Securing the S/4HANA Extension App

PUBLIC

THE BEST RUN SAP

Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP’s intentional or gross negligence.

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, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

© 2019 SAP SE or an SAP affiliate company. All rights reserved. ǀ PUBLIC

Securing the Extension App

Authorization and authentication

Authentication

… answers the question “Who is the user?”

Authorization

… answers the question “What is the user allowed to do?”

© 2019 SAP SE or an SAP affiliate company. All rights reserved. ǀ PUBLIC

Identity Federation

Identity federation is the **concept of linking and reusing electronic identities** of a user **across multiple identity providers**.

This frees an application from the obligation to obtain and store users' credentials for authentication.
Instead, the application reuses an identity provider that is already storing users' electronic identities for authentication, provided that the application trusts this identity provider.

This makes it possible to **decouple and centralize authentication and authorization** functionality.

© 2019 SAP SE or an SAP affiliate company. All rights reserved. ǀ PUBLIC

SAML

The Security Assertion Markup Language (SAML) is
an **open standard based on XML**
for **exchanging authentication and authorization data** of a user
between an **identity provider (IdP)** and a **service provider (SP)**

The data is exchanged using messages called **bearer assertions.**

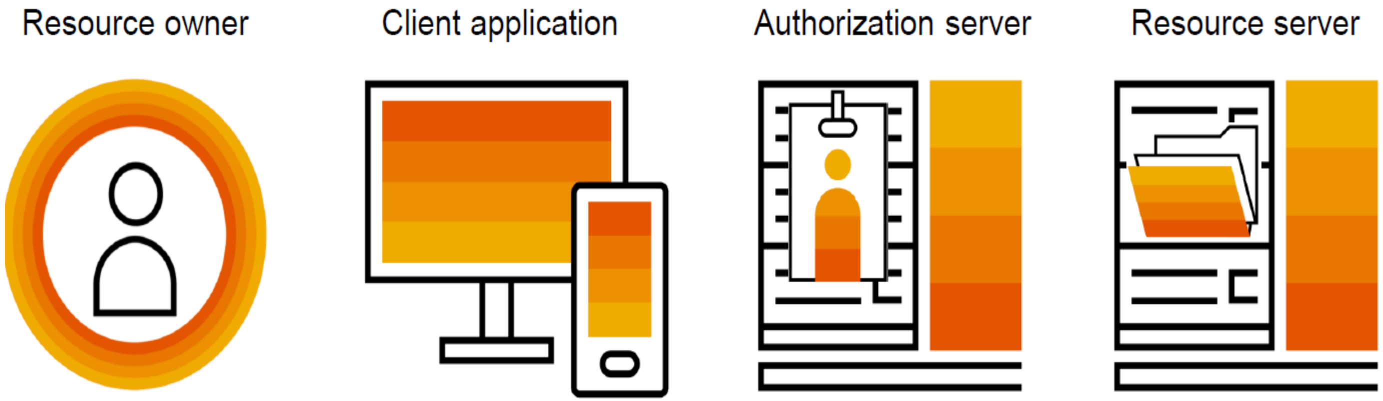
A bearer is any party in possession of the assertion.

The integrity of the assertion is protected by XML encryption and an XML signature.

SAML addresses the requirement of web browser **single sign-on** across the Internet.

© 2019 SAP SE or an SAP affiliate company. All rights reserved. ǀ PUBLIC

OAuth 2.0 authorization framework



OAuth 2.0 is an open standard framework that can securely issue and validate tokens for services on the Internet.

Resource owner or user who owns the data.
Client application who wants to access or manipulate the user data. It can be a Web or mobile app.
Authorization server that issues access tokens to the client application which are used to request access to the user data.
Resource server retrieves the user data if the Resource Owner authorizes it.

© 2019 SAP SE or an SAP affiliate company. All rights reserved. ǀ PUBLIC

JWT Token

JSON Web Token (JWT) is an emerging **open standard** that defines
a **compact token format**
for **securely transmitting information** between parties
as a **JSON object**.

This information can be verified and trusted because it is **digitally signed** with the private key of the authorization server (UAA service).

© 2019 SAP SE or an SAP affiliate company. All rights reserved. ǀ PUBLIC

App Router

App router is
a **Node.js application**
provided by SAP
that is the **central entry point** for our application in SAP Cloud Platform

Using the app router allows us to dissect our application into multiple microservices, while hiding the resulting complexity from our end users.

App router **dispatches requests to our application/micro-service** in SAP CP, and thus, **acting as a reverse proxy**.

The **back-end application/microservices shall not be directly accessible** to the client.

