SAP BTP
Cloud Identity and Security Services

Ian Sulaeman, SAP
Technology Consultant
November, 2022
PUBLIC
Agenda

Overview

Cloud Identity services
- Authentication
- Provisioning

Secure Development services
- Authorization and Trust Management
- Cloud Application Programming Model
- Audit Log

Connectivity services
- Connectivity and Destination
- Cloud Connector

Encryption
- At Rest
- Credential Store
- In Transit
- Custom Domains

Business services
- Data Retention Manager
- Personal Data Manager
- Data Privacy Integration
Overview
Enable every enterprise to become an intelligent, sustainable enterprise
SAP Trust Center
Security, privacy, and compliance – we keep your data safe

Learn about our security and data protection measures, regular compliance checks through internal reviews and audits, and availability of our cloud services worldwide.

- Transparency: Gain insights on service availability worldwide and access cloud service performance history on personalized dashboards
- Explore SAP security products and services
- View data protection guidelines and explore global compliance to data protection laws
- Find global, local and industry specific compliance certificates
- Learn about SAP’s process for cloud service delivery and SAP data centers
- Browse agreements for cloud software, and service offerings from SAP, find SLAs and General Terms and Conditions

More information: SAP.com product page
SAP BTP services certifications and attestations

SAP BTP services and the underlying infrastructure hold various certifications and attestations. The BTP services attestations and certifications can be found under the naming of SAP Cloud Platform in the SAP Trust Center.

SAP BTP runs in secure and certified environments
- World-class data centers
- Advanced network security
- Reliable data backup
- Built-in compliance, integrity, and confidentiality

Infrastructure with 99.9% availability

- For more details, see
  - SAP Data Center
  - SAP Cloud Trust Center
  - Overview of the current service availability

Certifications & Attestations

- ISO 27001 Cert. for Information Security Management Systems
- ISO 22301 Business Continuity Management
- SOC 1 SSAE 18, SOC 2 Type 2
- TISAX Trusted Information Security Assessment Exchange
- FSTEC Federal Service for Technical and Export Control
- C5 (BSI Germany)
Cloud Identity Services
SAP Cloud Identity Services

Overview

SAP Cloud Identity Services

End User

Identity Authentication

Identity Provisioning

Identity Lifecycle Management

Delegated Authentication

Corporate Identity Provider

User Store

Authentication & Single Sign-On

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 provides central user authentication, single Web sign-on, and user management as software-as-a-service. Based on open industry standards SAML 2.0, OIDC, OAuth and SCIM.

Key capabilities
- Simple central configuration
- Flexible configuration options
- Secure authentication with multiple factors
- User management and self-services
- Pre-configured trust configuration
- Out-of-the-box disaster recovery setup

Benefits
- All connected SAP Cloud applications can offer their users the same authentication mechanism
- Flexible integration with customers’ existing IAM infrastructure
- Use as landscape-wide identity provider

Discovery Center : Identity Authentication
SAP Cloud Identity Services - Identity Authentication

Detailed view

SAP Cloud Identity Services

Identity Federation

Authentication

Identity Authentication

Username/password
X.509
Kerberos / SPNEGO
2FA (TOTP, WebAuthn, RSA, SMS)
Corporate user store

SAML / OpenID Connect

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
SAP Cloud Identity Services - Identity Authentication

SAP BTP user access

- S-User accounts
- User base owned and managed by SAP
- Fixed password policy
- Non-configurable MFA* for SAP BTP Cockpit and console client access

SAP BTP

https://accounts.sap.com

- Default
- Configurable

SAP ID Service

- Your Application
  - Java or SAPUI5

BTP Cockpit

Console Client

https://<tenantid>.accounts.ondemand.com

- Default
- Configurable

IAS tenant user store

On-premise user store (e.g. AD)

End users / Platform users

- Full user and group lifecycle management
- Integration with on-premise user store
- Configurable password policy
- Risk-based MFA*
- Customizable user interface
- ...

IAS tenant user store

On-premise user store (e.g. AD)

SAP Cloud Identity Services

Identity Authentication

- Multi-Factor Authentication

© 2022 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC
SAP Cloud Identity Services – Identity Provisioning

SAP Cloud Identity Services, Identity Provisioning offers a comprehensive, low-cost approach to identity lifecycle management in the cloud.

