Cloak and Dagger Stories

Absichern von Anwendungen mit Keycloak

Wer bin ich?

Gregor Tudan

GregOrT
gregor.tudan@cofinpro.de

State of IT-Security

Have I been pawned?

COFINPRO

haveibeenpwned.com

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address | pwned?

Generate secure, unique passwords for every account — Learn more at 1Password.com

Why 1Password?

365	7,858,388,981	95,948	117,300,702
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
593,427,119	Exploit.In accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts

Recently added breaches

41,960	Ordine Avvocati di Roma accounts
161,143	OGUsers accounts
49,681	Appartoo accounts
1,688,176	Club Penguin Rewritten accounts
2,467,304	Morele.net accounts
13,369,666	Bukalapak accounts
760,561	DataCamp accounts

Warum sichere Anmeldung schwer ist:

Provider bauen Mist

- Roll your own crypto
- Kennwörter im Klartext
- seltsame Password-Policies
- veraltete Verfahren (keine 2FA)
- Sicherheitslücken (XSS, Injection…)

User bauen Mist

- zu leichtes Kennwort
- selbes Kennwort überall
- Social Engineering
- zu faul für 2FA

»Lege nicht alle Eier in einen Korb«
— Sprichwort

»Lege all deine Eier in einen Korb – und dann gib recht acht auf den Korb«
— Marc Twain

Worüber rede ich?

1. kleine Einführung in OAuth
2. das Keycloak-Projekt
3. Absichern von Anwendungen
   - "klassische" Webanwendungen
   - Single-Page-Apps
   - Mobile Apps

OAuth

"Wir machen OAuth!"

Meistens sind hier mehrere Dinge gemeint:

- OAuth 2.0
- OpenID Connect
- JSON Web-Tokens

OAuth 2.0

Resource Owner

hat eine "Resource" die geschützt werden soll

hat Credentials

Client

App mit der ein RO auf die Resource zugreift

Resource Server

hier liegt die Resource des Owners (API)

Auth-Server

prüft die Credentials des Resource-Owners

stellt einen Token für den Zugriff auf Resourcen aus

OpenID-Connect

erweitert die OAuth-Spec um:

- eine REST-API für OAuth
- die Möglichkeit Informationen zum User auszutauschen
- ein einheitliches Token-Format in JSON

