Services - Identity Authentication enables single sign-on for SAP’s cloud-based business applications, with two usage options

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

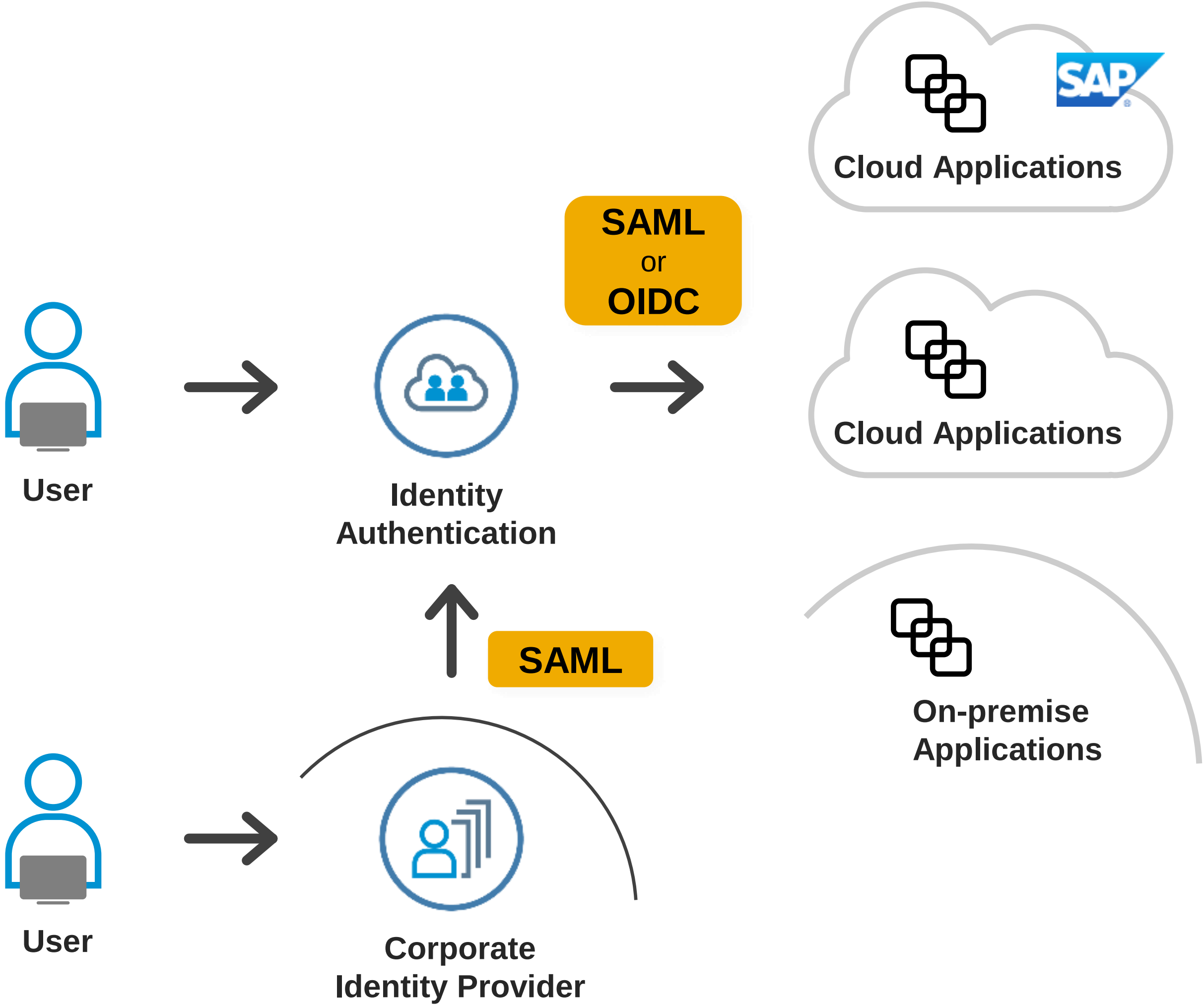


Based on open security standards

Interoperable

with all applications supporting SAML* 2.0 standard

or OpenID Connect (OIDC)



*SAML = Security Assertion Markup Language

OpenID Connect Authentication

What is OpenID Connect (OIDC)?

“OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.” (https://openid.net/connect/)

How are OIDC and SAML connected ?

“*The Security Assertion Markup Language (SAML) is an XML-based federation technology used in some enterprise and academic use cases.*

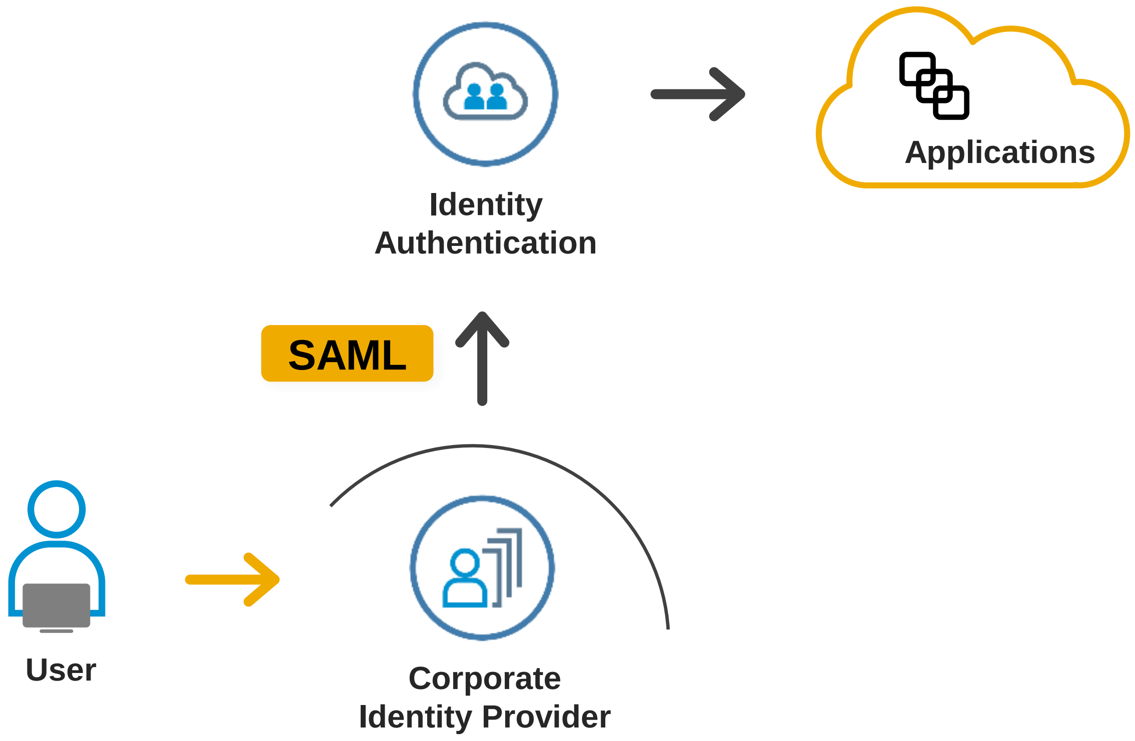
OpenID Connect can satisfy these same use cases but with a simpler, JSON/REST based protocol. OpenID Connect was designed to also support native apps and mobile applications, whereas SAML was designed only for Web-based applications. ” (https://openid.net/connect/faq/)