Key capabilities
- Integrated with SAP Identity Management for hybrid landscapes and for non-SAP IDM solutions using the SCIM* standard
- Dedicated connectors for important 3rd party cloud platforms
- Policy-based assignments
- Mapping between identity models
- Simple and agile on-boarding of users and applications
- Support of industry standard protocol SCIM*

Benefits
- Integration option for on-premise and cloud identity lifecycle management
- Focus on the SCIM industry standard for provisioning identity data
- Extended coverage of source and target systems

*System for cross-domain identity management

Discovery Center: Identity Provisioning
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
Secure Development Services
SAP Authorization and Trust Management Service

XSUAA

Authorization Service is the central service in SAP BTP, CF environment for authorization. It allows to confine access to eligible persons or system users. Primary use case are the authorization of business users and system to system authorization and authentication. Authorization Service is also known as XSUAA (eXtended Service UAA).

Key capabilities

▪ Authorization of business users
▪ Authentication and Authorization of system to system communication
▪ Use of standards like SAML, Oauth, JWT tokens

Benefits

▪ Integration with SAML Identity Provider (IDP) from SAP (IAS) or non-SAP

SAP BTP

INTERNET

Business User

App Router

Your Application

Backend services

Authorization Service

XSUAA

SAP Cloud Identity Services

IAS

Discovery Center: Authorization and Trust Management Service
SAP Authorization and Trust Management Service

User Management

Key capabilities

- Authorization management support for platform and business users within our different environments
- Configurable authorization assignments to users defined within the SAP BTP cockpit or assigned during runtime with identity federation supported by the SAML 2.0 standard
- Structured authorization assignments with support of role collections

Benefits

- Flexible authorization management
- Fast implementation of authorization management
SAP Authorization and Trust Management Service
User, Role & Role Collection

Role Collection

User is assigned to (static OR federated assignment)

Role

is assigned to (static assignment)

Scopes Attributes

Administrator

Administrator Developer

© 2022 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC
SAP Authorization and Trust Management Service
Roles and Scopes
SAP Authorization and Trust Management Service
xs-security.json – Designtime / Developer

```json
{
    "xsappname": "sec161-teched-instance-based-auth",
    "scopes": [
        {
            "name": "$XSAPPNAME.Edit",
            "description": "Edit scope"
        },
        {
            "name": "$XSAPPNAME.Delete",
            "description": "Delete Scope"
        }
    ],
    "attributes": [
        {
            "name": "country",
            "description": "country",
            "valueType": "s"
        }
    ],
    "role-templates": [
        {
            "name": "Editor",
            "description": "Editor for Project Documentation",
            "scope-references": ["$XSAPPNAME.Edit", "$XSAPPNAME.Delete"],
            "attribute-references": ["country"]
        }
    ]
}
```

Role Template: "Editor"

**SCOPE:** "Edit"
**SCOPE:** "Delete"

**ATTRIBUTE:** "Country"
SAP Authorization and Trust Management Service
User, Role & Role Collection  Runtime / Admin

Role Collection

is assigned to
(static OR federated assignment)

User

is assigned to
(static assignment)

Role

SCOPE: "Edit"
ATTRIBUTE: "DE"

Role Template: "Editor"

Administrator

Role: "Editor_project"
An Administrator can define role collections using the administrative UIs.

Multiple roles from different applications can be assigned to a single role collection.

Using the CF Cockpit, a role collection can be assigned to a user or mapped to a SAML Group.
SAP Authorization and Trust Management Service
Federated role assignment

Users in department „Sales“

- Assigned by mapping rule

Users in department „Controlling“

- Assigned by mapping rule

SAP BTP

- Group „SalesEmployees“
  - Role „Manager“ (Application A)
  - Role „AccountExec“ (Application B)
- Group „Finance“
  - Role „Controller“ (Application A)
SAP Authorization and Trust Management Service
Sources for federated role authorizations

<Response ...>
  ...
  <NameID>jdoe</NameID>
  ...
  <Attribute Name="Groups">
    <AttributeValue>Sales</AttributeValue>
  </Attribute>
  ...
</Response>
Principal propagation allows the seamless access to resources without needing to provide the identity every time. Users can be verified against the called system using principal propagation. The called system can be other cloud or on-premise solutions. Depending on the solution different scenarios are used.

**Scenarios**
- CF app to CF app
- CF app to on premise SAP system
- CF app to 3rd party cloud app
- CF app to SAP Cloud solution

*Help.sap.com: Propagate User Information Between Applications or Services*
SAP Cloud Application Programming Model

SAP Cloud Application Programming Model (CAP) is an integrated framework of tools, languages, and libraries for building extension applications in a full-stack development approach. Build multi-tenant enabled extensions using CAP and be guided by best practices so you can focus on your domain expertise.

Benefits

- Efficient and rapid development
- Minimal complexity of models and code
- No lock-in to specific language, DB and tools
- Full-stack development from persistence to UI
- Cloud native platform services integration
- 1st-class support for S/4HANA extension scenario
- Built-in security qualities
SAP BTP

APIs to develop secure software

SAP BTP offers various APIs to develop secure software applications.

