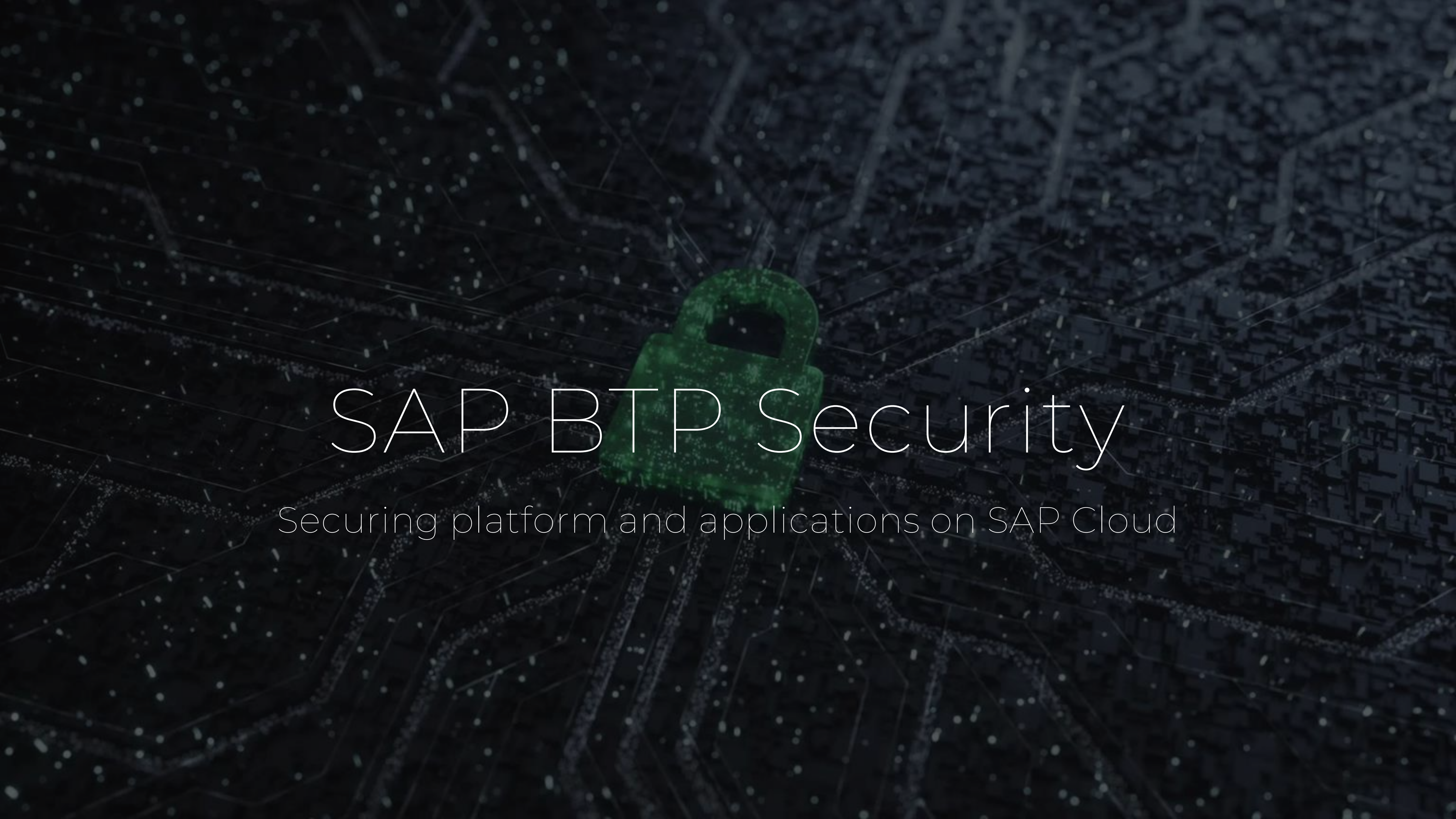


SAP BTP Security

Securing platform and applications on SAP Cloud

Commencement

Introduction

Trainer name: Saurabh Agarwal

Expertise:

- Solution Architecture of SAP Cloud Apps (BTP and allied systems)
- Web and Mobile app development

Experience: 12 years

Skills:

- Cloud - SAP BTP, AWS
- Languages – JavaScript, Java, Python
- Frameworks – Angular, React, Node, UI5, Spring, Django
- Mobile Dev – Flutter, React Native
- SAP – SAP Conversational AI, SAP CDC

Training Agenda

Objective: Understand and appreciate how SAP BTP security works and its various components so that it can be used productively in a project.

S. No.	Subject
1	SAP Business Technology Platform (BTP)
2	SAP BTP security basics
3	SAP Identity Authentication Service (IAS)
4	SAP Identity Provisioning Service (IPS)
5	Securing BTP apps
6	On-premise connectivity
7	End to end application demo
8	Conclusion

General guidelines

Identify Take-aways

It is important to understand trainings objective and identify with it.

Ask Questions

All questions are valid and important. Utilize this opportunity fully and ask as many questions as you can.

Practice → Perfect

Practice makes perfect. Try out the concepts covered in training on your own.

Software requirements

JDK (v1.8_192)

Pre-requisite for using SAP Cloud Connector.

SAP Cloud Connector

Required to integrate BTP applications with on-prem resources.

Postman

REST client. Required for testing API end points.

NodeJS (v14)

For local development and testing of the sample application which will be deployed to BTP.

CF CLI (v7)

Required to deploy apps to BTP. Can also be used to manage the cloud foundry environment from CLI.

IDE

Any IDE to see and write code. E.g. Visual Studio Code, Atom.

