SAP Cloud Identity Services
Discovery Center Mission Overview
December 2023
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.
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.
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

<table>
<thead>
<tr>
<th>Organization</th>
<th>Awareness</th>
<th>Security Governance</th>
<th>Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>Regulatory Process Compliance</td>
<td>Data Privacy &amp; Protection</td>
<td>Audit &amp; Fraud Management</td>
</tr>
<tr>
<td>Application</td>
<td>User &amp; Identity Management</td>
<td>Authentication &amp; Single Sign-On</td>
<td>Roles &amp; Authorizations</td>
</tr>
<tr>
<td>Environment</td>
<td>Network Security</td>
<td>Operating System &amp; Database Security</td>
<td>Client Security</td>
</tr>
</tbody>
</table>
SAP BTP - Application layer security

SAP Cloud Identity services
- Identity Authentication service
- Identity Provisioning service

Simplified Authentication and Authorization

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 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

Build securely

Security solutions and features
SAP Cloud Identity Services

Overview

SAP Cloud Identity Services

End User

Identity Authentication

Identity Provisioning

Delegated Authentication

Corporate Identity Provider

User Store

Authentication & Single Sign-On

Identity Lifecycle Management

SAP Cloud Business Applications

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

SAP Cloud Identity Services

Identity Authentication
- Username/password
- Biometric authentication
- X.509
- Kerberos / SPNEGO
- Multi-factor (TOTP, WebAuthn, Email, RSA, SMS)
- Corporate user store

Authentication

Identity Federation

SAML / OpenID Connect

Cloud Connector

Corporate Identity Provider
- Microsoft ADFS / Azure
- 3rd party IdP

On-Premise User Store
- AS ABAP
- MS Active Directory
- LDAP

SAP and non-SAP Business Applications
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
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:

<table>
<thead>
<tr>
<th>Custom Password Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password Policy Name:</strong> Corporate_Policy</td>
</tr>
<tr>
<td><strong>Password Length:</strong></td>
</tr>
<tr>
<td><strong>Password Lifetime:</strong></td>
</tr>
<tr>
<td><strong>Maximum Duration of User Inactivity:</strong></td>
</tr>
<tr>
<td><strong>Number of Last Used Passwords that Cannot Be Reused:</strong></td>
</tr>
<tr>
<td><strong>Number of Allowed Failed Logon Attempts:</strong></td>
</tr>
<tr>
<td><strong>Password Locked Period:</strong></td>
</tr>
<tr>
<td><strong>Password Behavior:</strong></td>
</tr>
</tbody>
</table>
  - [ ] 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](https://www.fidoalliance.org) compatible

### OTP via authenticator app
- 6-digit OTP generated on mobile device
- SAP Authenticator for iOS or Android
- [RFC 6238](https://tools.ietf.org/html/rfc6238) 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

- Member of User Group
- IP-Address Range
- User Type
- Assignment to Application
- Self-registered?
- Email verified?
- Allow
- Deny
- 2-factor 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](#)
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?

- Manual creation
- CSV-upload
- Programmatically through SCIM
- Sync through IPS*
- Self-registration

* 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
SAP Cloud Identity Services
Identity Provisioning
SAP Cloud Identity Services - 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 Identity Services - Identity Provisioning
Management of identities & authorizations
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**

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
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](https://www.linkedin.com)