**UNIT 6**

**Security**

### Lesson 1

[Introducing Application Security](#_bookmark0) 277

Lesson 2

[Explaining Platform Security](#_bookmark1)

[Exercise 7: Perform a Conscious Login to SAP Cloud Platform](#_bookmark2)

281

287

### Lesson 3

[Explaining Application Security](#_bookmark3) 293

UNIT OBJECTIVES

* Figure out, how the domain model works and name the main services
* Differentiate between authentication and authorization and how both are used on the SAP Cloud Platform
* Appreciate the secure implementation of a microapp

Unit 6

Lesson 1

# Introducing Application Security

LESSON OBJECTIVES

After completing this lesson, you will be able to:

* Figure out, how the domain model works and name the main services

### The Domain Model

In particular, we'll look at the following topics in this lesson:

* Current Domain Model
* SAP Product Context

Current Domain Model

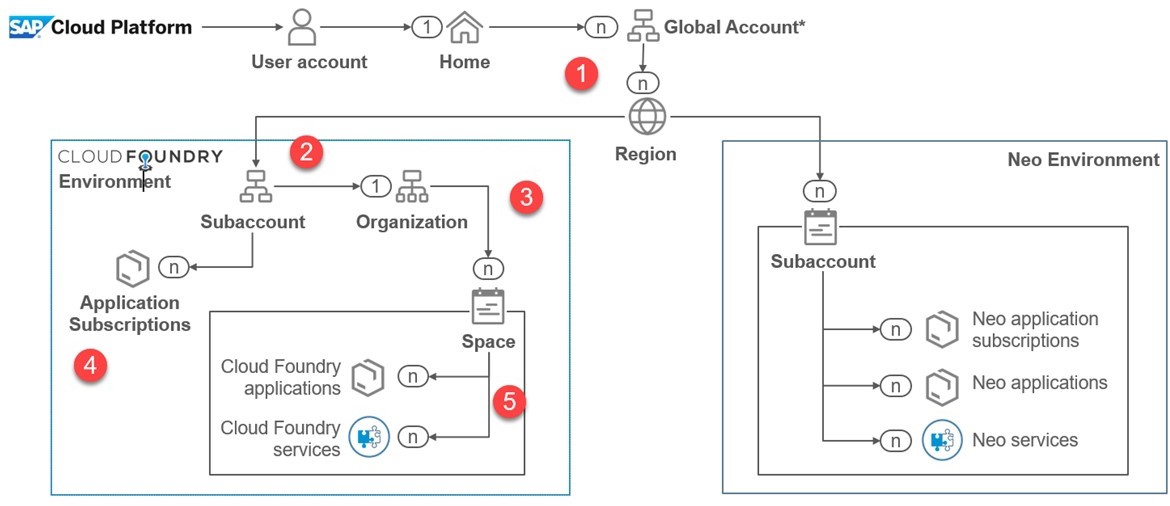


Figure 181: Current Domain Model

The figure above illustrates the current domain model.

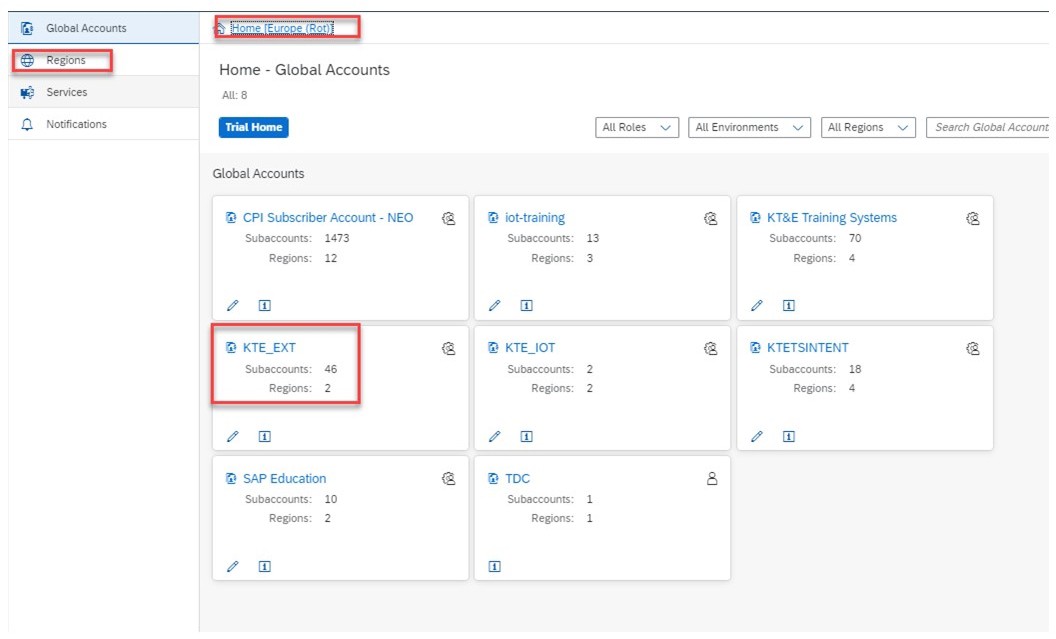
Global Account



Figure 182: Global Account

A global account has a region, here red (1).

Subaccount

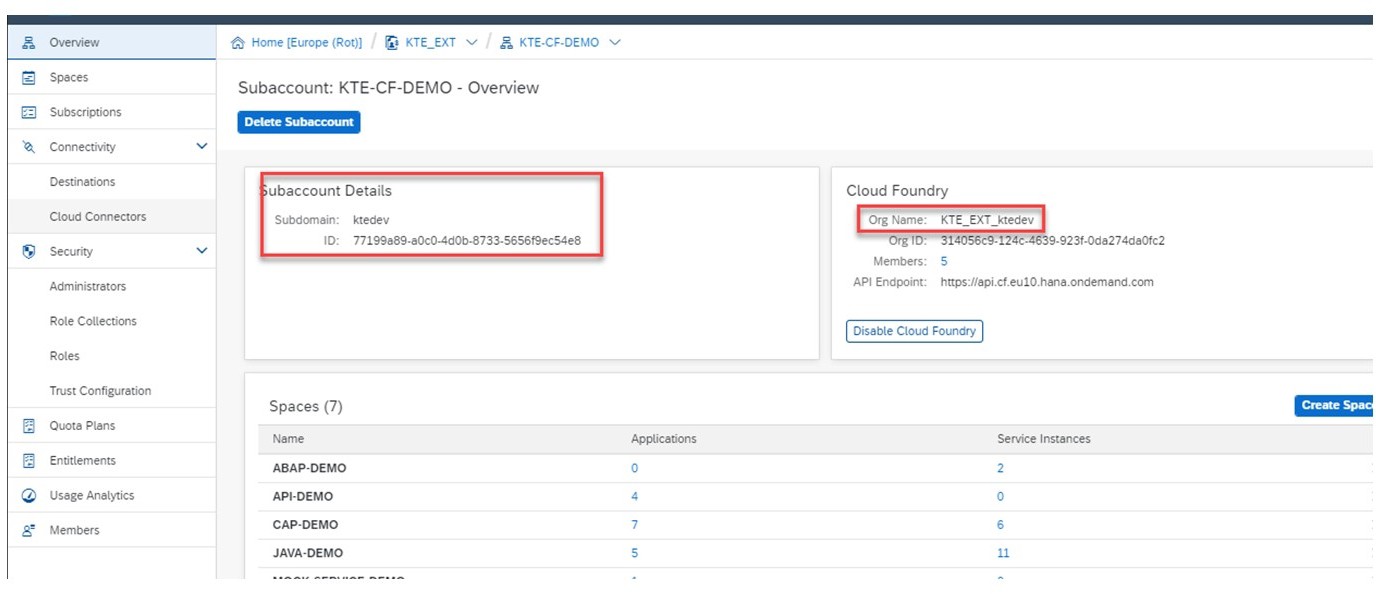


Figure 183: Subaccount

The figure illustratses, that a subaccount has a subaccount ID and exactly one organization

(2) and (3).

Lesson: Introducing Application Security

Spaces

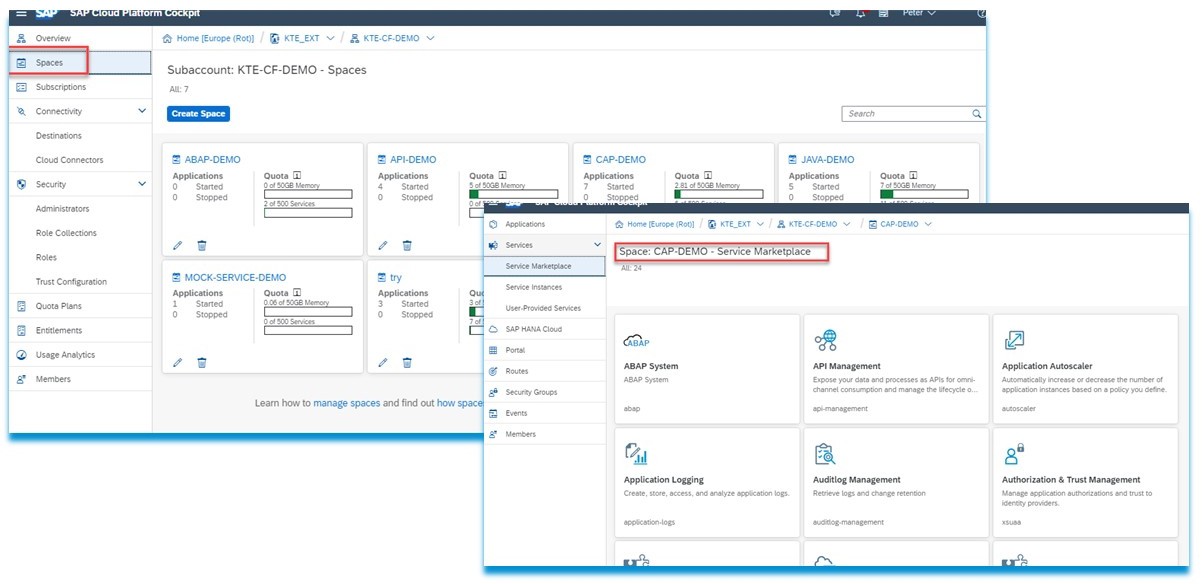


Figure 184: Spaces

The figure illustrates, that a subaccount has n Spaces (5) with services and applications in the Marketplace.

SAP Product Context

First, an overview of the services and tools in the area of security.



Figure 185: SAP Product Context

The figure illustrates the SAP product context. In detail:

Authentication & Single Sign-on

* + SAP CP Identity Authentication
  + SAP Single Sign-On Identity Management
  + SAP CP Identity Provisioning service
  + SAP Identity Management Governance, Risk & Compliance
  + SAP Cloud Identity Access Governance
  + SAP Access Control

We focus on the services SAP Cloud Platform Identity Authentication and SAP Cloud Platform Identity Provisioning that help us to work safely.

Information about the SAP Cloud Platform Identity Authentication:

* Simplify and secure cloud-based access to business processes, applications, and data with state-of-the-art authentication mechanisms, single sign-on, on-premise integration, and convenient self-service options
* These are:
  + Two-factor authentication
  + Customer and partner onboarding
  + Secure integration

SAP Cloud Identity Access Governance

Streamline identity and access management (IAM) in complex on-premise and cloud environments with SAP Cloud Identity Access Governance software. You can improve IAM practices with an intuitive, dashboard-driven interface and a simple single sign-on (SSO) experience in the cloud.

Information about SAP Cloud Platform Identity Provisioning:

* Automate identity lifecycle processes to provision identities and their authorizations to cloud and on-premise applications.
* Define user access based on identity attributes such as current group or role assignment and location.

LESSON SUMMARY

You should now be able to:

* Figure out, how the domain model works and name the main services

Unit 6

Lesson 2

# Explaining Platform Security

LESSON OBJECTIVES

After completing this lesson, you will be able to:

* Differentiate between authentication and authorization and how both are used on the SAP Cloud Platform

### Platform Security

In particular, we'll look at the following topics in this lesson:

* SAP Cloud Platform Identity Authentication - IDP.
* SAP Cloud Platform Identity Authentication - Service.
* User and Role Management on SAP Cloud Platform.
* SAP Cloud Identity Provisioning Service.
* Bringing all together.