A suite of services for user authentication and lifecycle management: SAP Cloud Identity Services

Manage application authorizations and trust for SAP BTP: SAP Authorization and Trust Management Service

Functionality for subaccount members managing: Platform Authorizations Management API

Manage destinations and securely connect to on-premise systems: SAP Connectivity Service

Managing passwords and keys: SAP Credential Store Service

Functionality for retrieving audit logs: Audit Log Retrieval API
SAP Audit Log Service

SAP Audit Log Service records security-related system information such as user record changes and unsuccessful logon attempts. Records that are considered as relevant for auditing can be retrieved by the customer SIEM* system via the audit log retrieval API.

Key capabilities
- Protected against unwanted access
- Keeps a record of security-related activities
- Provides a REST-based retrieval API
- Audit Log Viewer for platform and customer auditors

Benefits
- Recording of audit relevant activities
- Providing a higher level of transparency
- Enables the reconstruction of a series of events

*SIEM = Security Information and Event Management

SAP Audit Log Service, API
Connectivity
SAP Connectivity and Destination Service

SAP Connectivity Service allows cloud applications running on the SAP BTP to access remote services securely that run on the Internet or on-premise.

Key capabilities
- Consume APIs and data from APIs and data provided by any Internet service via HTTP(s) using destinations
- Consume APIs, data and users provided by on-premise systems via HTTP, RFC, or even with TCP using destinations and the Cloud Connector

Benefits
- Separation of concerns
- Security
- Re-useability
- Access via Tools

Discovery Center: Connectivity Service
Discovery Center: Destination Service
SAP Cloud Connector

The SAP Cloud Connector establishes a secure VPN connection between the SAP Business Technology Platform and on-premise systems.

**Key capabilities**
- Fine grained access control lists of allowed cloud and on-premise resources
- Fine grained audit logging for traceability
- Principal propagation from cloud to on-premise
- Trust relation with on-premise system based on X.509 certificates

**Benefits**
- No change in the existing corporate firewall configuration is needed.
- He initiates encrypted connections to cloud application from inside the on-premise network to the cloud
- Firewall and DMZ remain unchanged

Blog: Cloud Connector Setup
Encryption
SAP BTP Services use the storage encryption of persistence services. They often use the IaaS layer underlying the SAP BTP. This is configured in the respective IaaS accounts used by SAP BTP. Encrypted backups are stored in a persistence using a strong encryption algorithm.

All these keys are stored in a key management service provided by the underlying IaaS layer.

- AWS encryption
- Azure encryption
- GCP encryption

Data Encryption Strategy (help.sap.com)
SAP Document Management Encryption

SAP Document Management uses the hyperscaler offerings. For example, Postgres for metadata storage, and S3 and Blob Store for Content storage on AWS via Object store. SAP ObjectStore uses default server-side encryption that involves AWS managed keys only. AWS itself generates, encrypts and rotates keys for data encryption. This is configured in the respective IaaS accounts used by SAP BTP.

Regarding backup, ObjectStore-aaS enables the respective hyperscaler offerings.

SAP uses the AWS managed keys (SSE-S3) stored in AWS Key Management Service. AWS itself generates, encrypts and rotates keys for data encryption. How it does so is totally abstracted from SAP.

- Data Encryption Strategy (help.sap.com)
- AWS encryption

SAP BTP Service Stack

Applications

App services

DB services

OS management

Orchestration and account configuration

Administration platform & API management

Provide HW incl. setup

Provide DC facility

Scope of service providing organisation

SAP or other

Scope of SAP certifications and attestations

- Service Fabrik with services MongoDB, PostgreSQL, RabbitMQ, Redis
- Object Store service

Scope of IaaS provider certifications & attestations

- Block Store
- Blob Store on AWS, Azure, GCP

© 2022 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC
HANA Cloud (managed by SAP)
Comprehensive encryption

**Communication encryption**
Encrypt data in transit using TLS/SSL

**Data at rest encryption**
Encrypt data stored on disk using data volume encryption and log encryption

**Backup encryption**
Encrypt backups with SAP HANA native functionality
SAP Credential Store

SAP Credential Store service provides a secure repository for credentials (passwords, keys) to the applications hosted on SAP BTP, CF environment. Customers can use them in various cryptographic operations such as signing and verifying of digital signatures, encrypting and decrypting messages, and performing SSL communication.

