Identity Access Management for the Intelligent Enterprise

February 26th 2020

THE BEST RUN **SAP**

Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, 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 presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or 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 presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation 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 non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP's intentional 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.

Agenda

Introduction

SAP Cloud Platform Identity Authentication

SAP Cloud Platform Identity Provisioning

Demo

Roadmap

Further information

SAP Intelligent Enterprise Framework

THE INTELLIGENT ENTERPRISE

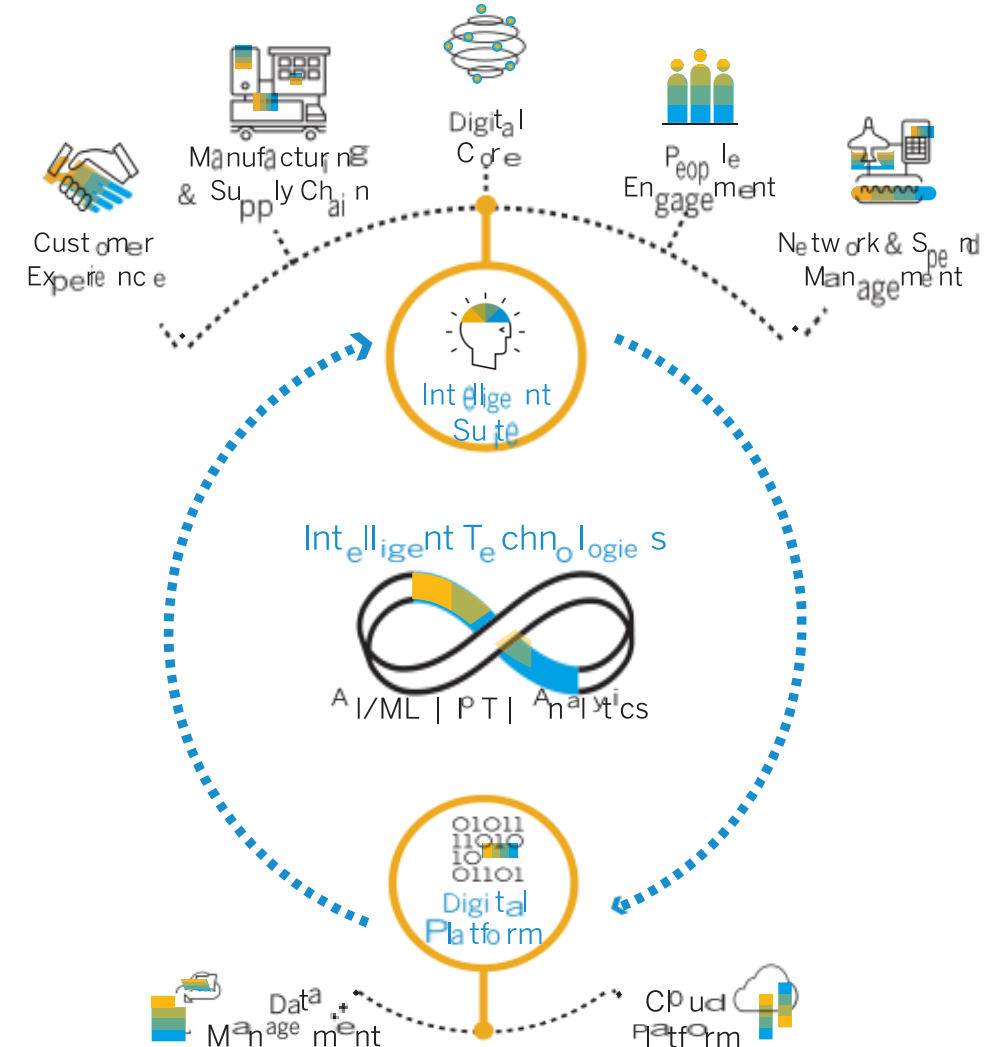features **3 KEY COMPONENTS:**

Intelligent Suite
Enables our customers to automate their day-to-day business processes and better interact with their customers, suppliers, employees, etc. through applications that have intelligence embedded in them.

Digital Platform
With SAP Cloud Platform and the HANA Data Management Suite, we can facilitate the collection, connection, and orchestration of data as well as the integration and extension of processes within the Intelligent Suite
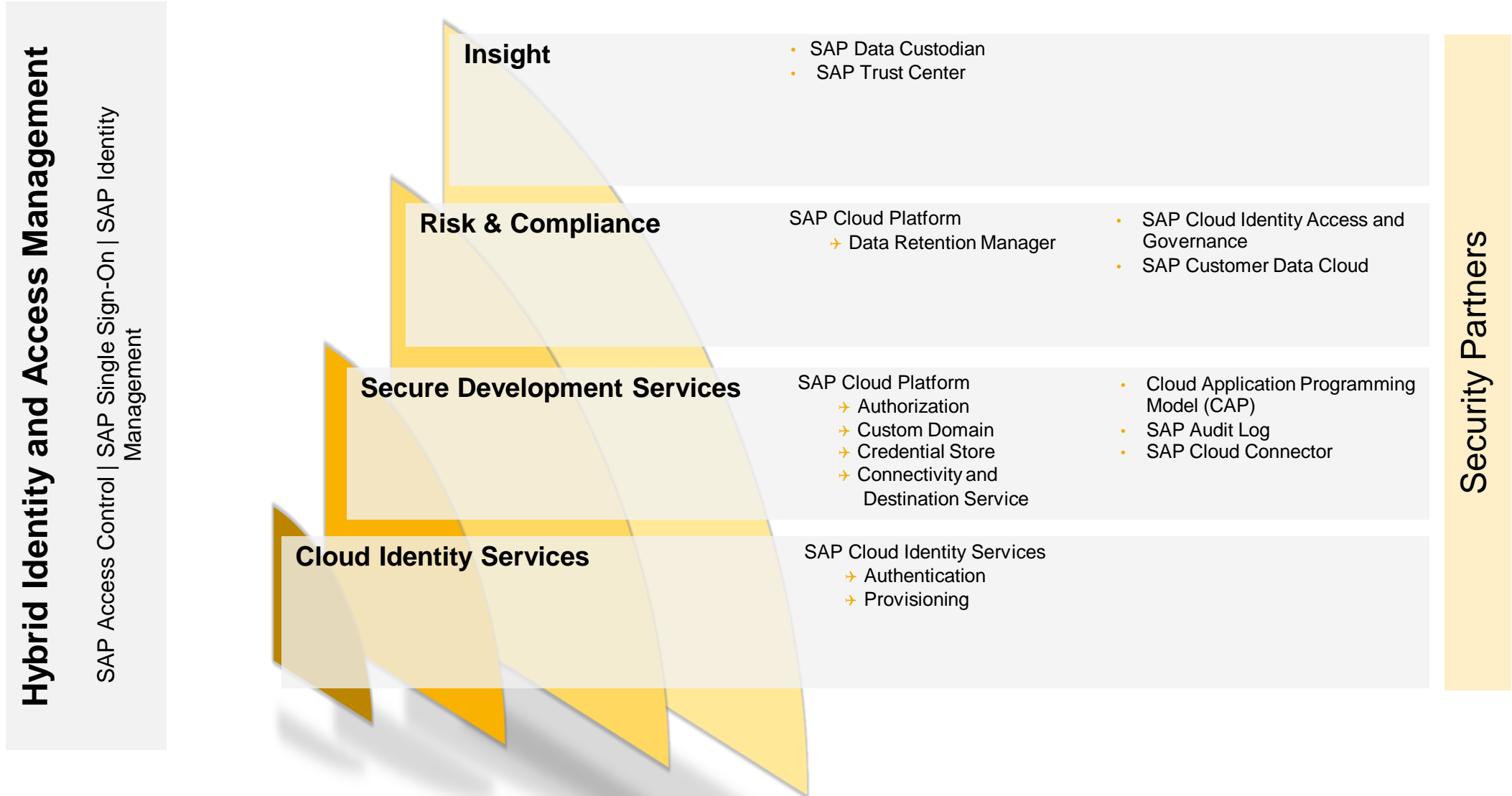
Intelligent Technologies
SAP Leonardo enables our customers to leverage their data to detect patterns, predict outcomes, and suggest actions.