Tokens

COFINPRO

Lufthansa
Nonstop you

GATE 101
SEAT 2C

SAN FRANCISCO
SFO

FRANKFURT
FRA

FLIGHT	DATE	BOARDING	CLASS	DATA
LH455	22OCT12	14:45	Business	APIS

PASSENGER
Traveller/Happy Mrs

STATUS
SEN

PRIORITY BOARDING

LH455/22OCT12, BN0007

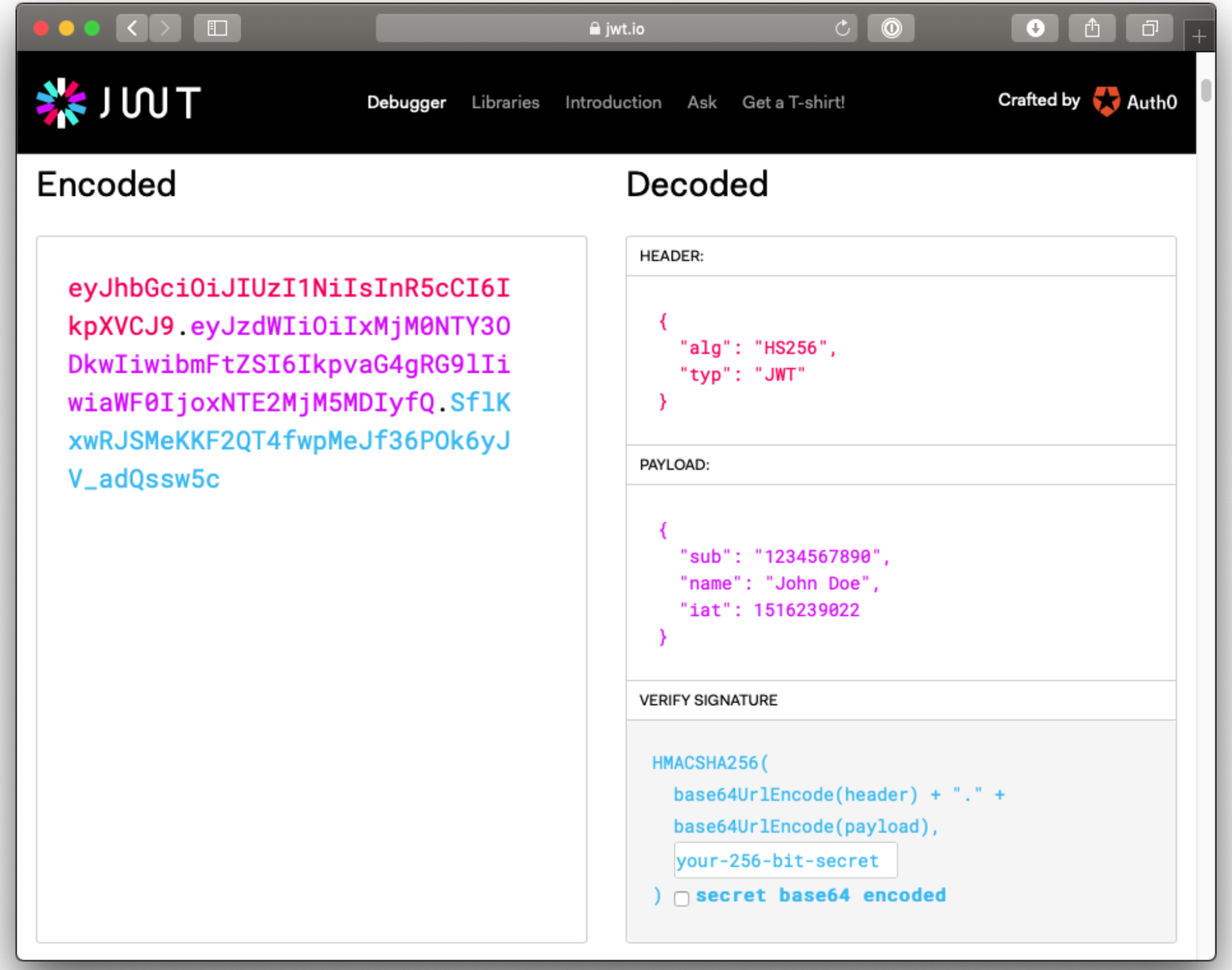
Warum Tokens?

entkoppeln Authentifizierung und Authorisierung

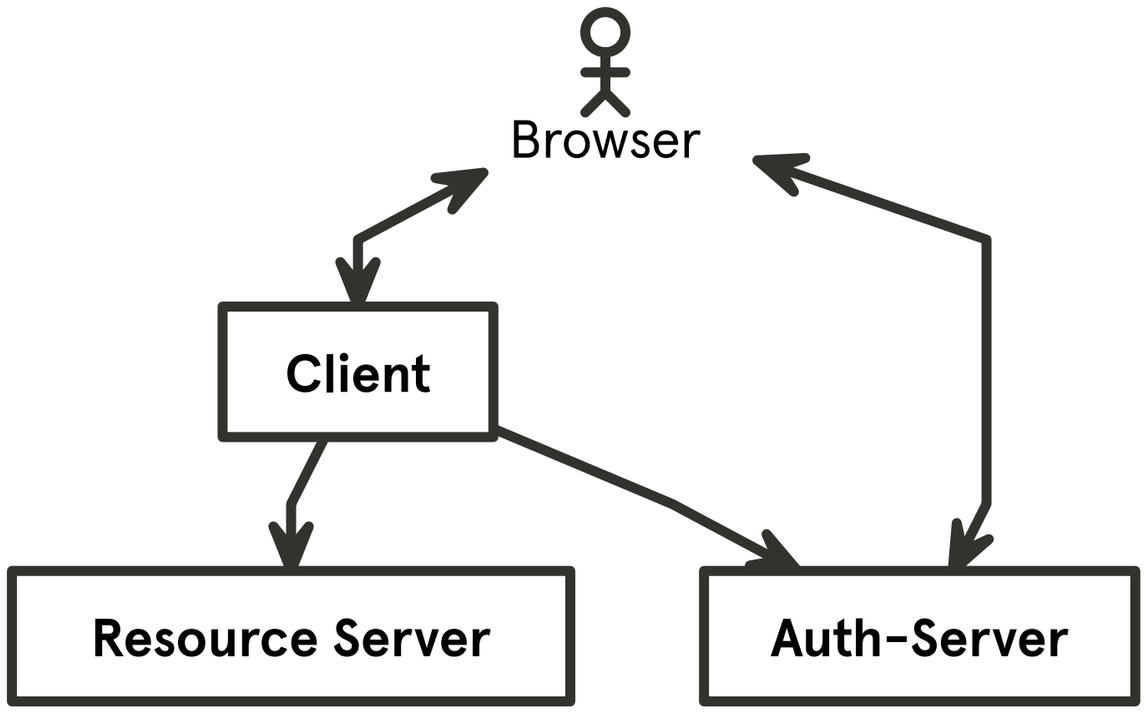
- leicht weiterzureichen
- Echtheit kann überprüft werden
- begrenzte Lebenszeit
- können Zusatzinfos enthalten