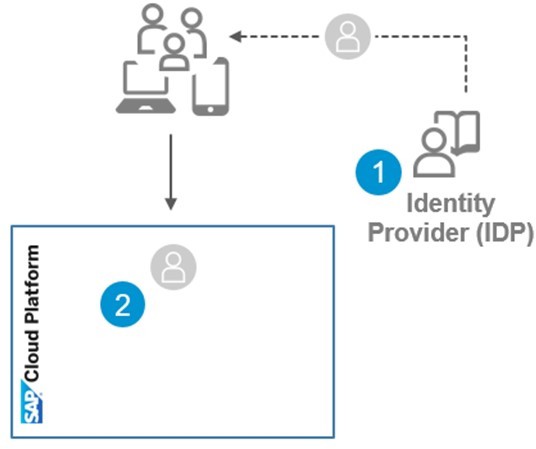
SAP Cloud Platform Identity Authentication - IDP



Figure 186: SAP Cloud Platform Identity Authentication - IDP

SAP CP uses out of the box, the Identity Providers (IDP) for user authentication. He has the role of a user store:

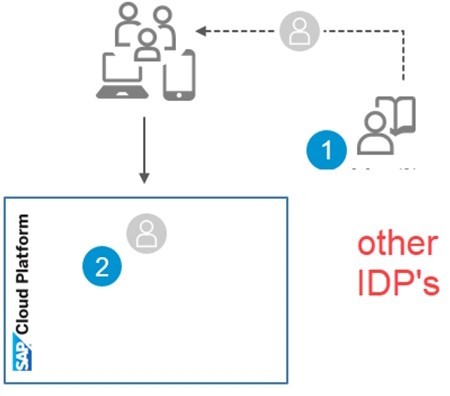
1. External Authentication providers (SAML).
2. Authenticated identity is used inside SAP Cloud Platform.

Freedom of choice of IDP

SAML2 standard provides choice of authentication provider.



Figure 187: Freedom of Choice of IDP

SAP\_CP\_Identity\_Authentication can use on-premise IDP's (AD, LDAP, SAP) for user authentication:

* Re-use existing IDP, easy to implement.
* Maintain central user repository (no user sync needed). SAML2 capable IDP's can be integrated, for example:
* MS ADFS
* MS AZURE
* …

Change the IDP on Subaccount Level

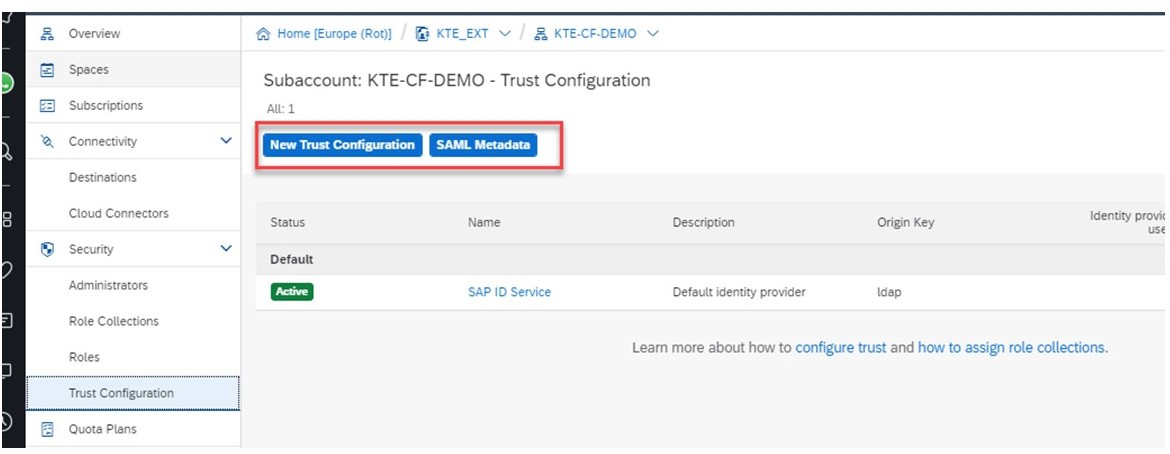


Figure 188: Change the IDP on Subaccount Level

You can change the SAML 2.0 IDP Provider on Subaccount level.

SAML 2.0 Response after successful Login to IDP

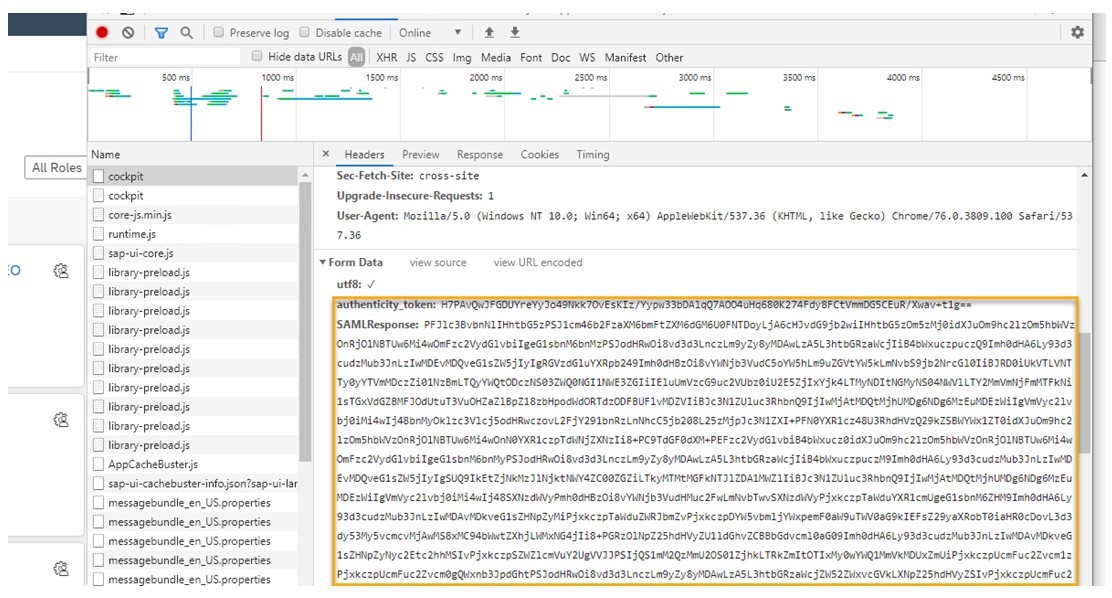


Figure 189: SAML 2.0 Response After Successful Login to IDP

Here is the SAML 2.0 Response from IDP to SAP Cloud Platform after successfull login.

SAP Cloud Platform Identity Authentication - Service

By default, SAP always uses the IDP as the identity provider. However, it only offers basic functions like User Authentication as a user store.

To take advantage of all possibilities, the Identity Authentication Service can be licensed. It offers almost all conceivable options based on SAML 2.0 or OpenID Connect Standard.

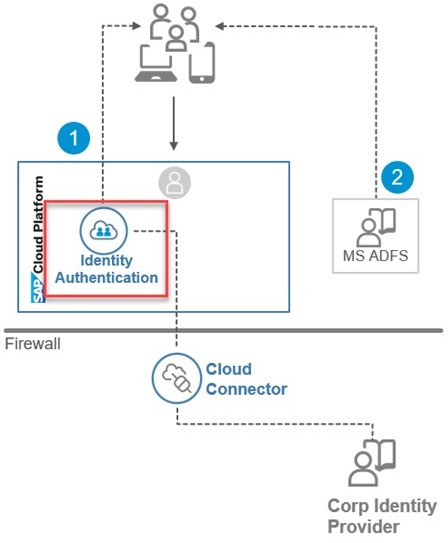
Additionally, you still need an Identity Provider, for example the IDP from SAP or from third- party companies.



Figure 190: SAP Cloud Platform Identity Authentication - Service

The example above uses two IDPs. The Features are:

* Basic authentication
* Re-use of Windows Domain Logon
* Two-factor authentication
* Delegated logon

Information about User and Role Management on SAP Cloud Platform

Table 6: User and Role Management on SAP Cloud Platform

|  |  |  |
| --- | --- | --- |
| Type | Description | Authentication Configuration |
| Platform Users | Member on Clobal - and Sub- account, Members on Sapce Level | Platform IDP, on Global Ac- count Level |
| Application Developer) Users | User that use Subscriptions and/or Market Place Serv- ices . Developers or Business developer | IDP on Subaccount Level |
| Business User | User that use business apps | IDP on Subaccount Level |

No user identities are held on the SAP Cloud Platform. However, domain-dependent system and service roll and groups are used.

These roles and groups are either created directly on the SAP Cloud Platform, for example, or existing ones are imported and mapped to the Platform Roles or Groups. This is done with the SAP Cloud Identity Provisioning Service.

You can identify the following user types. A developer can also be a business.

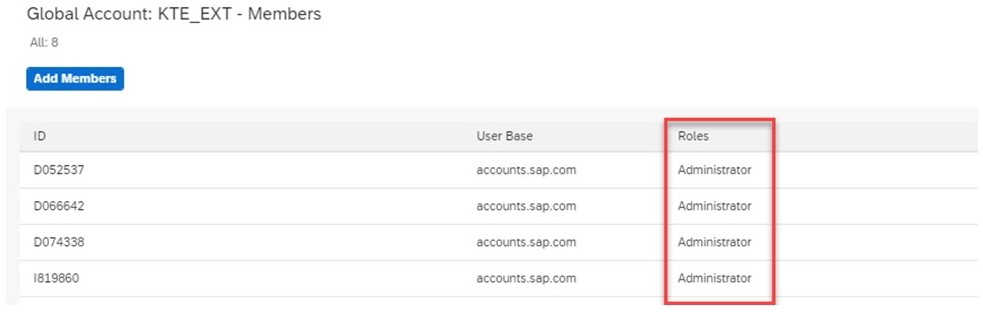
Roles and Groups on the SAP Cloud Platform - Platform Users



Figure 191: Platform Users - Global Account

On global level the Administrator role is assigned.

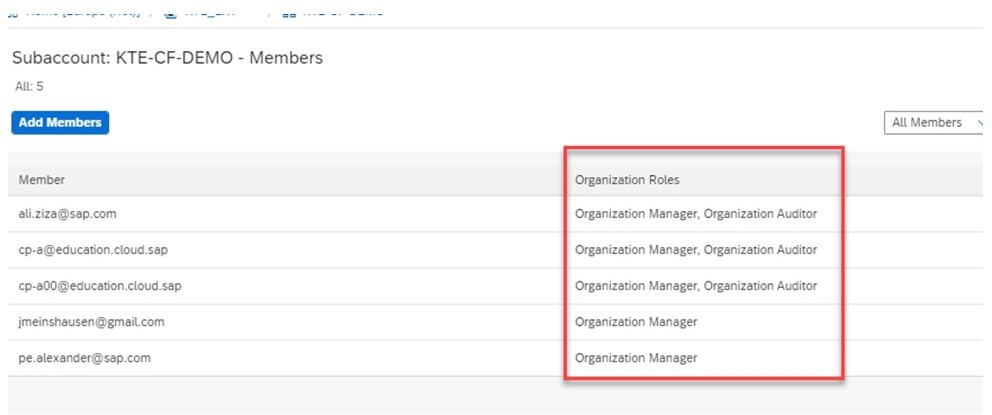
Roles and Groups on the SAP Cloud Platform - Platform Users



Figure 192: Platform Users - Subaccount

On subaccont level, the Organisation Roles are assigned.

Roles and Groups on the SAP Cloud Platform - Platform Users

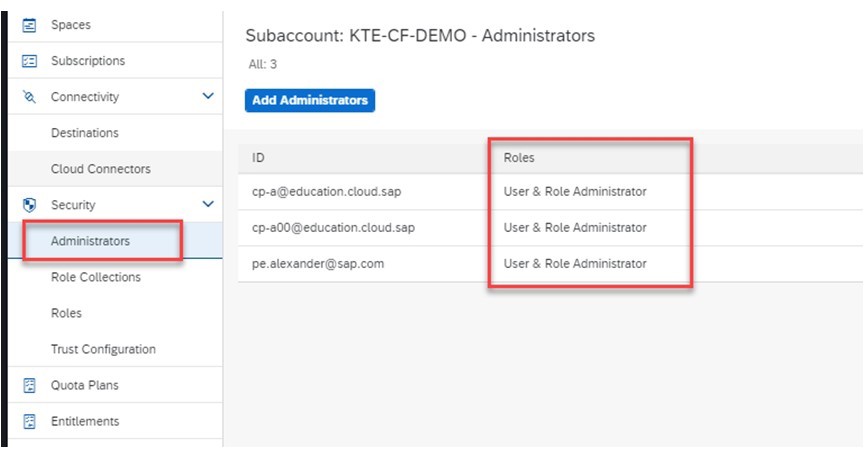


Figure 193: Platform Users - Subaccount - Security Administrator

On subaccont level also the Security Administrators are assigned.