© 2019 SAP SE or an SAP affiliate company. All rights reserved. ǀ PUBLIC

XSUAA - User Account and Authentication service

XSUAA is an **SAP-specific extension of Cloud Foundry's UAA service** to deal with authentication and authorization.

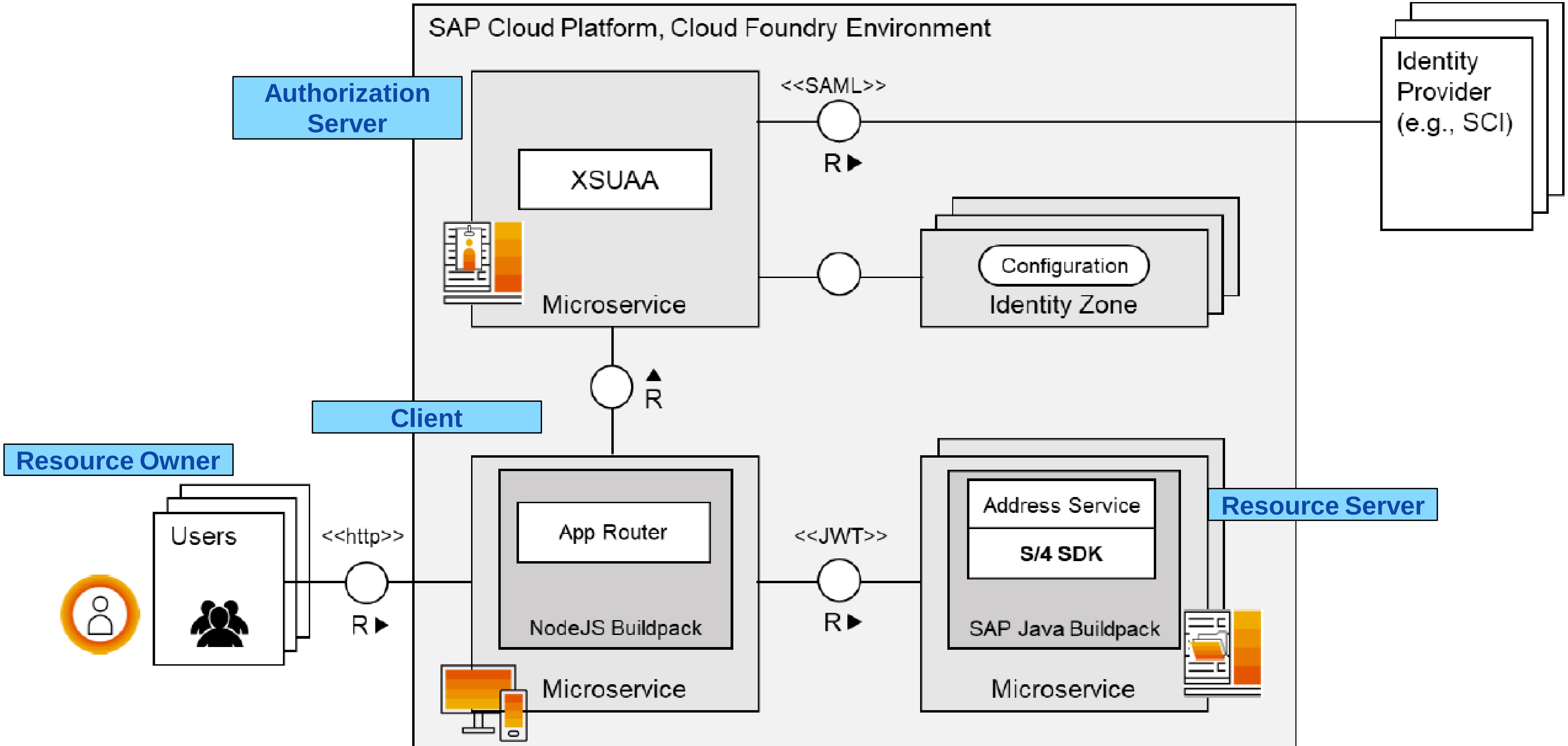
XSUAA is connected to an identity provider (IdP)

