



Week 6: Additional Topics

Unit 1: Multitenant Identity and Access Management

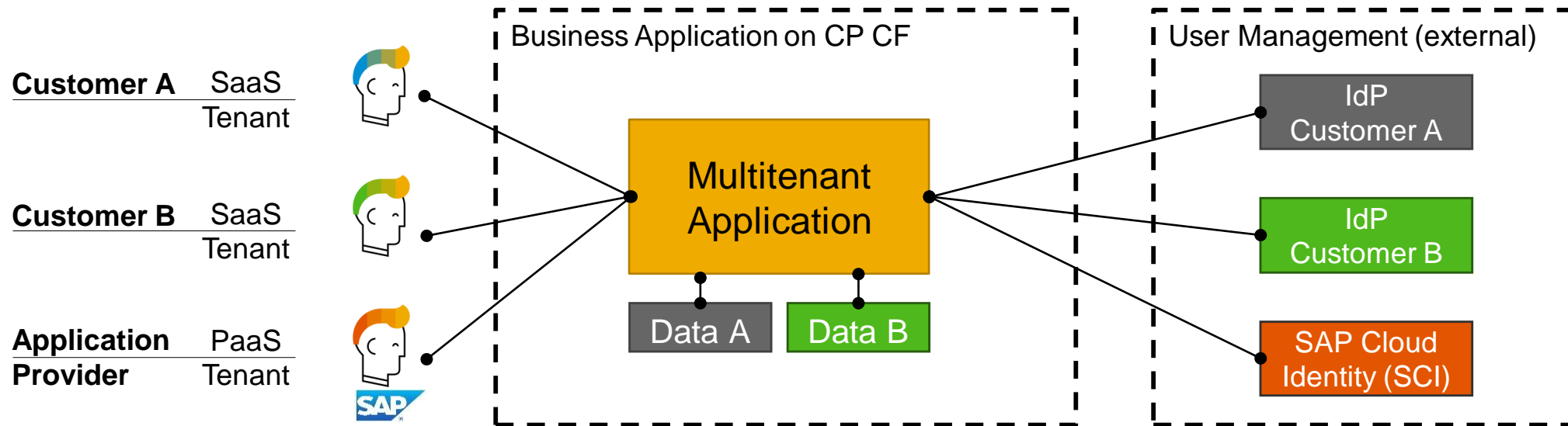
Multitenant Identity and Access Management

What is a multitenant cloud application?

One application instance can serve requests from multiple customers.

Definition

Multitenancy refers to a software architecture in which multiple customers (a.k.a. tenants) share the same technical resources while keeping **Identity and Access Management (IAM)** and data separated.



Multitenant Identity and Access Management

Multitenancy @ SAP Cloud Platform

1. In SAP Cloud Platform, each tenant has a separate **identity zone in SAP UAA**. This allows isolated user management per tenant.
2. This concept includes a multitenant-enabled application router which is deployed with a multitenant application. A multitenant application is called with a **tenant-specific URL**.
URL schema: <https://<tenant>.<app>.<domain>>