Roles and Groups on the SAP Cloud Platform - Platform Users

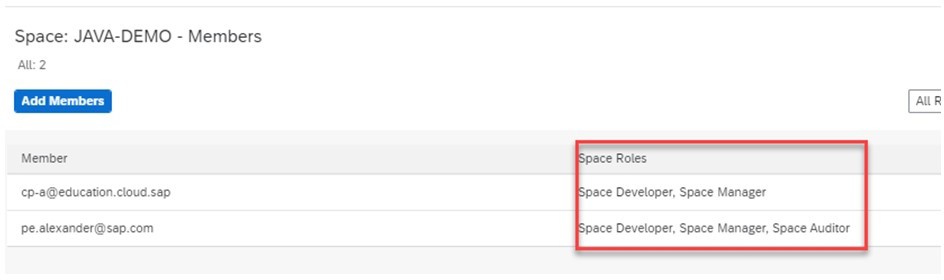


Figure 194: Platform Users - Space

On space level the Spaces Roles are assigned.

Appication Users - Service Roles

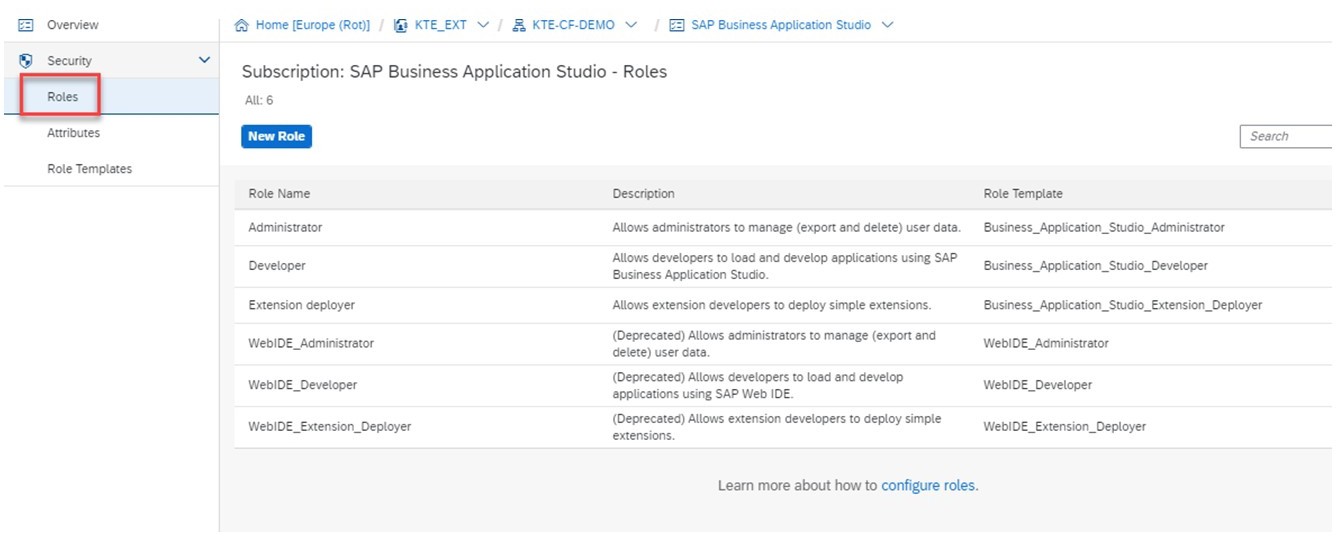


Figure 195: Appication Users - Service Roles

However, the service roles still have to be assigned to the corresponding user. You can see how this can be done in the case of your own service in the next Lesson with a Business User.

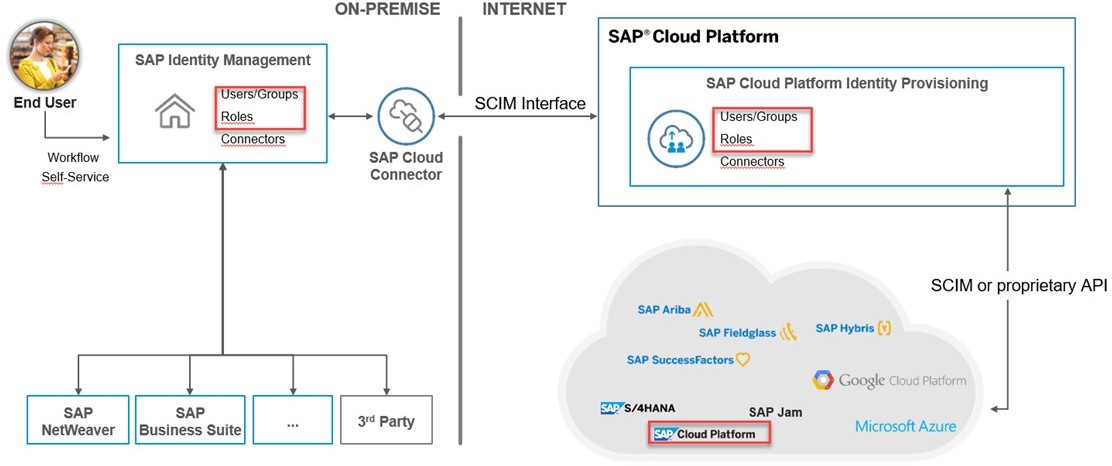
SAP Cloud Identity Provisioning Service



Figure 196: SAP Cloud Identity Provisioning Service

In order to use existing roles and groups, for example in the SAP Cloud Platform, these can be mapped manually via the SAP Cloud Platform Identity Provisioning Service.

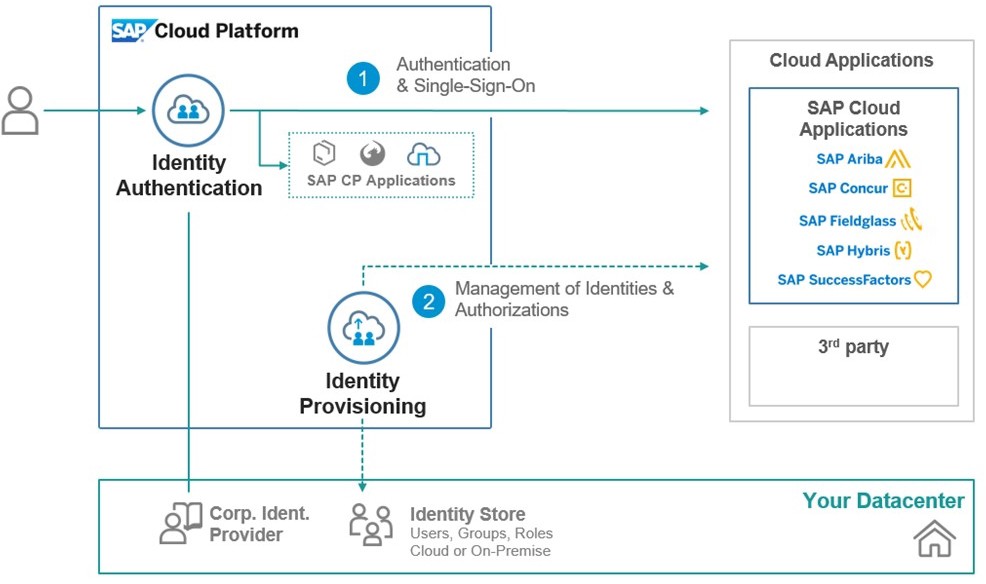
Bringing all together



Figure 197: Bringing all together

The combination of authentication and authorization looks like. This would also be the architecture to be aspired to. The SAP Cloud Platform as a security hub

Unit 6

Exercise 7

# Perform a Conscious Login to SAP Cloud

Platform

Business Scenario

In this exercise you will use a different way to log on to your CF subaccount.



Note:

In the exercise Assign To and Set up your Training Environment you have created work folders. In these work folders, you find all required information to successfully perform this exercise. In case of issues, refer to this exercise or ask your trainer.



Note:

In this exercise, when the values include ##, replace ## with your group number.

Logon to Your CF Subbaccount

1. Logon to your CF Subbaccount.

Unit 6

Solution 7

# Perform a Conscious Login to SAP Cloud

Platform

Business Scenario

In this exercise you will use a different way to log on to your CF subaccount.



Note:

In the exercise Assign To and Set up your Training Environment you have created work folders. In these work folders, you find all required information to successfully perform this exercise. In case of issues, refer to this exercise or ask your trainer.

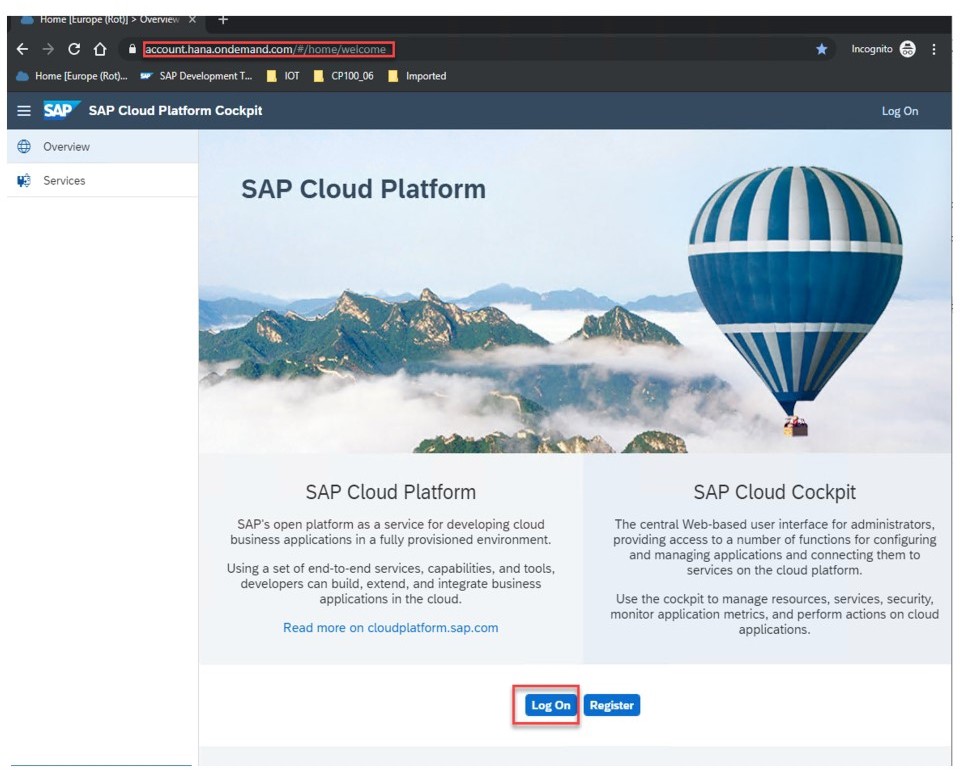


Note:

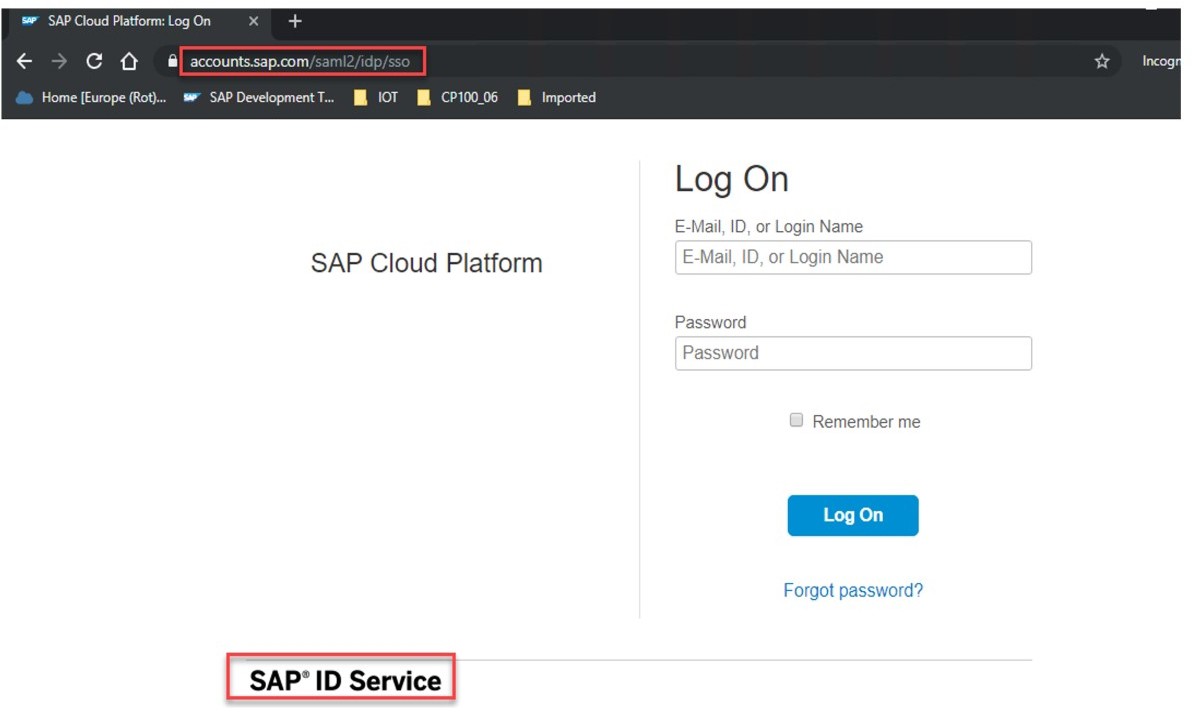
In this exercise, when the values include ##, replace ## with your group number.

Logon to Your CF Subbaccount

1. Logon to your CF Subbaccount.
   1. If not already there, choose *dy-ecc617ciscc-###*.
   2. Close all browser windows or open a incognito window.
   3. Insert the url: [https://account.hana.ondemand.com/#/home/welcome](https://account.hana.ondemand.com/%23/home/welcome)



* 1. Choose *Log On* and see that the URL has changed.



* 1. Enter your user and password. Use the following data:

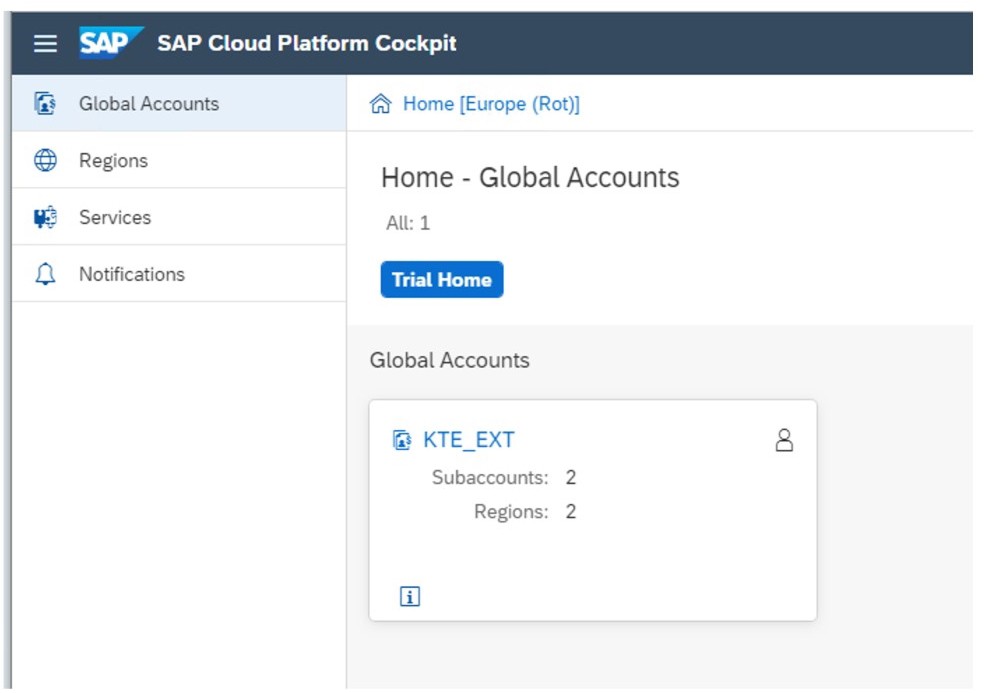
|  |  |
| --- | --- |
| Field | Value |
| E-Mail | [cp-a##@education.cloud.sap](mailto:cp-a%23%23@education.cloud.sap) |
| Password | Welcome1 |



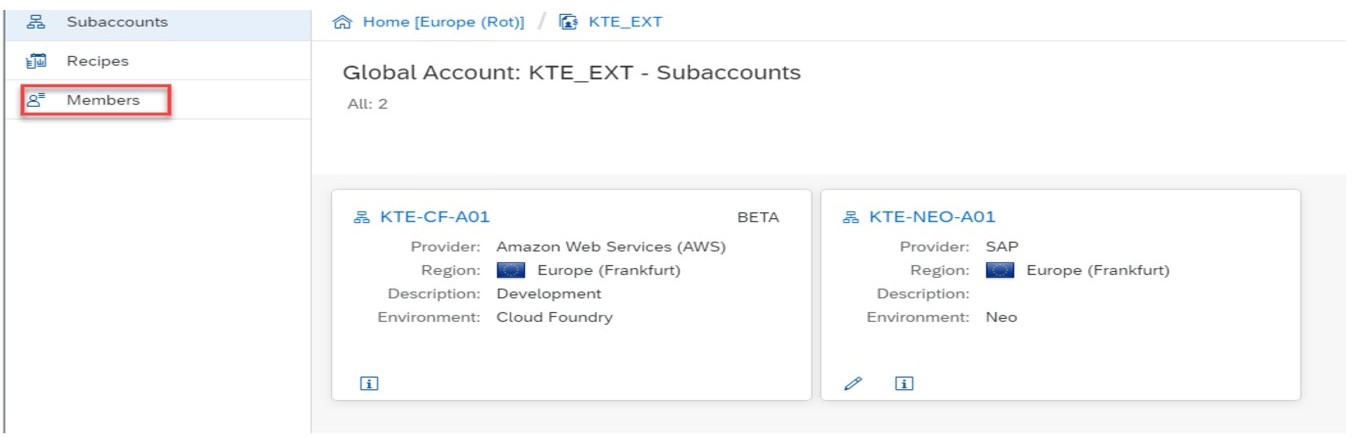
Note:

This information is subject to change. In case of issues, refer either to the SSG, or the *Settings* file in your work folder.

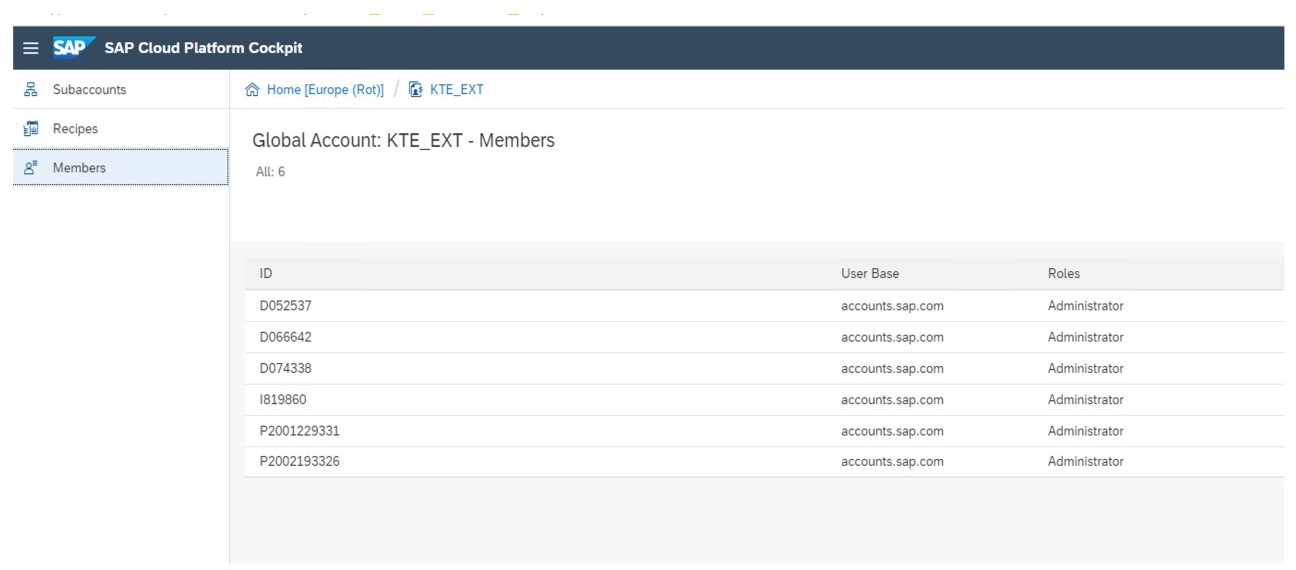
* 1. Only the Global Accounts in which there are Subaccounts with you as a member, display.



* 1. Click on the Globalaccount *KTE\_EXT* to find Subaccounts in which you are a member.



* 1. Click on the menu link *Members* to see if you are a member of this subaccount.



LESSON SUMMARY

You should now be able to:

* + - Differentiate between authentication and authorization and how both are used on the SAP Cloud Platform

Unit 6

Lesson 3

# Explaining Application Security

LESSON OBJECTIVES

After completing this lesson, you will be able to:

* Appreciate the secure implementation of a microapp

### Application Security

In particular, we'll look at the following topics in this lesson:

* How Application Security works
* The Approuter
* Json Web Token (JWT)
* Extended Services for User Account and Authentication (XSUAA)
* Assigning Users to Application Roles

How Application Security works

We limit ourselves to what we're doing in Cloud Foundry. The following example describes a microservices in Java.

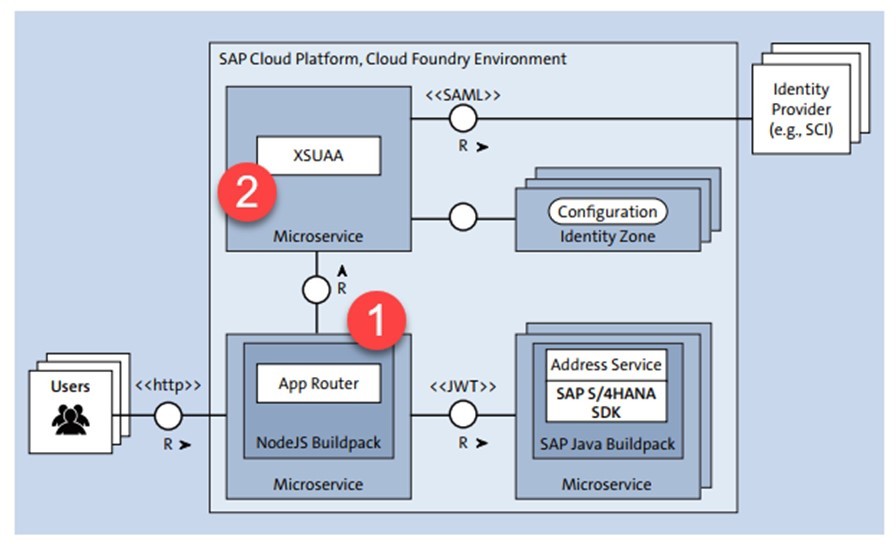


Figure 198: Main Blocks of Application Security

The figure above illustrates a high-level authentication setup. Further details:

The App Router (1) Its tasks are:

* The App Router is the central entry point for our application it dispatches requests to our back end microservices, thus acting as a reverse proxy. The back end microservices should not be directly accessible by the client.
* The App Router can serve static content such as web pages, SAPUI5, or another client-side code.
* The App Router manages the authentication flows for our entire application

For authentication (who the user is) and authorization (what the user is allowed to do), the App Router takes all incoming, unauthenticated request and initiates an OAuth2 flow (authorization code grant) with the Extended Services for User Account and Authentication (XSUAA) service of the SAP Cloud Platform in the Cloud Foundry environment .