**Key capabilities**
- Secure storage of data objects ensuring confidentiality and integrity
- Secure key management, such as storage, exchange, use and deletion
- Audit logs are written in the customer subaccount

**Benefits**
- Compliance to several standards can be achieved
- Keys can be shared between interconnected applications

**Diagram:** SAP BTP, CF environment

- SAP BTP subaccount
- Credential Store Service
- Key Management Service
- BTP Cockpit
- Space Developer
- CLI
- Database (Mongo DB)
- PostgreSQL
- Service Broker

**Discovery Center:** SAP Credential Store
SAP BTP - Encryption in Transit
Transport Layer Security (TLS) Connectivity Support

SAP BTP uses encrypted communication channels based on HTTPS/TLS, supporting TLS version 1.2 or higher.

TLS versions 1.0 and 1.1 are no longer supported.

Make sure you use HTTP clients (such as Web browsers) that support TLS version 1.2 or higher for connecting to SAP BTP.

It is possible to opt-in for the use of TLS 1.3 in the Custom Domain Manager. This allows the use of TLS1.3 with Applications running on SAP BTP.

SAP Custom Domain Service

The Custom Domain Certificates self-service comes with a convenient command line interface plugin and a REST API that allows customers to provide the TLS server certificates needed for use with their custom domains (example, https://myApp.MyDomain.com).

Key capabilities
- Self-service to manage TLS server certificates and the client trust for custom domains
- CF command line interface (CLI) plugin that provides commands for all needed administrative operations
- Secure generation and storage of cryptographic keys inside the landscape

Benefits
- Enable the use of custom domains for branding purposes by providing the necessary security assets for TLS communication
- PaaS and Saas custom domain support
- Secure communication between your application and clients

Discovery Center: Custom Domain
Busines Services
SAP Data Retention Manager

SAP Data Retention Manager is a reuse service on SAP BTP that supports deletion orchestration of Application data. It allows your Data Protection Officer and your Data Privacy and Protection Specialists to identify

- Data subjects which have completed residence time and can be blocked from regular access and
- Data subjects which have completed retention period and must be deleted

Allow System Administrator to

- Manage the archiving and destruction of transactional data

supporting the “Right to be Forgotten” requirement of the General Data Protection Regulation and other local legal regulations. It helps applications to define residence and retention rules against legal grounds to manage lifecycle of business data.

Capabilities

- **Business Purpose App**
  Maintain Business Purposes defining the legal grounds based on which Personal Data is stored. Define Residence (time after which data will be blocked) and Retention (time after which data will be deleted) Rules

- **Delete Data Subject Information App** – identify list of Data Subjects that can be deleted/blocked as End of Residence is reached

- **Trigger Archiving and Destruction of Transactional Data** without the context of Data Subject

Discovery Center: SAP Data Retention Manager
SAP Personal Data Manager

SAP Personal Data Manager is a re-use service on SAP BTP that supports the DPP information framework. It allows the Customer Service Representative (CSR) to identify data subjects and inform them about which of their personal data is stored and used by an application and process requests from the data subjects regarding their personal data.

Capabilities

- Manager Personal Data
  Find data subjects records and inform data subjects about their personal data used and stored by applications.
- Export of Personal Data in a human-readable or machine readable format
- Create request to correct or delete personal data
- Inform Data Subjects about End of Purpose Date
- Multi-language support

Discovery Center: SAP Personal Data Manager
SAP Data Privacy Integration

SAP Data Privacy Integration service supports applications to reach GDPR Compliance. With the help of the service, applications can ensure that information processing is done in a compliant manner based on a valid business purpose.

Capabilities
- Configure and manage business context/purposes
- Ensure information processing based on business purposes
- Retrieve, correct, and export personal data
- Delete personal data

Benefits
- Data privacy configuration and runtime apps
- APIs for data privacy
- Easy integration through annotations
- Cross-landscape capabilities
- Availability on extension factory project “Kyma” runtime
- End-to-end data privacy

Discovery Center: SAP Data Privacy Integration
Roadmap Explorer – Security

- Authentication and Identity Lifecycle services
- Secure Development services
Further information
Where to find more information

SAP BTP Security

- SAP Business Technology Platform Security Community
- SAP Cloud Identity Services Community
- SAP Security Software Community
- SAP Security Products and Solution Newsletter
- SAP Cloud Trust Center

Learning Topics

- SAP Business Technology Platform Security Documentation
- SAP Cloud Identity Services – Identity Authentication Documentation
- SAP Cloud Identity Services – Identity Provisioning Documentation
- SAP Credential Store Documentation
- SAP Custom Domain Service
- Audit Logging in the Cloud Foundry Environment
Thank you.

Contact information:

Ian Sulaeman
Security Technology Consultant
SAP SE
69190 Walldorf, Germany
ian.sulaeman@sap.com