XSUAA acts as a Authorization Server

© 2019 SAP SE or an SAP affiliate company. All rights reserved. ǀ PUBLIC

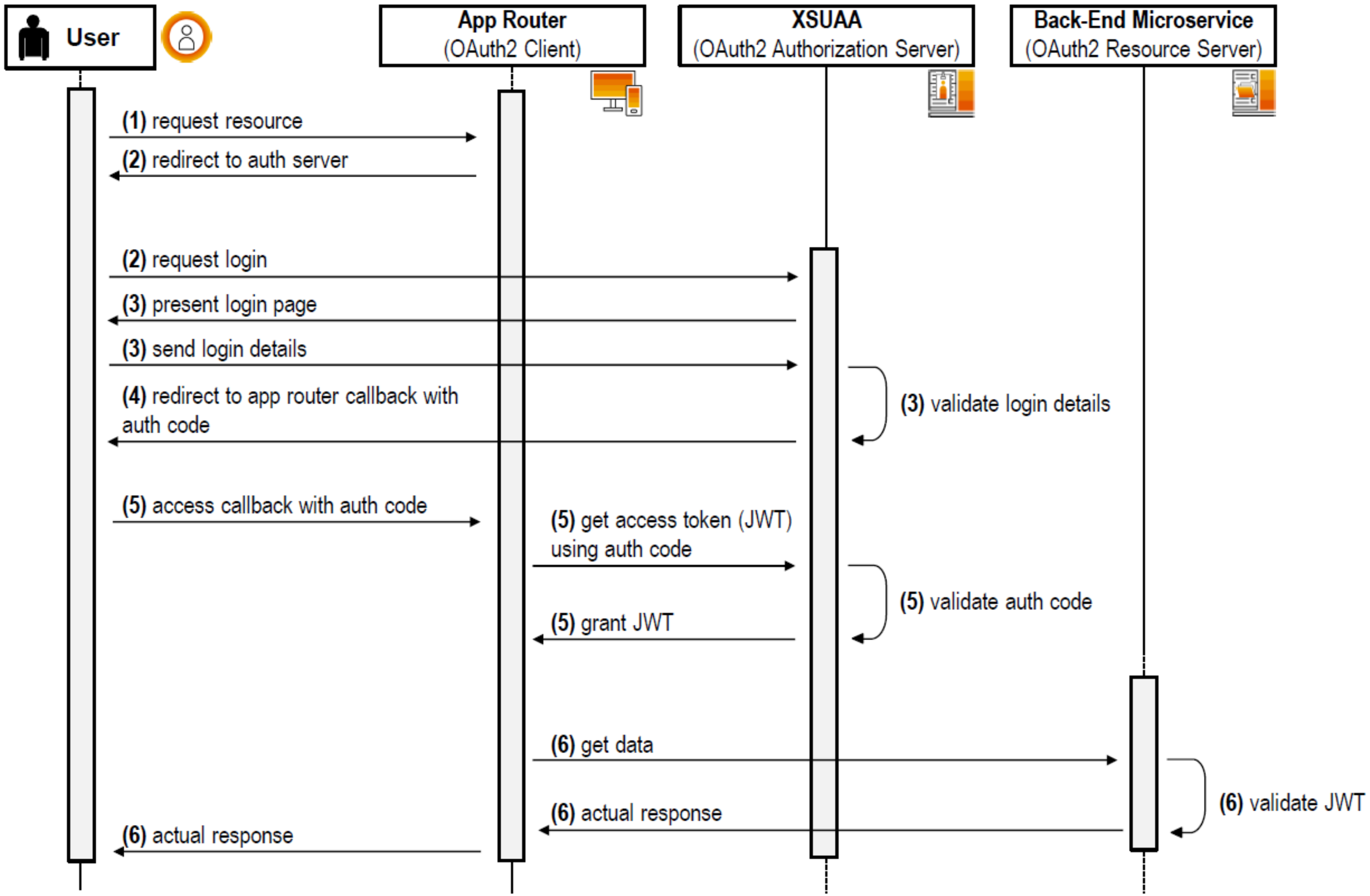
Securing the Extension App

Security on SAP Cloud Platform: high-level authentication setup with app router and XSUAA



© 2019 SAP SE or an SAP affiliate company. All rights reserved. I PUBLIC

Call Flow



User

App Router
(OAuth2 Client)

XSUAA
(OAuth2 Authorization Server)

Back-End Microservice
(OAuth2 Resource Server)

