SAP Cloud Identity Services in a nutshell

Sonia Petrescu, SAP
March 16, 2023

PUBLIC

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

What's IAM ?

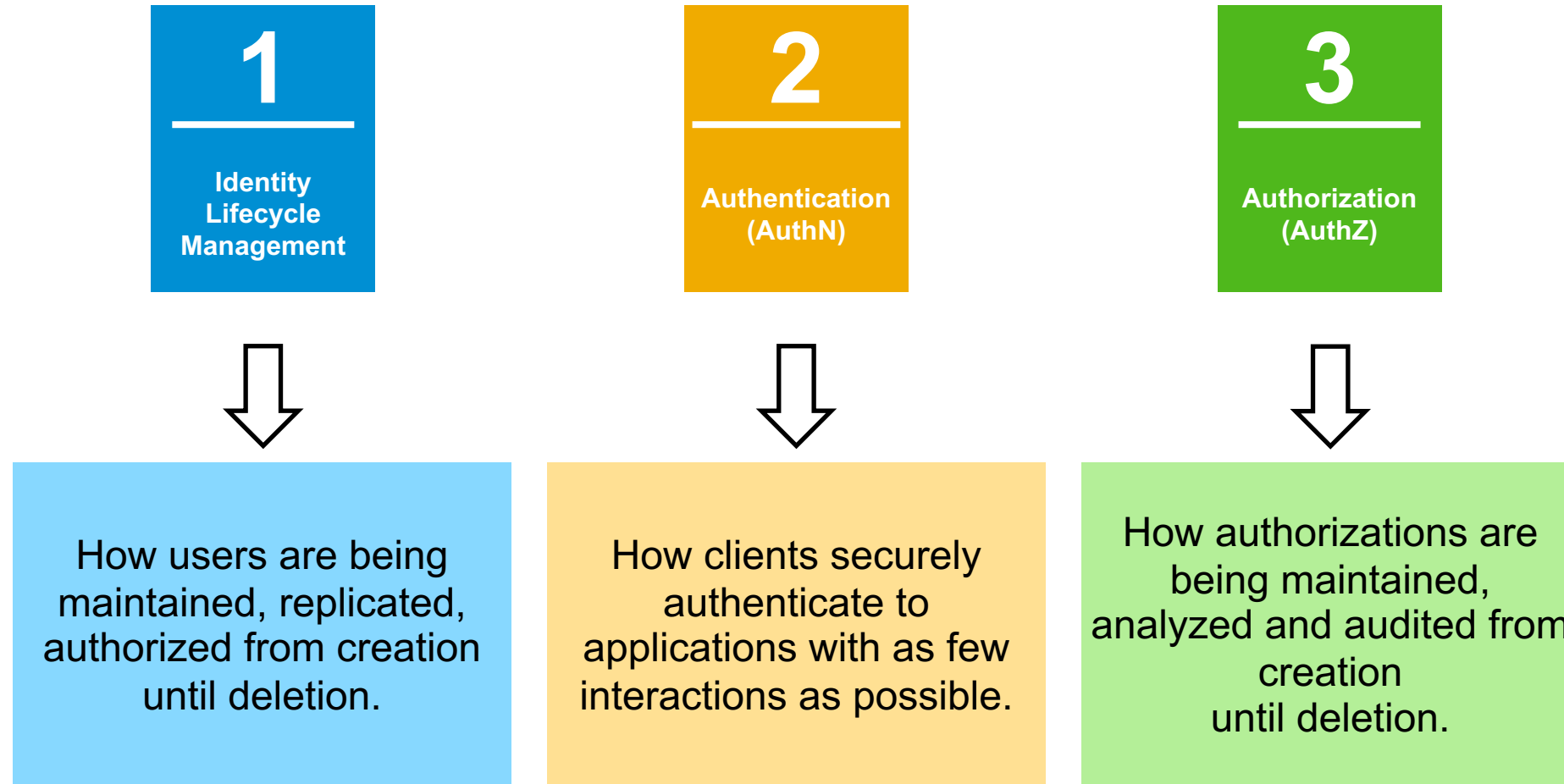What are the SAP Cloud Identity Services?

Why to use them ?

How would my architecture look like ?

Wrap-up and feedback

What's IAM?