SAP Business Technology Platform

Fundamentals Walkthrough

SAP BTP – Overview

SAP Business Technology Platform History

2012

SAP NetWeaver Cloud

2013

SAP HANA Cloud Platform

2017

SAP Cloud Platform

2021

SAP Business Technology Platform

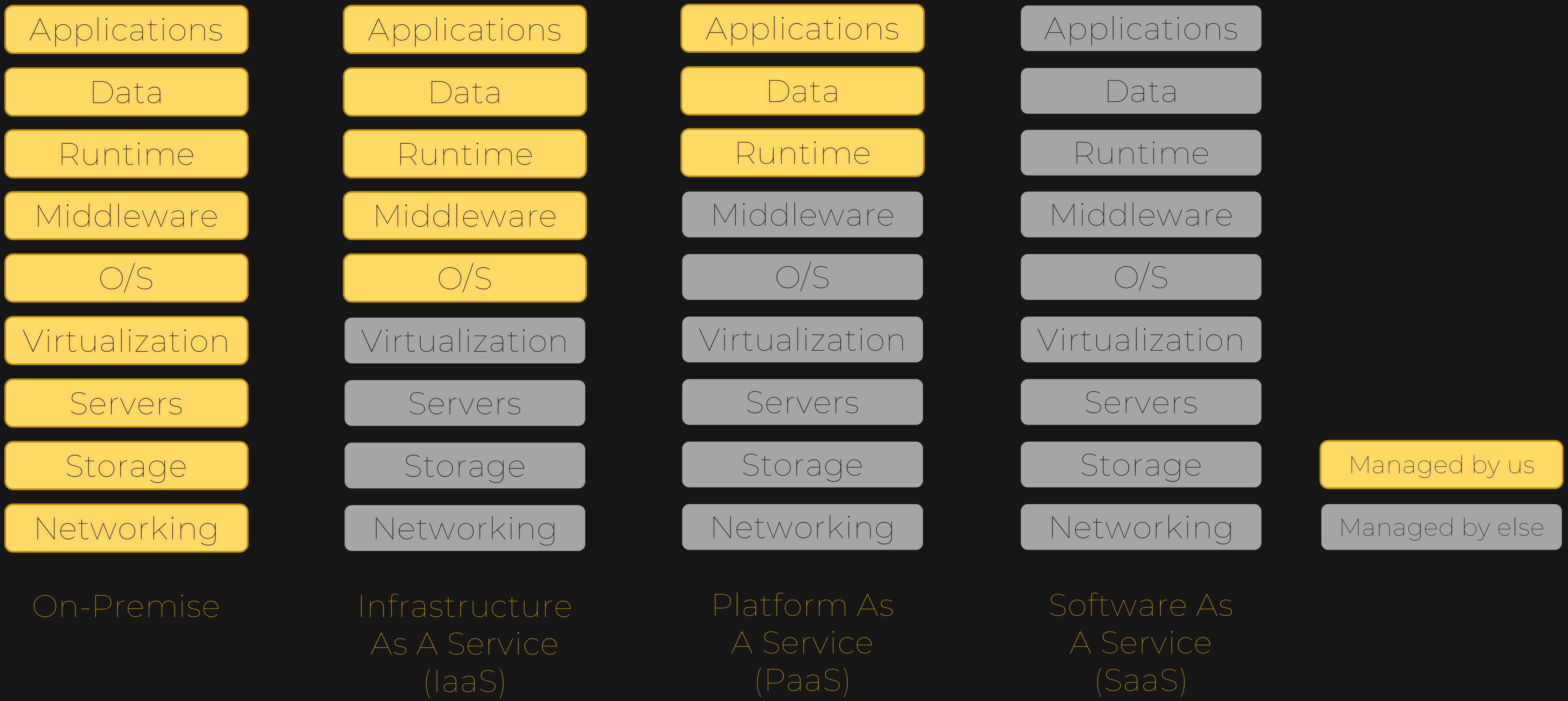
Neo

SAP's infrastructure

Cloud Foundry

Hyperscalars' infrastructure

SAP BTP – Types of Cloud



On-Premise	Infrastructure As A Service (IaaS)	Platform As A Service (PaaS)	Software As A Service (SaaS)
🟨 Applications	🟨 Applications	🟨 Applications	⬜ Applications
🟨 Data	🟨 Data	🟨 Data	⬜ Data
🟨 Runtime	🟨 Runtime	🟨 Runtime	⬜ Runtime
🟨 Middleware	🟨 Middleware	⬜ Middleware	⬜ Middleware
🟨 O/S	🟨 O/S	⬜ O/S	⬜ O/S
🟨 Virtualization	⬜ Virtualization	⬜ Virtualization	⬜ Virtualization
🟨 Servers	⬜ Servers	⬜ Servers	⬜ Servers
🟨 Storage	⬜ Storage	⬜ Storage	⬜ Storage
🟨 Networking	⬜ Networking	⬜ Networking	⬜ Networking

🟨 Managed by us

⬜ Managed by else

SAP BTP – Accounts and Regions

Global Accounts

Entry point into SAP BTP. Based on a commercial model and enables creation of sub-accounts

Sub-Accounts

Regions specific accounts with their own user management, quota of entitlements and environment.

Regions

Various regions spread across the globe to provide low latency to users and cater to data privacy requirements.

Environments

Flavours of SAP BTP – Neo, Cloud Foundry, ABAP, Kyma

Hyperscalars

IAAS to support various functionalities of SAP BTP

Commercial Model

How to pay for the services used?

SAP BTP – Trial account

What is a SAP BTP trial account?

SAP BTP trial account enables people who want to understand the usage of SAP BTP. It provides limited access to the BTP features and services to give a sense of what all can be achieved.

What all services are there in trial account?

SAP BTP free tier gives access to 29 services (as of today)

How to create a trial account?

https://www.sap.com/india/products/business-technology-platform/trial.html

SAP BTP – Cockpit walkthrough

Account Explorer

Explore and manage the various sub-accounts and directories for the global account.

Resource Provider

Register and use non-SAP resources to be used with SAP BTP.

System Landscape

Add various systems in your SAP landscape (such as SuccessFactors, Concur, etc) to enable their APIs' usage within BTP.

Usage Analytics

Provides statistics and costs associated with various sub-accounts, directories and services linked to the global account.

Boosters

Meant for developers – provide guided steps to create applications and use various BTP services.

Entitlements

Shows the services and features that are allowed to be used in the global account. Administrators can manage the entitlements for sub-accounts.

SAP BTP – Global Account Access

Add Users

Add users to the global account.

Assign Role Collection

Assign relevant role collection to user (admin / viewer).

Role Collection	Roles
Global Account Administrator	Global Account Admin, Global Account Usage Reporting Viewer, System Landscape Administrator, User and Role Administrator
Global Account Viewer	Global Account Usage Reporting Viewer, Global Account Viewer, User and Role Auditor

SAP BTP – Services & Entitlements

Services

Features provided by SAP BTP to use in the applications.

Service Plans

Limits for using that particular service.

Service Assignment

See how much quota each service has for the global account.

Entity Assignment

See what all services and plans are assigned to a particular sub-account.

Service Marketplace

See what all services and plans are assigned to a particular sub-account.

Service Instances

See what all services and plans are assigned to a particular sub-account.

SAP BTP – Service instances

Assign Entitlements

Assign service entitlements to a sub-account.

