31.8.–3.9.2015
in Nürnberg

Herbstcampus

Wissenstransfer
par excellence

Plug & Play Benutzerverwaltung

Web-Anwendungen absichern mit OAuth 2 und JBoss Keycloak

Alexander Schwartz

msg systems ag

Plug & Play Benutzerverwaltung mit JBoss Keycloak

1 Die Killerapplikation 4

2 Vorstellung von JBoss Keycloak 8

3 Absicherung einer JEE Webanwendung 13

4 Integration externer Authentifizierungsquellen 16

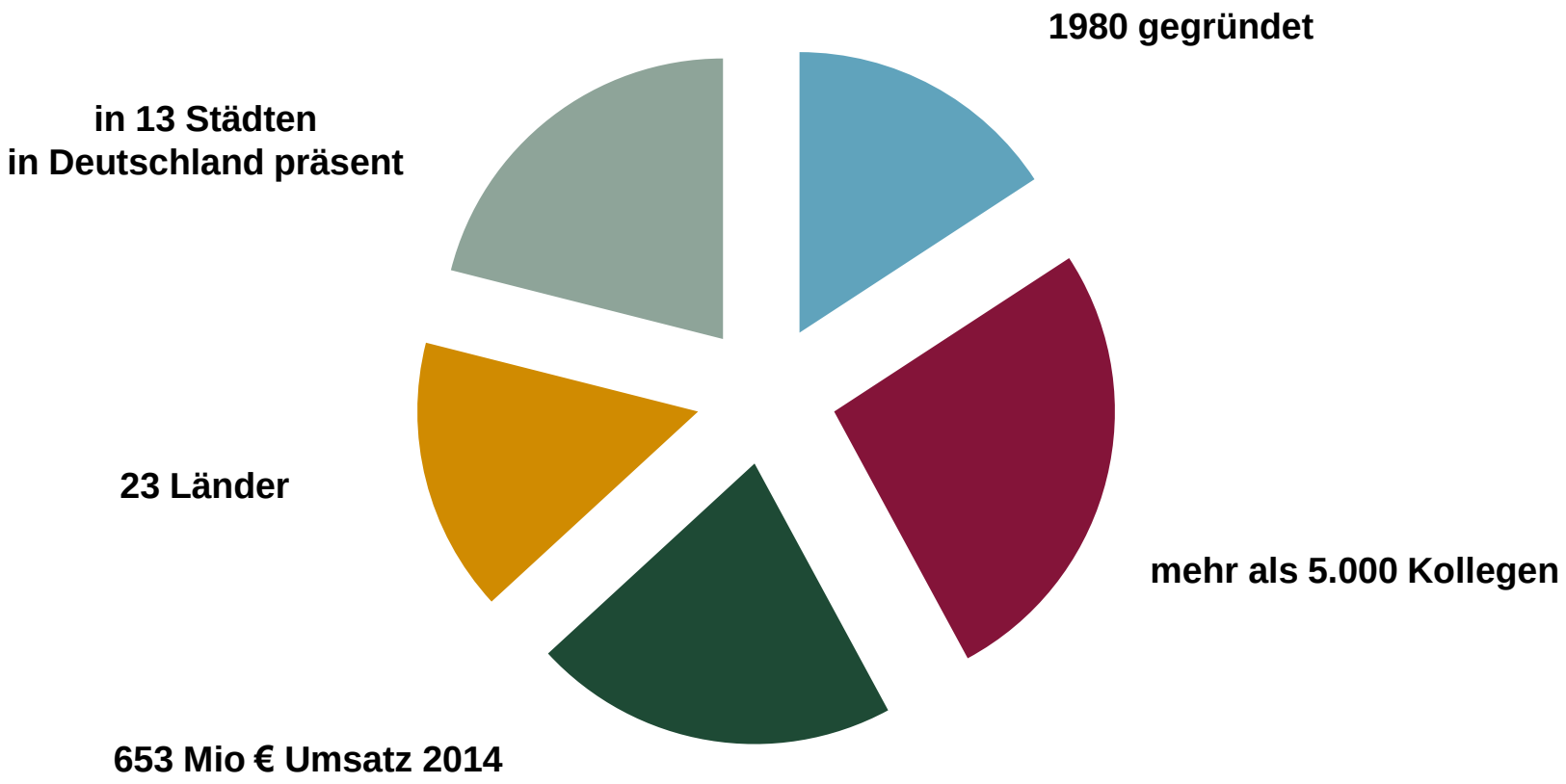
5 Absicherung einer JavaScript Single Page Application 18