What's IAM?
Main Domains

1	2	3
Identity Lifecycle Management	Authentication (AuthN)	Authorization (AuthZ)

How users are being maintained, replicated, authorized from creation until deletion.

How clients securely authenticate to applications with as few interactions as possible.

How authorizations are being maintained, analyzed and audited from creation until deletion.

What's IAM?
Portfolio

CUSTOMER

ENTERPRISE USER

| IDENTITY MANAGEMENT | GOVERNANCE, RISK & COMPLIANCE | AUTHENTICATION & SINGLE SIGN-ON |

SAP Cloud Identity Access Governance

SAP Customer Data Cloud / Platform

SAP Cloud Identity Services

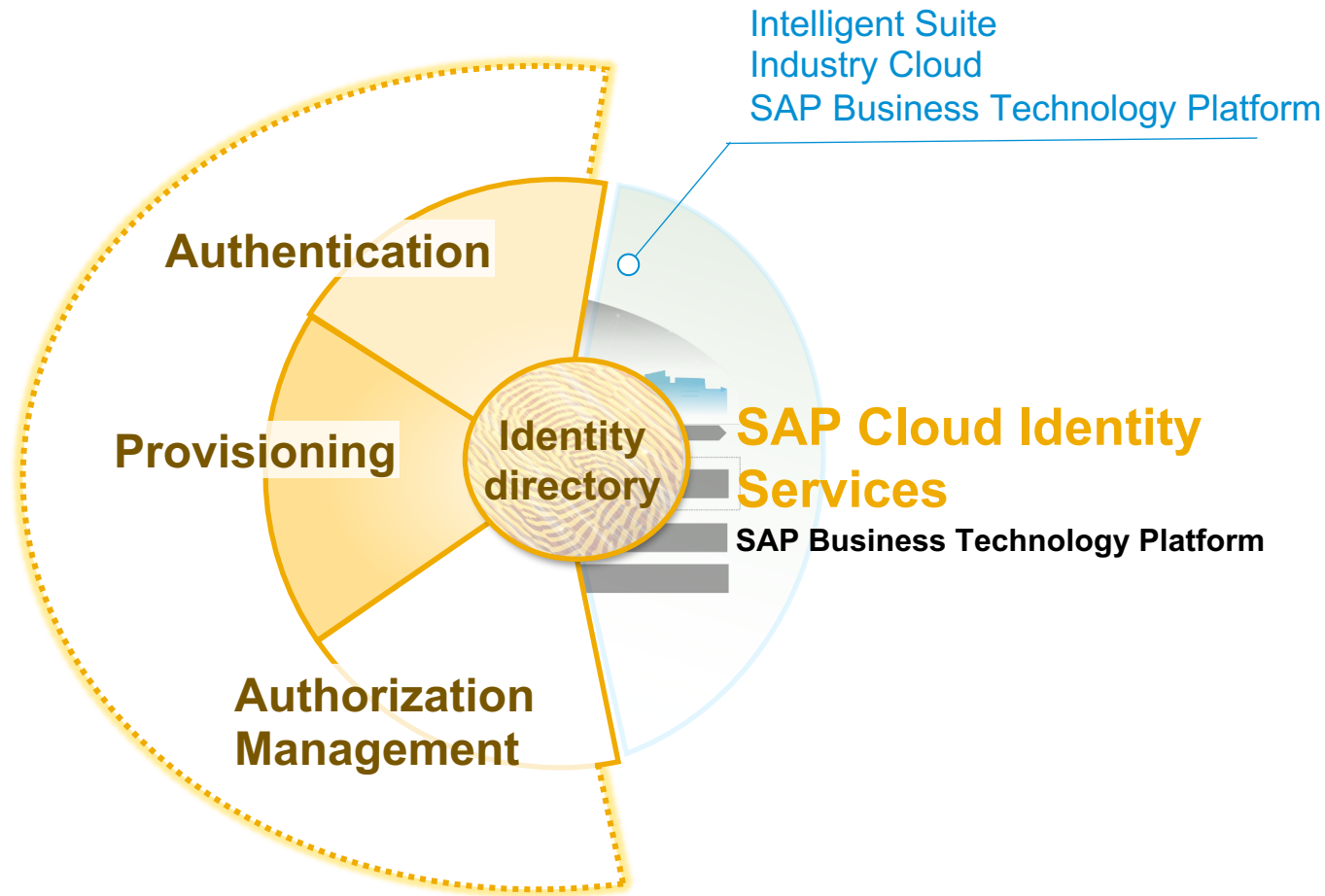| Identity Lifecycle Management (Provisioning) | Identity Directory (Storage) | Authorization Management (AuthZ) | Identity Authentication (AuthN) |

Public Cloud

SAP Identity Management

SAP Access Control

SAP Single Sign-On

On-Premise / Private Cloud

What are the SAP Cloud Identity Services?

