SAP InsideTrack
İstanbul
#sitIST
2025

SAP Cloud Identity Services

Abdulbasıt Gülşen
SAP Inside Track İstanbul
10.05.2025

Abdulbasıt Gülşen

❑ SAP BTP Technology/Security Architect

❑ SAP Technology Experience since 2000

❑ SAP Press Author - 100 Things You Should Know About ABAP Workbench (2012)

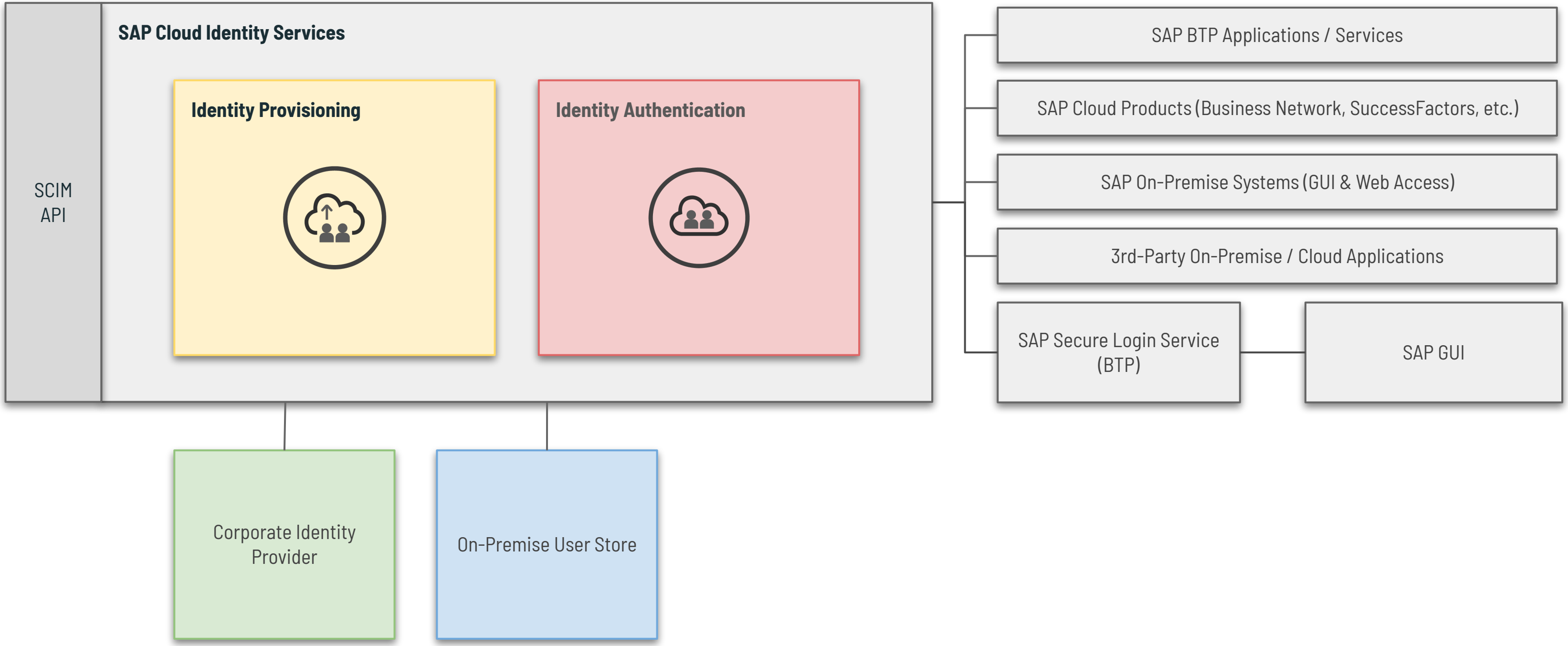
❑ SAP Mentor (2012 -)

abdulbasit@gulsen.net
~~https://x.com/abdulbasitg~~
https://bsky.app/profile/abdulbasit.gulsen.net
https://www.linkedin.com/in/abdulbasitg/