Install via Service Marketplace

The App Router is a *Node.js* component, distributed via the publically available SAP NPM registry.

The Application Router's Design-Time Descriptor: xs-app.json



Figure 199: Router's Design-Time Descriptor: xs-app.json

The xs-app.json file can be used to configure many more aspects at design-time of the AppRouter like authentication types, cache control, compression threshold for outgoing traffic (by default, 1 KB), client-initiated logout, custom settings for CSRF protection, and much more.

The AppRouter's Runtime Configuration within the manifest.yaml



Figure 200: Runtime Configuration Within the manifest.yaml

Besides destinations and tenant host patterns, the AppRouter understands many different parameters that can be changed during runtime, without redeploying the entire AppRouter,

which is consistent with the twelve-factor application principles. Recognized parameters include cross-origin policies, session timeouts, compression thresholds, JWT refresh times, etc.

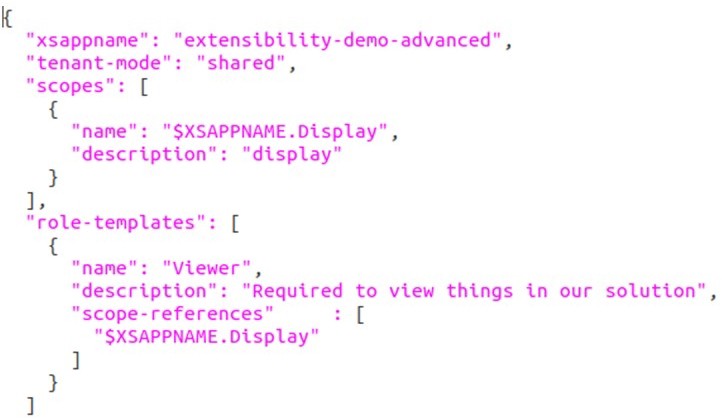
The Application Security Descriptor: xs-security.json



Figure 201: Security Descriptor: xs-security.json

The xs-security.json descriptor is an important design-time artifact to provide authorization scopes, role templates, and other attributes of the application itself as well as foreign applications. This file will be imported while the XSUAA Service will be create.

Json Web Token (JWT)

JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self- contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret (with the HMAC algorithm) or a public/private key pair using RSA or ECDSA.

Although JWTs can be encrypted to also provide secrecy between parties, we will focus

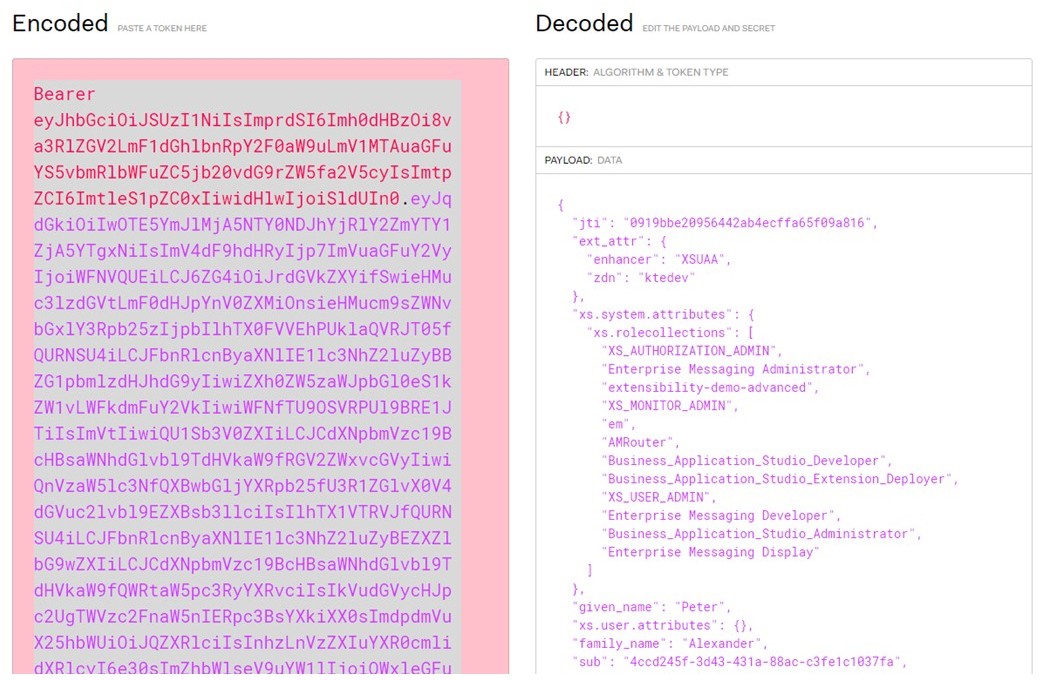
on signed tokens. Signed tokens can verify the integrity of the claims contained within it, while encrypted tokens hide those claims from other parties. When tokens are signed using public/ private key pairs, the signature also certifies that only the party holding the private key is the one that signed it.



Figure 202: JWT Sample

The figure shows an example of a JWT.

When should you use JSON Web Tokens?

Here are some scenarios where JSON Web Tokens are useful:

Authorization

This is the most common scenario for using JWT. Once the user is logged in, each subsequent request will include the JWT, allowing the user to access routes, services, and resources that are permitted with that token. Single Sign On is a feature that widely uses JWT nowadays, because of its small overhead and its ability to be easily used across different domains.

Information Exchange

JSON Web Tokens are a good way of securely transmitting information between parties. Because JWTs can be signed-for example, using public/private key pairs-you can be sure the senders are who they say they are. Additionally, as the signature is calculated using the header and the payload, you can also verify that the content hasn't been tampered with.

User Assignment to Application Roles



Figure 203: Assigning Users to Application Roles

In the xs-security.json we define Role Templates, Roles and Scopes. We need to assign these to users who want to use our app in the subaccount under *Trust*.

To do this, we need to create a role collection in the subaccount and assign the role-template from the xs-security.json.

Procedure to assign users:

* Create the *Role Collection* in the Subaccount.
* Assign the role template from the xs-security.json to the *Role Collection*.
* Under *Trust Configuration* select the current SAP ID service and enter the corresponding user as email address.
* Add the Role Collection to the user.

Protecting the back end application

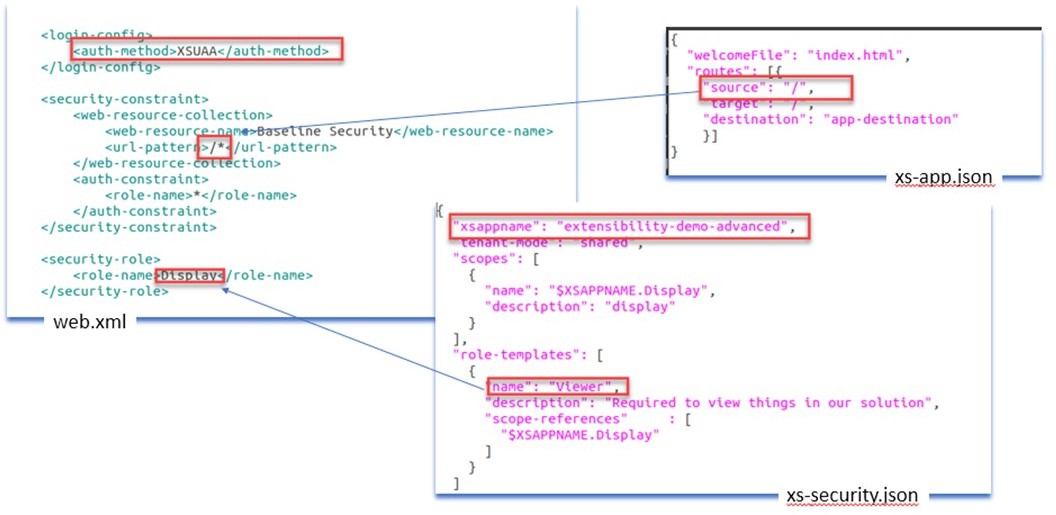


Figure 204: Use Scopes to Protect Your App

Now that we've introduced scopes and role templates to the XSUAA service instance, we'll need to protect our application accordingly. Basically, two places exist where you can check authorizations: inside the AppRouter and in the back end microservices.

Use Scopes to protect your app:

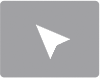
* + Within the xs-app.json you define the protected routes.
  + In the web.xml of your back end service you set the security requirements for Authentication and Authorisation.

Protect the Implementation



Figure 205: Protect the Implementation

At the method level in *my implementation* you assign the scope.

How to Add Authentication and Authorization to an Microservice What are you going to show?

* + Architecture of a state of the Art microapp.
  + Authentication via XSUAA.
  + .Authorization via XSUAA

Workflow of the Applications

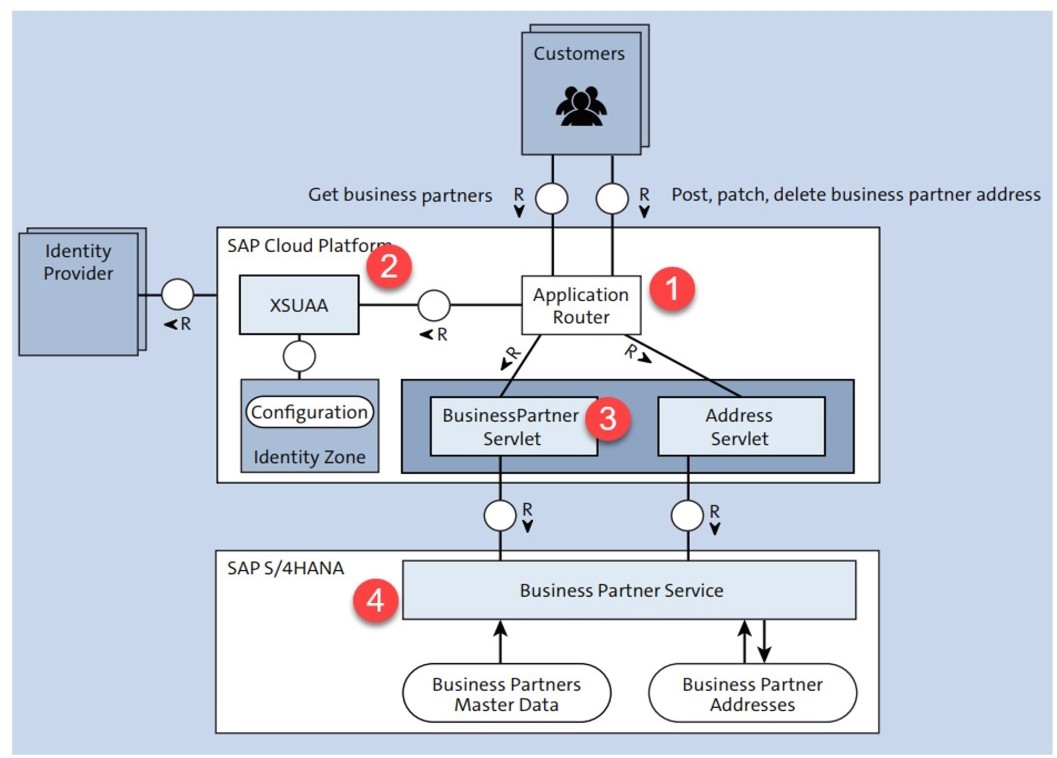


Figure I-5: Architecture of the Apps



Note:

In the exercise Assign To and Set Up Your Training Environment work folders are created. In these work folders, you find all required information to successfully perform this demonstration. Please perform this exercise first or refer to the SSG.



Note:

The following demo is performed in the training landscape *dy-ecc617ciscc-###*.

The demonstration consists of the following parts:

* Explain the workflow of the applications: step 1.
* Explanation for the trainer: step 2.
* Perform Authentication: step 3.
* Authorization via oAuth2: step 4.
* Configuration in web.xml - Infos for Trainer: step 5.
* Assignment of the role to a specific user in the subaccount KTE\_EXT > KTE-CF-DEMO: step 6.
* Check if the Authorization works: step 7.