SAP Cloud Identity Services
What are they?

Intelligent Suite
Industry Cloud
SAP Business Technology Platform

Authentication

Provisioning

Identity directory

Authorization Management

SAP Cloud Identity Services

SAP Business Technology Platform

SAP Cloud Identity Services are the **default** to authenticate and provision users in cloud solutions from SAP.

- Identity authentication
- Identity provisioning
- Authorization management
- Integrated through the common identity directory

The number of **pre-integrated SAP solutions** that require **SAP Cloud Identity Services** will increase**.**

One cloud service from SAP is used to integrate any 3rd party identity management (IDM) system.

Identity Authentication

see also Single Sign-On: Authentication with a Single SAP Cloud Identity Services Tenant and a Single Corporate Identity Provider

Corporate Identity Provider

5. Corp.IdP authentication

5. redirect to SAP Cloud Identity Services

2-FA

1. User access App

7. User authenticates to the app

Cloud Applications

Business User

2. Redirect to SAP Cloud Identity Services

On-premise Applications

4. If no X.509 present, Corp.IdP forwarding

3. Rule-Check

6. „SAP ID Token" creation & redirect to App

SAML2 or OIDC trust relation

SAP Cloud Identity Services

2-FA (optional)

SAML2 or OIDC trust relation

SAML: Security Assertion Markup Language - OIDC: OpenID Connect - JWT: JSON Web Token

2-FA: Two Factor Authentication

SAP managed

Identity Provisioning Connector Types

- Source System Connectors
- Target System Connectors
- Proxy System Connectors
- Check the [Documentation](#) for updated list of Supported IPS System Connectors
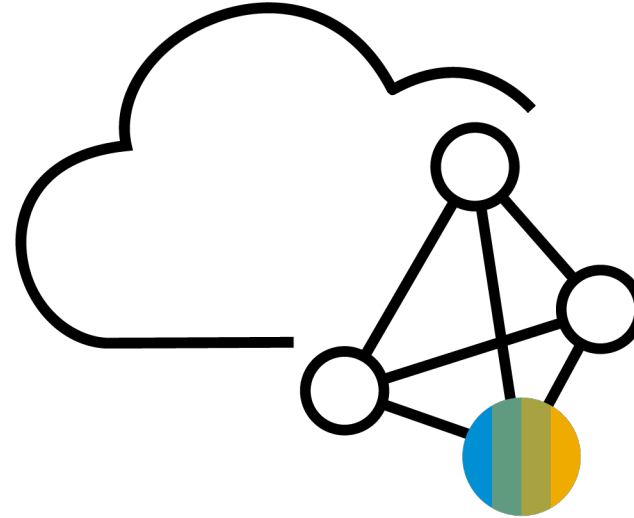
Out of the box configuration for user provisioning and authentication

Identity Directory

What is the Identity Directory ?

- Identity Directory is the central component for persisting users and groups inside the SAP Cloud Identity Services

How to access the Identity Directory ?

- With the Identity Provisioning service SAP Cloud Identity Services – Identity Provisioning