Cloud Enterprise Security Suite

Security for the Cloud Age

Hybrid Identity and Access Management

SAP Access Control | SAP Single Sign-On | SAP Identity Management

Insight
- SAP Data Custodian
- SAP Trust Center

Risk & Compliance

SAP Cloud Platform
→ Data Retention Manager

- SAP Cloud Identity Access and Governance
- SAP Customer Data Cloud

Secure Development Services

SAP Cloud Platform
→ Authorization
→ Custom Domain
→ Credential Store
→ Connectivity and Destination Service

- Cloud Application Programming Model (CAP)
- SAP Audit Log
- SAP Cloud Connector

Cloud Identity Services

SAP Cloud Identity Services
→ Authentication
→ Provisioning

Security Partners

SAP Cloud Platform **Identity Authentication**

SAP Cloud Platform Identity Authentication

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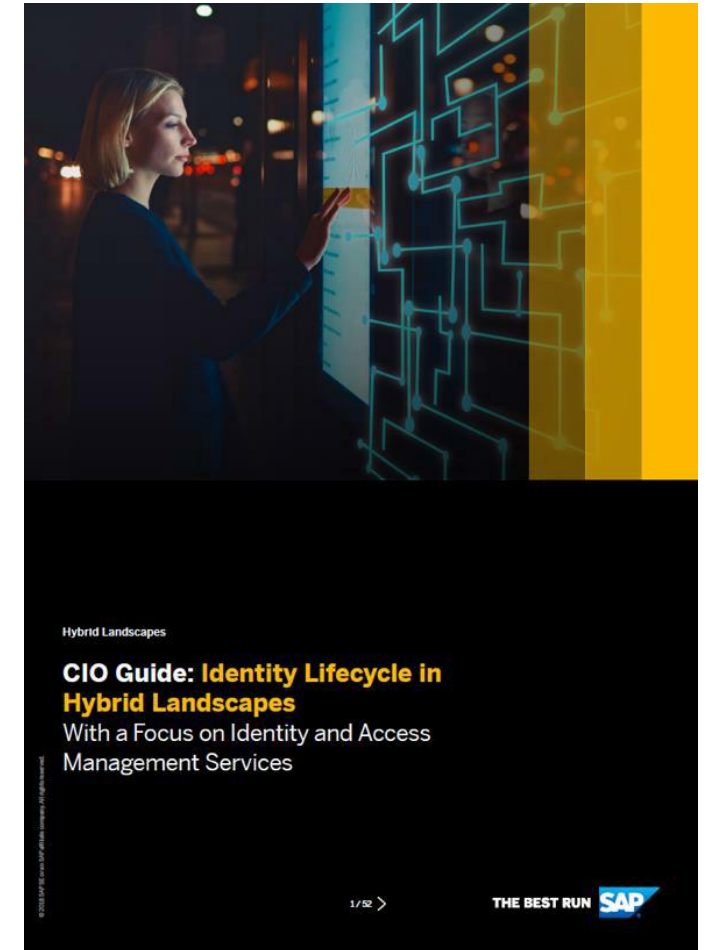
SAP Cloud Platform Identity Authentication enables single sign-on for SAP's cloud-based business applications, with two usage options