6 Absicherung von REST Services 20

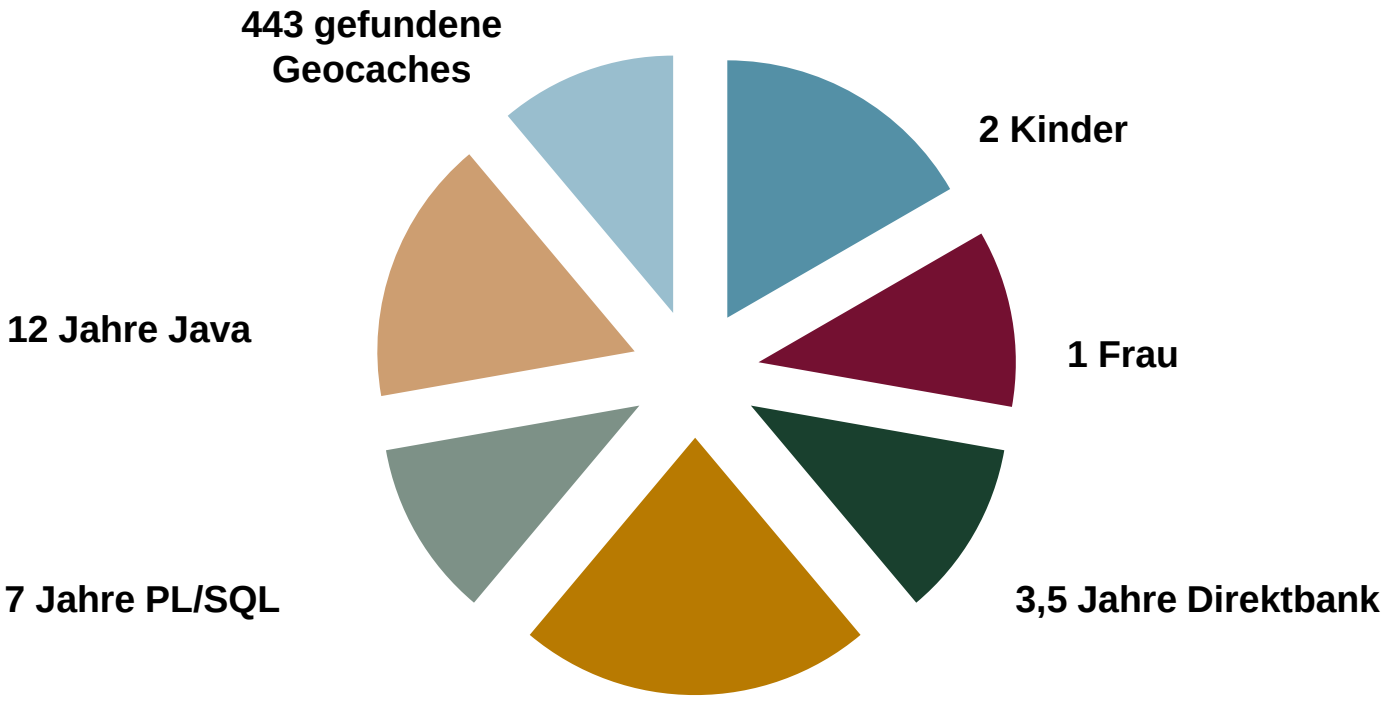
7 Ausblick 23

8 Secure all the things! 25

Mein Sponsor und Arbeitgeber – msg systems ag



Wer ich bin – Alexander Schwartz



@ahus1de

Plug & Play Benutzerverwaltung mit JBoss Keycloak

1 **Die Killerapplikation** **4**

2 Vorstellung von JBoss Keycloak 8

3 Absicherung einer JEE Webanwendung 13

4 Integration externer Authentifizierungsquellen 16

5 Absicherung einer JavaScript Single Page Application 18

6 Absicherung von REST Services 20

7 Ausblick 23

8 Secure all the things! 25

Mit meiner Lotto-Nummern-Vorhersage mache ich ein Vermögen!

