ManfredSteyer

Login & Access Control in Angular

Manfred Steyer
SOFTWAREarchitekt.at

Contents

- Motivation
- OAuth 2
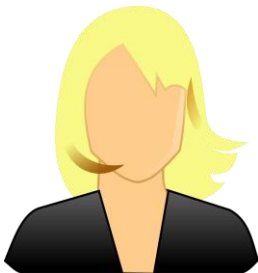- Single Sign on and OpenId Connect
- Social Login
- DEMO
- Single Sign out

SOFTWAREarchitekt.at

Motivation

SOFTWARE*architekt.at*

Access to App and Backend

SOFTWARE*architekt.at*

Requirements for Modern Apps

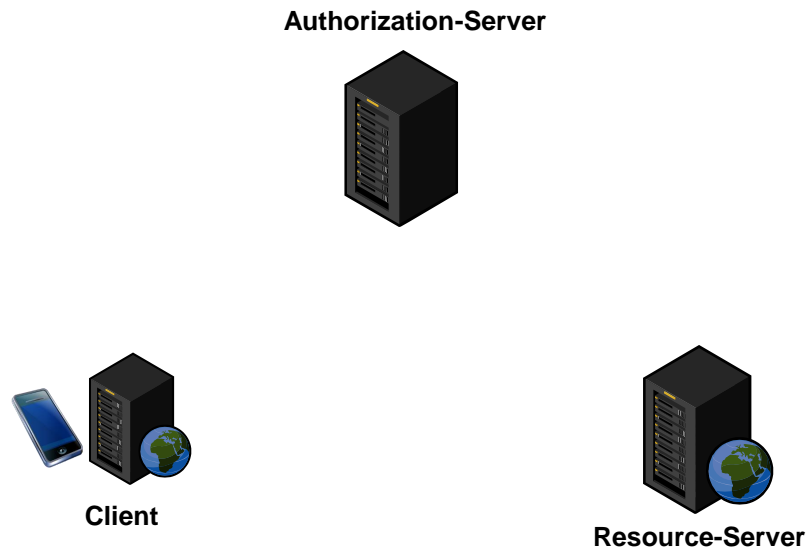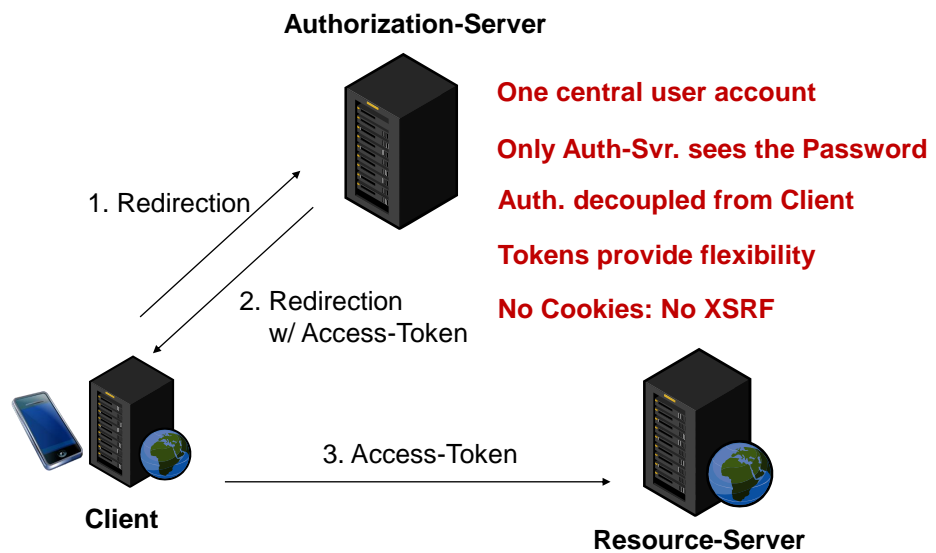|		
Service delegates to other services	Cross Origin Requests	Using existing Identity Solutions
Loosely Coupling to Identity Solution	Single Sign on/ out	Protect from XSRF

SOFTWARE *architekt.at*

SOFTWARE *architekt.at*

Roles

Authorization-Server

Client

Resource-Server

Folie▪ 10

SOFTWARE*architekt.at*

Flow

Authorization-Server

One central user account

Only Auth-Svr. sees the Password

1. Redirection

Auth. decoupled from Client

Tokens provide flexibility

2. Redirection
w/ Access-Token

No Cookies: No XSRF

3. Access-Token

Client

Resource-Server

Folie▪ 11

SOFTWARE*architekt.at*

Authorization Server === just some endpoints ;-)

SOFTWARE_architekt.at_

Roles

Authorization-Server
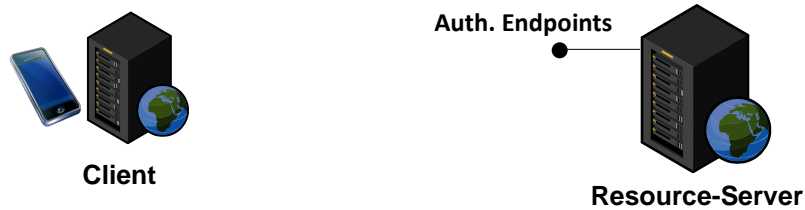
Client

Resource-Server

Folie▪ 13

SOFTWARE_architekt.at_

Roles (simplified Scenario)