Delegated authentication

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

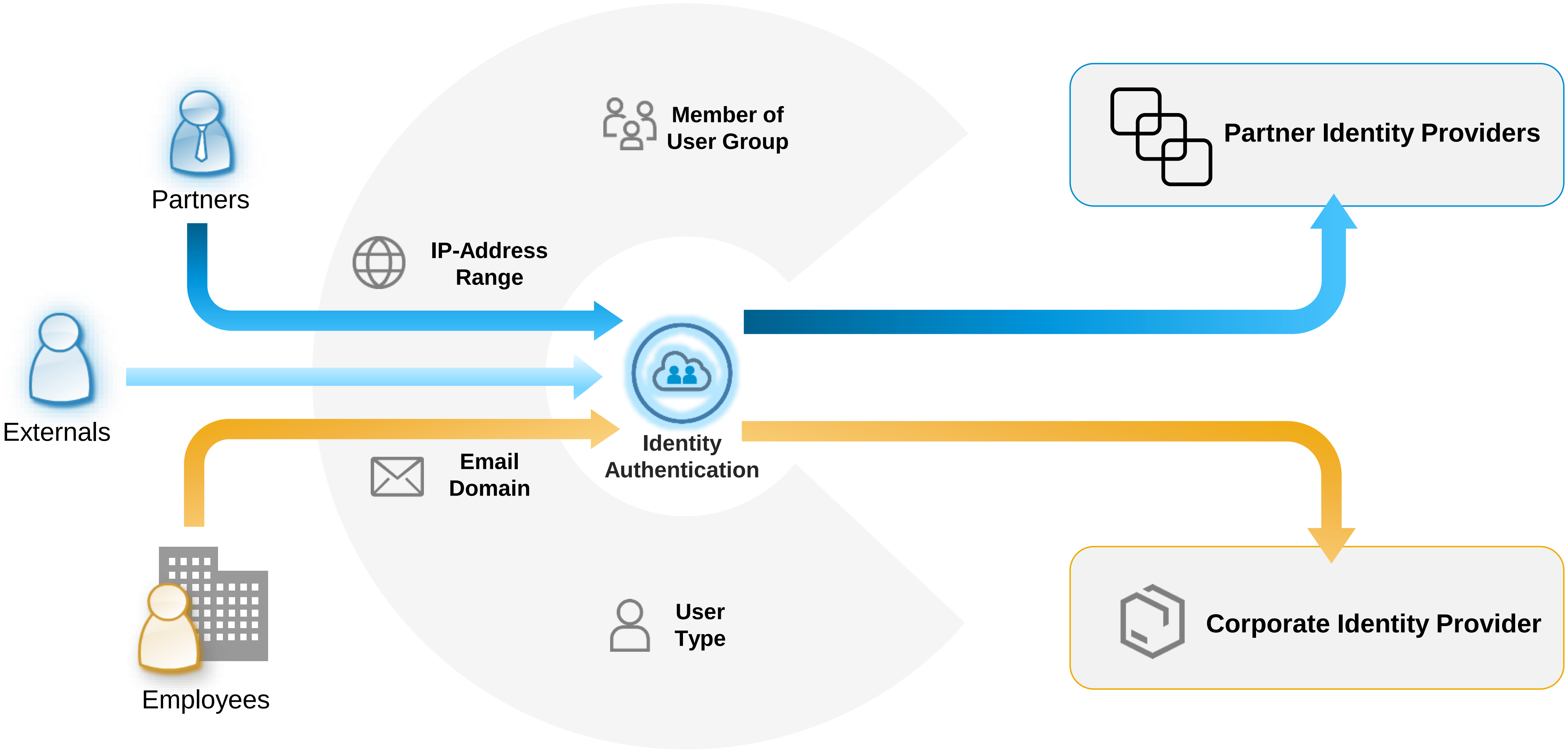
Identity provider proxy

- 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 towards multiple identity providers

Conditional authentication



Partners

Externals

Employees

Member of User Group

IP-Address Range

Email Domain

User Type

Identity Authentication

Partner Identity Providers

Corporate Identity Provider

SAP Cloud Identity Services - Identity Authentication

Value proposition 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

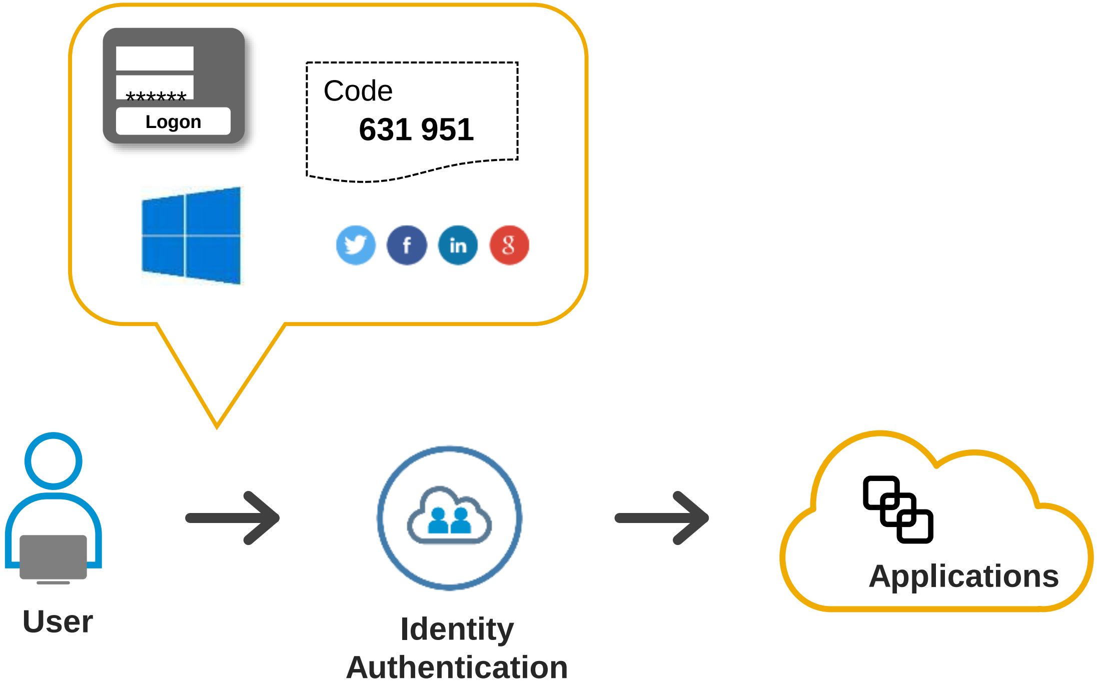
- Use of Kerberos token for single sign-on