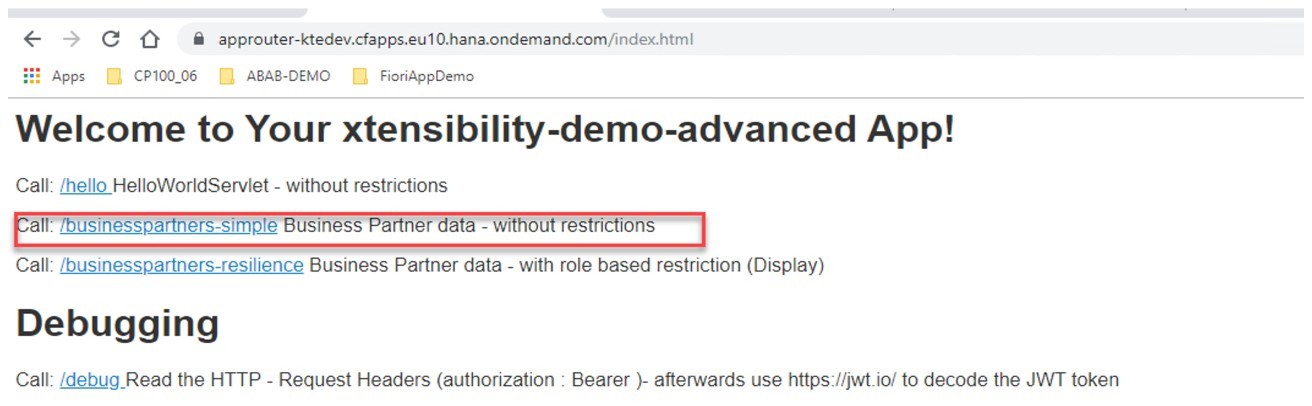
1. Explain the workflow of the applications.
   1. Access the URL via Application Router (1): https://approuter- ktedev.cfapps.eu10.hana.ondemand.com
   2. As login enter the following data:

|  |  |
| --- | --- |
| Field | Value |
| User | [cp-a@education.cloud.sap](mailto:cp-a@education.cloud.sap) |
| Password | Welcome1 |



Note:

This information is subject to change. in case of issues, refer to the SSG. Until further note other user will not work.



* 1. Call the Business Partner Servlet (3) with click on the link */businesspartners-simpl*.



* 1. Call the Business Partner Servlet (3) with click on the link */businesspartner-resilience*.



Figure I-6: CP100\_06\_D11\_fig3\_scr.pptx



Note:

This interface returns more data than the previous call.

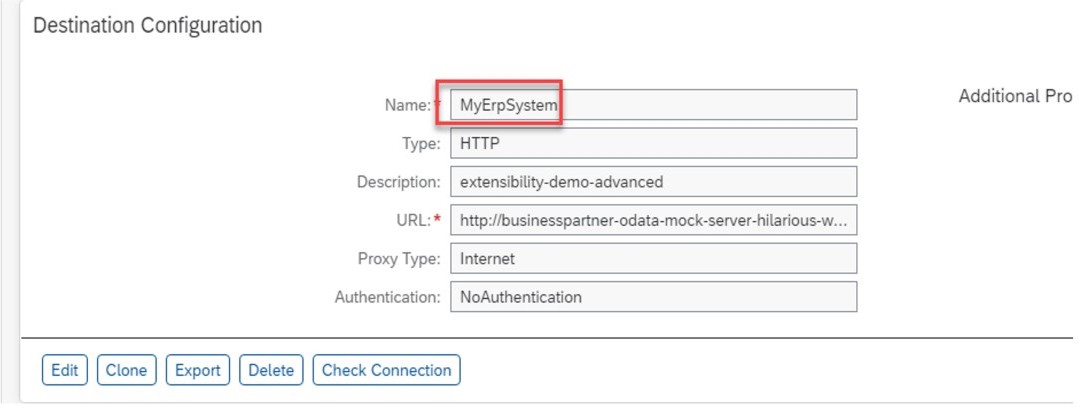
1. Infos for Trainer

The following information is only intended for the trainer to understand. With experience in Java coding, this fragment can also be shown.

* 1. Connect via *destination* to the interface as defined in BussinessPartnerServletSimple.java - MyERPSystem.



* 1. Show configure of this destination at subaccount level:



1. Perform Authentication.

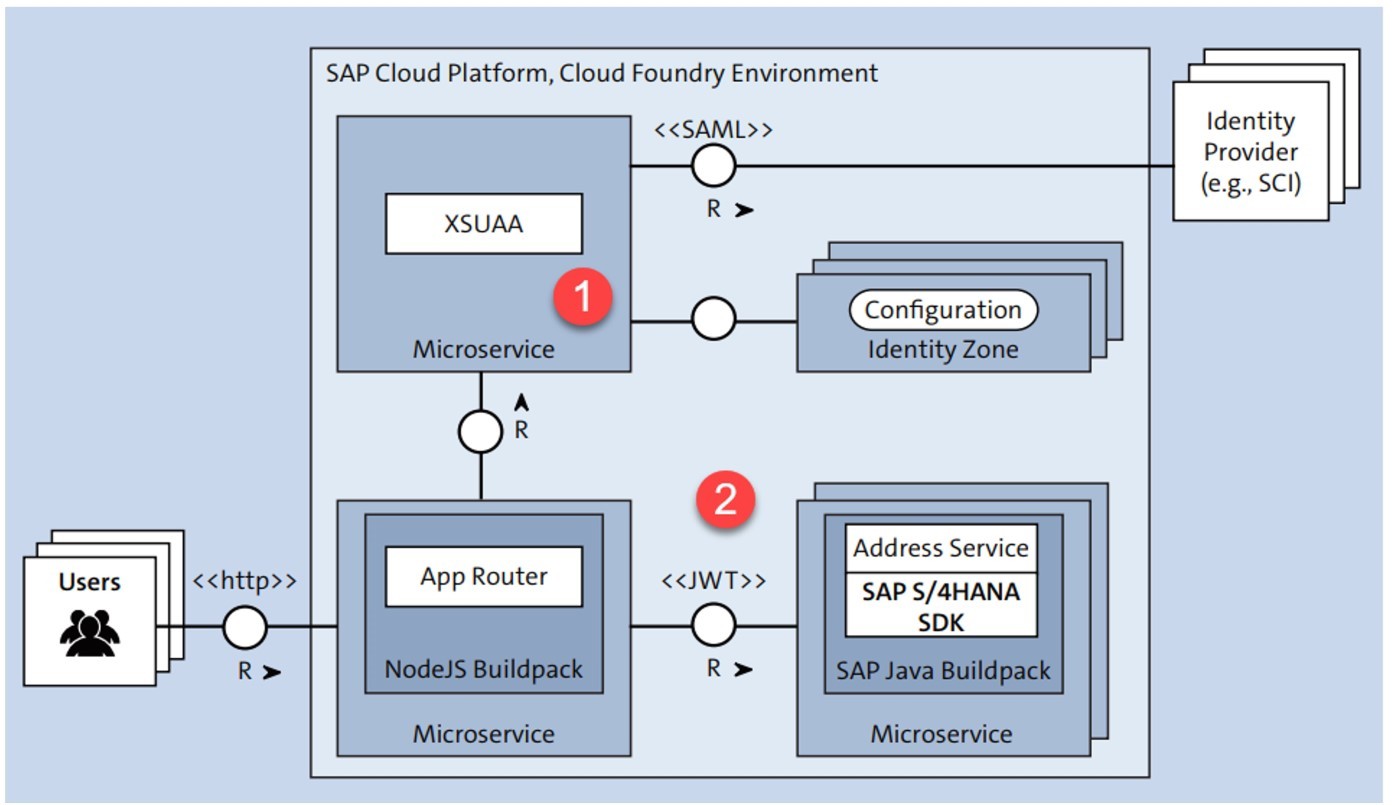
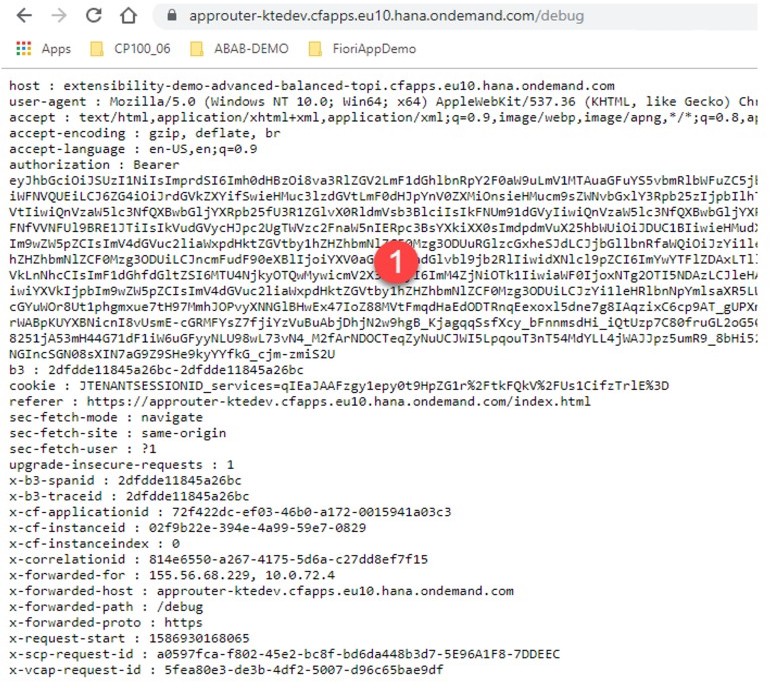
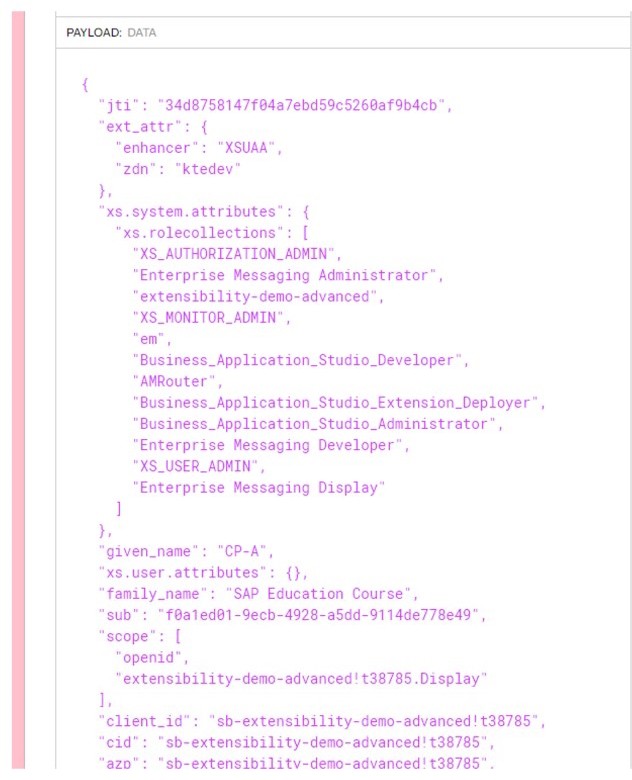


Figure I-7: Flow of Authentication Information

* 1. The *XSUAA* (1) is securely connected to the Identity Provider (IP or IAS) via SAML.
  2. The *XSUAA* authenticates the requesting user via the associated IP.
  3. After successful authentication, the XSUAA provides a Json Web Token (JWT) from which it is now delivered to the actual application when forwarding.
  4. The actual app now checks again the received JWT against the XSUAA .
  5. Calling the link /debug



* 1. Copy the JWT (1 from authorization) and decrypting [https://jwt.io](https://jwt.io/) on the website.