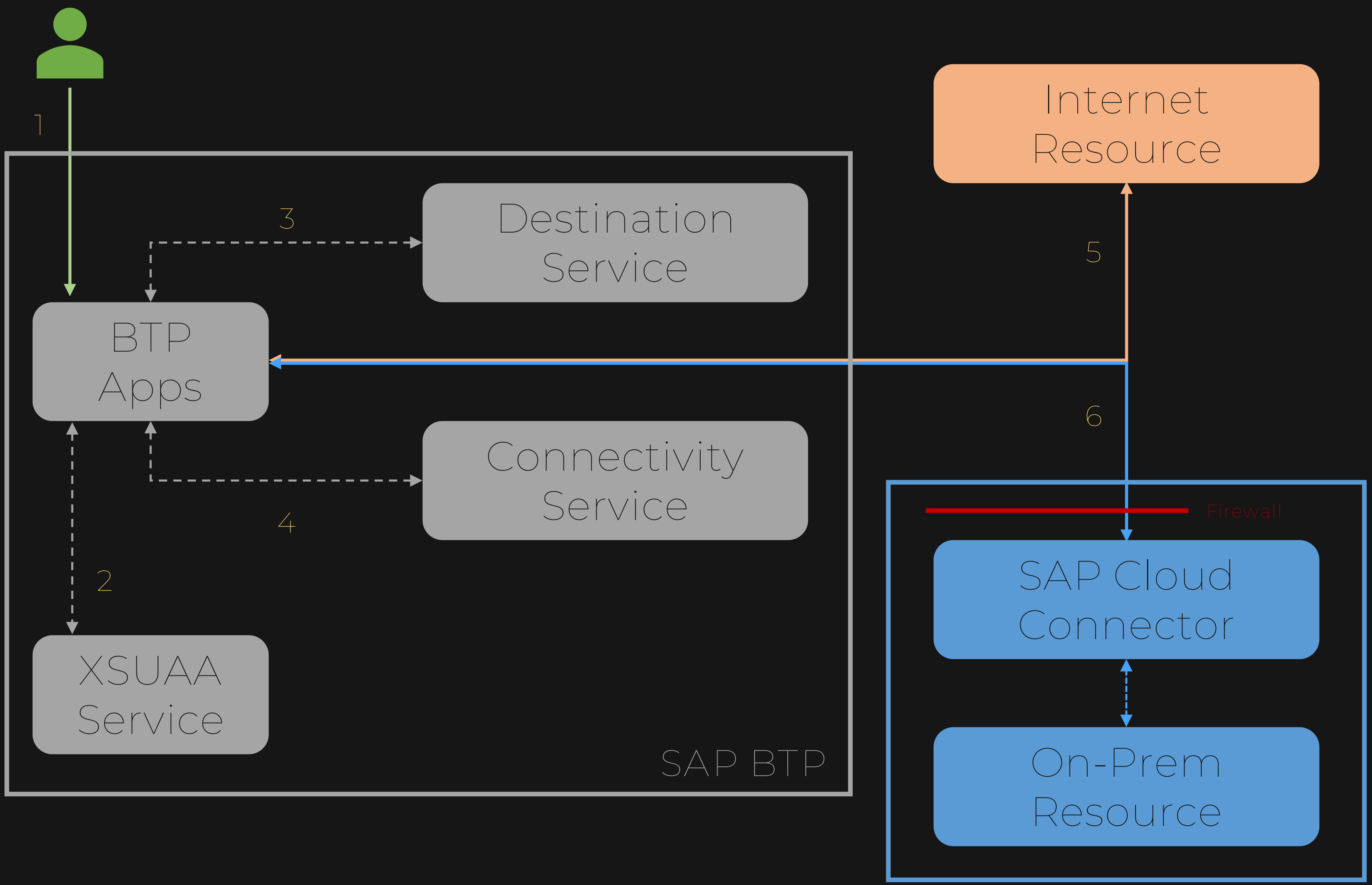
Create Spaces

Create spaces in sub-account to create service instances.

Create instances

Create service instances for the services in a space.

SAP BTP – Connecting other systems



Connection steps

1. User accesses the BTP application.
2. App fetch oAuth token from XSUAA service to use Destination and Connectivity services.
3. App fetches destination config – for on-prem and Internet scenarios.
4. App fetches connectivity config – for on-prem scenario.
5. App connects to the Internet resource using HTTP(s).
6. App connects to the on-prem resource through SAP Cloud Connector.

SAP BTP – Feature Sets

Behaviour	Feature Set A	Feature Set B
Directories	Not applicable	Organize and manage sub-accounts in a tree like structure.
Labels	Not applicable	Categorization and identification of directories, sub-accounts, service instances, etc. Provide additional filtering options.
APIs for SAP BTP	Not applicable	Manage global and sub-accounts using REST APIs.
SAP BTP CLI	Not applicable	Manage global and sub-accounts using BTP CLI. Possibility of automation.
Global account security	No concept of role collections on Global accounts.	SAP provided predefined role collections to fully manage or view the global account. We can create our own role collections using SAP provided roles.
Sub-account security	Admins are directly assigned as security admins. Sub-account and CF org members are directly assigned under the Members tab	Level of access controlled by role collections. SAP provides a predefined list of role collections. Access to CF org is independent of access to sub-account.

SAP Business Technology Platform

SAP BTP Security Basics

BTP Security – Users & Roles

Platform users

User who need to access the global account or the sub-account. They maintain the accounts, access and applications.

Business users

Users who don't need to access the global account or sub-account. They just need access to the business applications.

Roles

Role contain permissions to do a certain task. SAP provides predefined roles on global and sub-account levels. Developers can define their own roles based on the application requirements.

Role Collections

Collection of different roles. SAP provides predefined role collections on global account and sub-account levels. Administrators (global and sub-account) can define their own role collections based on business requirements.

BTP Security – Segregation of duties

Global Account Admins

- Assign permissions to other global account members.
- Manage global account.

Sub-Account Admins

- Assign permissions to other sub-account members and developers.
- Manage sub-account.
- Create role collections for application roles.

Application Developers

- Develop, deploy and test applications in a space in sub-account.
- Create application level security artifacts.
- Covers both technical and functional roles.

Business Users

- Access applications deployed by Developers.

BTP Security – Sub-Account Access

Add Users

Add users to the global account.

Assign Role Collection

Assign relevant role collection to user (admin / viewer).

Provide CF Org access

Assign relevant role collection to user (admin / viewer).

BTP Security – Sub-Account RCs

Just for platform users

Role Collection	Roles
Cloud Connection Administrator	Cloud Connector Administrator
Connectivity and Destination Administrator	Cloud Connector Administrator, Destination Administrator
Destination Administrator	Destination Administrator
Subaccount Administrator	Cloud Connector Administrator, Destination Administrator, Subaccount Admin, Subaccount Service Administrator, User and Role Administrator
Subaccount Service Administrator	Subaccount_Service_Admin
Subaccount Viewer	Cloud Connector Auditor, Destination Viewer, Subaccount Service Auditor, Subaccount Viewer, User and Role Auditor

BTP Security – Overview of UAA

CF UAA

- User Account and Authentication.
- Open source implementation provided by Cloud Foundry.
- Enables Single Sign On.
- Acts as a oAuth server.

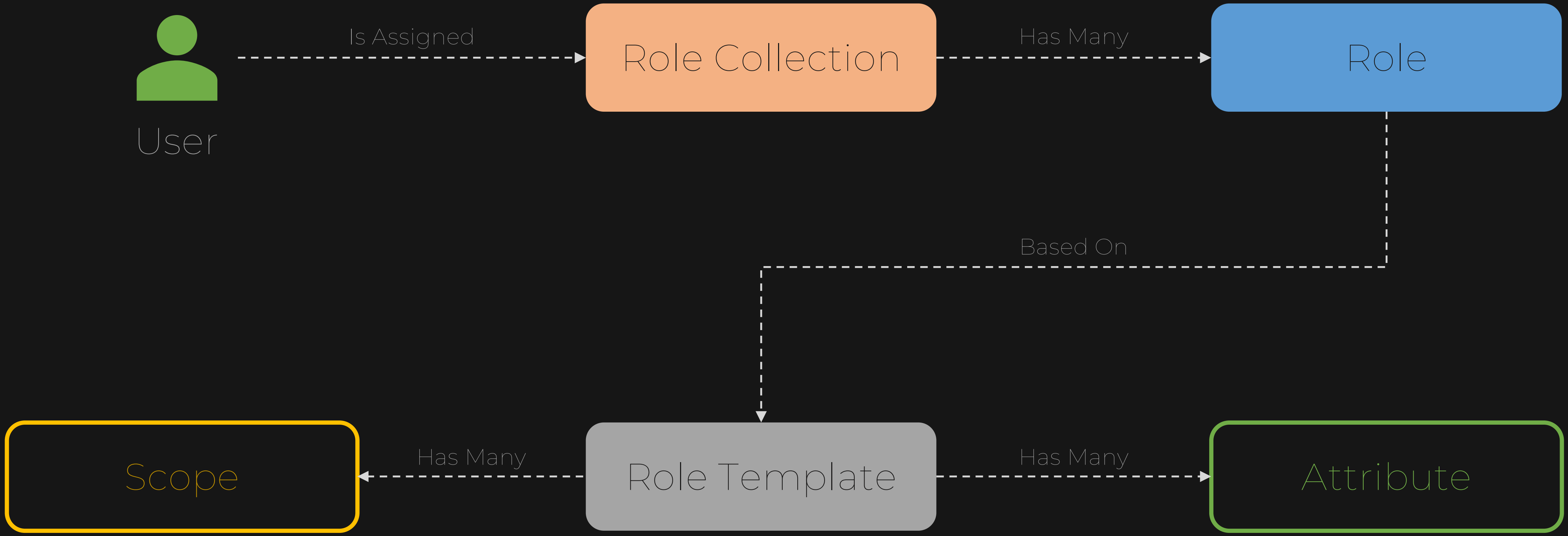
Platform UAA

- UAA auth server required to authenticate the platform users.
- Generates oAuth tokens for platform users to administrate platform.
- Isn't a user store.
- Isn't visible to platform or business users.