Two-factor authentication

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

Delegated logon

- Social IdPs
- Corporate IdP

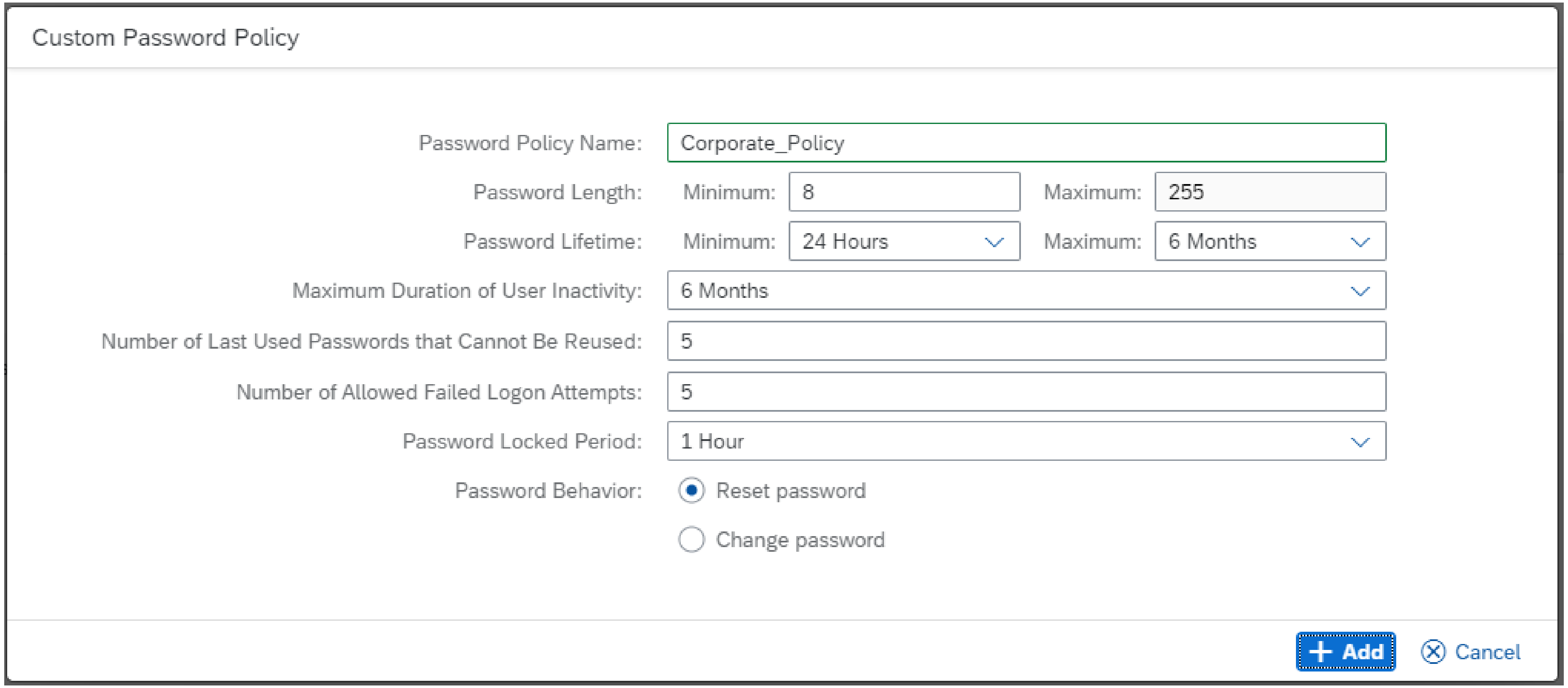


*Radius support enabled upon request

**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			

Multi-factor authentication options

Authentication methods for second factor:

- Web authentication with a FIDO2(Fast IDentity Online) 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)

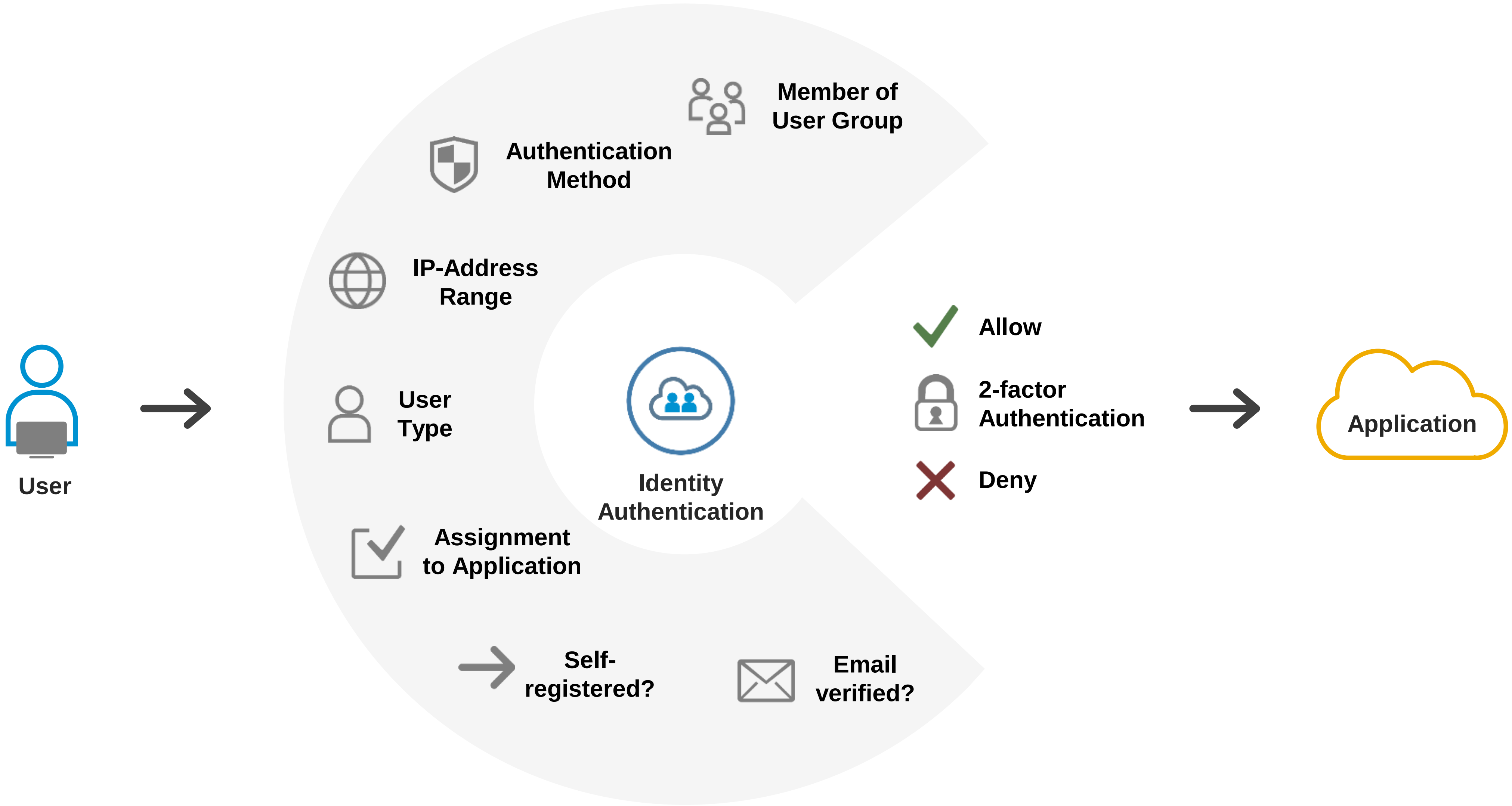
OTP via SMS

- 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

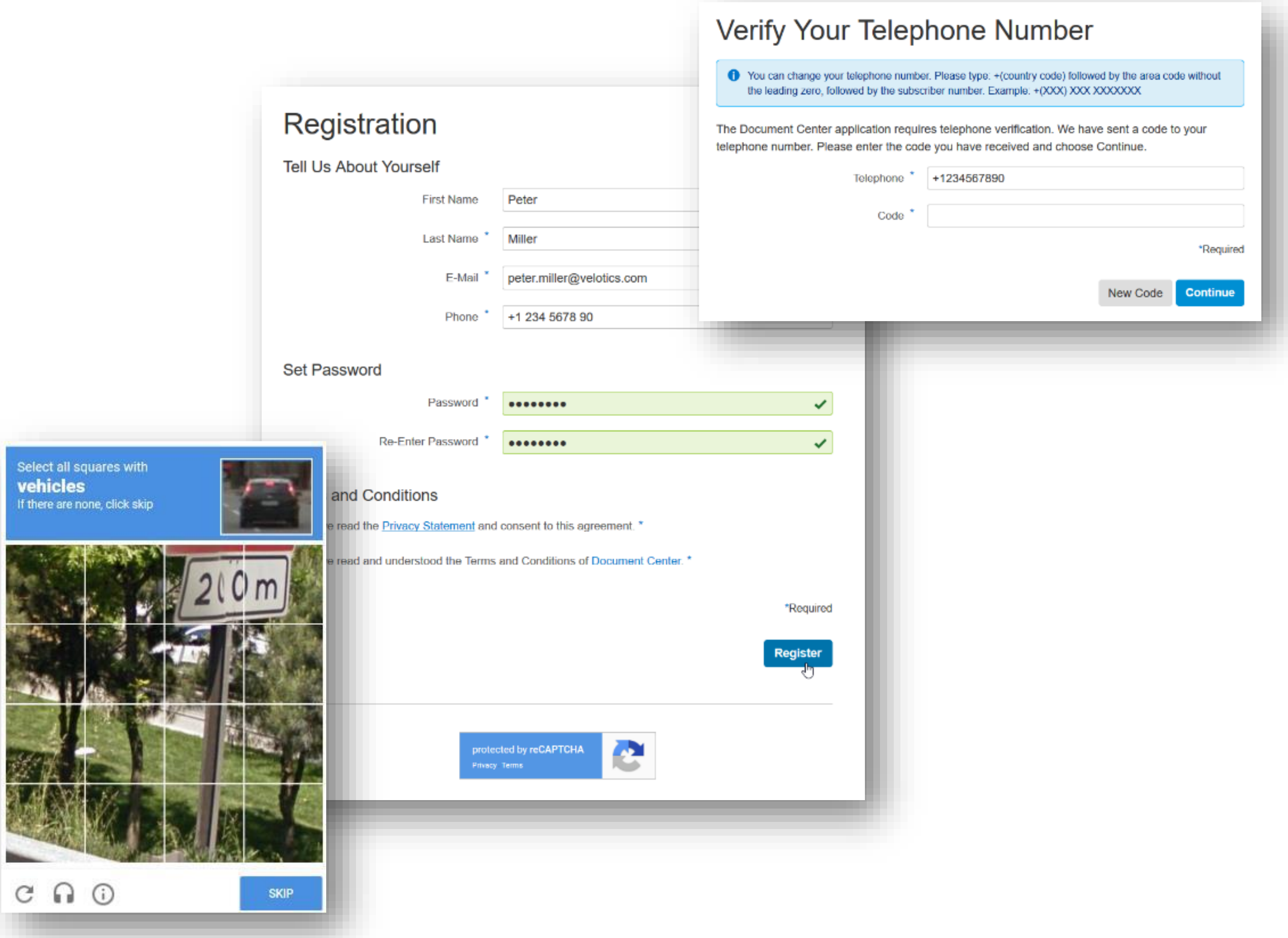


Supports both local authentication and IdP proxy

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]