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

Hybrid Landscapes

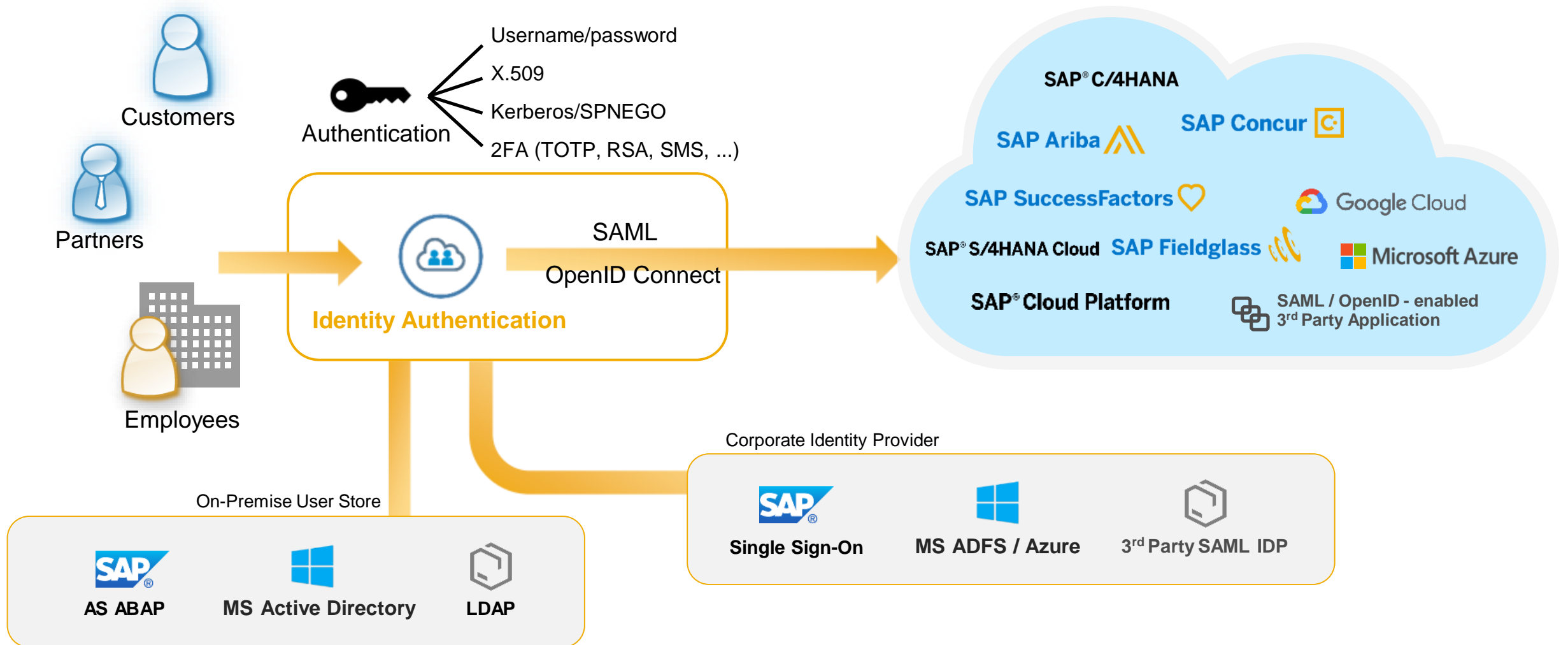**CIO Guide: Identity Lifecycle in Hybrid Landscapes**
With a Focus on Identity and Access Management Services

1 / 52 >

THE BEST RUN SAP

https://www.sap.com/documents/2018/05/38ce7d25-067d-0010-87a3-c30de2ffd8ff.html

SAP Cloud Platform Identity Authentication

Secure authentication & single sign-on

Customers

Partners

Employees

Authentication
- Username/password
- X.509
- Kerberos/SPNEGO
- 2FA (TOTP, RSA, SMS, ...)

Identity Authentication

SAML
OpenID Connect

SAP® C/4HANA

SAP Ariba

SAP Concur

SAP SuccessFactors

Google Cloud

SAP® S/4HANA Cloud   SAP Fieldglass

Microsoft Azure

SAP® Cloud Platform

SAML / OpenID - enabled
3rd Party Application

On-Premise User Store

AS ABAP   MS Active Directory   LDAP

Corporate Identity Provider

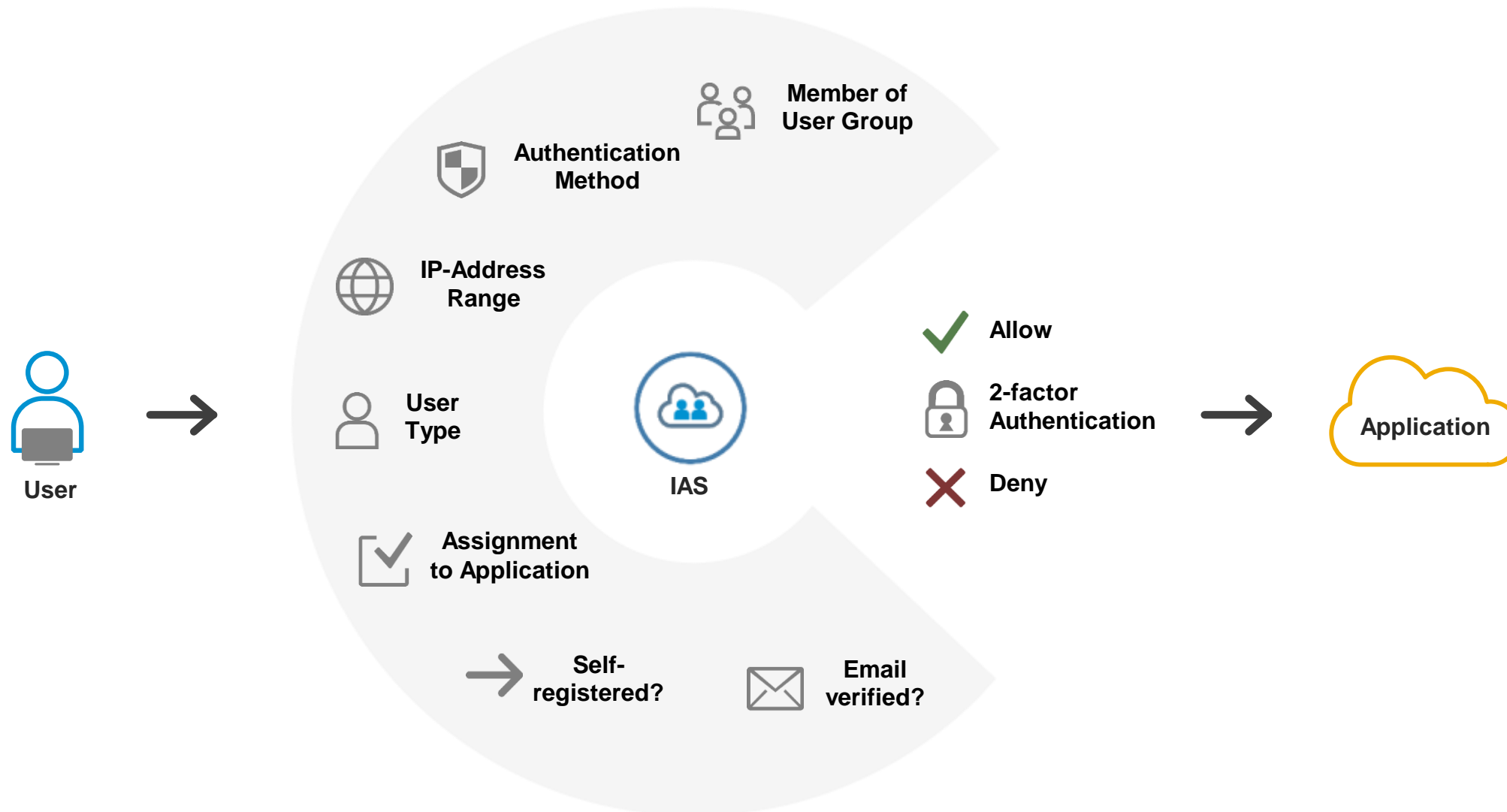Single Sign-On   MS ADFS / Azure   3rd Party SAML IDP