- Via the SCIM 2.0 API SAP Cloud Identity Services – Identity Directory

- Via the SAP Cloud Identity services admin UI
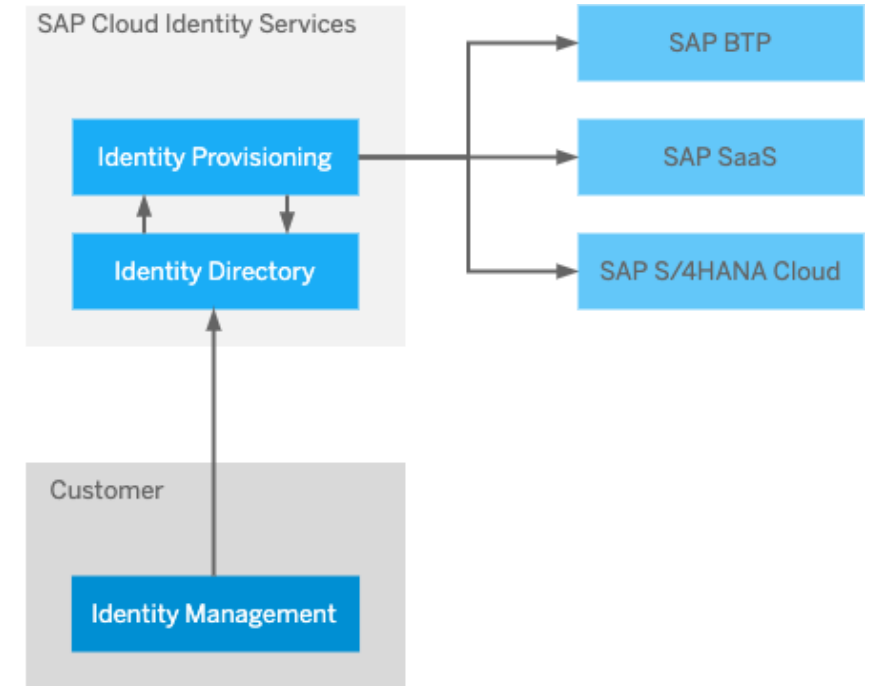
Identity Directory

- The usage of the Identity Directory simplifies how customers are connecting to our SAP SaaS applications, by using it as a central point of truth for the SAP cloud environment.

- A SCIM 2.0 API allows you to programmatically access the identities inside the directory

- APIs for viewing the predefined schemas but also to define own custom schemas with own attributes.

- Up to 20 custom schemas per tenant, each schema having a maximum of 20 attributes. The multivalued attributes (type *complex*) allow 20 sub-attributes.

SAP Cloud Identity Services

Identity Provisioning → SAP BTP

Identity Provisioning → SAP SaaS

Identity Provisioning ↕ Identity Directory

Identity Directory → SAP S/4HANA Cloud

Customer

Identity Management
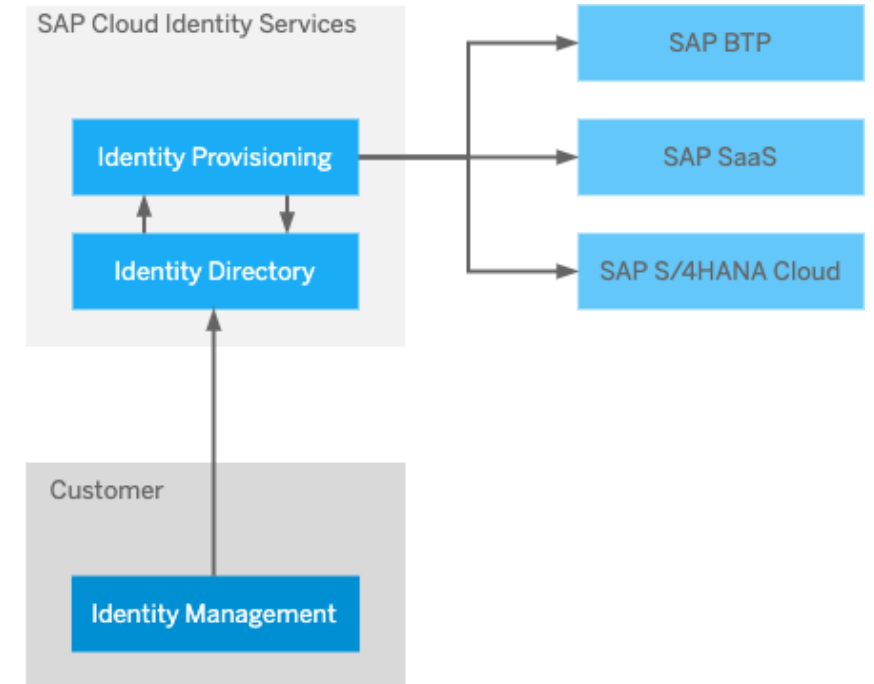
Authorization Management

- Authorization Management Service (AMS) provides a central management of end-user authorizations for business applications based on the SAP Business Technology Platform

- AMS user interfaces for configuration and assignment of policies to users are integrated into the SAP Cloud Identity Services administration console