Registration

Tell Us About Yourself

First Name	Peter
Last Name *	Miller
E-Mail *	peter.miller@velotics.com
Phone *	+1 234 5678 90

Set Password

Password *	•••••••• ✓
Re-Enter Password *	•••••••• ✓

and Conditions

e read the Privacy Statement and consent to this agreement. *

e read and understood the Terms and Conditions of Document Center. *

*Required

Verify Your Telephone Number

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 XXXXXXX

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.

Telephone *	+1234567890
Code *	

*Required

Select all squares with **vehicles**

If there are none, click skip

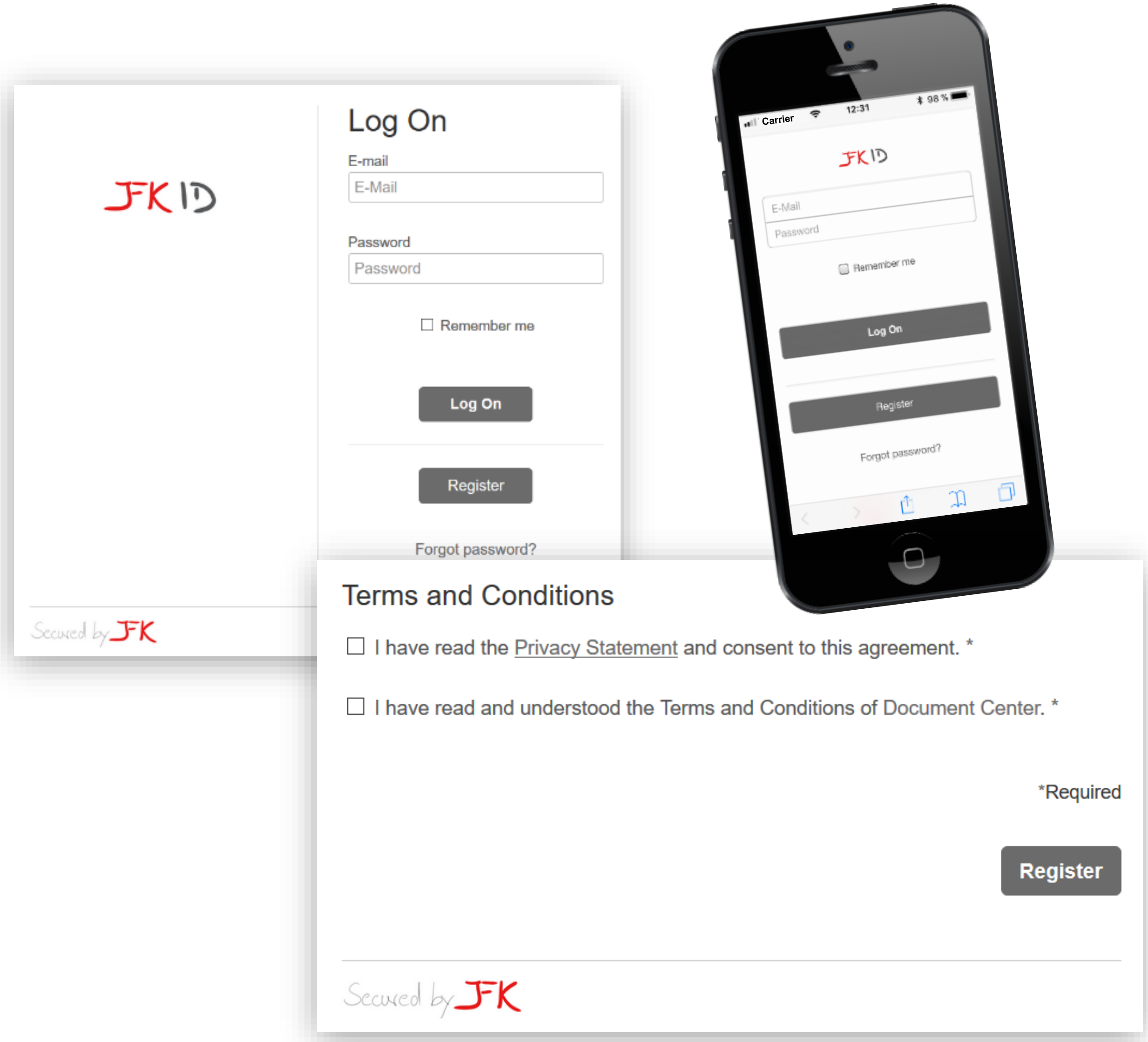
Branding and customization

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



Terms and Conditions

□ I have read the Privacy Statement and consent to this agreement. *

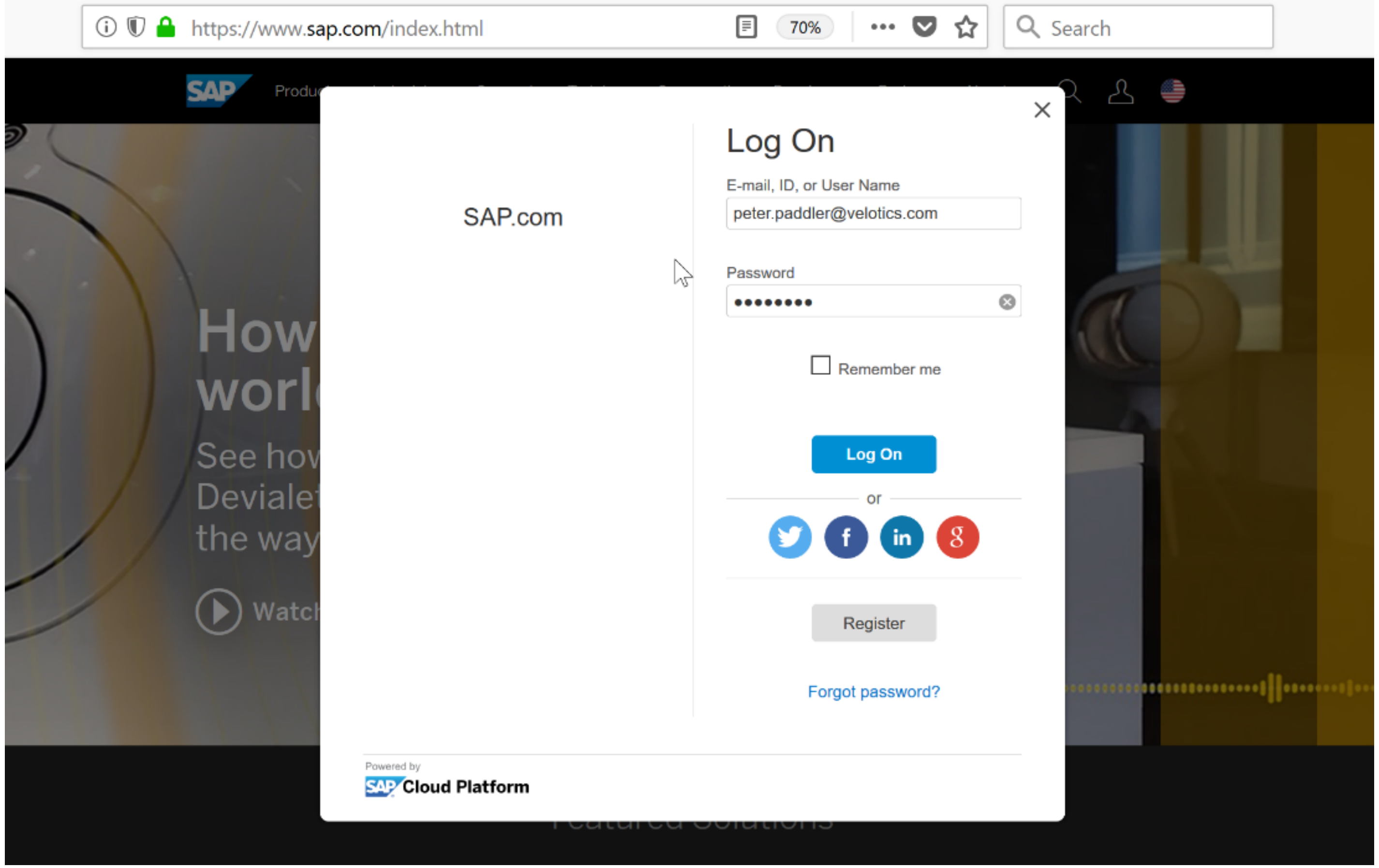
□ I have read and understood the Terms and Conditions of Document Center. *