(1) request resource

(2) redirect to auth server

(2) request login

(3) present login page

(3) send login details

(3) validate login details

(4) redirect to app router callback with auth code

(5) access callback with auth code

(5) get access token (JWT) using auth code

(5) validate auth code

(5) grant JWT

(6) get data

(6) validate JWT

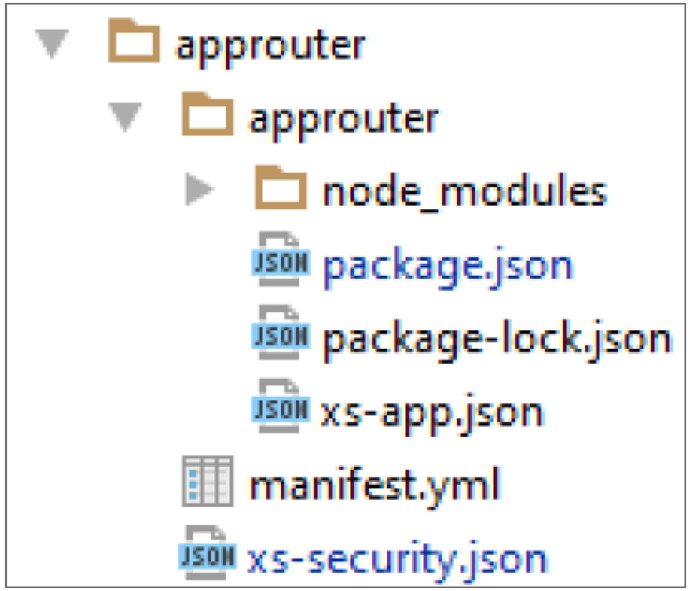
(6) actual response

(6) actual response

© 2019 SAP SE or an SAP affiliate company. All rights reserved. ǀ PUBLIC

Securing the Extension App

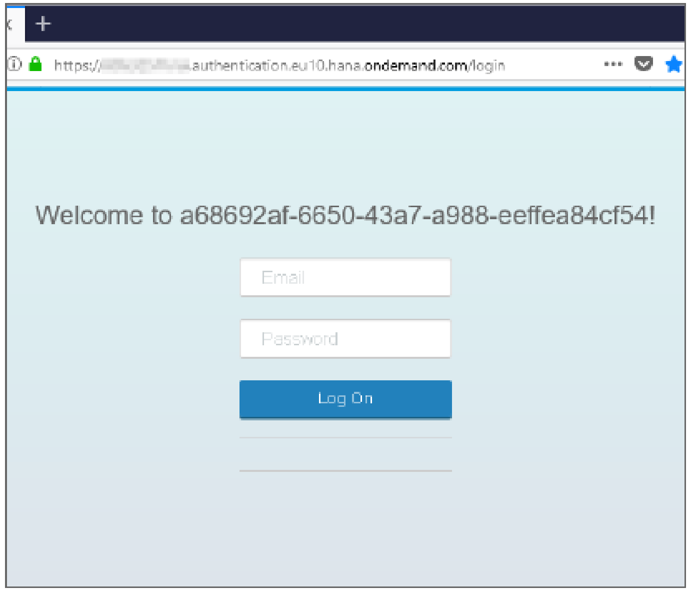
Set up authentication: required steps



```
approuter
  approuter
    node_modules
    package.json
    package-lock.json
    xs-app.json
  manifest.yml
  xs-security.json
```

Set up the app router

- App router is a NodeJS component that is distributed via the publicly available SAP NPM registry. It will play the role of OAuth 2.0 client in our setup

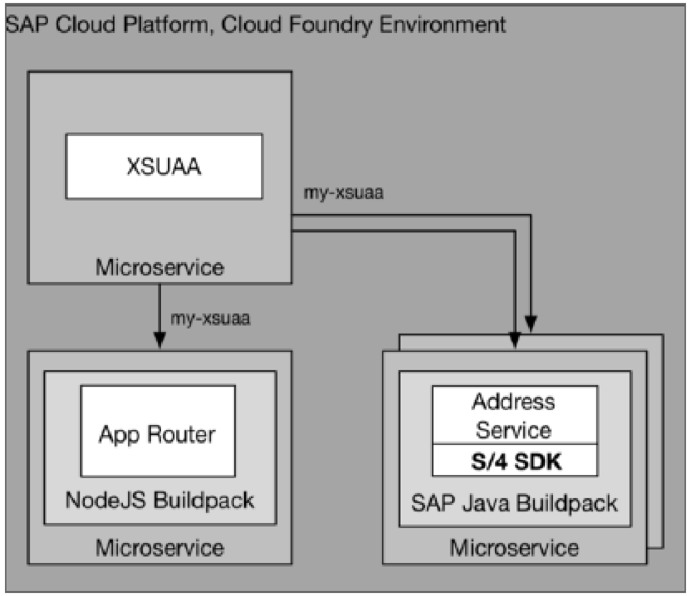


https:/[redacted].authentication.eu10.hana.ondemand.com/login

Welcome to a68692af-6650-43a7-a988-eeffea84cf54!