XSUAA

- SAP's implementation of CF UAA to be used in SAP realm.
- Generates oAuth tokens for business users to use deployed applications.

BTP Security – Security Artifacts



What is JavaScript Object Notation?

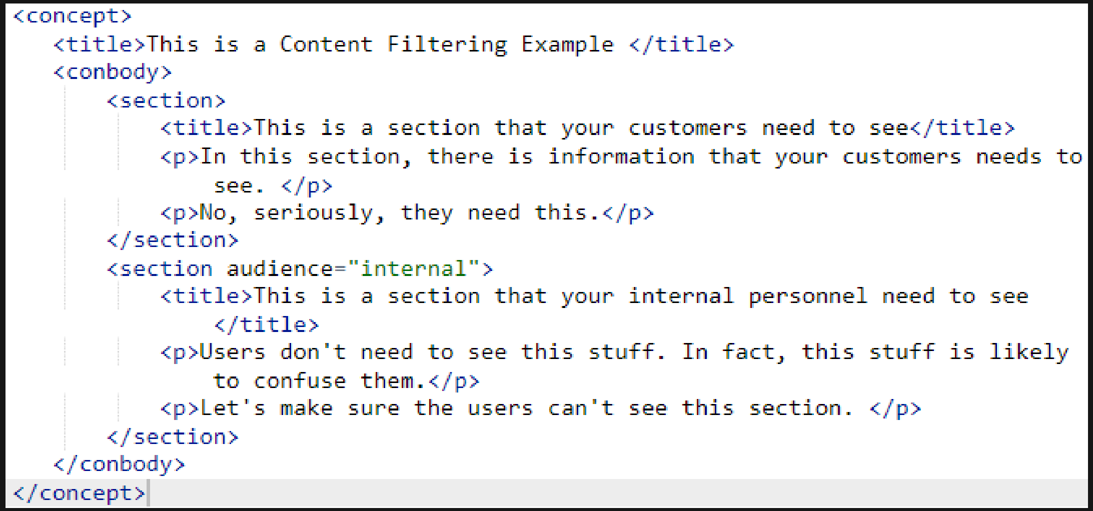
Data Interchange

Machine Readable

Human Readable

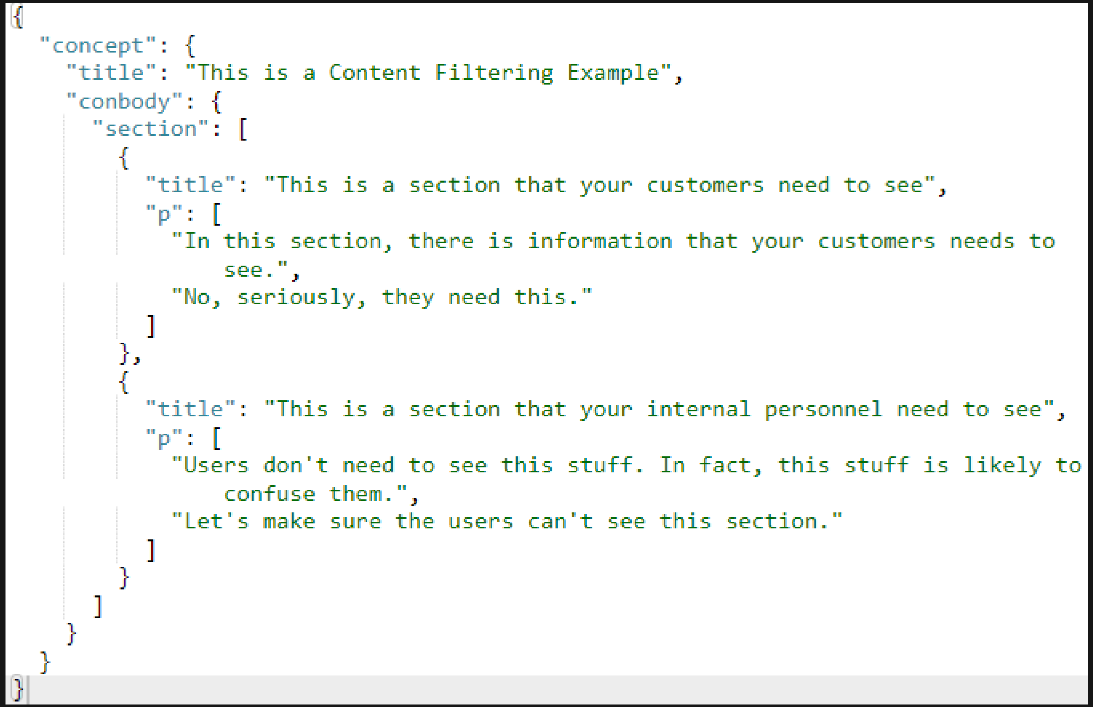
Concise Format

XML



```xml
<concept>
   <title>This is a Content Filtering Example </title>
   <conbody>
       <section>
           <title>This is a section that your customers need to see</title>
           <p>In this section, there is information that your customers needs to
               see. </p>
           <p>No, seriously, they need this.</p>
       </section>
       <section audience="internal">
           <title>This is a section that your internal personnel need to see
               </title>
           <p>Users don't need to see this stuff. In fact, this stuff is likely
               to confuse them.</p>
           <p>Let's make sure the users can't see this section. </p>
       </section>
   </conbody>
</concept>
```

JSON



```json
{
  "concept": {
    "title": "This is a Content Filtering Example",
    "conbody": {
      "section": [
        {
          "title": "This is a section that your customers need to see",
          "p": [
            "In this section, there is information that your customers needs to
                see.",
            "No, seriously, they need this."
          ]
        },
        {
          "title": "This is a section that your internal personnel need to see",
          "p": [
            "Users don't need to see this stuff. In fact, this stuff is likely to
                confuse them.",
            "Let's make sure the users can't see this section."
          ]
        }
      ]
    }
  }
}
```

BTP Security – xs-security.json

✓

Sample Security Descriptor

BTP Security – oAuth overview

oAuth is an authorization protocol used for allowing an application to access resources on behalf of the user. It can be used with browser based applications, mobile applications, server-to-server communications, IoT devices.

oAuth Roles

Resource Owner

System that owns the protected resources. E.g. Business user

Client

System that requires access to protected resources. Access token is must. E.g. Web browser

Authorization Server

Server which authenticates the request from client and grants access token. E.g. XSUAA