1. CC0 / https://pixabay.com/de/lotto-lottoschein-schein-gewinn-484782/
   CC0 / https://pixabay.com/de/geldschwemme-500-euro-euro-stapel-432688/

Aber: Je mehr Leute zugreifen, desto geringer ist mein Losgewinn!

Absicherung ist notwendig:

- Anmeldeseite
- Datenbank für Benutzernamen und Passwörter
- Verschlüsselte Speicherung von Passwörtern
- Zurücksetzen von Passwörtern
- Ändern von Passwörtern
- …

1. CC BY-SA 3.0 "Work life balance rat race" by KVDP, Shokunin, Aungkarns https://commons.wikimedia.org/wiki/File:Work_life_balance_rat_race.png

Benutzerverwaltungen haben doch auch schon andere gebaut?

Es gibt Best Practices für Benutzerverwaltungen:

- Open Web Application Security Project (OWASP) hält Cheat Sheets zur Implementierung bereit (Anmeldung, Passwort ändern, Passwort zurücksetzen)
- Fertige Benutzerverwaltungen als Framework oder Teil der Anwendung (z. B. Apache Shiro, integriert in z. B. in Grails)
- Fertige Benutzerverwaltungen, die über eine Schnittstelle eingebunden werden (z. B. JBoss Keycloak)

Links:

https://www.owasp.org/index.php/Authentication_Cheat_Sheet

http://shiro.apache.org/

http://keycloak.jboss.org/

Plug & Play Benutzerverwaltung mit JBoss Keycloak

1 Die Killerapplikation 4

2 **Vorstellung von JBoss Keycloak** **8**

3 Absicherung einer JEE Webanwendung 13

4 Integration externer Authentifizierungsquellen 16

5 Absicherung einer JavaScript Single Page Application 18

6 Absicherung von REST Services 20

7 Ausblick 23

8 Secure all the things! 25

JBoss Keycloak ist eine Benutzerverwaltung als Service

- Single Sign On und Single Sign Out für Browser-Anwendungen
- Benutzer- und Rollenverwaltung
- Account-Management und Admin-GUI
- Grafische Anpassung des Account Managements über Themes
- Optionale Integration von LDAP/Active Directory und Social Login
- Event-Listener für alle Aktionen