- AMS is integrated with SAP's development models on SAP Business Technology Platform

- AMS offers a runtime for policy decisions that is integrated with the policy authoring and administration environment

- AMS is based on the existing Identity Directory of SAP Cloud Identity Services and enables customers to manage assignments of policies to users based on the Identity Directory SCIM API

- AMS is part of the SAP Cloud Identity services and does not require dedicated licensing

Assigning policies to user

- In SAP Cloud Identity, every policy has a corresponding group in the identity directory

- Assignment of policies to users is done by making the user a member of the policy group

- Customers can assign SAP-provided or customer-derived policies to users in the Identity Directory:
  - Using the UIs in the SAP Cloud Identity console
  - Using the SCIM API of the Identity Directory

Why to use them?

Why to use them?

Security and integration

- **One point to synchronize user information, enable single sign-on,** and maintain **trust relationships** for cloud solutions from SAP

- **No additional cost*** for usage related to SAP hybrid landscapes

- Delivery of **integrated, ready-to-use, secure** cloud solutions from SAP

- **Identity directory** as **central point of truth for users** with access to SAP's cloud landscape and to meet **compliance** requirements

- **Support and availability** from authentication to transaction – no unclear responsibilities across cloud vendors

Innovate and build

- **Support for innovation** by giving our developers an agreed upon structure that they can use

- **Building extensions** on SAP BTP based on the users maintained in an SAP on-premise system
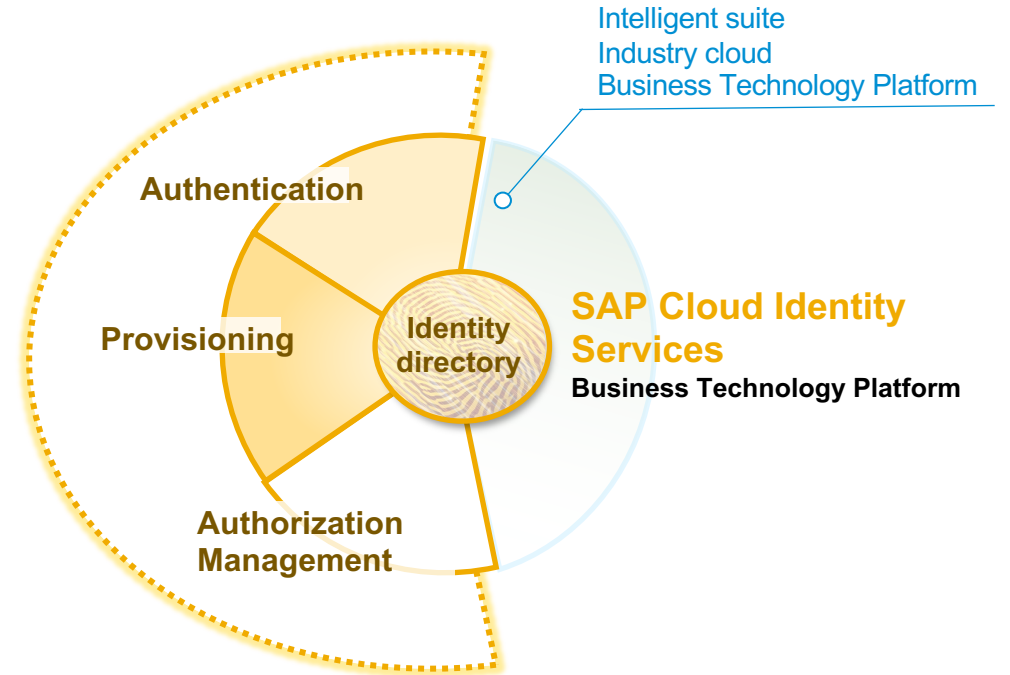
Intelligent suite
Industry cloud
Business Technology Platform

Authentication

Provisioning

Identity directory

Authorization Management

SAP Cloud Identity Services
Business Technology Platform

How would my architecture look like ?

High-level Reference Architecture with the SAP Cloud Identity Services

How ?