Auth. Endpoints

Client

Resource-Server

SOFTWAREarchitekt.at

Lots of Auth Server out there …

On Premise

Active Directory Federation Services	Identity Server (.NET)	Readhad Keycloak (Java)	Okta
Auth0	Firebase	Azure Active Directory	…

Identity as a Service
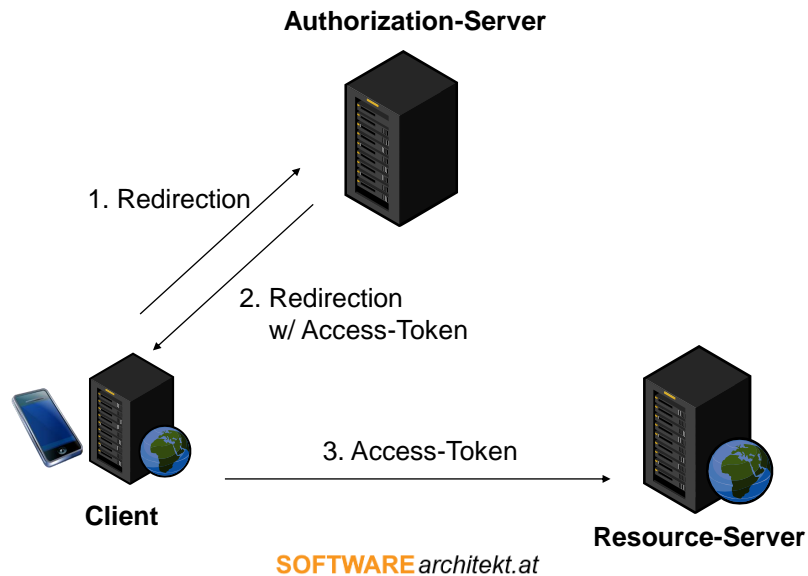
SOFTWAREarchitekt.at
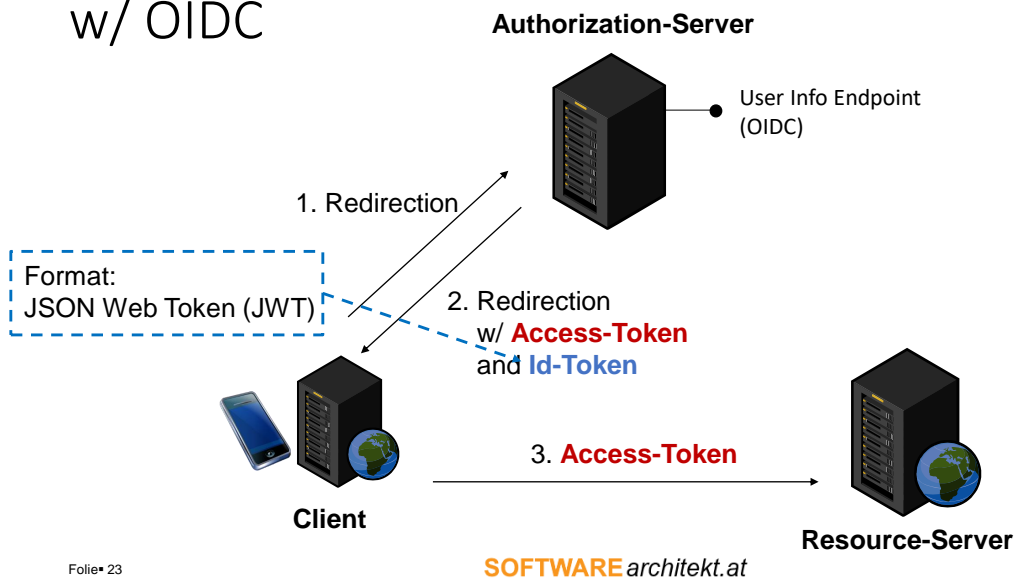
OAuth 2

What is OAuth 2?

- Developed by Twitter and Ma.gnolia
- Protocol to delegate restricted rights
- Used by Companies like Google, Facebook, Flickr, Microsoft, Salesforce.com or Yahoo!
- Several Flows for different use cases
- Leverages HTTPS!

Folie▪ 17

SOFTWARE *architekt.at*

Implicit Flow for SPA

Authorization-Server

1. Redirection

2. Redirection
w/ Access-Token

3. Access-Token

Client

Resource-Server

SOFTWARE*architekt.at*

Implicit Flow
w/ OIDC

Authorization-Server

User Info Endpoint
(OIDC)

1. Redirection

Format:
JSON Web Token (JWT)

2. Redirection
w/ **Access-Token**
and **Id-Token**

3. **Access-Token**

Client

Resource-Server

SOFTWARE*architekt.at*

Fazit

Token: Flexibility, Cross Origin …	OAuth 2: Access to Service
OpenId Connect: SSO at Client	Implicit Flow

SOFTWAREarchitekt.at

Contact und Downloads

[mail] manfred.steyer@**SOFTWARE**architekt.at

[blog] **SOFTWARE**architekt.at

[twitter] ManfredSteyer

SOFTWAREarchitekt.at