1. Perform Authorization via oAuth2.

The following information is only intended for the trainer to understand. With experience in Java coding, this fragment can also be shown

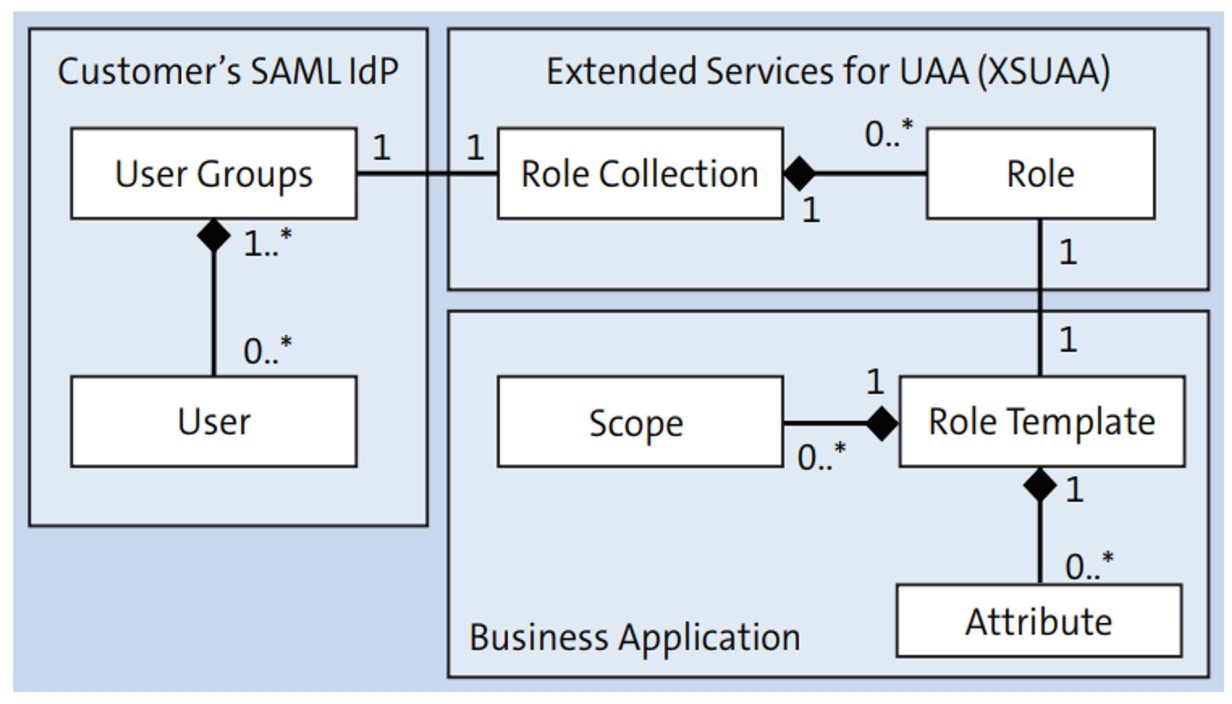
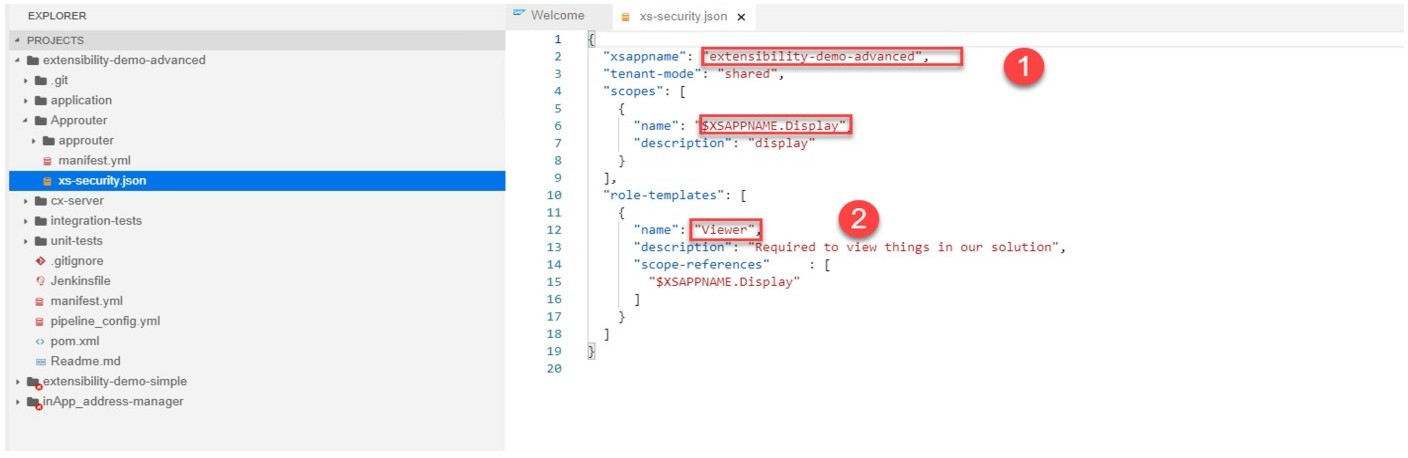
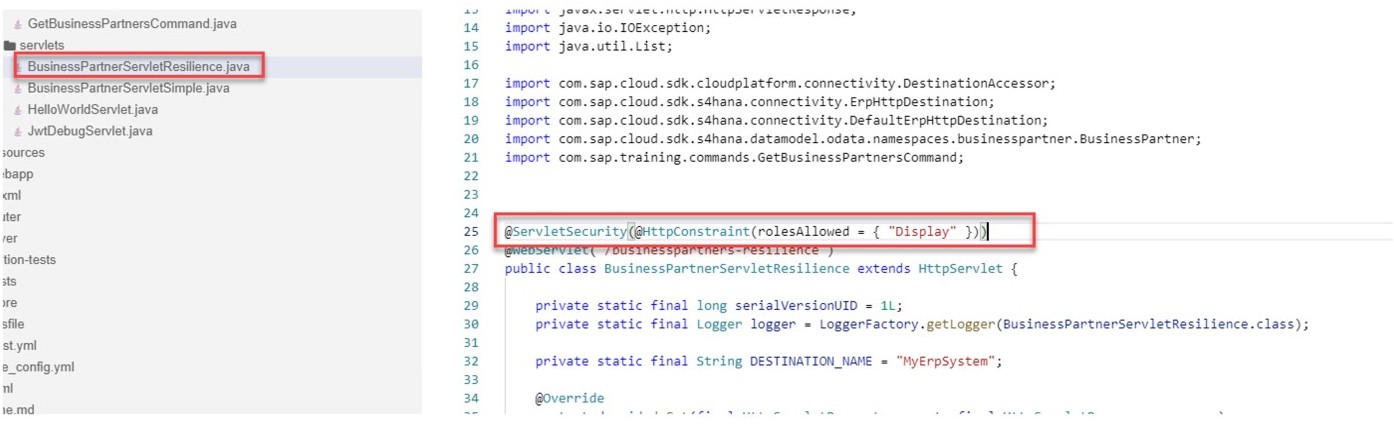


Figure I-8: Flow of information for oAuth2

* 1. When creating the XSUAA service, rolens and scopes are configured for the user and app via a json date. It determines who is allowed to do what and where.
  2. Here it is defined that a user with the role Viewer (2), the app extensibility-demo- advanced app can call and view the fragments assigned in the code of this role.



* 1. As an example, the roll Viewer in the Servlet *BusinessPartnerServletResilienc.java* can only call GET Requests.



1. Configuration in web.xml - Infos for Trainer.

The following information is only intended for the trainer to understand. With experience in Java coding, this fragment can also be shown

Here it is defined that the authentication should be done via XSUAA (1), which works on all calls with the URL /businesspartners-resilience where the role display is checked.



1. Assignment of the role to a specific user in the subaccount KTE\_EXT > KTE-CF-DEMO.
   1. Log in to the subaccount via the URL: [https://account.eu2.hana.ondemand.com/ cockpit#/globalaccount/822af597-cc75-4fbe-b83d-71c32cf0394a/subaccount/ 77199a89-a0c0-4d0b-8733-5656f9ec54e8/destinations](https://account.eu2.hana.ondemand.com/cockpit%23/globalaccount/822af597-cc75-4fbe-b83d-71c32cf0394a/subaccount/77199a89-a0c0-4d0b-8733-5656f9ec54e8/destinations)
   2. As login enter the following data:

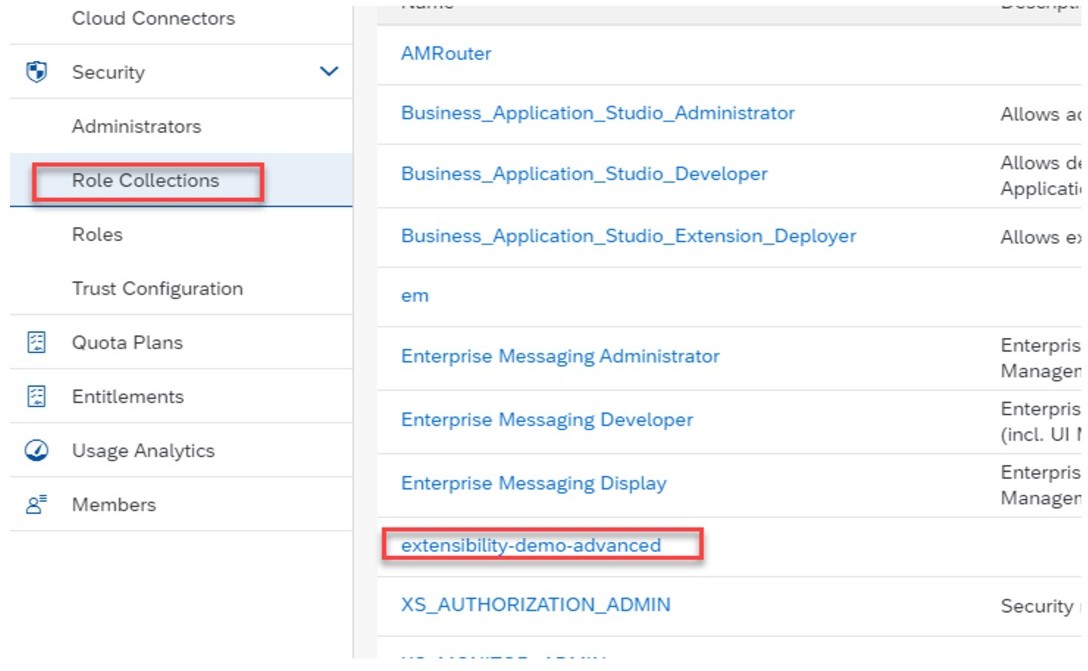
|  |  |
| --- | --- |
| Field | Value |
| User | [cp-a@education.cloud.sap](mailto:cp-a@education.cloud.sap) |
| Password | Welcome1 |



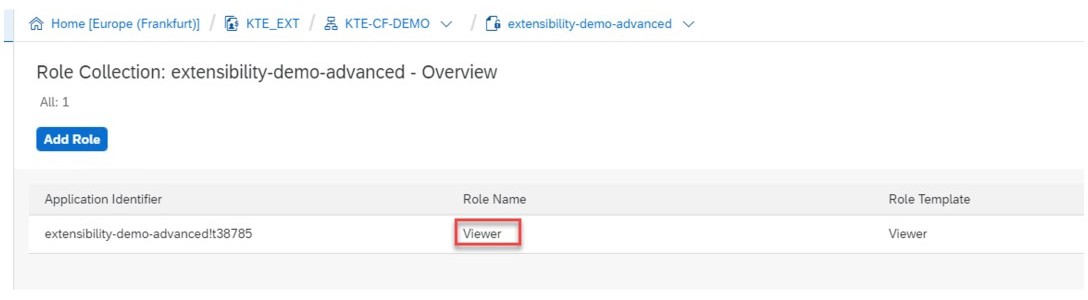
Note:

This information is subject to change. in case of issues, refer to the SSG.