JSON Web-Tokens (JWT)

COFINPRO

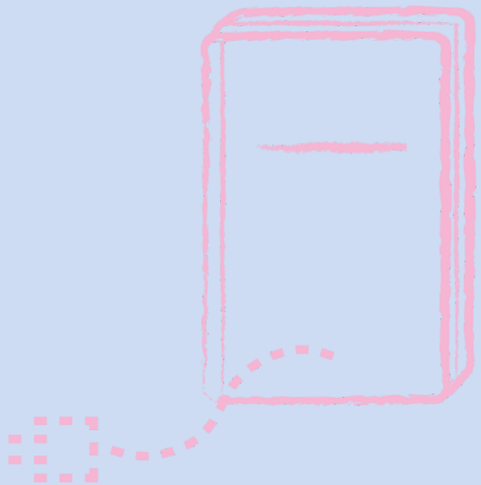

jwt.io
JWT
Debugger
Libraries
Introduction
Ask
Get a T-shirt!
Crafted by Auth0
Encoded
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
Decoded
HEADER:
{
"alg": "HS256",
"typ": "JWT"
}
PAYLOAD:
{
"sub": "1234567890",
"name": "John Doe",
"iat": 1516239022
}
VERIFY SIGNATURE
HMACSHA256(
base64UrlEncode(header) + "." +
base64UrlEncode(payload),
your-256-bit-secret
) secret base64 encoded

OAuth Flow



COFINPRO

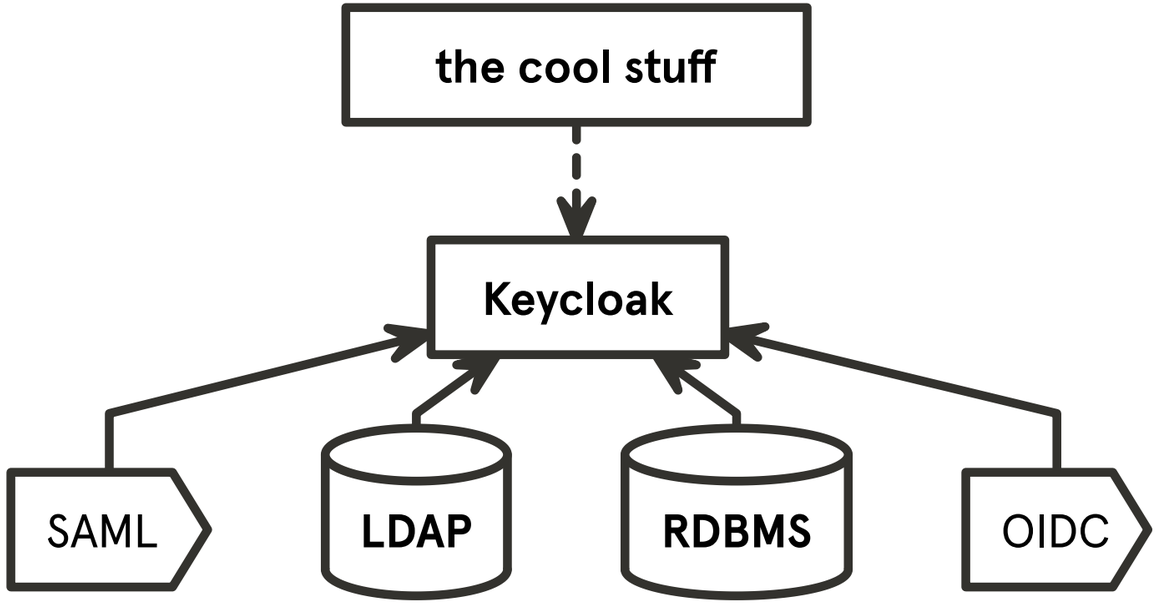
Keycloak



Keycloak ist

- ein Auth-Server für
  - OpenID Connect
  - SAML
- Open-Source
- nicht nur für Java
- von Redhat gesponsert
- der freie Ableger von Redhat Single Sign-On