Delegated authentication towards multiple identity providers

Conditional authentication
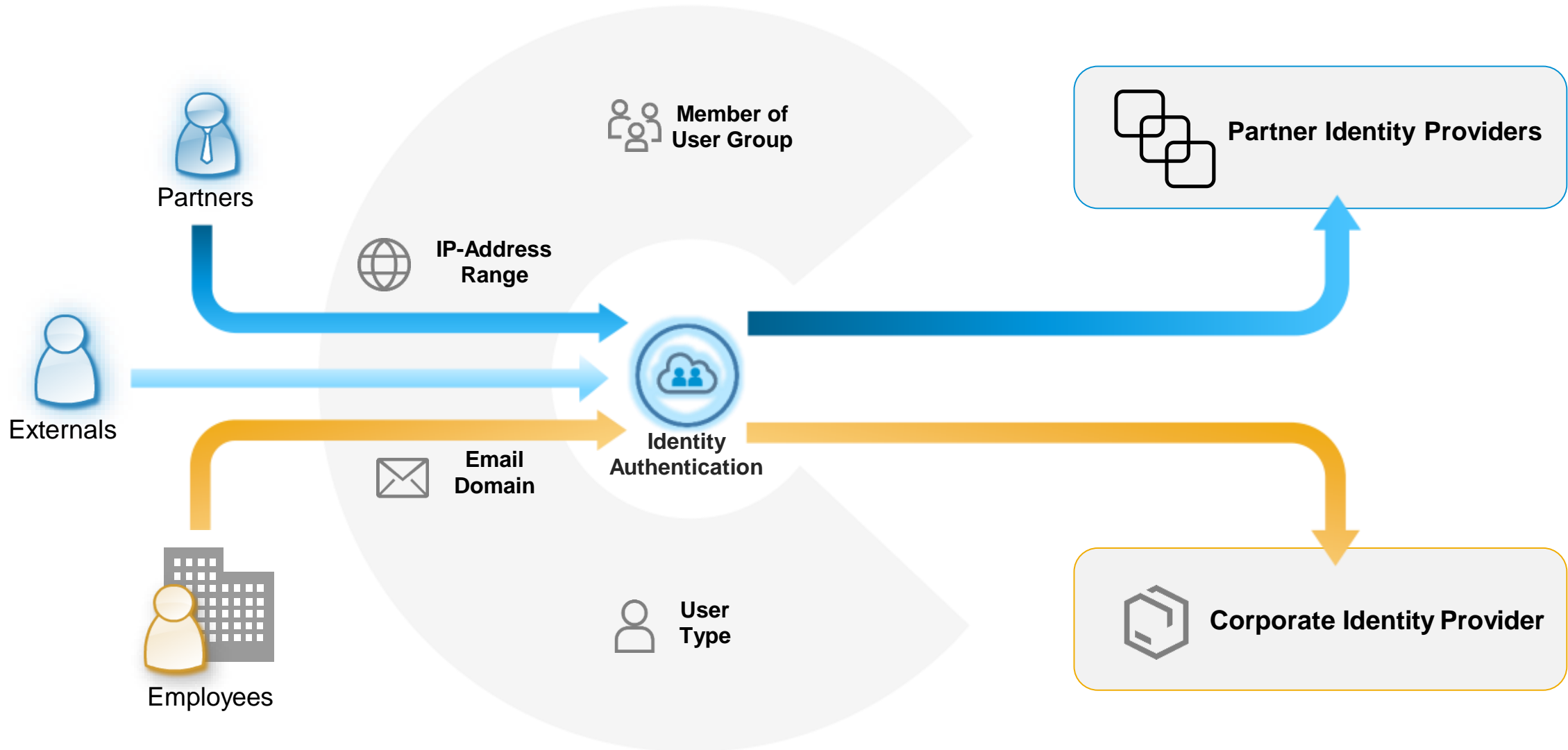
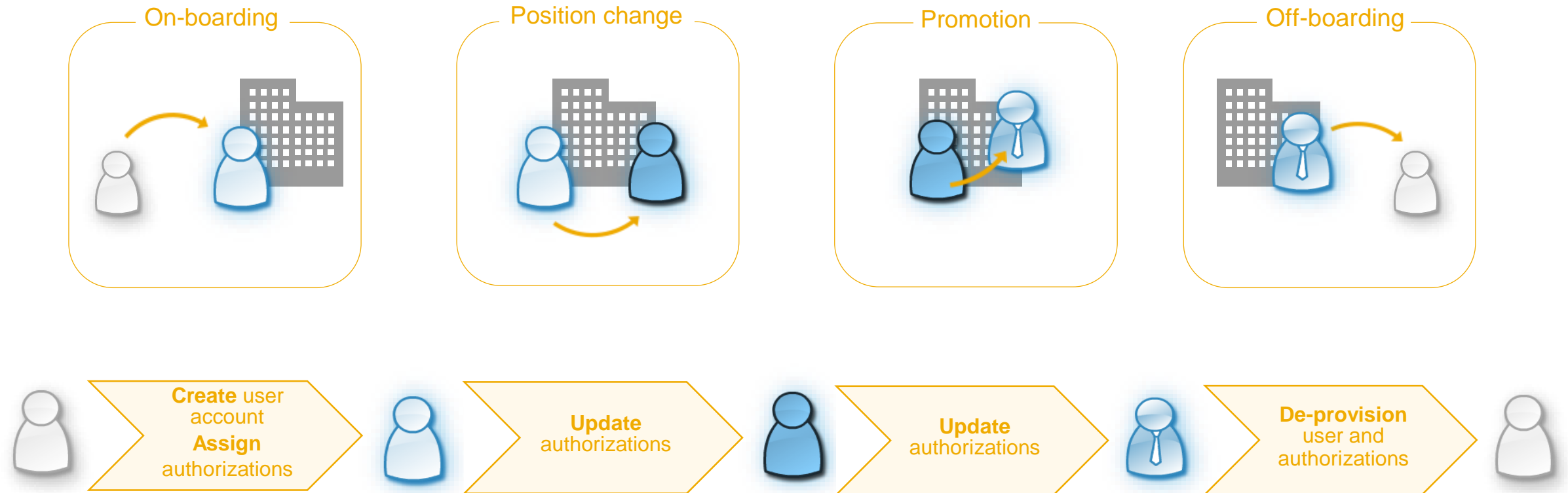# Control access to the application – risk-based authentication