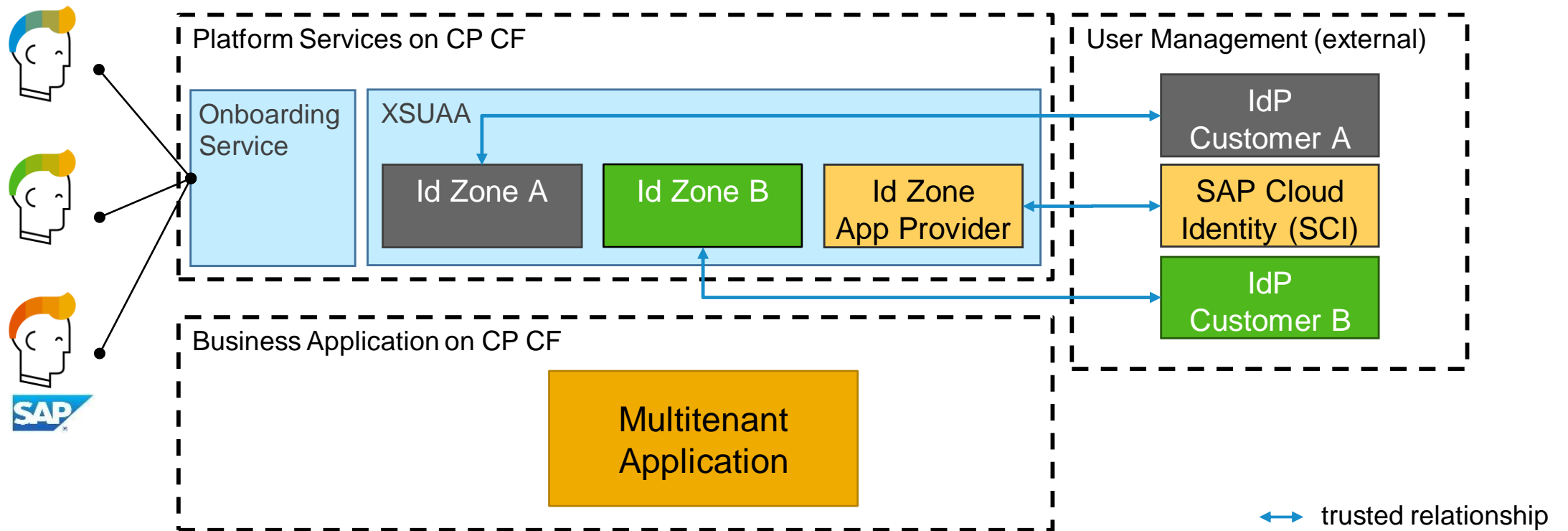
Labs preview:

3. SAP Cloud Platform provides **onboarding services** to create new tenants and to **subscribe** to a multitenant application.
4. A multitenant application can implement a **callback method** to be notified on new subscriptions.

Multitenant Identity and Access Management

Identity zones separate user management into different security realms for XSUAA

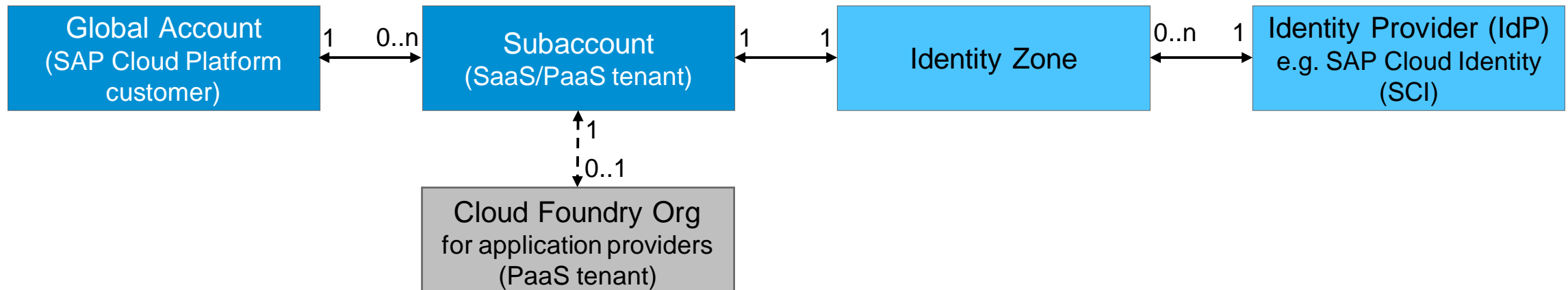
1. In SAP CP CF, each tenant has a separate **identity zone in SAP UAA**. This allows isolated user management per tenant.



Multitenant Identity and Access Management

Identity zones separate user management into different security realms for XSUAA

1. In SAP CP CF, each tenant has a separate **identity zone in SAP UAA**.
This allows isolated user management per tenant.