Resource Server

Server that protects the resource in question. E.g. Node application

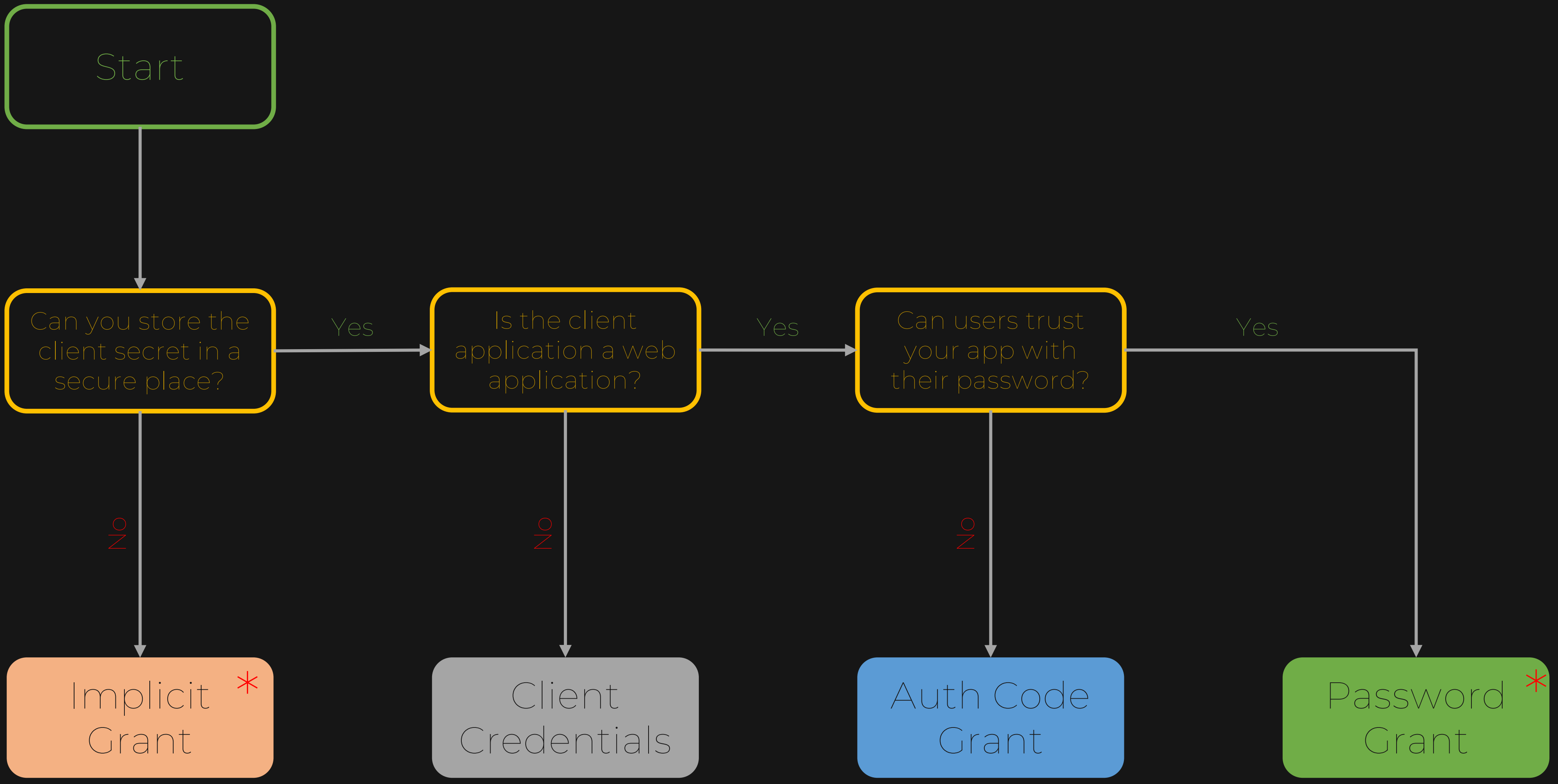
Assignment

With open house session

BTP Security – oAuth flows

oAuth flow	Needs frontend	Needs backend	User interaction	Needs client secret
Authorization Code	✓	✓	✓	✓
Implicit Grant	✓	✗	✓	✗
Client Credentials	✗	✓	✗	✓
Password Grant	✓	✓	✓	✓

BTP Security – oAuth flows cheat sheet


Start
Can you store the client secret in a secure place?
Yes
Is the client application a web application?
Yes
Can users trust your app with their password?
Yes
No
No
No
Implicit Grant *
Client Credentials
Auth Code Grant
Password Grant *

* - Not recommended

SAP Identity Authentication Service

SAP IAS – Overview

SAP IAS is a SaaS solution provided by SAP to allow controlled access to the cloud based business applications. It enables Single Sign-On (SSO), Risk Based Authentication, Self service as well as SCIM API for management.

Features

Authentication & SSO

Authentication using Form, Social, Two factor. SSO using SAML.

Risk Based Authentication

2FA based on user groups, user type and other parameters.

Delegate Authentication

Use a third party Identity Provider as the master user store for authentication

Easy and Versatile Management

Use SCIM API for user and groups management, customize texts and branding.

SAP IAS – Scenarios

B2C

Everyone can access the application, self-registration by new users is allowed.

Administrators

Configure application settings.

Consumer

Self registration before using application.

B2B

Only specified users can access application post account activation. No self registration.

Administrators

Configure application settings and register users.

Partner

Activates the account and uses application.

B2E

Assign relevant role collection to user (admin / viewer).

Administrators

Configure application and onboard employees.

Employee

Activates the account and uses application.

SAP IAS – Users & Authorization

Add users

Users maintained in the IAS tenant can access the applications linked to the IAS tenant.

Add administrators

Administrators can manage the IAS tenant and the applications and users linked to it.

Add user groups

Users can be grouped together to provide access to various business applications and resources.

SAP IAS – Adding Applications

Add new application

Features provided by SAP BTP to use in the applications.

Establishing Trust

Limits for using that particular service.

Trusted Domains

See how much quota each service has for the global account.

Risk Based Auth

See what all services and plans are assigned to a particular sub-account.

SAML 2.0 config

See what all services and plans are assigned to a particular sub-account.

Password Recovery

See what all services and plans are assigned to a particular sub-account.

SAP IAS – Tenant Settings

Logo

Features provided by SAP BTP to use in the applications.

MFA

Limits for using that particular service.

Trusted Domains

See how much quota each service has for the global account.

Risk Based Auth

See what all services and plans are assigned to a particular sub-account.

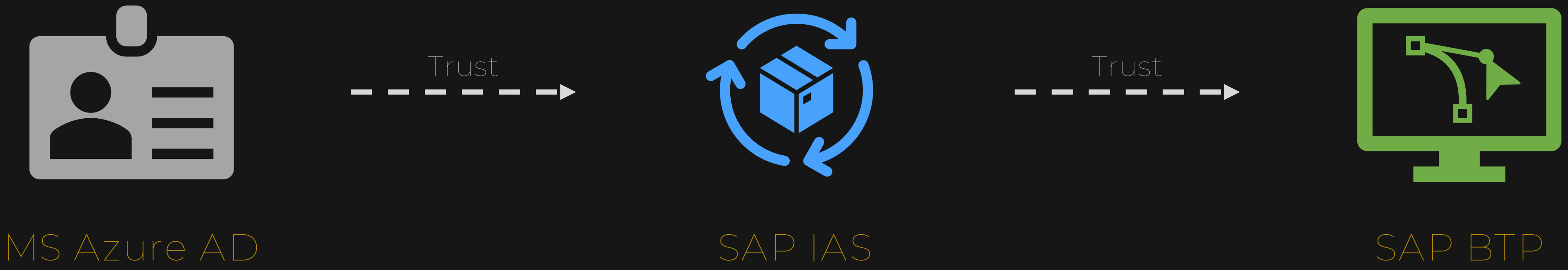
SAML 2.0 config

See what all services and plans are assigned to a particular sub-account.

Password Recovery

See what all services and plans are assigned to a particular sub-account.

SAP IAS – MS AAD Corporate IdP



SAP IAS – SCIM APIs

Within the BTP application configured in IAS tenant go to Trust → Client Authentication

Create a client secret for the client application.

Use client id (username) and client secret (password)

SAP IAS – Two factor authentication

For the IAS Tenant

1. Go to Tenant settings.
2. Go to Multi-Factor Authentication.
3. Turn on Multi-Factor Auth option.

When logging into the IAS tenant,

1. Use SAP Authenticator to link the tenant.
2. Once linked SAP Authenticator will provide TOTPs which will be used as passcode.