Supports both local authentication and IdP proxy
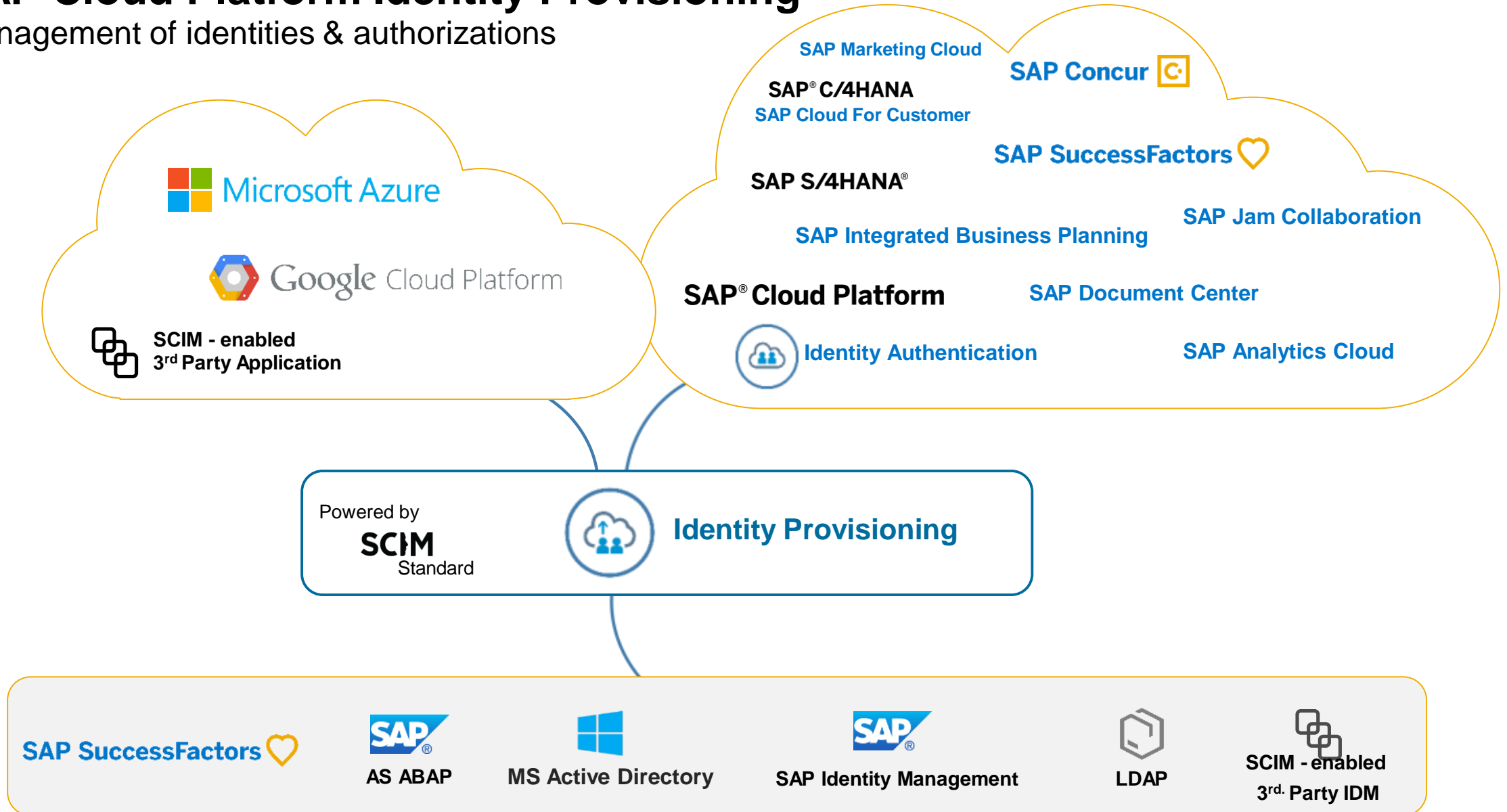
SAP Cloud Platform **Identity Provisioning**

SAP Cloud Platform Identity Provisioning

Employee lifecycle management in the cloud

On-boarding

Position change

Promotion

Off-boarding

Create user account
Assign authorizations

Update authorizations

Update authorizations

De-provision user and authorizations

SAP Cloud Platform Identity Provisioning

Management of identities & authorizations

Microsoft Azure

Google Cloud Platform

SCIM - enabled
3rd Party Application

SAP Marketing Cloud

SAP® C/4HANA
SAP Cloud For Customer

SAP Concur

SAP SuccessFactors

SAP S/4HANA®

SAP Jam Collaboration

SAP Integrated Business Planning

SAP® Cloud Platform

SAP Document Center

Identity Authentication

SAP Analytics Cloud

Powered by

SCIM
Standard

Identity Provisioning

SAP SuccessFactors

AS ABAP

MS Active Directory

SAP Identity Management

LDAP

SCIM - enabled
3rd. Party IDM

SAP Cloud Platform Identity Provisioning

Product description

Identity and Access Management for the cloud and hybrid
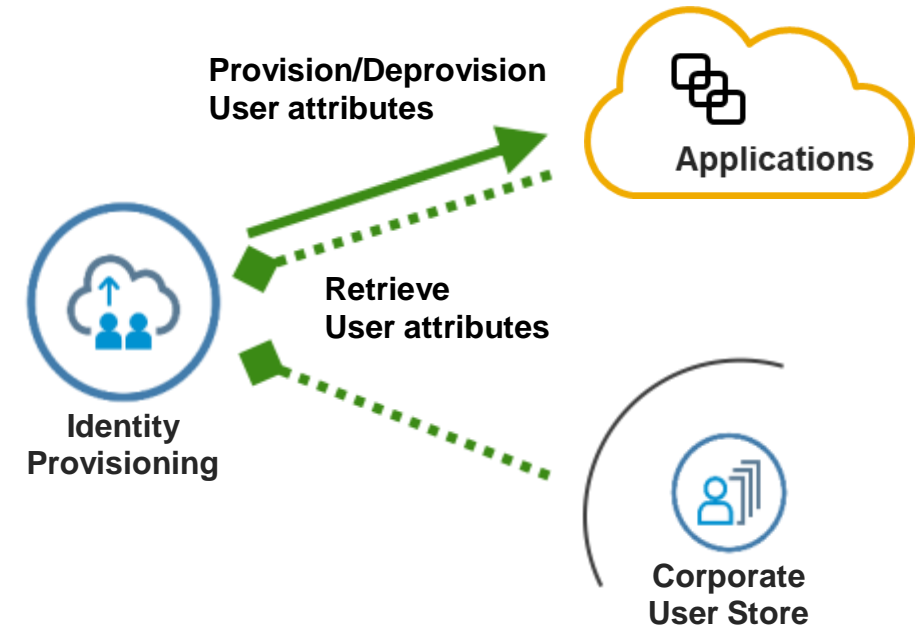
✦Service of the SAP Cloud Platform