Integration mit Keycloak

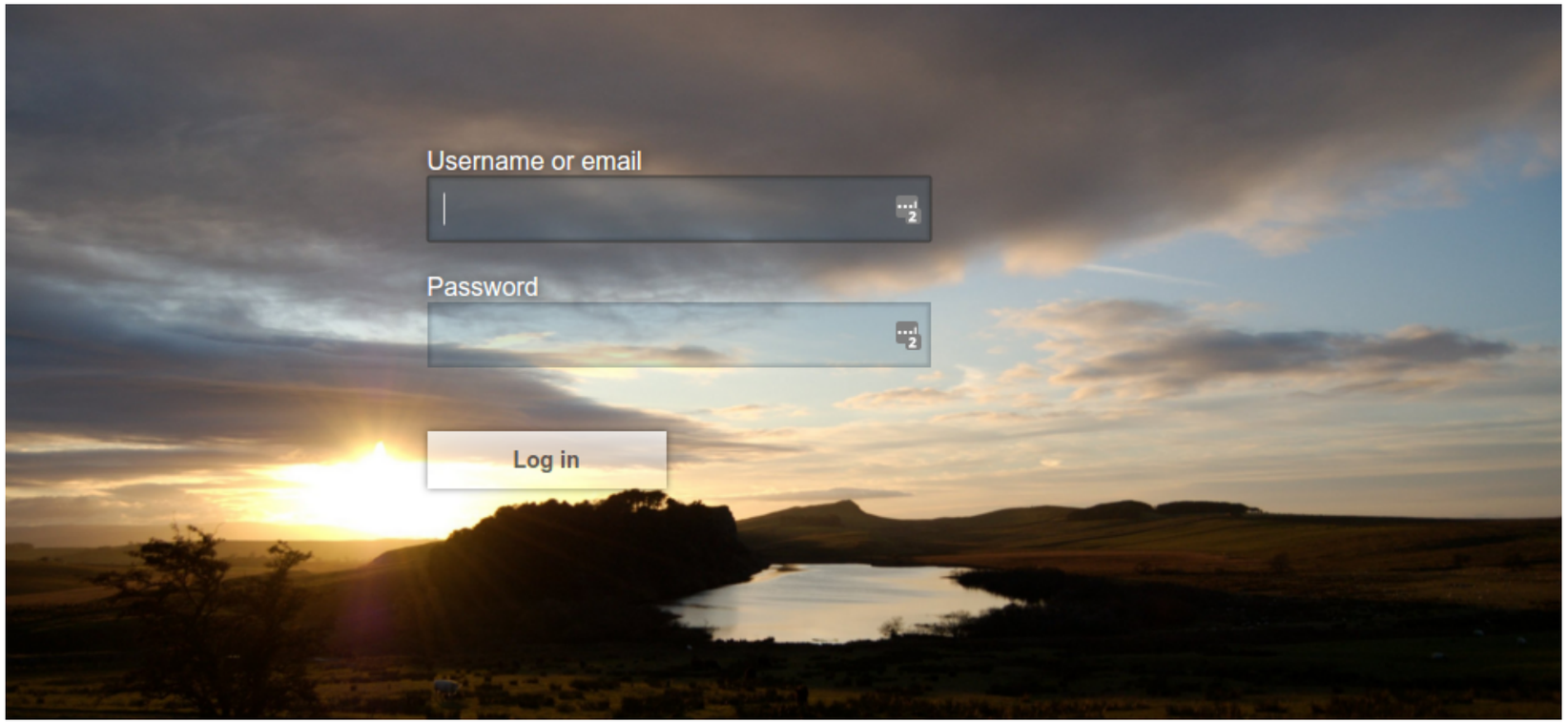


COFINPRO

mehr als Login

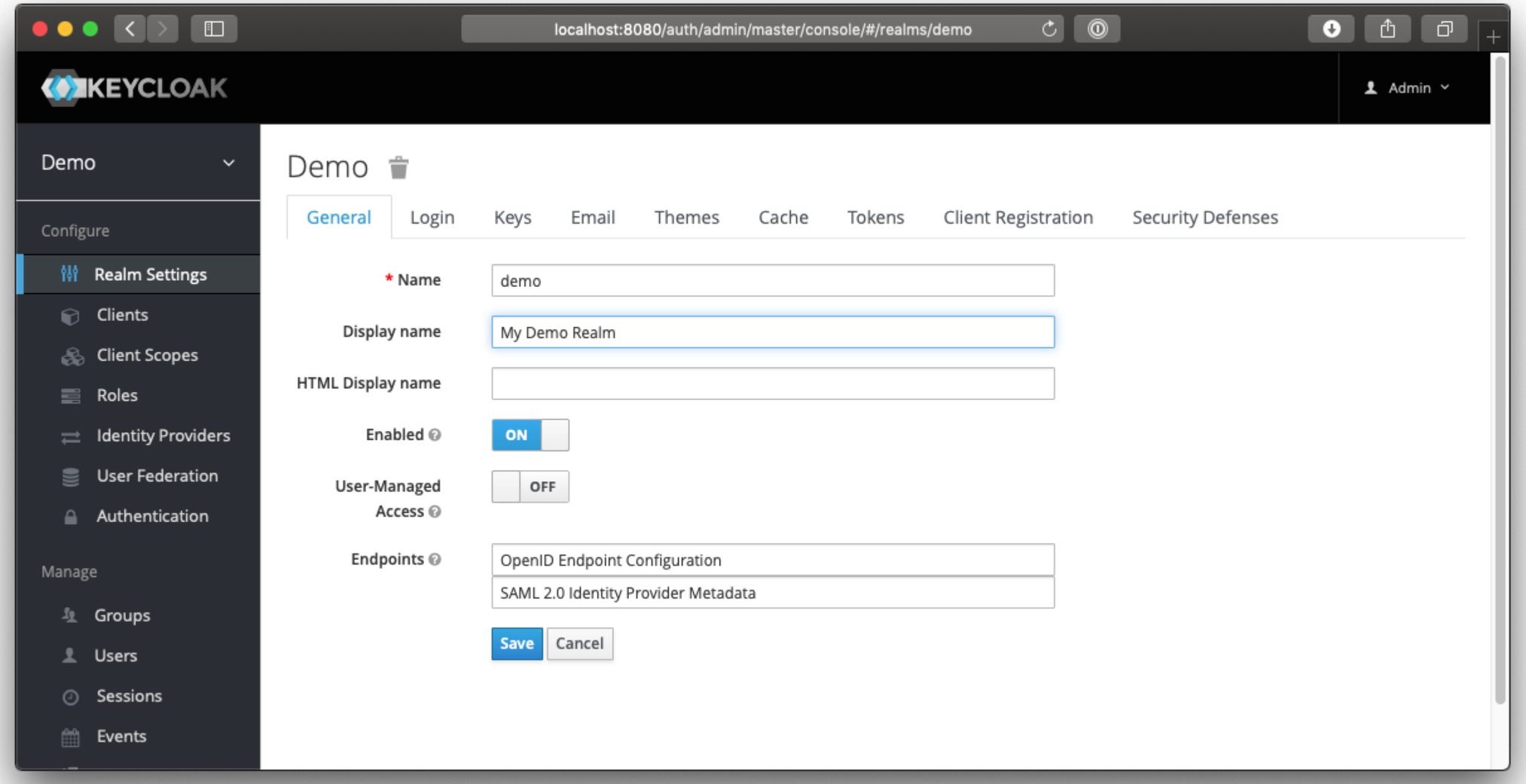
- Password vergessen
- Registrierung
  - Email-Verifizierung
  - Terms of Service
- Account verwalten
- ...

Custom Themes



Admin UI

COFINPRO

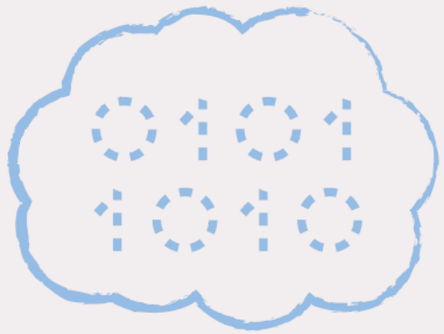


weitere Features

- Cluster-fähig
- User-Federation
- Social-Login
- Impersonation
- 2-Faktor Auth (TOTP)
- eigene Flows
- ...

COFINPRO

Anwendungen absichern



Adapter

Keycloak stellt fertige Adapter bereit für

- Java
  - Wildfly, Jetty, Tomcat, Fuse
  - Servlets, JAAS
  - Spring Boot, Spring Security
  - CLI, Desktop (z.B. Swing, JavaFX)
- Javascript/TS
  - Standalone, NodeJS
- Generic Proxy (Keycloak Gatekeeper)

weitere Integationen

jede Menge OIDC-Libraries für verschiedene Sprachen

- C#
- Python
- Android
- iOS
- ...
- Apache, Nginx

https://www.keycloak.org/docs/latest/securing_apps/

COFINPRO

Aufgaben der Adapter

- Token-Validierung
- Parsen des Tokens
- Setzen von Rollen/Berechtigungen
- Login/Logout (über Redirects)
- Token Refresh