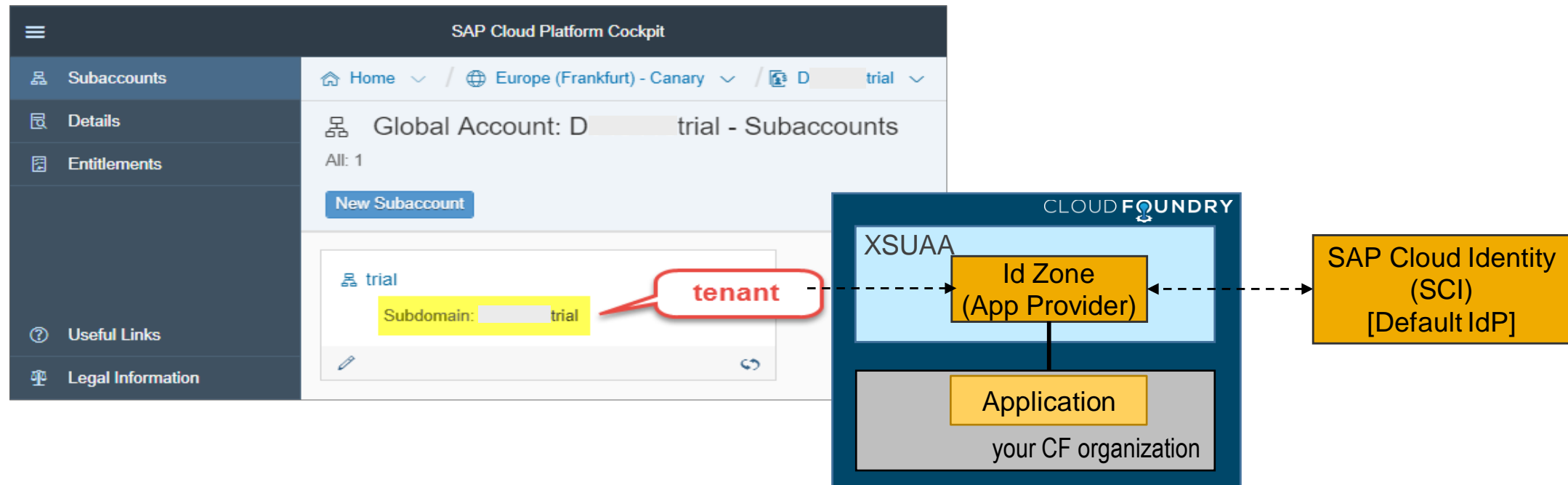


- Each customer (SaaS tenant) and application provider (PaaS tenant) requires a **subaccount** to attach via its corresponding **identity zone** their **IdPs**.

Multitenant Identity and Access Management

Identity zones separate user management into different security realms for XSUAA

1. In SAP CP CF, each tenant has a separate **identity zone** in **SAP UAA**. This allows isolated user management per tenant.