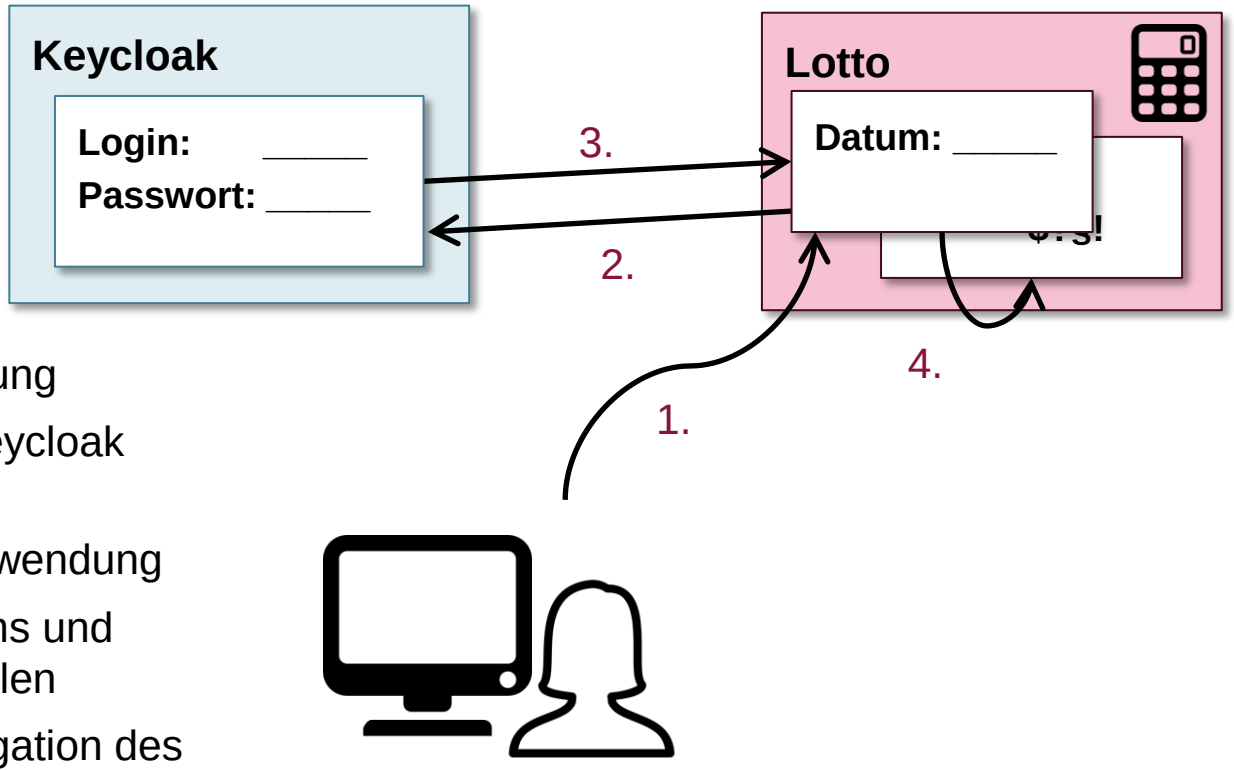
September 2014: Version 1.0

Juli 2015: Version 1.4

Link:

http://keycloak.org/

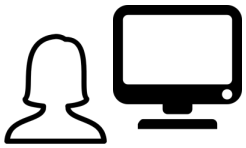
JBoss Keycloak läuft neben der Anwendung

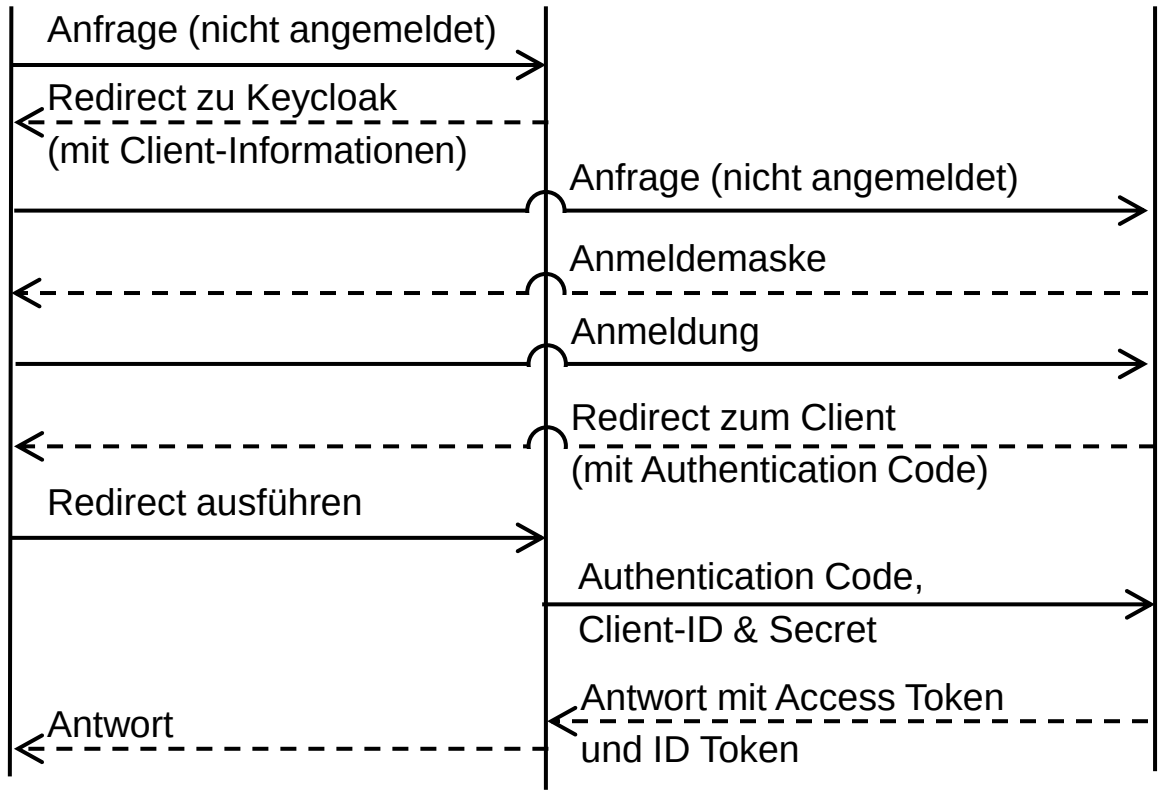


1. Aufruf der Anwendung
2. Weiterleitung zu Keycloak zur Anmeldung
3. Rückleitung zur Anwendung
4. Eingabe des Datums und Berechnen der Zahlen