For an application

1. Go to the application in question.
2. Go to Authentication and Access.
3. In Risk-Based Authentication either,
    1. Create a new rule for 2FA
    2. Enable 2FA by default

When logging into the application,

1. Use SAP Authenticator to link the tenant.
2. Once linked SAP Authenticator will provide TOTPs which will be used as passcode.

SAP Identity Provisioning Service

SAP IPS – Overview

SAP IPS is a SaaS solution provided by SAP to allow management and automation of lifecycle process of identities.

Features

User & Group Provisioning

Provision users and groups between various SAP and Non-SAP systems.

User & Group Filtering

Configure transformations and filtering properties to fine tune provisioning.

Full & Delta Read Mode

Provisioning job can run in full or delta mode to read all or only the changed identities.

Job Logging & Notifications

View and export job logs. Get notified for status of provisioning jobs.

SAP IPS – Concepts

Systems

Source, Target and Proxy systems used for provisioning.

Properties

Properties control the connection to systems and behavior of the provisioning job.

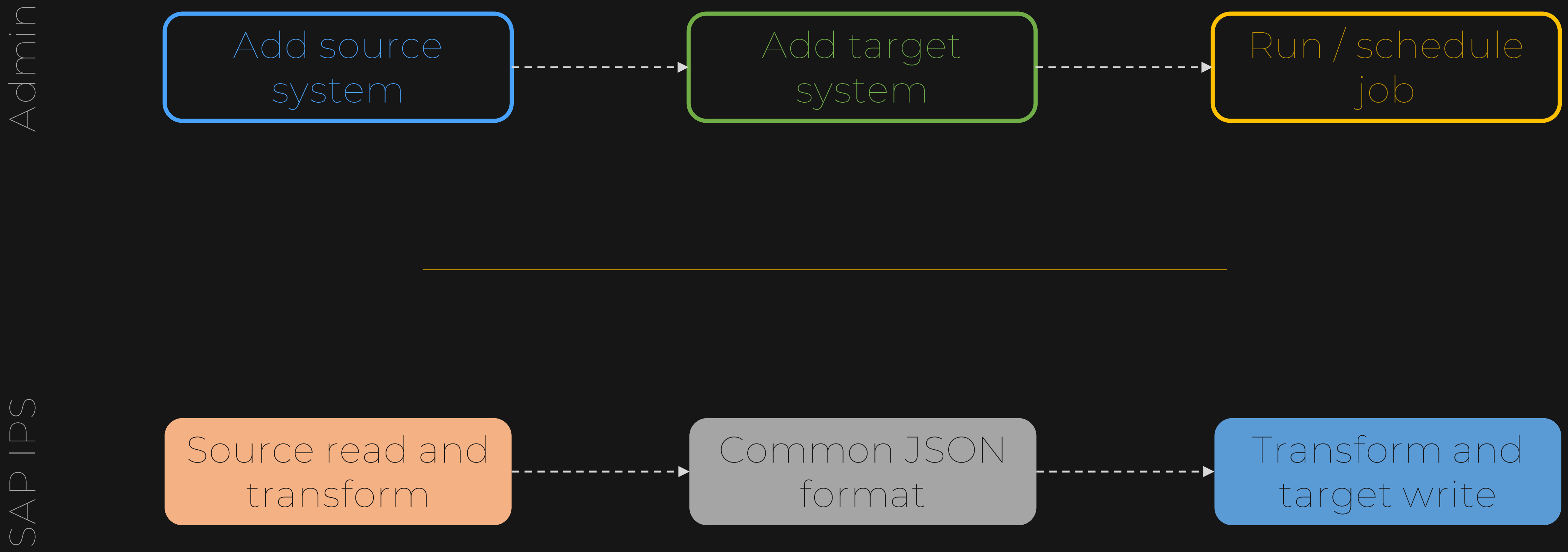
Transformations

Read (source) and write (target) transformations allow conversion of identities from one format to another.

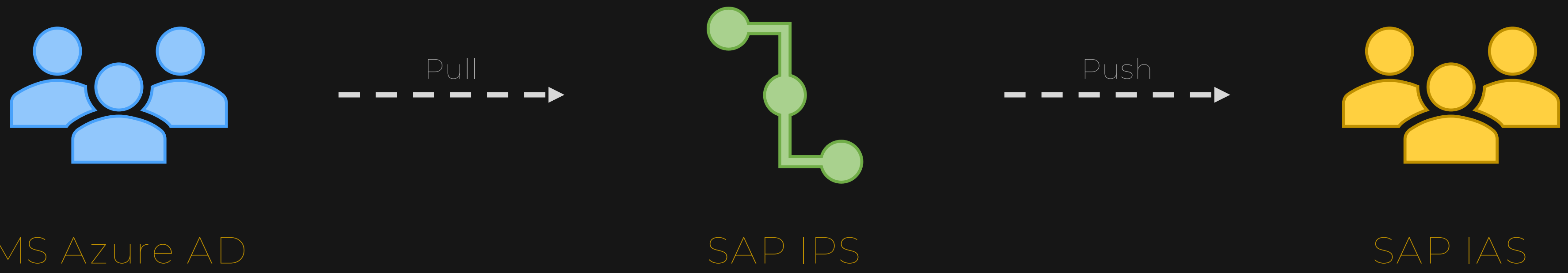
Jobs

Scheduled or ad-hoc on source system provisions identities in all relevant target systems.