✦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
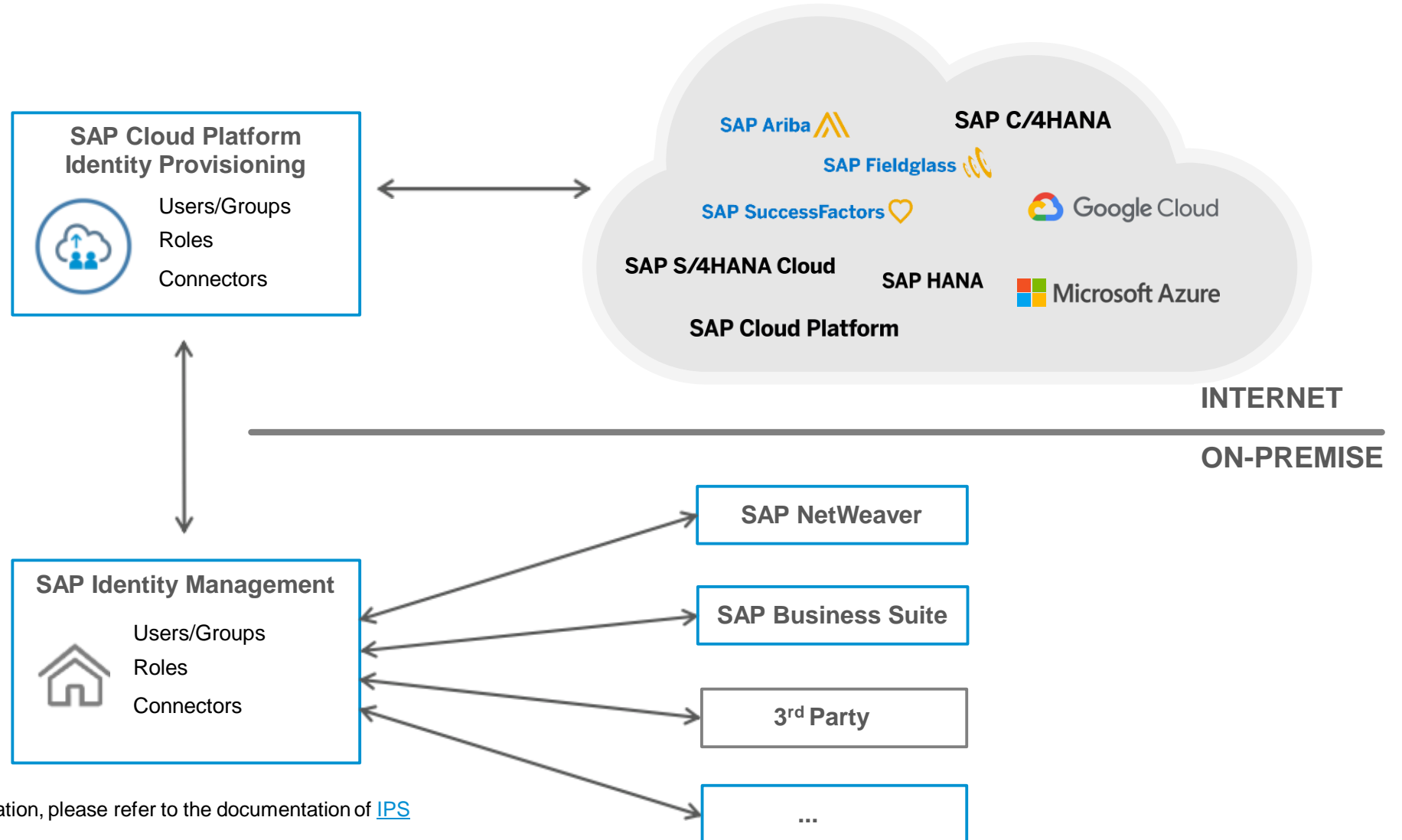
Openness and support of multi-vendor scenarios

✦Support of industry standard protocol SCIM*

✦Dedicated connectors for important 3rd party cloud platforms

Provision/Deprovision User attributes

Applications

Retrieve User attributes

Identity Provisioning

Corporate User Store

*SCIM = System for Cross-domain Identity Management

Identity Lifecycle Management in a hybrid landscape for SAP Identity Management customers*