(Pfeile zeigen die Navigation des Browsers)

OAuth 2.0 für Single-Sign-On, OpenID Connect als Erweiterung





Access Token als JSON Web Token

Access Token (+/- 1500 Bytes):

```
ey###J9.ey####n0.PD###uA
```

Inhalt:

```
{
  "alg": "RS256"
}
{
  "jti": "cd2461###e695c",
  "exp": 1436725029,
  "allowed-origins": [],
  "realm_access": {
    "roles": [
      "create-realm",
      "admin"
    ]
  },
"resource_access": {
   "my-realm": {
     "roles": [
       "view-realm",
       "manage-events",
       "manage-realm",
       "view-events",
       "manage-users",
       "view-users",
       "view-clients",
       "manage-clients",
       ...
     ]
   },
 },
  "name": "Administrator",
  "preferred_username": "admin"
}

RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  "-----BEGIN RSA PRIVATE KEY-----
  MII###Yw==
  -----END RSA PRIVATE KEY-----"
  )
```

Link:
http://jwt.io/

Plug & Play Benutzerverwaltung mit JBoss Keycloak

1 Die Killerapplikation 4

2 Vorstellung von JBoss Keycloak 8

3 **Absicherung einer JEE Webanwendung** **13**

4 Integration externer Authentifizierungsquellen 16

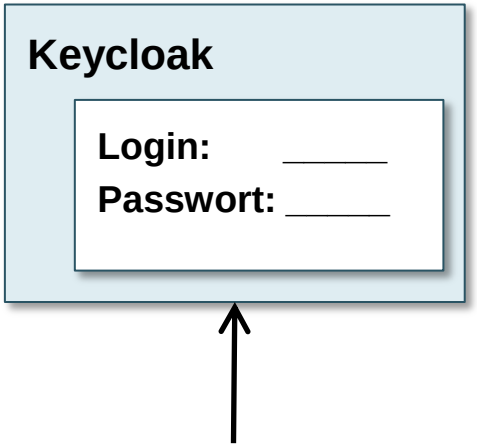
5 Absicherung einer JavaScript Single Page Application 18