Webanwendungen

Adapter installieren

- in Serververzeichnis entpacken oder
- Dependency hinzufügen

Webanwendungen

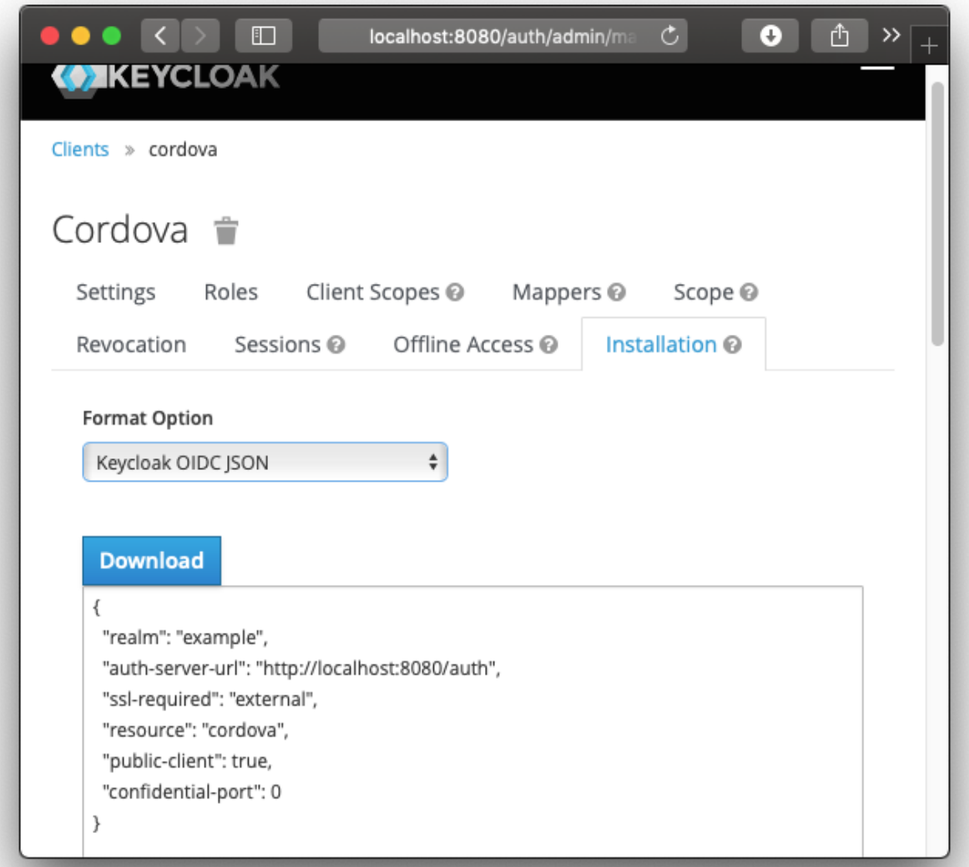
Client konfigurieren

über eigene Konfigurationsdatei (`keycloak.json`)

```
{
    "realm" :         "demo",
    "clientId" :      "hawtio-client",
    "url" :           "http://keycloak.example.com/auth",
    "ssl-required" : "external",
    "public-client" : true
}
```

Webanwendungen

Client konfigurieren



Webanwendungen

Berechtigungen konfigurieren

je nach Plattform

- Konfiguration (`application.yaml`, `web.xml`)
- Annotationen (`@RolesAllowed`)
- programmatisch

```
app.get('/complain', keycloak.protect(), complaintHandler);
```

Webanwendungen

Berechtigungen konfigurieren

```
<?xml version=""?>
<web-app>
    <security-constraint>
        <web-resource-collection>
            <web-resource-name>Admins</web-resource-name>
            <url-pattern>/admin/*</url-pattern>
        </web-resource-collection>
        <auth-constraint>
            <role-name>admin</role-name>
        </auth-constraint>
    </security-constraint>


    <login-config>
        <auth-method>KEYCLOAK</auth-method>
```

Single-Page-Apps

- über Javascript-Adapter
- darauf aufbauende Module
  - Keyloak-Angular
  - React-Keycloak
- OAuth-Code-Flow mit PKCE Extension