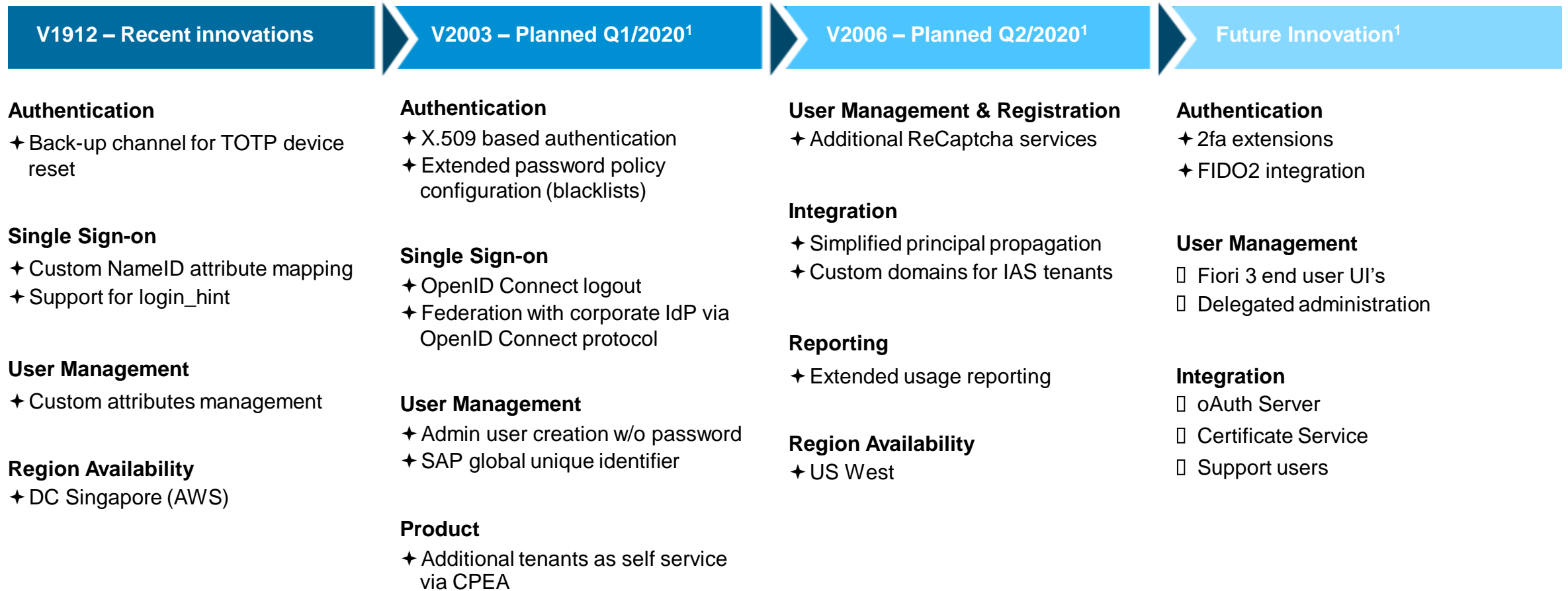Extends an existing on-premise SAP IDM towards the cloud, using IPS

SAP Cloud Platform Identity Provisioning

Users/Groups
Roles
Connectors

SAP Ariba
SAP C/4HANA
SAP Fieldglass
SAP SuccessFactors
Google Cloud
SAP S/4HANA Cloud
SAP HANA
Microsoft Azure
SAP Cloud Platform

INTERNET

ON-PREMISE

SAP Identity Management

Users/Groups
Roles
Connectors

SAP NetWeaver

SAP Business Suite

3rd Party

...

* For details on the specific support per application, please refer to the documentation of IPS

Road**map**

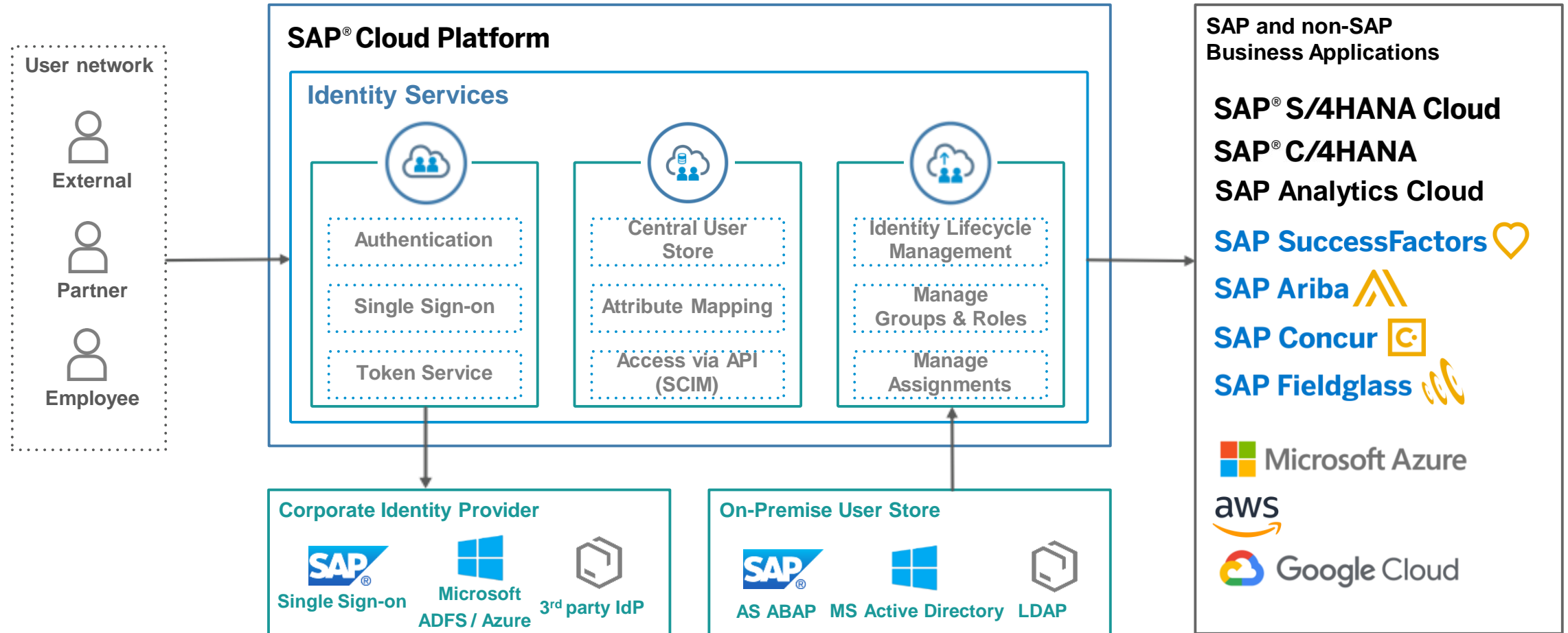# SAP Cloud Platform Identity Authentication

Product road map overview

| V1912 – Recent innovations | V2003 – Planned Q1/2020[1] | V2006 – Planned Q2/2020[1] | Future Innovation[1] |

V1912 – Recent innovations

Authentication
- ✦ Back-up channel for TOTP device reset

Single Sign-on
- ✦ Custom NameID attribute mapping
- ✦ Support for login_hint

User Management
- ✦ Custom attributes management

Region Availability
- ✦ DC Singapore (AWS)

V2003 – Planned Q1/2020[1]

Authentication
- ✦ X.509 based authentication
- ✦ Extended password policy configuration (blacklists)

Single Sign-on
- ✦ OpenID Connect logout
- ✦ Federation with corporate IdP via OpenID Connect protocol

User Management
- ✦ Admin user creation w/o password
- ✦ SAP global unique identifier

Product
- ✦ Additional tenants as self service via CPEA

V2006 – Planned Q2/2020[1]