*Required

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



https://www.sap.com/index.html

SAP.com

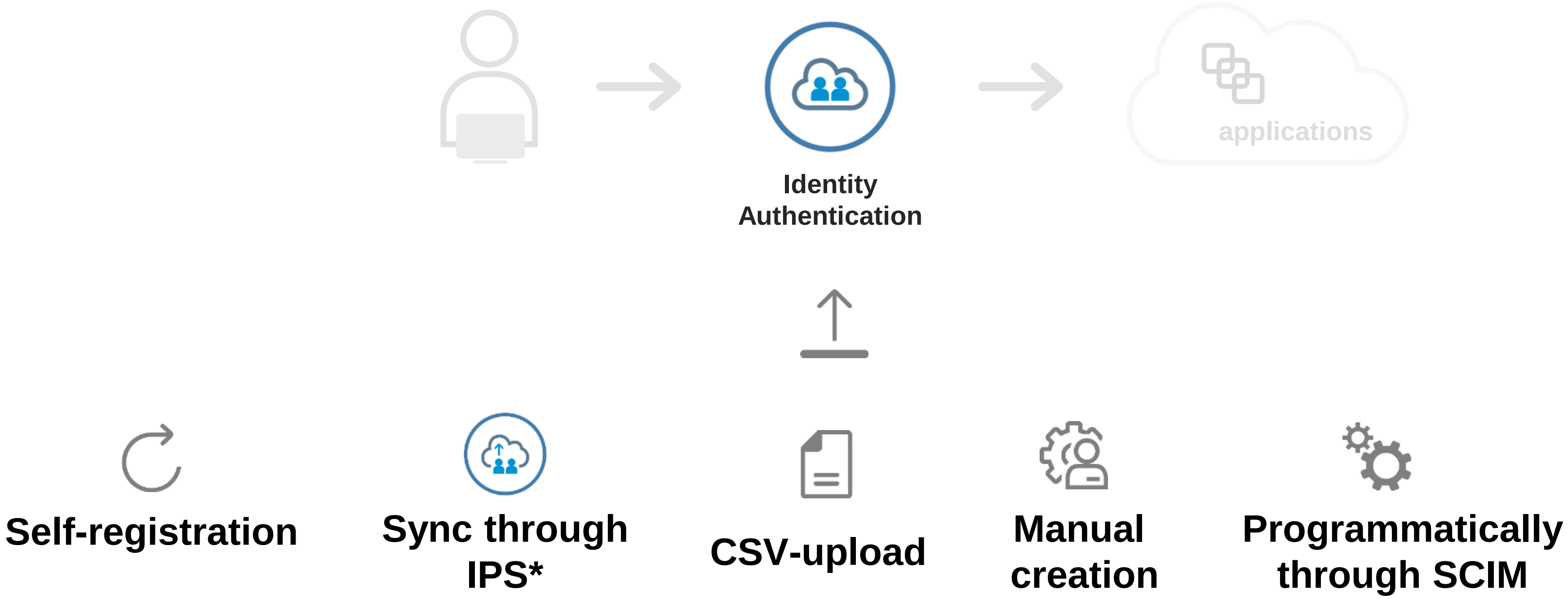
Log On

E-mail, ID, or User Name: peter.paddler@velotics.com

Password: ••••••••

□ Remember me

How can users be created?



Identity Authentication

applications

Self-registration

Sync through IPS*

CSV-upload

Manual creation

Programmatically through SCIM

* IPS: SAP Cloud Identity Services - Identity Provisioning

User & group management

User administration

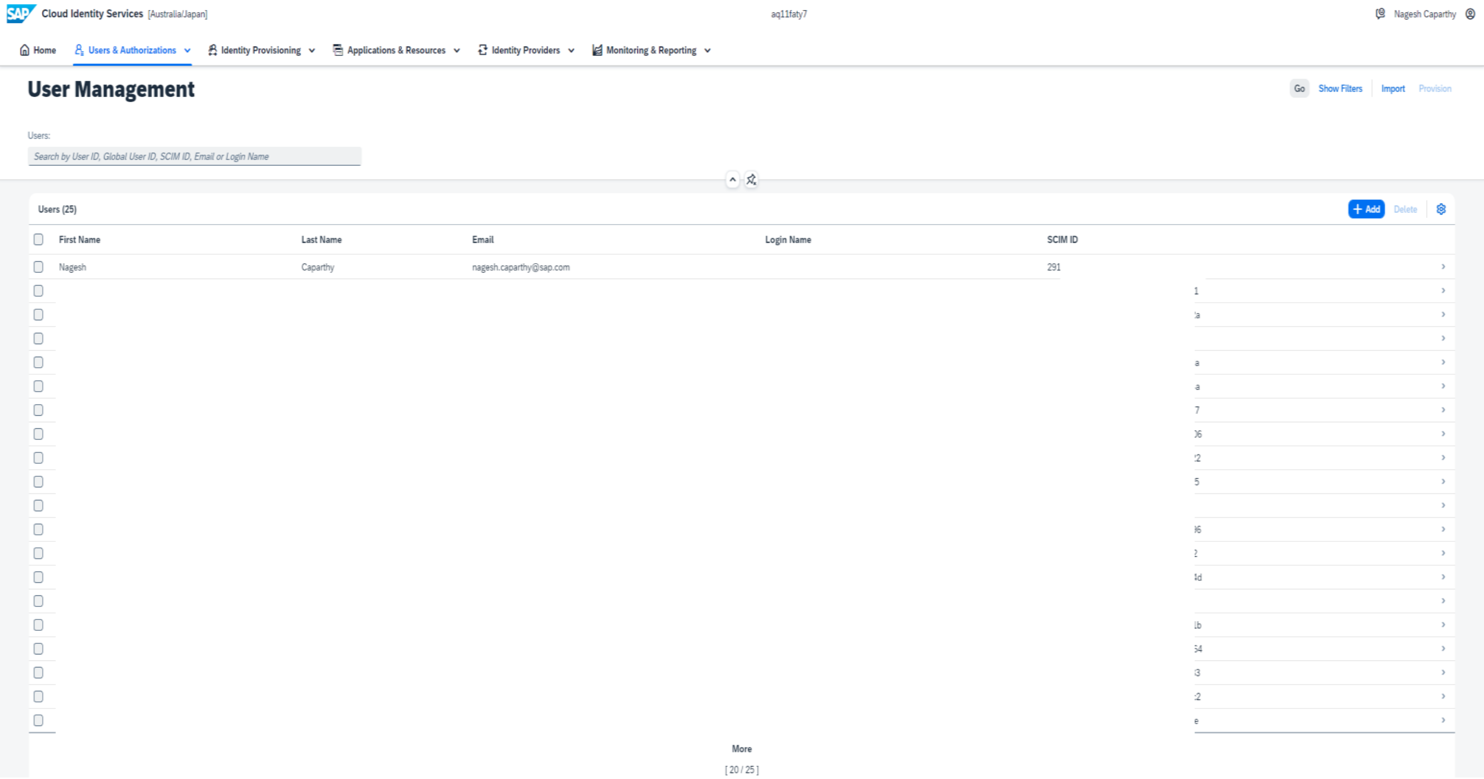
- Web based user management
- User search
- Mass user import/export
- Monitor user access