SAP IPS – Process overview



SAP IPS – Hands on

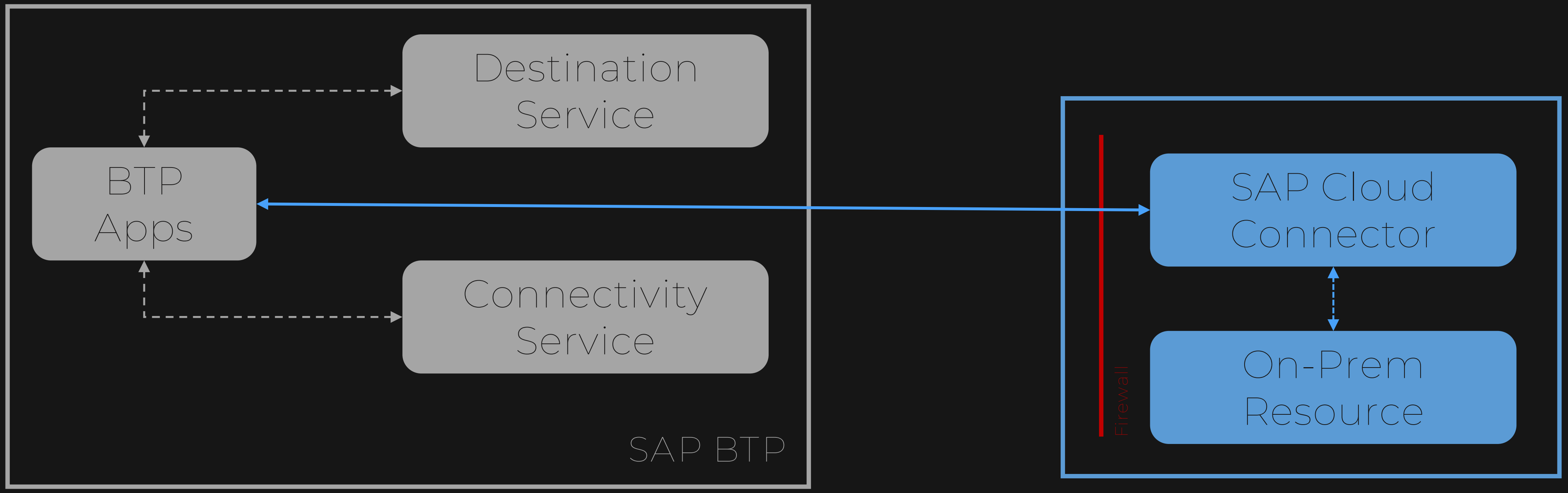


SAP Business Technology Platform

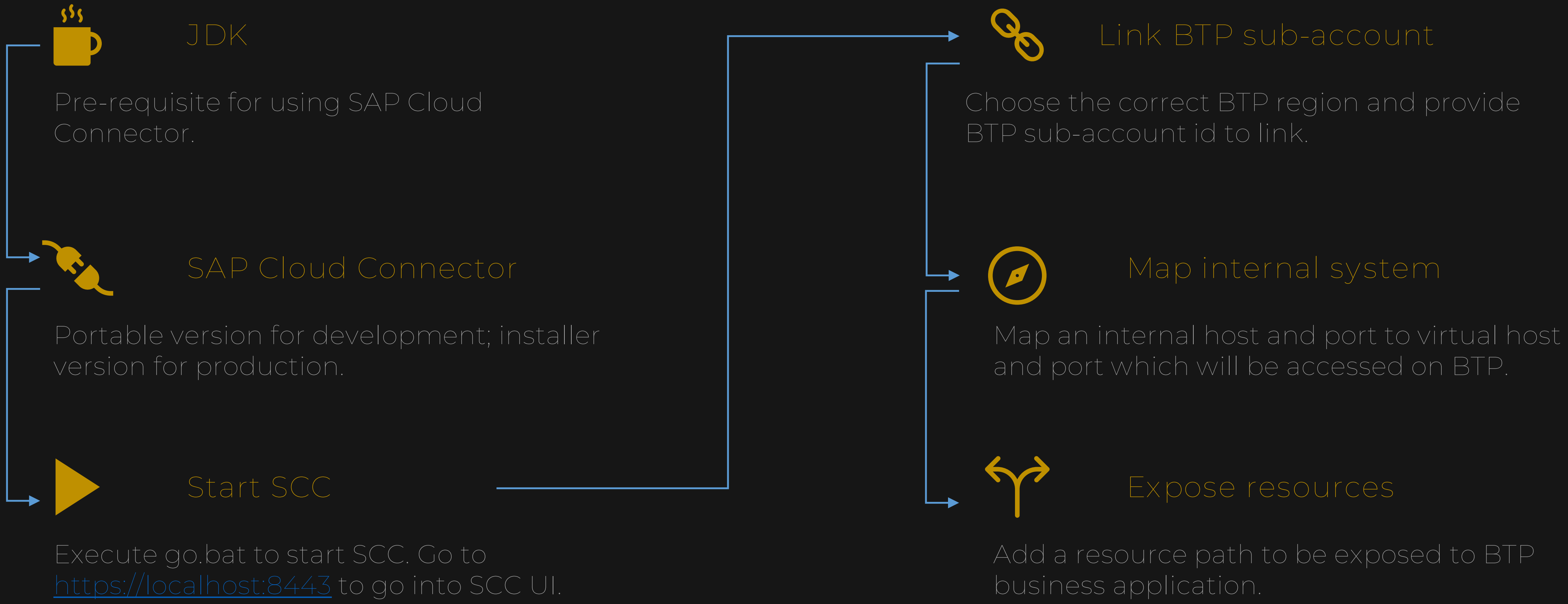
On Premise Connectivity

SAP BTP – On-Prem connectivity

In order to connect BTP business applications to an on-prem resource (SAP or Non-SAP) we need SAP Cloud Connector.



SAP BTP – SCC Setup



JDK

Pre-requisite for using SAP Cloud Connector.

SAP Cloud Connector

Portable version for development; installer version for production.

Start SCC

Execute go.bat to start SCC. Go to https://localhost:8443 to go into SCC UI.

Link BTP sub-account

Choose the correct BTP region and provide BTP sub-account id to link.

Map internal system

Map an internal host and port to virtual host and port which will be accessed on BTP.

Expose resources

Add a resource path to be exposed to BTP business application.

SAP BTP – SCC Setup (validation)

1 Cloud Connector should be available in BTP sub-account under Connectivity → Cloud Connectors

2 Destination pointing to the cloud connector resource should be able to connect (green tick)

Application Walkthrough & Demo

Capstone project – Requirements

Connectivity

Business app should be able to connect to an on-prem server to fetch data and perform operations.

Authentication

Authentication should be enabled on business app so that only the authenticated users are able to access the application.

Authorization

Users should have proper authorization in order to access the application.

Capstone project – Tech Design

Connectivity

SAP Cloud Connector will be setup and linked to the SAP BTP sub-account to establish on-prem connectivity.

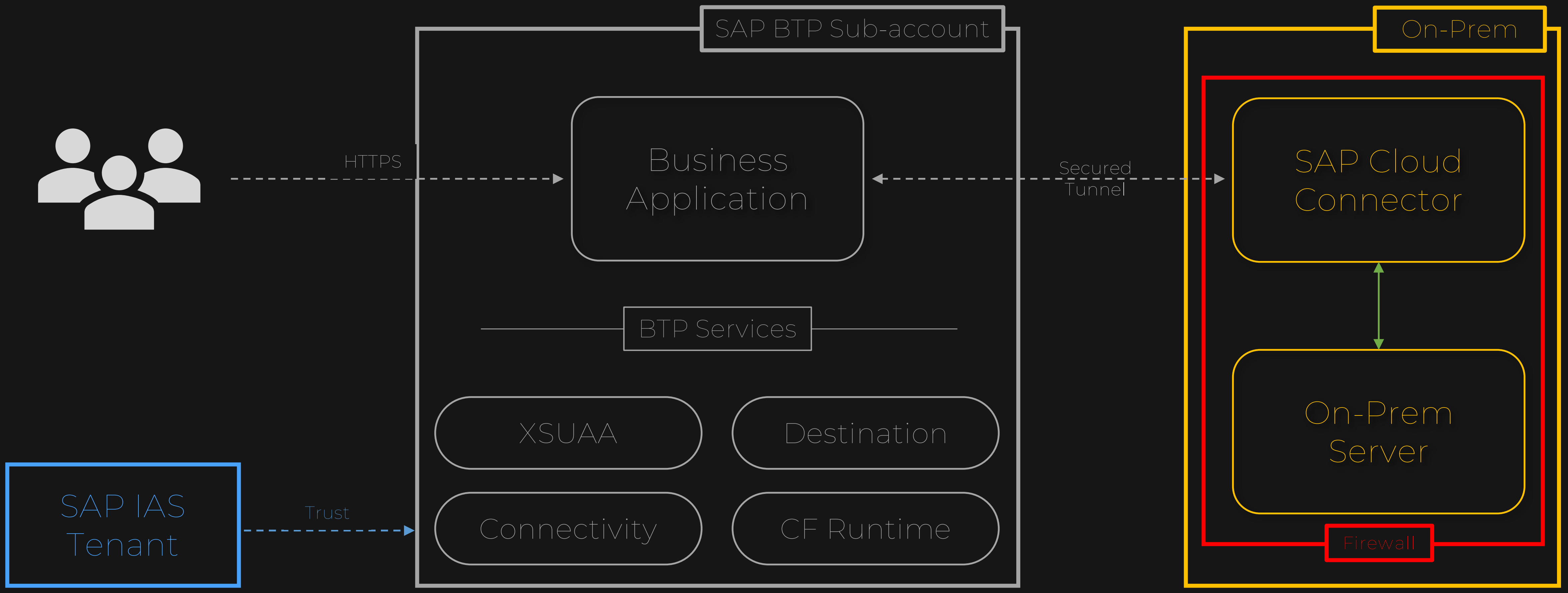
Authentication

SAP IAS tenant will be setup as the identity provider to supply the users.