- SAP Cloud Identity Services – Identity Directory acts as central user and groups repository

- SAP Cloud Identity Services – Identity Provisioning pre-configuration for SAP Cloud applications provisioning

- The Identity Management solution for on-premise provisioning
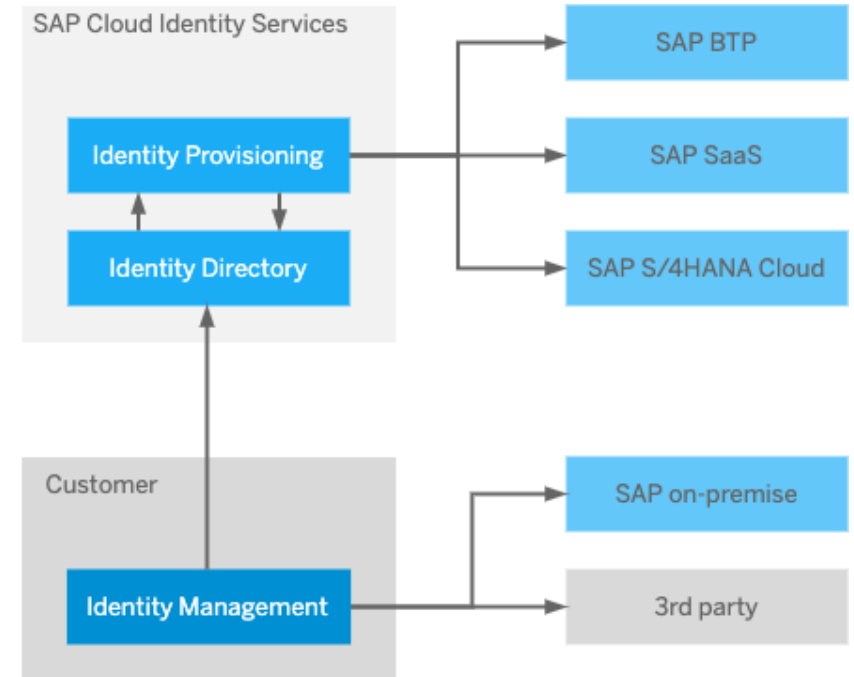
Global User ID
A single common user identifier

- 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**

SAP Cloud Identity Services
Identity Provisioning → SAP BTP, SAP SaaS, SAP S/4HANA Cloud
Identity Directory
SAP SYSUNAME
E-Mail | Login Name | SAP SYSUNAME | P-User | ...
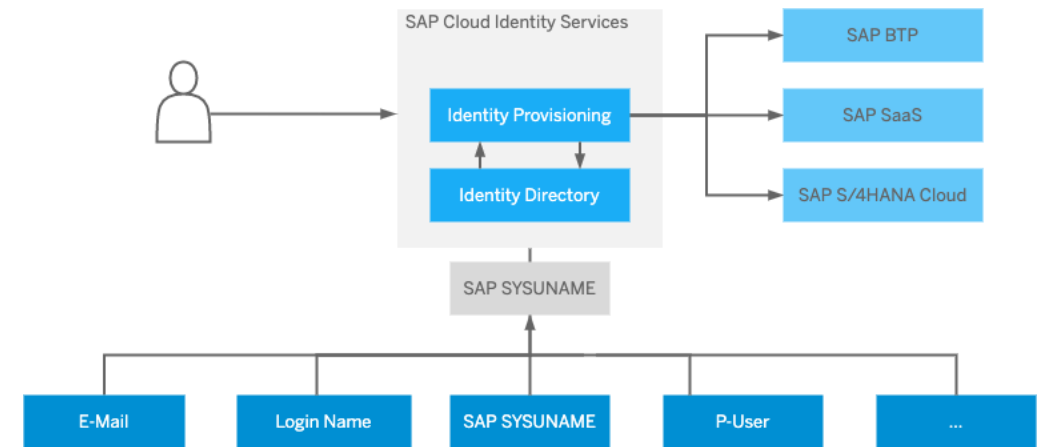
*User Unique Universal Identifier (User UUID)
**As soon as all relevant SAP applications used by the customer support this

see also Global User ID in Integration Scenarios

High-level Reference Architecture with the SAP Cloud Identity Services

Why ?