Agenda

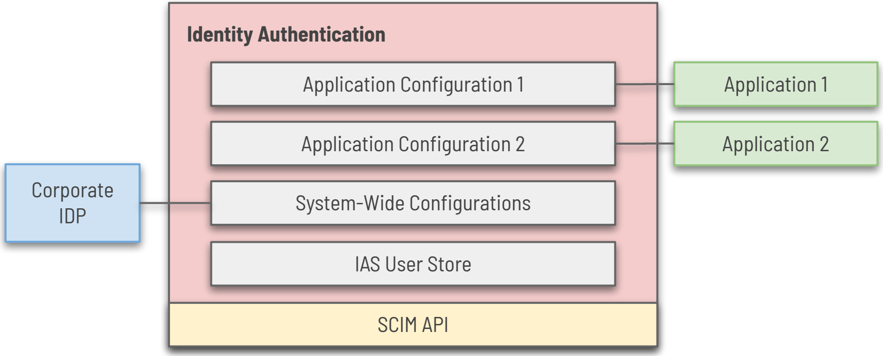
- ❑ SAP Cloud Identity Services - Architecture
- ❑ SAML & OpenID Connect - Overivew
- ❑ Identity Authentication
- ❑ Identity Provisioning

SAP Cloud Identity Services


SCIM
API
SAP Cloud Identity Services
Identity Provisioning
Identity Authentication
SAP BTP Applications / Services
SAP Cloud Products (Business Network, SuccessFactors, etc.)
SAP On-Premise Systems (GUI & Web Access)
3rd-Party On-Premise / Cloud Applications
SAP Secure Login Service (BTP)
SAP GUI
Corporate Identity Provider
On-Premise User Store

SAP Cloud Identity Services are a group of services, designed to enable identity and access management across cloud and on-premise systems. They aim to provide a seamless single sign-on experience for users while ensuring that system and data access are secure.

Identity Authentication – Features & Capabilities



❏ Supports SAML & OpenID

❏ Multi-Factor Authentication (SMS, E-Mail, TOTP)

❏ Social Sign-On (Google, Facebook, X, Linkedin)

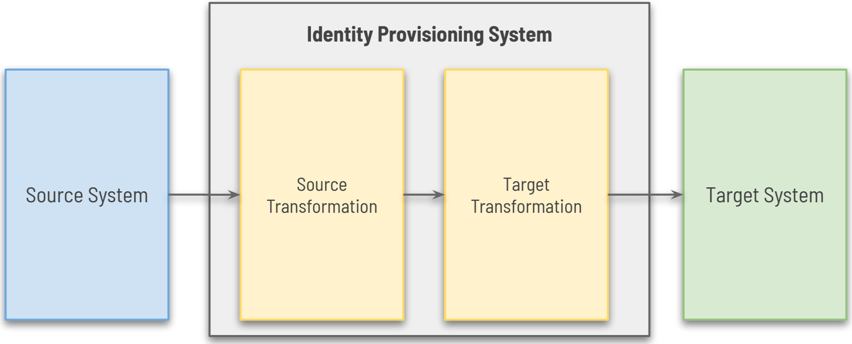
❏ Biometric Authentication

❏ Conditional / Risk-Based Authentication

❏ Custom Password Policies

❏ Application specific branding and layout customization for login screens

Identity Provisioning – Features & Capabilities



❑ Provision users and groups between source and target systems.