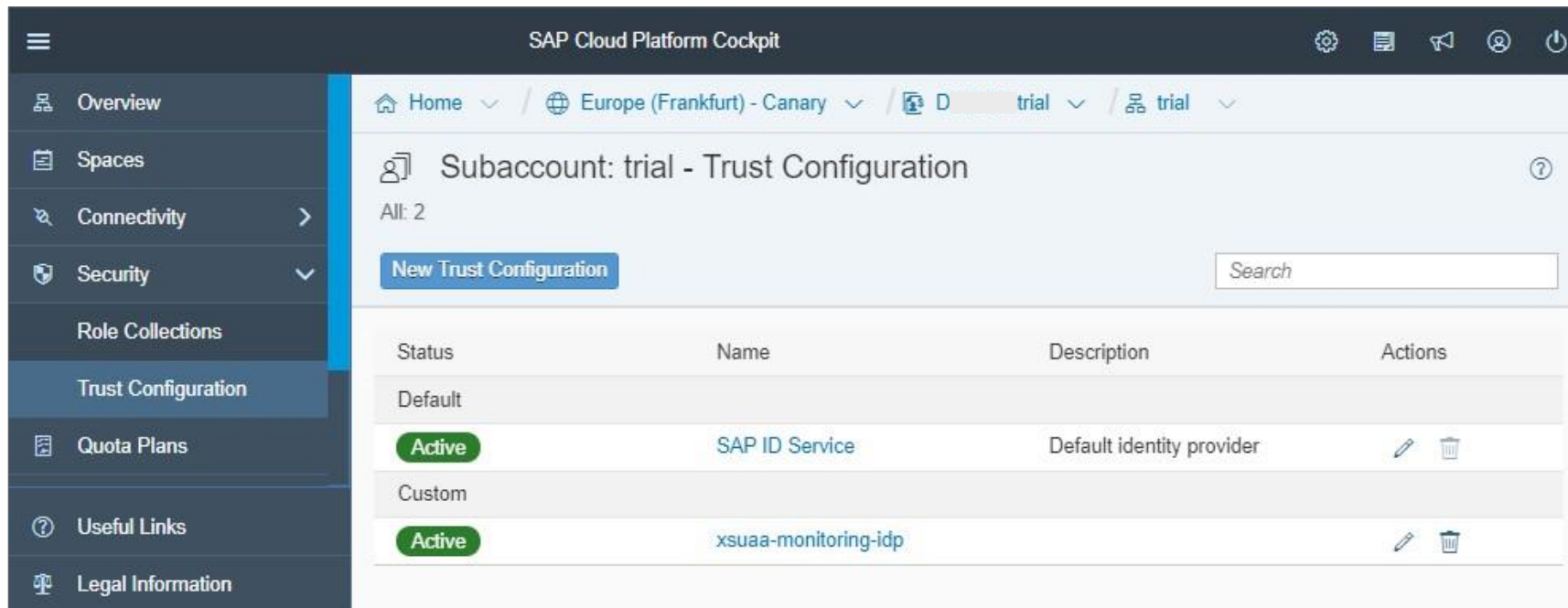


- During onboarding, the **identity zone** e.g. *d012345trial* is created automatically. The **subdomain** represents the **tenant** used in the Cloud Foundry environment.

Multitenant Identity and Access Management

Identity zones separate user management into different security realms for XSUAA

1. In SAP CP CF, each tenant has a separate **identity zone in SAP UAA**. This allows isolated user management per tenant.



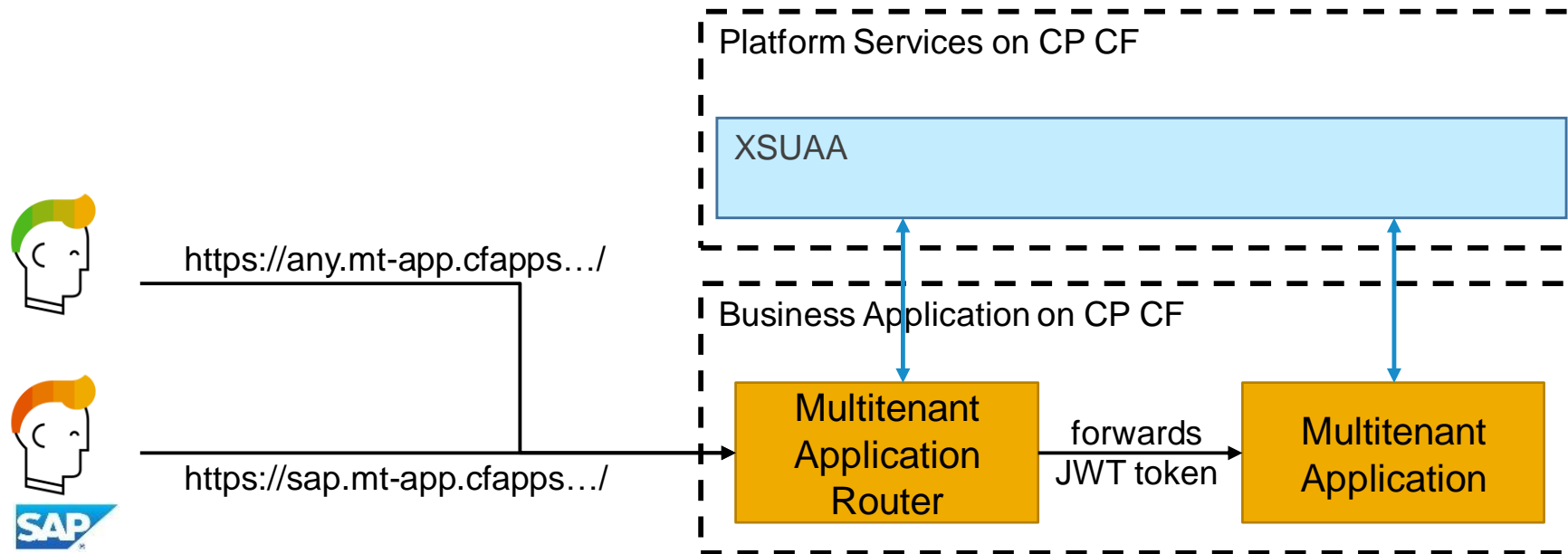
- The administrator on the customer side needs to establish trust between the XSUAA identity zone and the customer IdP for each subaccount.