User groups administration

- Define user groups
- Assign users to groups

Integration

- Programmatic integration via SCIM REST APIs



User Management

Users:

Search by User ID, Global User ID, SCIM ID, Email or Login Name

Users (25)

□	First Name	Last Name	Email	Login Name	SCIM ID
□	Nagesh	Caparthy	nagesh.caparthy@sap.com		291

More

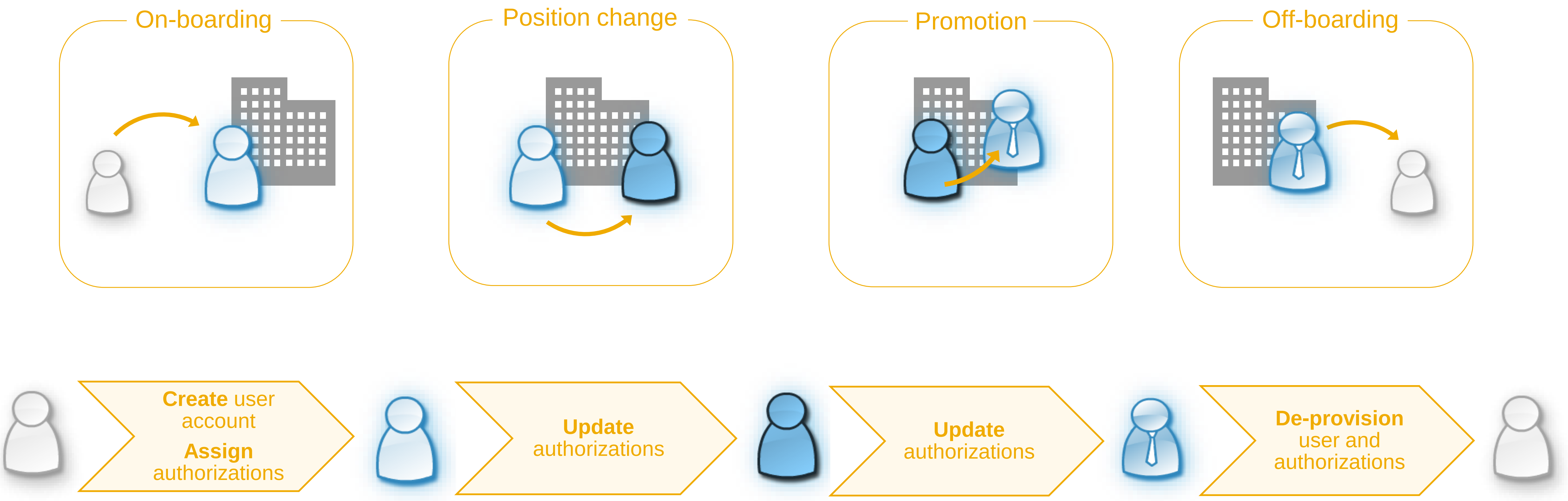
[20 / 25]

SAP Cloud Identity Services

Identity Provisioning

SAP Cloud Identity Services - Identity Provisioning

Employee lifecycle management in the cloud



Create user account
Assign authorizations

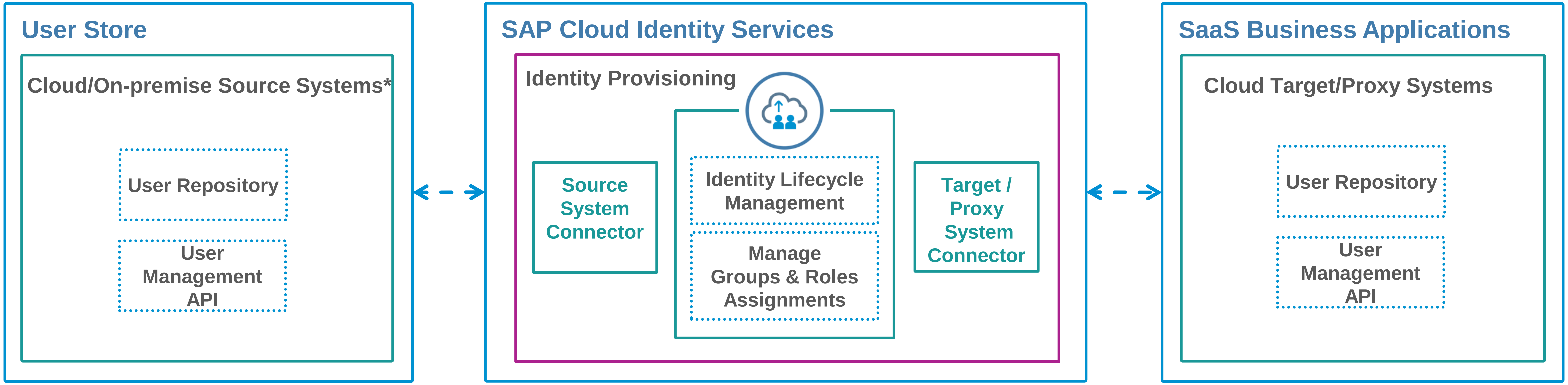
Update authorizations

Update authorizations

De-provision user and authorizations

SAP Cloud Identity Services - Identity Provisioning

Management of identities & authorizations



User Store
Cloud/On-premise Source Systems*
User Repository
User Management API
SAP Cloud Identity Services
Identity Provisioning
Source System Connector
Identity Lifecycle Management
Manage Groups & Roles Assignments
Target / Proxy System Connector
SaaS Business Applications
Cloud Target/Proxy Systems
User Repository
User Management API

SAP Cloud Identity Services - Identity Provisioning

Value Proposition

Identity and Access Management for the cloud and hybrid

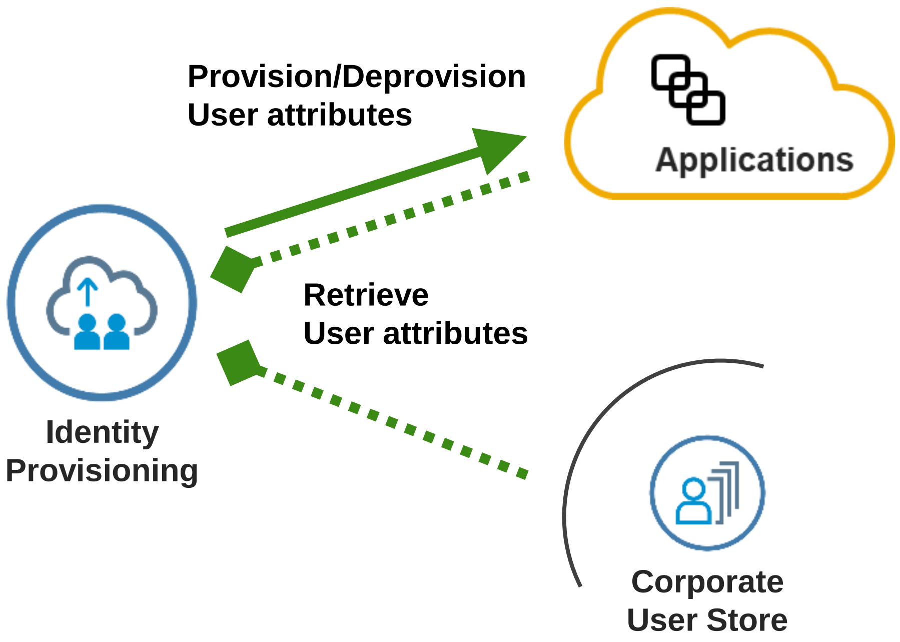
- Service of the SAP Business Technology Platform
- Identity lifecycle management for cloud-based business applications
- Integrated with SAP Identity Management for hybrid landscapes and also non-SAP IDM solutions using the SCIM* standard