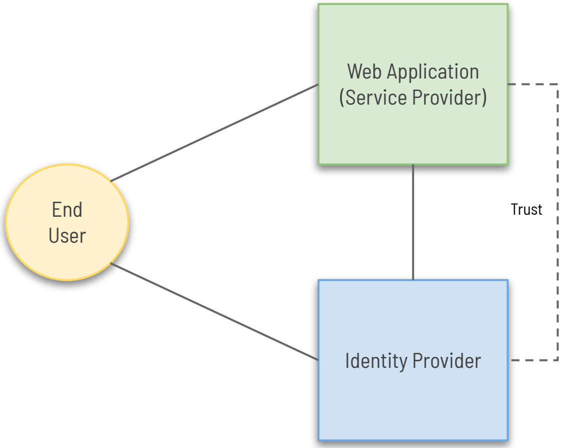
❑ Many SAP & non-SAP systems are supported for source and target.

❑ Any Identity system supports SCIM 2.0 compliant can be used.

❑ Performs complex transformations during provisioning.

❑ Supports scheduled runs to update the changes.

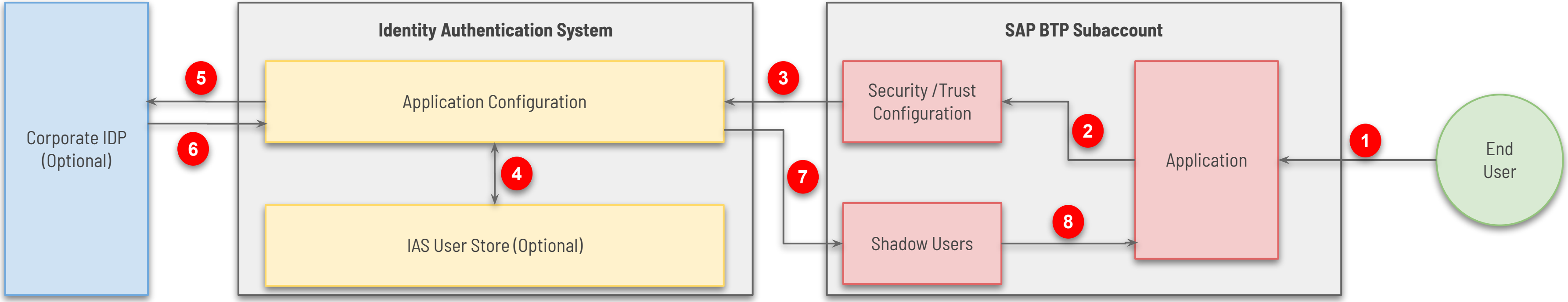
SAML & OpenID Connect



- ❑ Authentication is required when the user attempts to login to a web application. (or service).
- ❑ Web Applications rely on Identity Providers to handle all authentication related operations.
- ❑ **SAML** and **OpenID Connect (OIDC)** are the most common protocols used in the authentication flow for web applications and services.
- ❑ **SAML** (Security Assertion Markup Language) is an open standard used to securely exchange authentication and authorization data between an Identity Provider and Service Provider.
- ❑ **OpenID Connect** is another protocol designed on top of OAuth 2.0 protocol which is also commonly used for exchanging authentication and authorization data between Identity Provider and Service Provider.
- ❑ SAP recommends using **OpenID Connect** on BTP trust level. Applications that require direct authentication with SAP Cloud Identity Services (SAP Build WorkZone, SAP Build Apps) can only be used with **OpenID Connect**.