User Management & Registration
- ✦ Additional ReCaptcha services

Integration
- ✦ Simplified principal propagation
- ✦ Custom domains for IAS tenants

Reporting
- ✦ Extended usage reporting

Region Availability
- ✦ US West

Future Innovation[1]

Authentication
- ✦ 2fa extensions
- ✦ FIDO2 integration

User Management
- ❑ Fiori 3 end user UI's
- ❑ Delegated administration

Integration
- ❑ oAuth Server
- ❑ Certificate Service
- ❑ Support users

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

SAP Cloud Identity Services
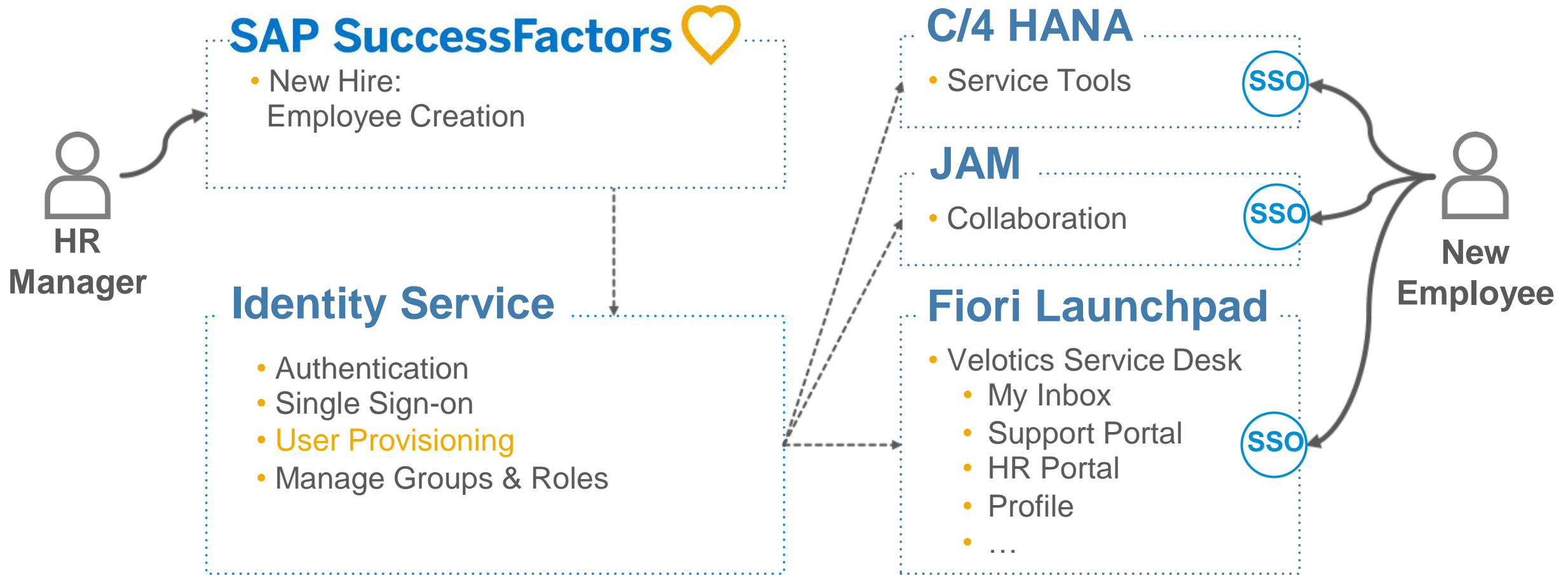
Product road map overview

SAP® Cloud Platform

Identity Services

Authentication	Central User Store	Identity Lifecycle Management
Single Sign-on	Attribute Mapping	Manage Groups & Roles
Token Service	Access via API (SCIM)	Manage Assignments

User network

- External
- Partner
- Employee

Corporate Identity Provider

- **SAP®** Single Sign-on
- **Microsoft** ADFS / Azure
- 3rd party IdP

On-Premise User Store

- **SAP®** AS ABAP
- MS Active Directory
- LDAP

SAP and non-SAP Business Applications

- **SAP® S/4HANA Cloud**
- **SAP® C/4HANA**
- **SAP Analytics Cloud**
- **SAP SuccessFactors**
- **SAP Ariba**
- **SAP Concur**
- **SAP Fieldglass**
- Microsoft Azure
- aws
- Google Cloud

Demo

DEMO - Identity Services

Scenario Hire to Retire: creation and provisioning of new employee

SAP SuccessFactors ♡
- New Hire:
  Employee Creation

HR Manager

Identity Service
- Authentication
- Single Sign-on
- User Provisioning
- Manage Groups & Roles

C/4 HANA
- Service Tools

SSO

JAM
- Collaboration

SSO

Fiori Launchpad
- Velotics Service Desk
  - My Inbox
  - Support Portal
  - HR Portal
  - Profile
  - …

SSO

New Employee

Where to find more information

Security software

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

SAP Cloud Platform Identity Authentication Service

https://community.sap.com/topics/cloud-platform-identity-authentication

SAP Cloud Platform Identity Provisioning Service

https://community.sap.com/topics/cloud-platform-identity-provisioning

Thank you.

Contact information:

Marko Sommer

Product Expert
SAP SE
69190 Walldorf, Germany
marko.sommer@sap.com

Acronym glossary

Acronym	Full Text	Acronym	Full Text
B2B	Business to Business	OTP	One-time password
B2C	Business to Consumer	REST	Representational State Transfer
B2E	Business to Employee	RSA	RSA is a public-key cryptosystem
C4C	SAP Cloud for Customer	SAML	Security Assertion Markup Language
CP	SAP Cloud Platform	SCIM	System for Cross-domain Identity Management
HR / HCM	Human Resources, Human Capital Management	SF / SFSF	SuccessFactors
IAM / IDM	Identity Access Management / Identity Management	SPNEGO	Simple and Protected GSSAPI Negotiation Mechanism (GSSAPI: Generic Security Service Application Program Interface)
IBP	SAP Integrated Business Planning	SSO	Single Sign-On
IdP / SP	Identity Provider / Service Provider (SAML)	TCO	Total Cost of Ownership
LDAP	Lightweight Directory Access Protocol	TFA / 2FA	Two-factor authentication
OAuth	Open Authorization Framework	X.509	in cryptography, X.509 is a standard for a public key infrastructure (PKI)

Follow us

THE BEST RUN SAP