Authorization

Application will define role collections and IAS groups will be mapped to those role collections.

Capstone project – Architecture



Capstone project – Steps

On-Prem

1. Install Java (JDK 1.8_192) as a pre-requisite to work with SAP Cloud Connector.
2. Install SAP Cloud Connector.
3. Add the BTP sub-account in SCC.
4. Create a Node application locally.
5. Run the local node server.
6. Expose the local node server resources through SCC.

BTP

1. Validate if cloud connector is linked with the BTP sub-account.
2. Create destination to connect from BTP to the connected cloud connector.
3. Check if destination is working properly (green tick).
4. Deploy an app on BTP (node-btp).
5. Create service instances of XSUAA, Destination and Connectivity services.
6. Bind services instances to the app.
7. Get destination service access token.
8. Get connectivity service access token.
9. Get destination configuration (use the destination access token from step 7).
10. Call the on-prem server from BTP app.
11. Add authentication in BTP app (app-router).
12. Add authorization in BTP app (xs-security.json).
13. Establish trust between BTP and IAS.
14. Create users in IAS.
15. Assign appropriate group in IAS.
16. Map IAS group to BTP role collection.

Capstone project – Hands-on

1. On-prem Node server

   Clone this git repo - https://github.com/sagedev2k16/local-node-server.git

2. BTP Node app

   Clone this git repo - https://github.com/sagedev2k16/node-btp.git

3. Setup Cloud Connector

   Install, configure and validate SCC configuration on SAP BTP

4. Deploy on BTP

   Deploy business app on BTP and update XSUAA service instance

5. Configure SAP IAS tenant

   Establish trust between BTP and IAS, create users and groups in IAS

6. IAS groups ⇔ BTP role collections

   Map IAS groups with BTP role collections.

SAP Identity Access Governance

SAP IAG – Overview

1 Streamline identity and access management (IAM) process of the organization for on-prem and cloud applications.

2 Built on SAP Business Technology Platform and available on CF environment (Azure and AWS).

2 IAG Bridge is a way to extend SAP Access Control (on-prem) and use the same risk definitions and mitigation controls on both sides.

SAP IAG – Key Capabilities

Identity Management

Secure environment for managing identities in various SAP applications.

Analyse Issues

Instant visibility into access issues with drill-down capabilities.

Intuitive

Simple, seamless and transparent processes.

Dashboard

Dashboard-based user interface based on the familiar SAP Fiori user experience.

Governance

Comprehensive access governance.

Identity Bundle

Up-to-date and scalable solutions (IAS, IPS and IAG) bundled together.

SAP IAG – Services

Access Analysis

The Access Analysis Service enables you to detect and remediate segregation of duties (SoD) and critical access risks.

Access Request

Provides provisioning of user access to on-premise and cloud applications by integrating with SAP BTP services.

Role Design

Enables defining and maintaining business roles directly in IAG to optimize role definition and streamline governance.

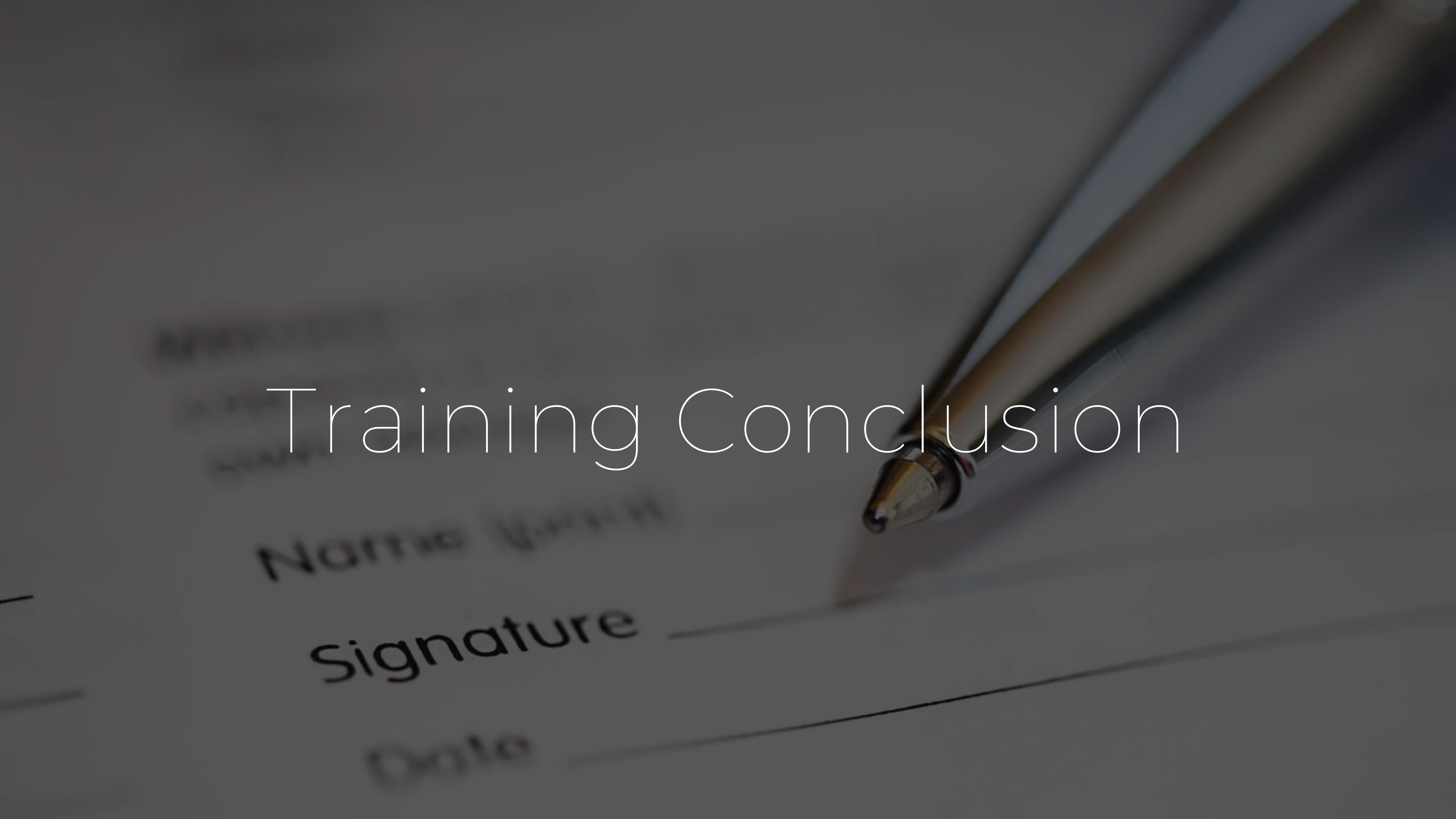
Access Certification

Allows review of user access, roles, risks and mitigation controls. Can be triggered for e.g. when an employee's job changes or periodically.

Privileged Access Management

Similar to Firefighter access in GRC to monitor access to sensitive and critical transactions.

Training Conclusion



SAP Training (SECCL1)

Security in BTP

SAP IAS

SAP IPS

SAP IAM in Cloud

OWASP Top 10 and Cheat sheets

Broken Access Control

Cryptographic Failures

Injection

Insecure Design

Security Misconfiguration

Vulnerable and Outdated Components

Identification and Authentication Failures

Software and Data Integrity Failures

Security Logging and Monitoring Failures

Server Side Request Forgery

https://owasp.org/www-project-top-ten/

https://cheatsheetseries.owasp.org/index.html

Thank you