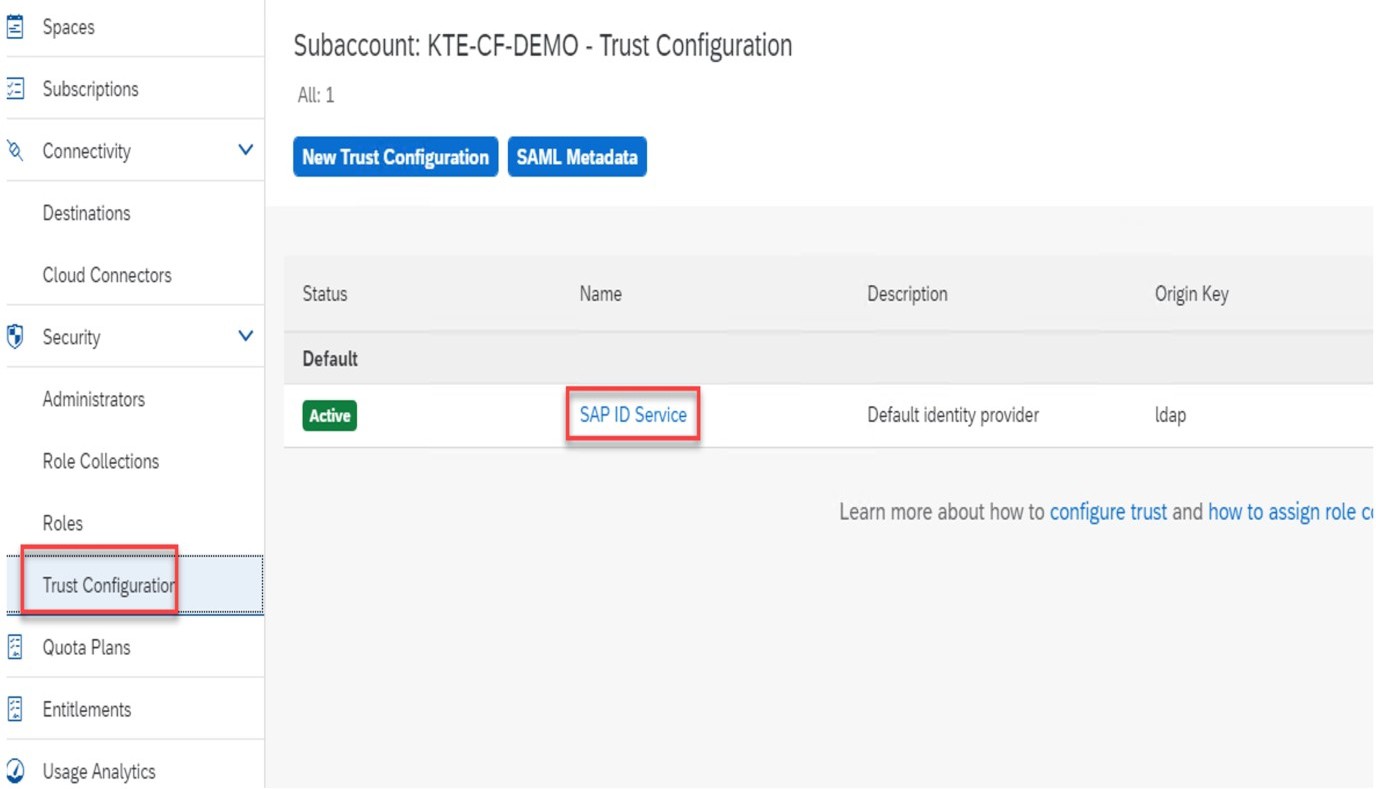
* 1. Call *Security* → *Role Collections* .
  2. Show the created Role Collection with name *extensibility-demo-advanced*.



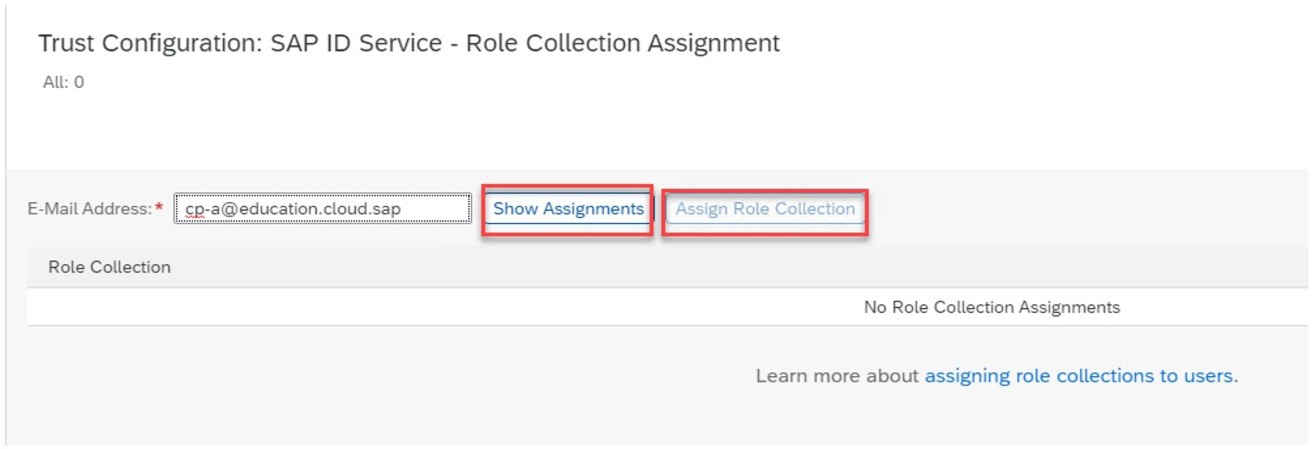
* 1. Click on the link *extensibility-demo-advanced* . This is assigned the role Viewer from the XSUAA configuration.

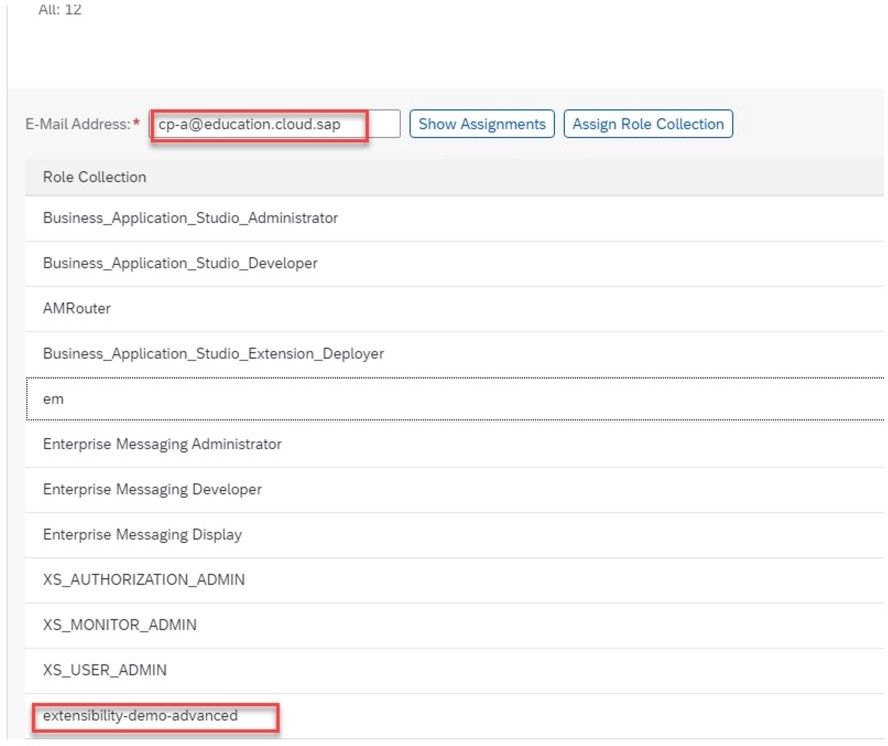


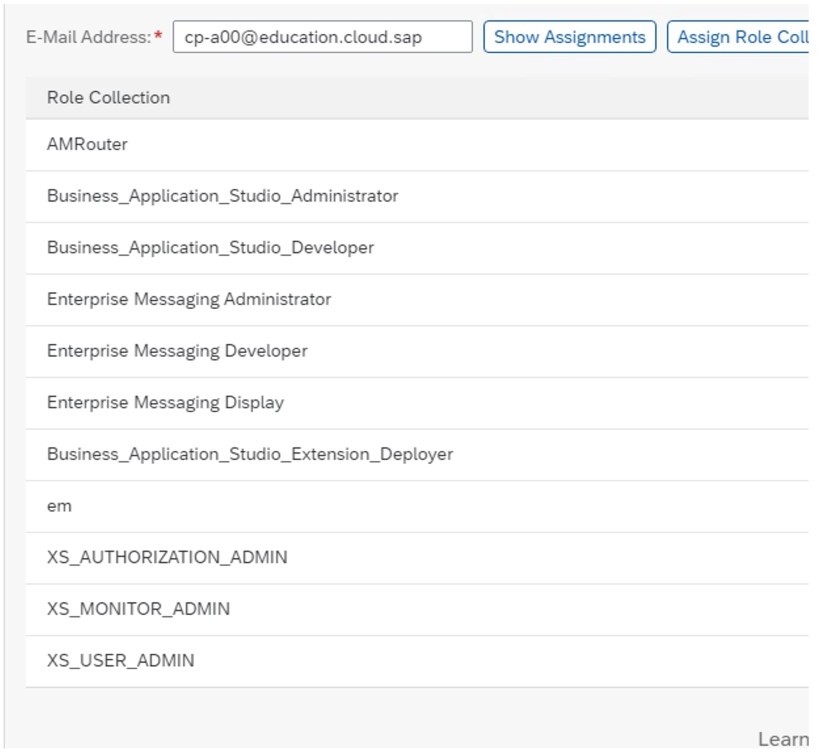
* 1. Call *Secucity Trust Configuration*.



* 1. Click on the *SAP ID Service* link and in the *E-Mail-Address* field enter **cp-** [**a@education.cloud.sap**.](mailto:a@education.cloud.sap)



* 1. Click on the link *Show Assignments* after that the link Assign Role Collection becomes active via this one you can then assign the previously created Role Collection.
  2. Assignment for user [cp-a@education.cloud.sap](mailto:cp-a@education.cloud.sap) - Assignment of the Role Collection extensibility-demo-advanced
  3. Assignment for user [cp-a00@education.cloud.sap](mailto:cp-a00@education.cloud.sap) - no assignment of the Role Collection extensibility-demo-advanced:



1. Check if the Authorization works.



Note:

* cp-a@education.cloud.sap/Welcome1 - is authorized for / businesspartners-resilience.
* cp-a00@education.cloud.sap/Welcome1 - is not authorized for / businesspartners-resilience.
  1. Call the app via: https://approuter-ktedev.cfapps.eu10.hana.ondemand.com
  2. As login enter the following data:

|  |  |
| --- | --- |
| Field | Value |
| User | [cp-a@education.cloud.sap](mailto:cp-a@education.cloud.sap) |
| Password | Welcome1 |



Note:

This information is subject to change. in case of issues, refer to the SSG.

* 1. If the call is successful:
  2. Login with the following data:

|  |  |
| --- | --- |
| Field | Value |
| User | [cp-a00@education.cloud.sap](mailto:cp-a00@education.cloud.sap) |
| Password | Welcome1 |



Note:

This information is subject to change. in case of issues, refer to the SSG.

* 1. Call the link */businesspartners-resilience*.
  2. If the call is not successful:



* 1. Login with the following data:

|  |  |
| --- | --- |
| Field | Value |
| User | [cp-a00@education.cloud.sap](mailto:cp-a00@education.cloud.sap) |
| Password | Welcome1 |



Note:

This information is subject to change. in case of issues, refer to the SSG.

* 1. Call the link */businesspartners-simple*. Call successul.

LESSON SUMMARY

You should now be able to:

* Appreciate the secure implementation of a microapp

Unit 6

# Learning Assessment

## 267

1. The current domain model consists of:

*Choose the correct answer.*

* 1. Space, Account, Subaccounts
  2. Domain host, Spaces, Accounts
  3. Account, Subaccount(s), Spaces

1. Identity providers (IDP) are used for user authentication.

*Determine whether this statement is true or false.*

True

False

1. The AppRouter is a Node.js component, distributed via the publically available SAP NPM registry.

*Determine whether this statement is true or false.*

True

False

Unit 6

# Learning Assessment - Answers

## 268

1. The current domain model consists of:

*Choose the correct answer.*

* 1. Space, Account, Subaccounts
  2. Domain host, Spaces, Accounts
  3. Account, Subaccount(s), Spaces

X

This is correct. Correct is: Account, Subaccount(s), Spaces.

1. Identity providers (IDP) are used for user authentication.

*Determine whether this statement is true or false.*

True

X

False

This is correct. The statement is correct.

1. The AppRouter is a Node.js component, distributed via the publically available SAP NPM registry.

*Determine whether this statement is true or false.*

True

X

False

This is correct. The statement is correct.