Identity Authentication

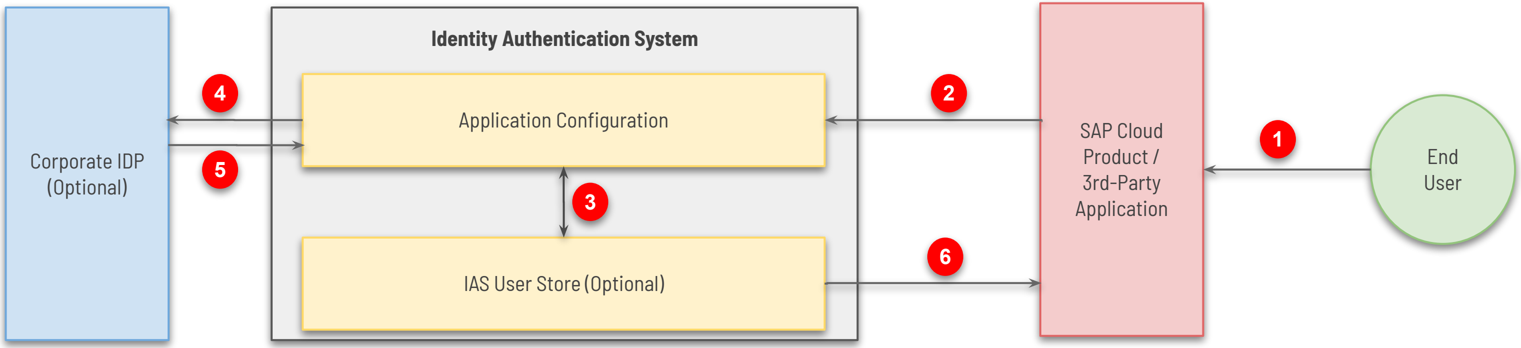
End-To-End Flow with SAP BTP Application



1. End-user tries to access the application.
2. Each BTP subaccounts has a separate trust configuration against IAS (or any other 3rd party identity system) and all applications running in the same subaccount are protected with this trust configuration. Although OpenID is recommended, both OpenID and SAML configurations are possible for authentication process.
3. BTP redirects the authentication request to the IAS and authentication process starts with the application-specific configuration on IAS.
4. IAS can store identities on its own user store. It is also possible to use IAS as a proxy and use the attributes received from the Corporate IDP.
5. If there is a Corporate IDP configured for an application, user is redirected to Corporate IDP to complete the authentication flow. If not, IAS completes the authentication.
6. After authentication process is completed, IAS performs the additional checks, enrichments etc.
7. Users accessing any application on the same subaccount needs to be created as a “shadow user” (if not created already) on a subaccount level. This can be done manually or automatically depending on the use case.
8. Finally application receives the token and authentication flow is completed.

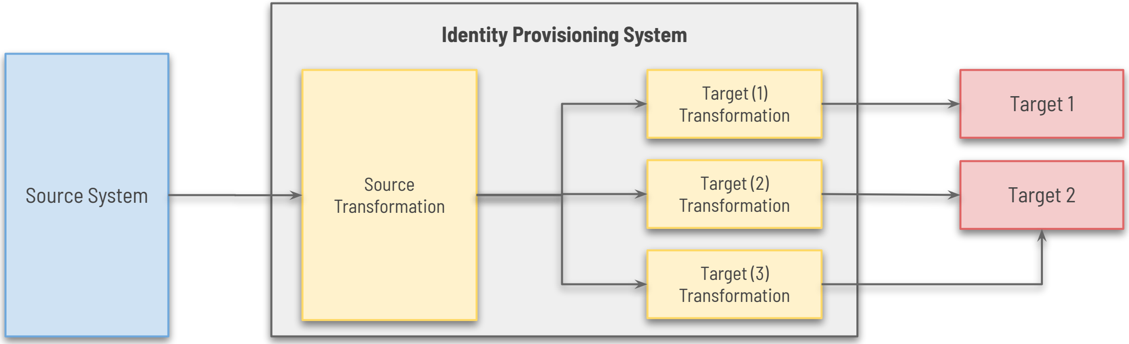
Identity Authentication

End-To-End Flow with SAP Cloud System / 3rd-Party Application


Corporate IDP
(Optional)
4
5
Identity Authentication System
Application Configuration
3
IAS User Store (Optional)
2
6
SAP Cloud
Product /
3rd-Party
Application
1
End
User

1. End-user tries to access the application.
2. Application redirects the authentication request to the IAS and authentication process starts with the application-specific configuration on IAS.
3. IAS can store identities on its own user store. It is also possible to use IAS as a proxy and use the attributes received from the Corporate IDP.
4. If there is a Corporate IDP configured for an application, user is redirected to Corporate IDP to complete the authentication flow. If not, IAS completes the authentication.
5. After authentication process is completed, IAS performs the additional checks, enrichments etc.
6. Finally application receives the token and authentication flow is completed.