6 Absicherung von REST Services 20

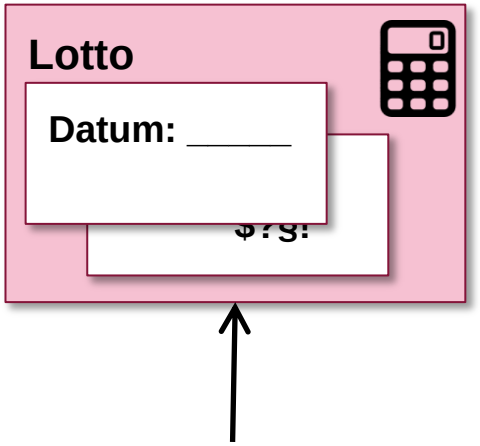
7 Ausblick 23

8 Secure all the things! 25

Keycloak einrichten



- Realm anlegen oder bestehenden Realm benutzen
- Anwendung registrieren



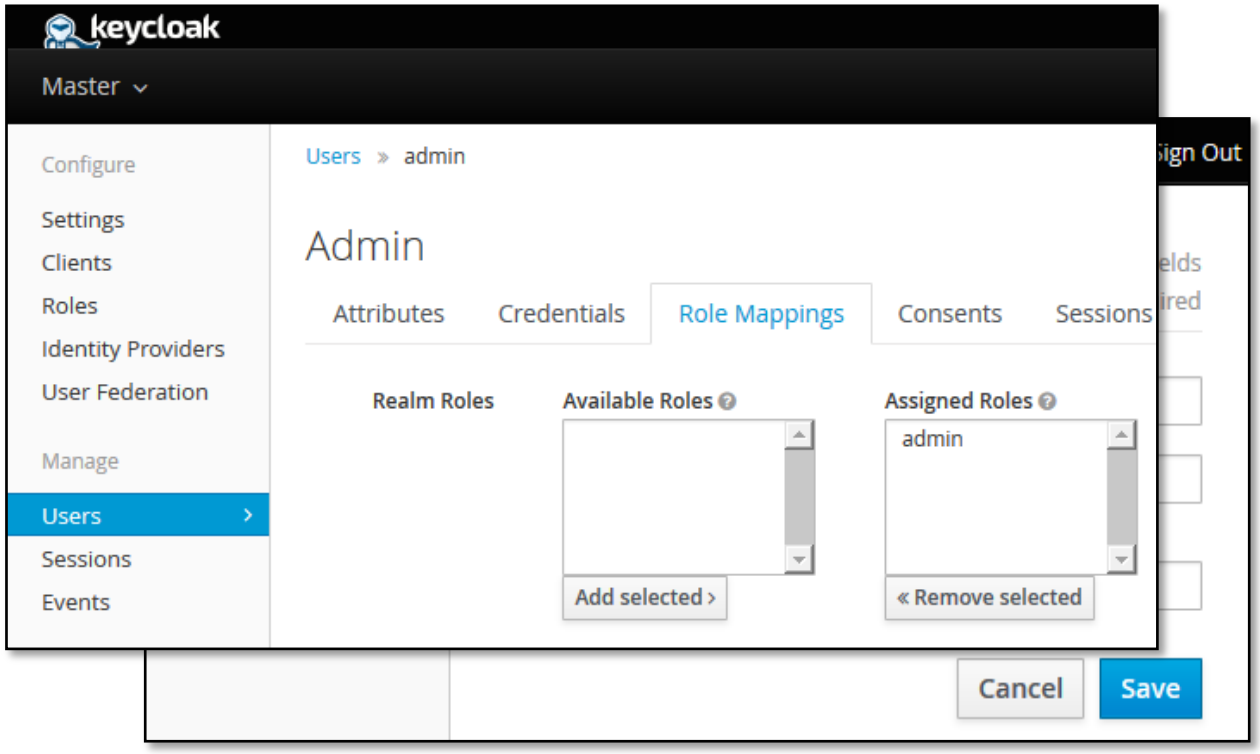
- Keycloak-Bibliothek einbinden
- Keycloak Konfigurationsdatei einbinden
- web.xml Konfiguration anpassen

Demo Time

Funktionen der Benutzerverwaltung

Über Konfiguration können folgende Funktionen aktiviert werden:

- Verwaltung von Nutzern und Rollen
- Passwort-Policy
- Zurücksetzen des Passworts für Administratoren
- Zurücksetzen des Passworts durch Nutzer
- Passwort vergessen