Multitenant Identity and Access Management

Tenant-aware application security setup

2. This concept includes a multitenant-enabled application router which is deployed with a multitenant application. A multitenant application is called with a **tenant-specific URL**.

URL schema: <https://<tenant>.<app>.<domain>>



[Related Exercises: 22 - 24](#)

Note: With no customer-specific subdomain, the URL schema to be used is <https://<tenant>-<app>.<domain>> (requires no SSL certificate configuration)

Multitenant Identity and Access Management

Tenant-aware application security setup

2. This concept includes a multitenant-enabled application router which is deployed with a multitenant application. A multitenant application is called with a **tenant-specific URL**.

URL schema: <https://<tenant>.<app>.<domain>>

SAP Cloud Platform Cockpit

Home / Europe (Frankfurt) - Canary / D-!t500 trial / dev / bulletinboard-ads

Application: bulletinboard-ads - Roles

All: 2

New Role

Search

Application Identifier	Role Name	Role Template	Description	Actions
bulletinboard-d-!t500	Advertiser	Advertiser	Default instance	+ ✎ 🗑
bulletinboard-d-!t500	Viewer	Viewer	Default instance	+ ✎ 🗑

`$XSAPPNAME == <XSAPPNAME>!t<tenant index> == unique app id`

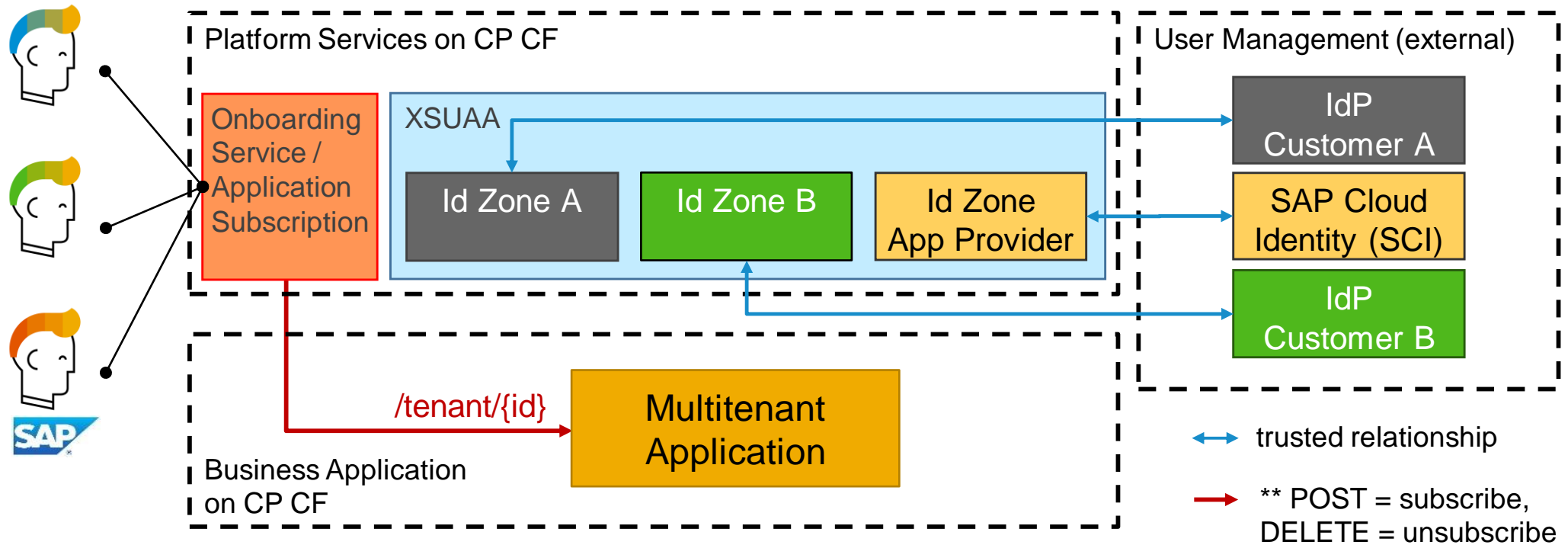
- Note: XSUAA creates tenant index to ensure unique app ids when the same application is deployed into several spaces. XSAPPNAME is suffixed with !t<tenant index>.