Identity Provisioning

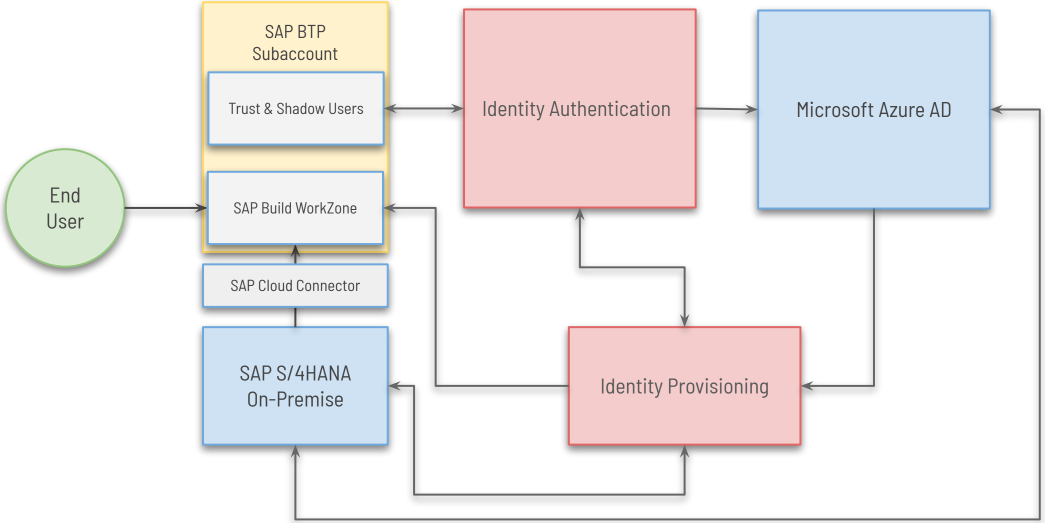

Identity Provisioning System
Source System
Source Transformation
Target (1) Transformation
Target (2) Transformation
Target (3) Transformation
Target 1
Target 2

❏ Any SCIM 2.0 compliant system can be configured as source or target system.

❏ One source system can be transformed and provisioned into multiple target systems with different configurations and mappings.

❏ Several transformation operations can be done in the transformation part.

End-to-End Sample Scenario



Scenario: You want to create a SAP Build WorkZone site for end-users to access Fiori applications on S/4HANA on-premise system.

First, you need to create Trust Configuration on BTP Subaccount and SAP Identity Authentication system to authenticate users via IAS.

Microsoft Azure AD needs to be configured as the Corporate Identity Provider in IAS.

Principal Propagation needs to be configured on Cloud Connector between BTP Subaccount and S/4HANA Backend

Identity Provider System helps us to provision users and authorizations between systems.:

- ❏ IAS Users (and Groups) can be provisioned from Azure AD.
- ❏ S/4HANA Users (and Roles) can be provisioned from IAS or Azure AD.
- ❏ WorkZone Users and Roles can be provisioned from S/4HANA backend
- ❏ BTP Subaccount shadow users can be provisioned from IAS

SAP InsideTrack
İstanbul

#sitIST
2025

Thank You / Q&A

abdulbasit@gulsen.net

~~https://x.com/abdulbasitg~~

https://bsky.app/profile/abdulbasit.gulsen.net

https://www.linkedin.com/in/abdulbasitg/

SAP InsideTrack
İstanbul
#sitIST
2025

/thank you

abdulbasit@gulsen.net
~~https://x.com/abdulbasitg~~
https://bsky.app/profile/abdulbasit.gulsen.net
https://www.linkedin.com/in/abdulbasitg/