Simple and agile solution with short time-to-value

- Developed with cloud qualities in mind
- Simple and agile on-boarding of users and applications

Openness and support of multi-vendor scenarios

- Support of industry standard protocol SCIM*
- Dedicated connectors for important 3rd party cloud platforms



*SCIM = System for Cross-domain Identity Management

SAP Cloud Identity Services - Identity Provisioning

Capabilities of the transformation engine

Policy-based assignments

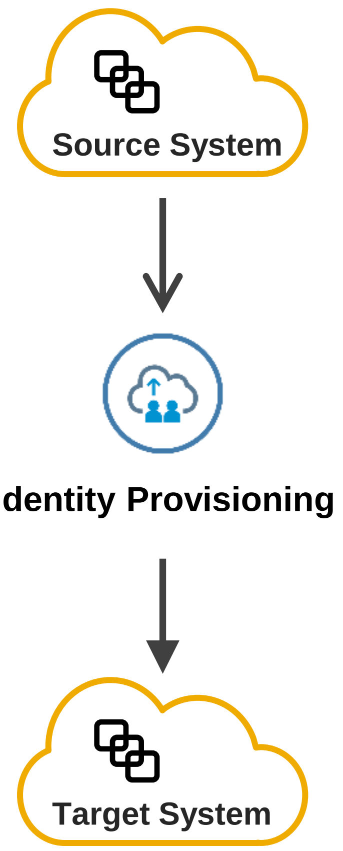
- Define rules for assignments based on the input data
- Take for example the value of an identity's organizational unit to decide on the required roles

Mapping between identity models

- Map between attributes in different models, for example surname to family name
- Adjust the data format, for example for time- or number-formats

Filtering

- Decide in detail which objects shall be read or written



SAP Cloud Identity Services - Identity Provisioning

Integration with SAP Identity Management

SAP Identity Management is recommended for on-premise landscapes

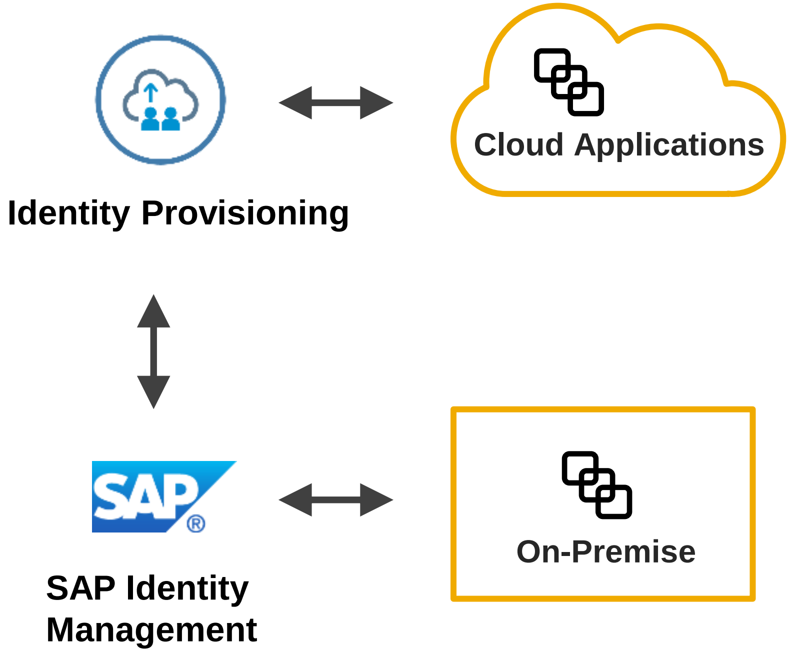
- Optimized for on-premise applications (customization, performance)

Identity Provisioning is recommended for cloud systems

- Offers a deployment model and simplicity suitable for cloud-based business applications
- Allows customers to efficiently on-board new applications

Hybrid scenarios recommendation

- Customers of SAP Identity Management can extend their identity lifecycle management to the cloud using Identity Provisioning
- Integration of SAP Identity Management with Identity Provisioning allows customers to benefit from the advantages of both worlds

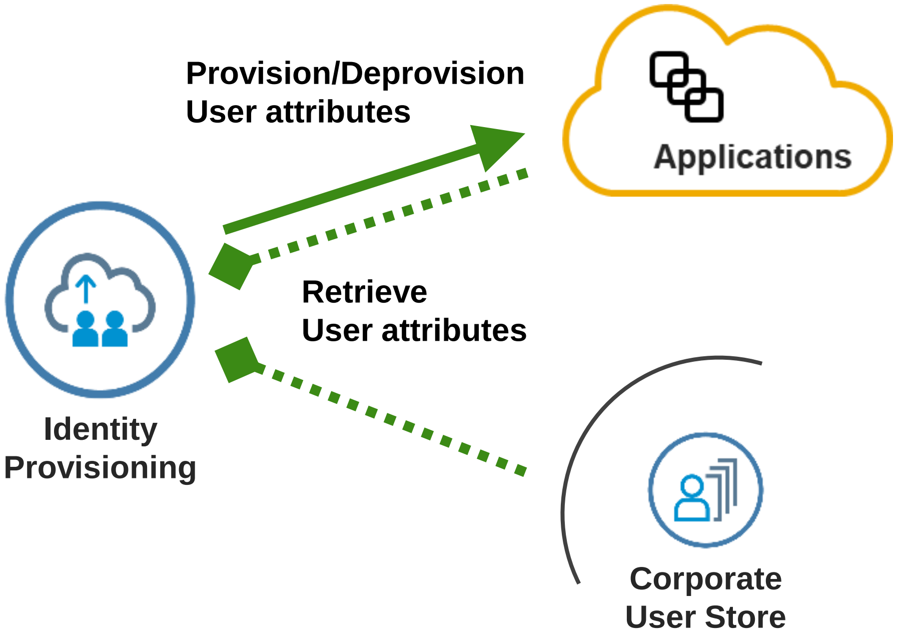


SAP Cloud Identity Services - Identity Provisioning

Connector Types

Identity Provisioning Connector Types

- Source System Connectors
- Target System Connectors
- Proxy System Connectors
- Refer Documentation for list of Supported IPS System Connectors



SAP Global User ID

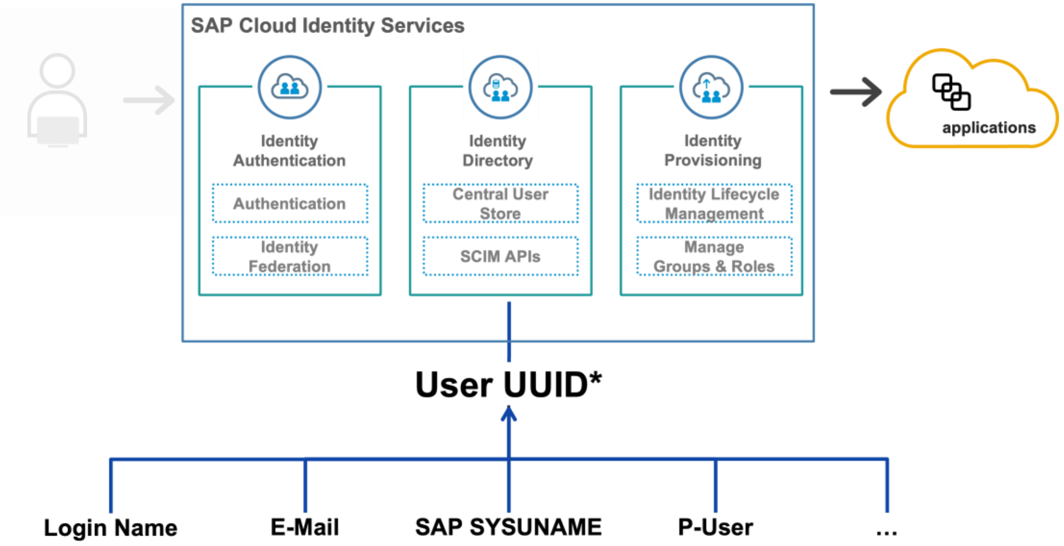
Concept & Implementation

A single common user identifier

- This Global User ID uniquely identifies a user across SAP business applications and services. Therefore, it replaces the need for a correlation of different external user identifiers.