Multitenant Identity and Access Management

Not public available: application subscription

Labs Preview

3. SAP CP provides **onboarding services** to create new tenants and to **subscribe** to a multitenant application.



Multitenant Identity and Access Management

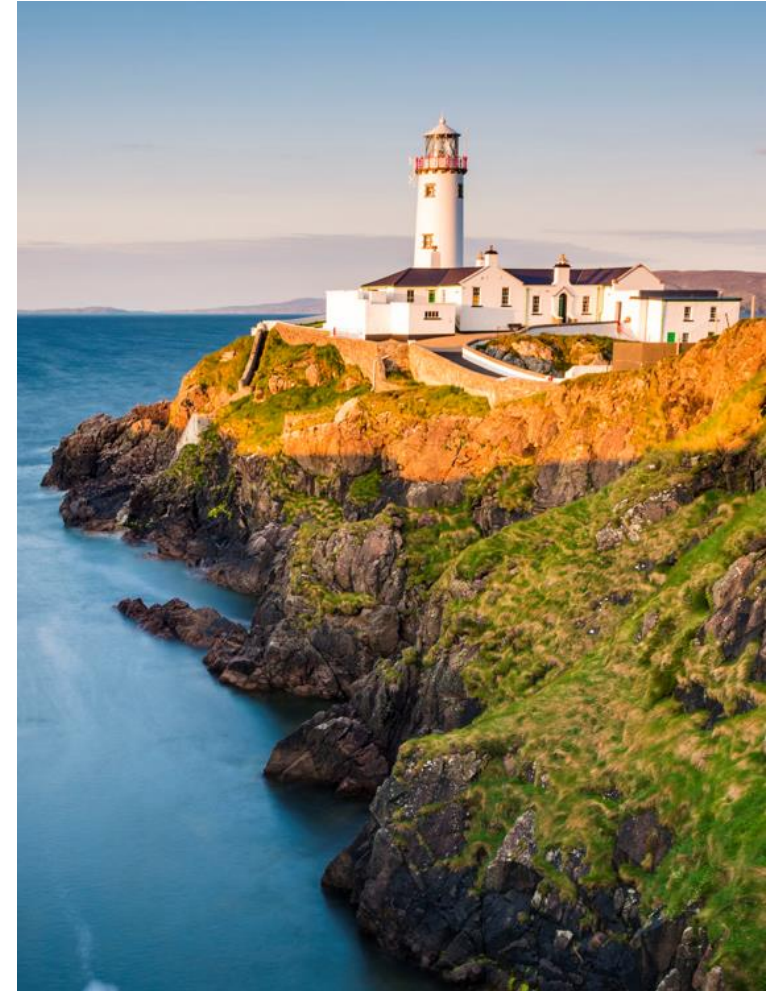
Demo



Multitenant Identity and Access Management

What you've learned in this unit

- What a multitenant cloud application is
- Multitenant identity and access management @ SAP Cloud Platform
 - How it works
 - How to set up user management



Thank you.

Contact information:

open@sap.com

© 2018 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See <http://global.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.