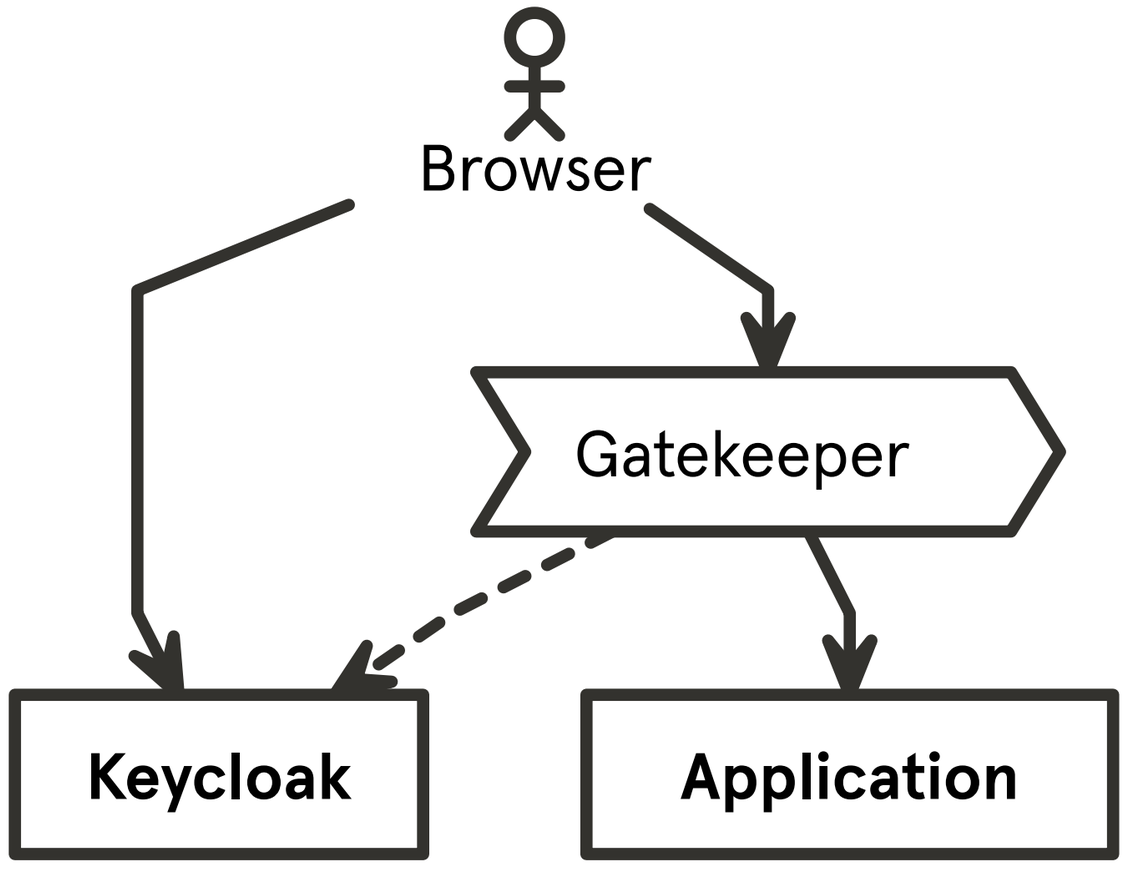
OAuth und Single-Page-Apps

RFC-Draft: OAuth 2.0 for Browser-Based Apps

Problem

- Browser und Client in Einem
- mögen Redirects nicht
- viel Validierung im Client
- sicheres Speichern von Tokens?