- Apps like SAP Task Center with cross-application features require the Global User ID maintained for all users in all systems in scope

- Global User ID generation
  - SAP Cloud Identity Services
  - Customer ID**



*User Unique Universal Identifier (User UUID)

**As soon as all relevant SAP applications used by the customer support this

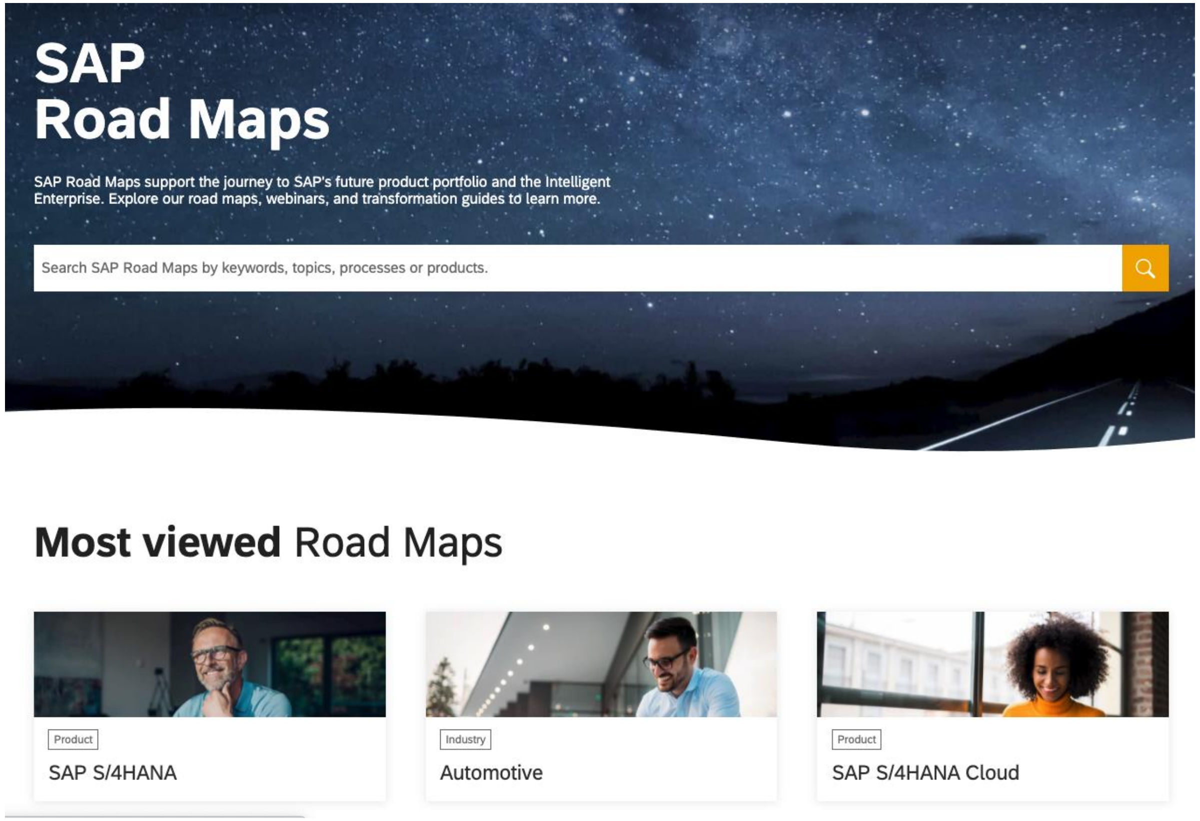
The recommended way is to generate and distribute the Global User ID with SAP Cloud Identity Services

Roadmap

SAP Cloud Identity Services

Product road map

- Roadmap Explorer
  - Roadmap SAP Cloud Identity Services
  - IAS Roadmap
  - IPS Roadmap



SAP Road Maps

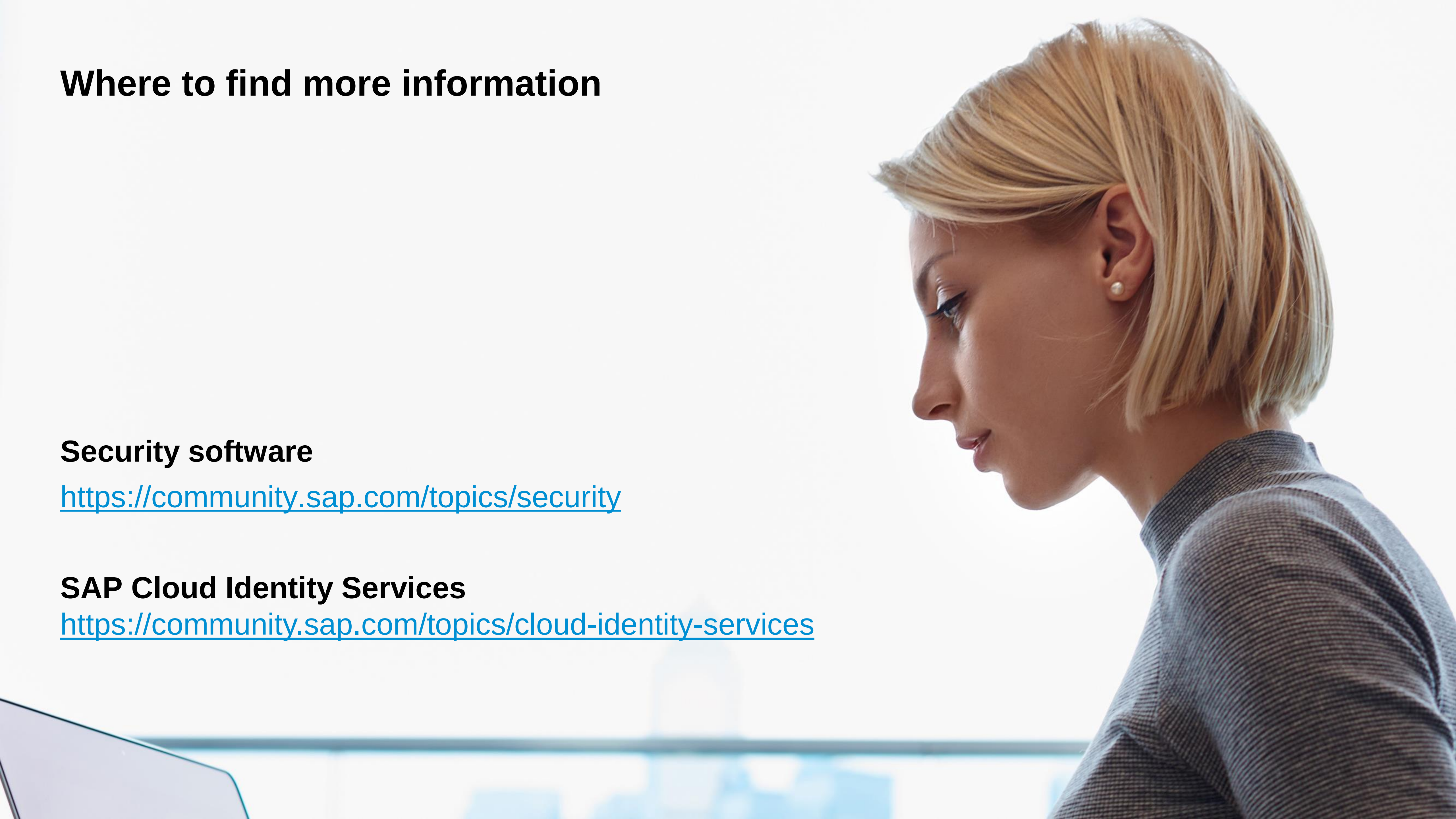
SAP Road Maps support the journey to SAP's future product portfolio and the Intelligent Enterprise. Explore our road maps, webinars, and transformation guides to learn more.

Search SAP Road Maps by keywords, topics, processes or products.

Most viewed Road Maps

Further information

Where to find more information



Security software

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

SAP Cloud Identity Services
https://community.sap.com/topics/cloud-identity-services

Thank you.

Contact information:

Nagesh Caparthy
SAP BTP Onboarding Advisor

Follow me on LinkedIn