Protect back-end microservice

- Only accept requests with valid JWTs for the current user provided by the app router



Bind microservices to XSUAA

- This will enable microservices to verify the JWT signatures

© 2019 SAP SE or an SAP affiliate company. All rights reserved. I PUBLIC

Securing the Extension App

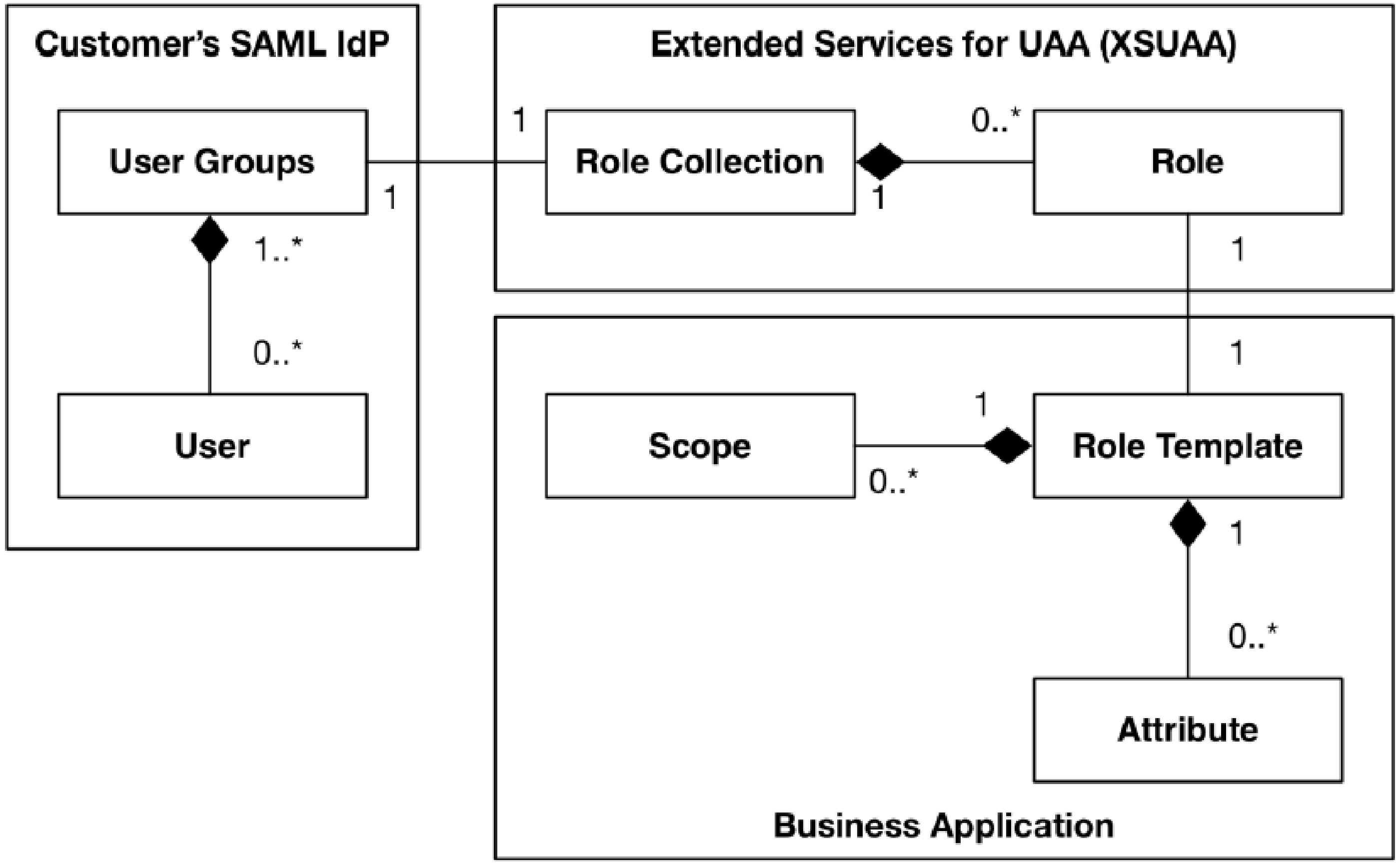
Set up authorization: relationships of authorization concepts on SAP Cloud Platform

Scope: for functional authorization checks

Attribute: for instance-based (data) authorizations (e.g. the name of a cost center)

Role template: description of roles (for example, “employee” or “manager”) to apply to a user and any attributes that apply to the roles

Roles: are created based on role templates at configuration time in the SAP Cloud Platform cockpit



© 2019 SAP SE or an SAP affiliate company. All rights reserved. ǀ PUBLIC

Demo

Questions & answers

Thank you.

Run Simple

© 2019 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.