Keycloak Gatekeeper

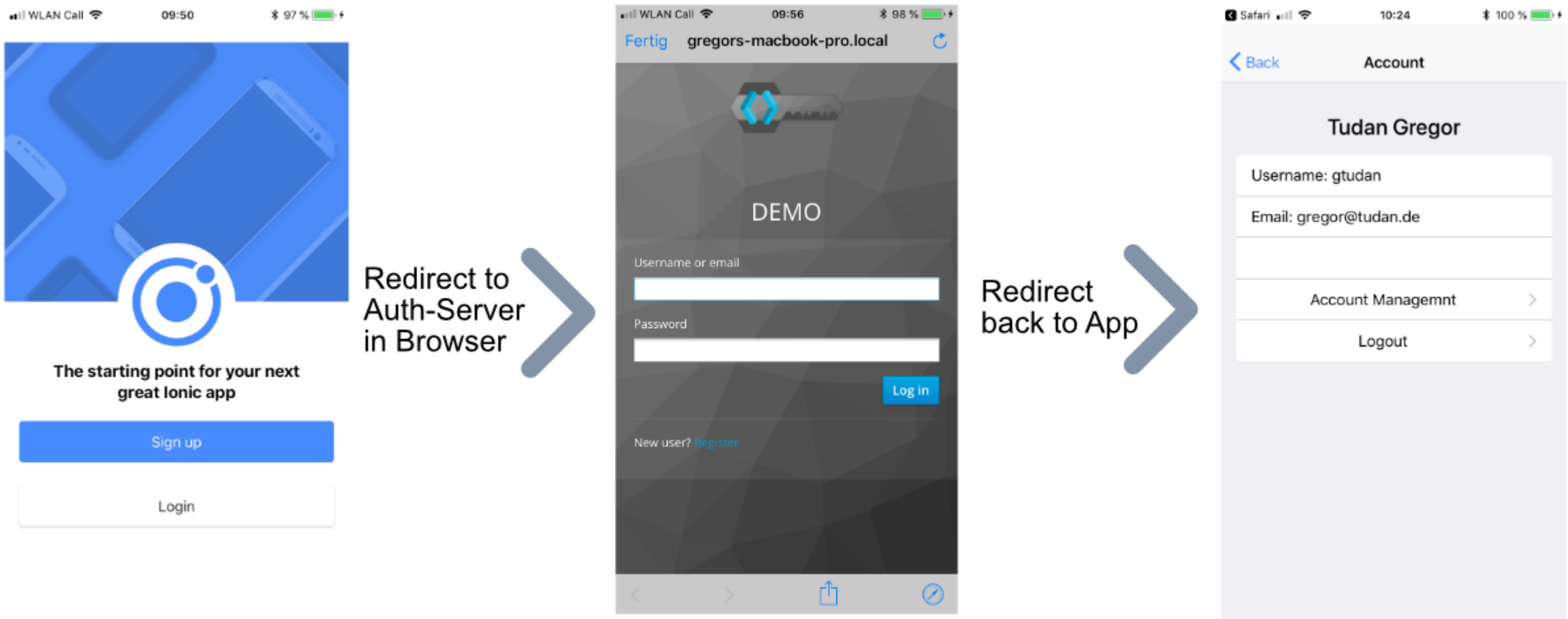


COFINPRO

Mobile Apps

Mobile Apps

RFC-8252: OAuth 2.0 for Native Apps



Hybride Apps mit Cordova

Hybride Apps mit Cordova

In-App Browser

- Web-View in Web-View
- eigenes UI
- hat einige Quirks
- App sieht Interaktion

Hybride Apps mit Cordova

In-App Browser

- Web-View in Web-View
- eigenes UI
- hat einige Quirks
- App sieht Interaktion

Native

- nutzt native Browser-Views
  - Chrome Custom-Tabs
  - `SFSafariViewController`
- App hat keinen Zugriff
- Redirect zur App notwendig

Cordova In-App Browser

COFINPRO

Cordova Native

iOS Web-View-Race

1. `UIWebView` (In-App Browser - don't do it)

iOS Web-View-Race

1. `UIWebView` (In-App Browser - don't do it)
2. `SFSafariViewController`

iOS Web-View-Race

1. `UIWebView` (In-App Browser - don't do it)
2. `SFSafariViewController`
3. `SFAuthenticationSession` (iOS 11)
   - Login für 3rd-Party-Apps mit OAuth
   - Single-Sign-On für Apps

iOS Web-View-Race

1. `UIWebView` (In-App Browser - don't do it)
2. `SFSafariViewController`
3. `SFAuthenticationSession` (iOS 11)
   - Login für 3rd-Party-Apps mit OAuth
   - Single-Sign-On für Apps
4. `ASWebAuthenticationSession` (iOS 12)
   - schützt User-Credentials

iOS Web-View-Race

1. `UIWebView` (In-App Browser - don't do it)
2. `SFSafariViewController`
3. `SFAuthenticationSession` (iOS 11)
   - Login für 3rd-Party-Apps mit OAuth
   - Single-Sign-On für Apps
4. `ASWebAuthenticationSession` (iOS 12)
   - schützt User-Credentials

Android: In-App Browser oder Custom-Tabs 🤷‍♀️

native mobile Apps

(generische) 3rd-Party Libraries

- App-Auth
- AeroGear

COFINPRO

Diskussion und Fragen

Bitte geben Sie uns jetzt Ihr Feedback!

Cloak-and-Dagger-Stories: Absichern von Anwendungen mit OAuth und Keycloak

Gregor Tudan

Nächste Vorträge in diesem Raum

13:30 Testautomatisierung ohne Assertions, *Dr. Jeremias Rößler*

14:30 TDD demystified, *Tilmann Glaser, Peter Fichtner*

15:45 Legacy Code im Griff dank Mikado Methode, *Falk Sippach*