- Fast adoption of SAP solutions through out-of-the-box integrations (bundles)

- Rapid scenario extensions with optimized SAP connectors

- Reduced point-to-point connections effort

- Modular architecture with fast adoption

- Standard integration with SAP Identity Management available

- SCIM compatible integration with 3rd party Identity Management solutions

- Only one provisioning target for the SAP cloud landscape

- Optimized connectivity for the SAP BTP applications
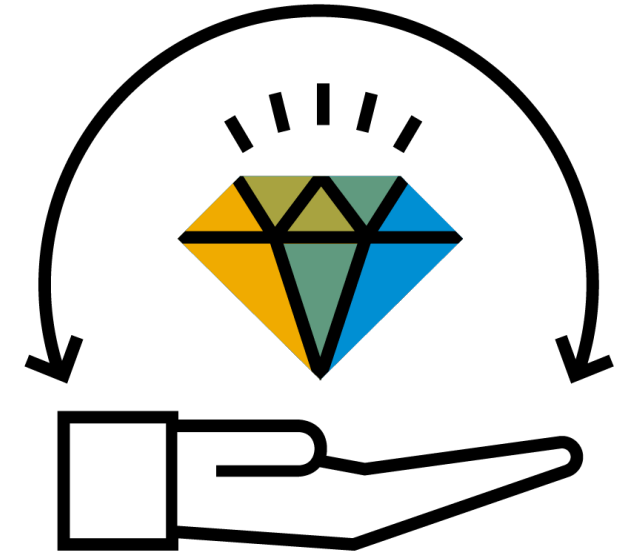
Wrap-up & Feedback

Wrap-up & Feedback
Recent enhancements and future development
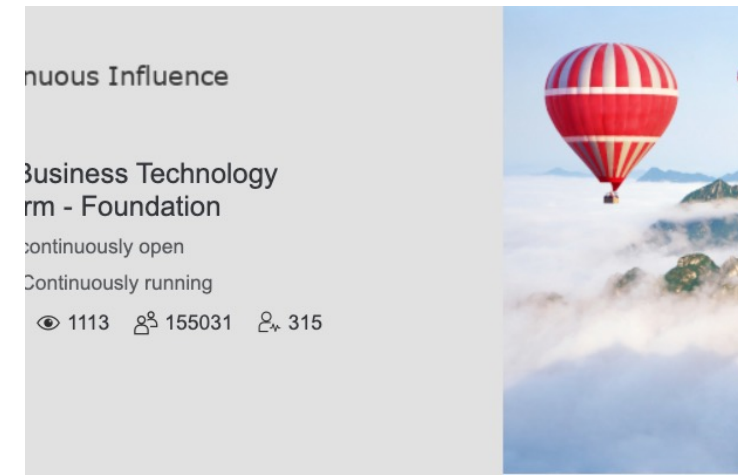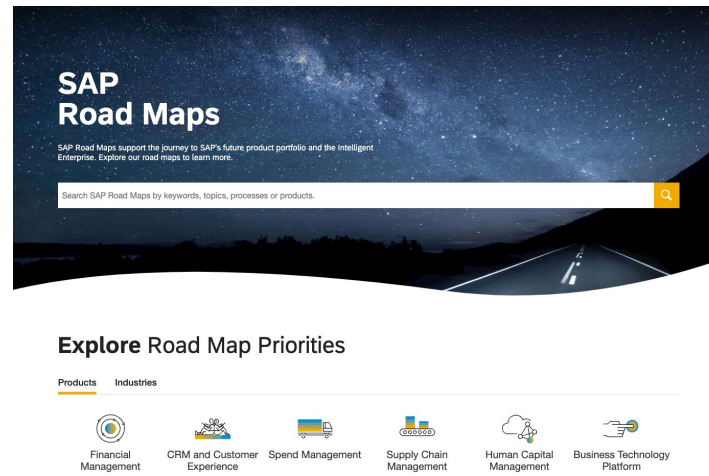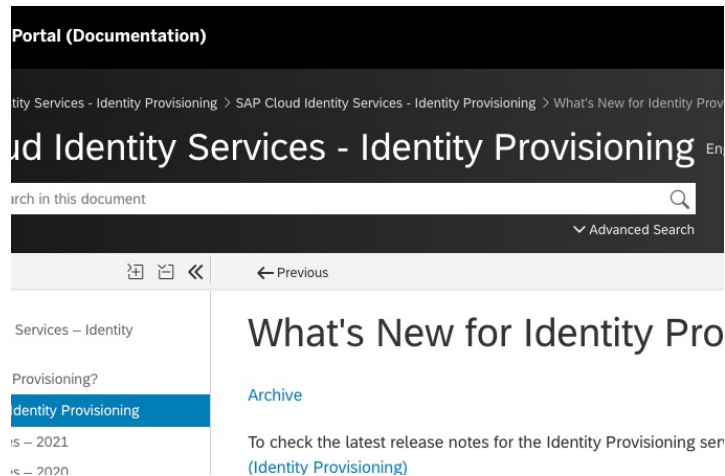
[What's New for Identity Authentication](#)

[What's New for Identity Provisioning](#)

[SAP Cloud Identity Services Roadmap](#)

[Submitting Improvement Requests](#)

Usefull links

Product Infos

- [SAP Community - Identity Services](#)
- [SAP Cloud Identity Services](#)
- [Application documentation IAS](#) - [Application documentation IPS](#)
- [Configuring Authorization Policies](#)
- [Assign Authorization Policies](#)

IAM Strategy

- [System Integration Guide for SAP Cloud Identity Services](#)

Developer Tools & Infos

- [SCIM API Reference](#) (API Hub)
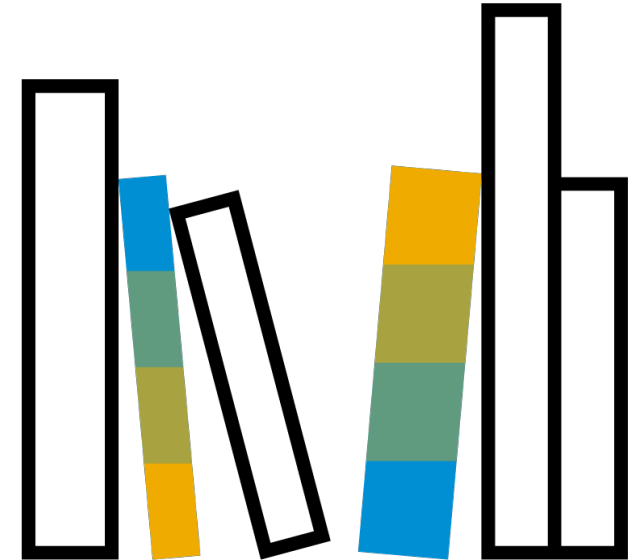
In a nutshell

The Cloud Identity Services are the SAP central point for Identity Access Managemnt in the cloud.

The Identity Authentication service acts as an authentication broker but benefits from the close integration with the rest of the Cloud Identity services.

The recommended way is to use the Identity Directory as a single SAP user & assignment store, in order to allow automation and easier integration.

Optional point to point distribution channels can be manually configured, without laveraging future automation.

SAP Cloud Identity Access Governance integrations offer the full scope control.
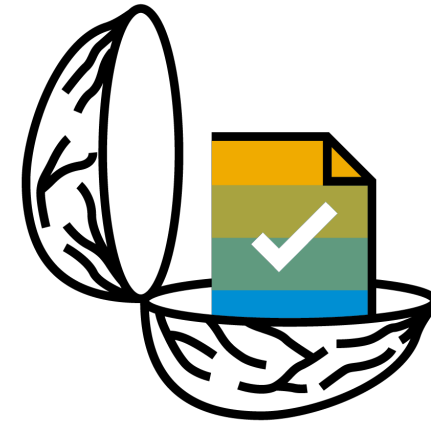
Thank you.
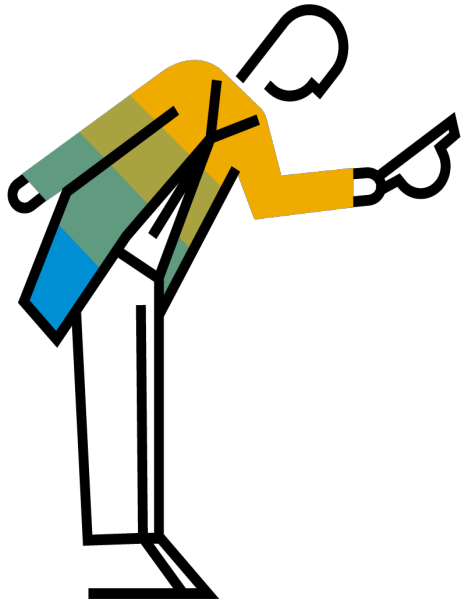
Sonia Petrescu
Security Product Manager

Follow us

THE BEST RUN SAP