.msg

Plug & Play Benutzerverwaltung mit JBoss Keycloak

1 Die Killerapplikation 4

2 Vorstellung von JBoss Keycloak 8

3 Absicherung einer JEE Webanwendung 13

4 **Integration externer Authentifizierungsquellen** **16**

5 Absicherung einer JavaScript Single Page Application 18

6 Absicherung von REST Services 20

7 Ausblick 23

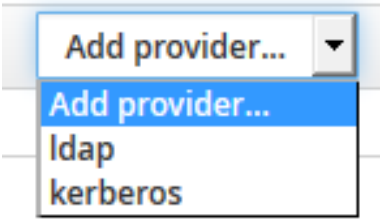
8 Secure all the things! 25

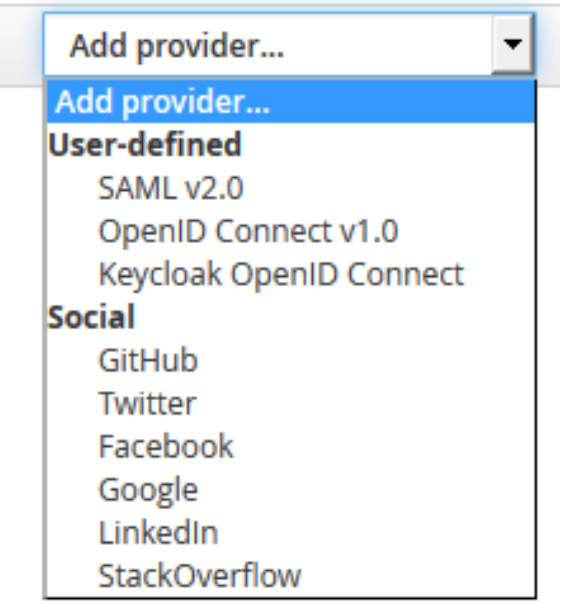
Funktionen der Benutzerverwaltung

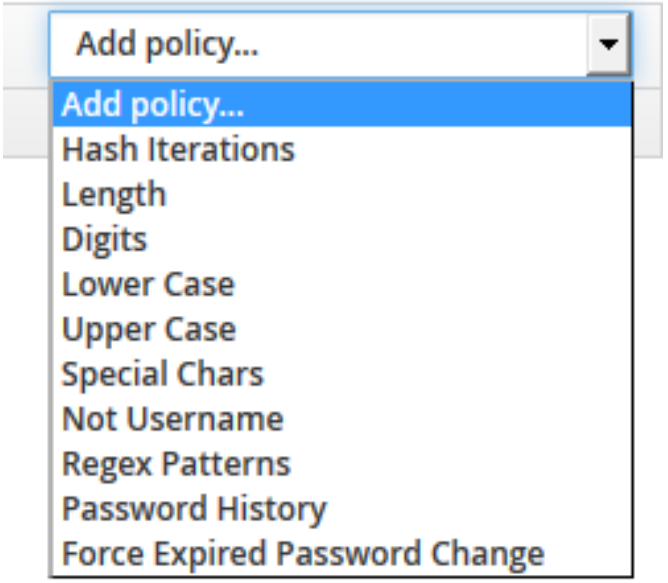
Über Konfiguration können folgende Funktionen aktiviert werden:

- One Time Passwords (OTPs)
- Social Login via Facebook, Twitter, etc.
- Integration mit LDAP

... und viele mehr







1 Die Killerapplikation 4

2 Vorstellung von JBoss Keycloak 8

3 Absicherung einer JEE Webanwendung 13

4 Integration externer Authentifizierungsquellen 16

5 Absicherung einer JavaScript Single Page Application 18

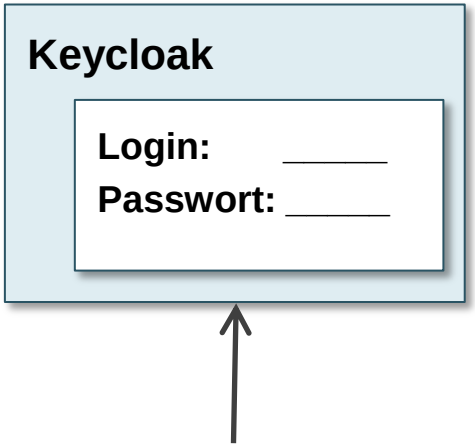
6 Absicherung von REST Services 20

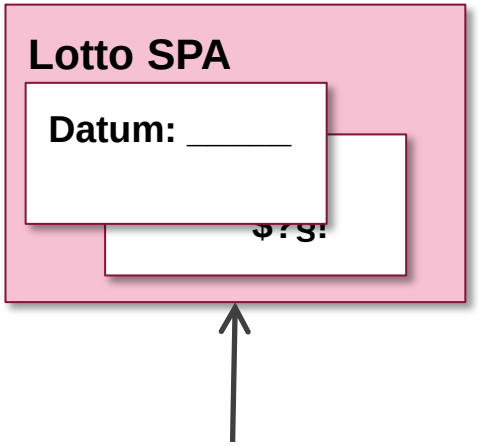
7 Ausblick 23

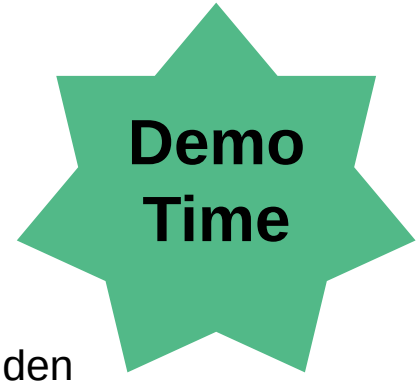
8 Secure all the things! 25

Registrierung der Single Page Application als separate Anwendung

…







- Anwendung registrieren mit Access Type „public“

- JavaScript-Bibliothek einbinden
- Bei asynchronen Aufrufen Token mitschicken

Plug & Play Benutzerverwaltung mit JBoss Keycloak

1 Die Killerapplikation 4

2 Vorstellung von JBoss Keycloak 8

3 Absicherung einer JEE Webanwendung 13

4 Integration externer Authentifizierungsquellen 16

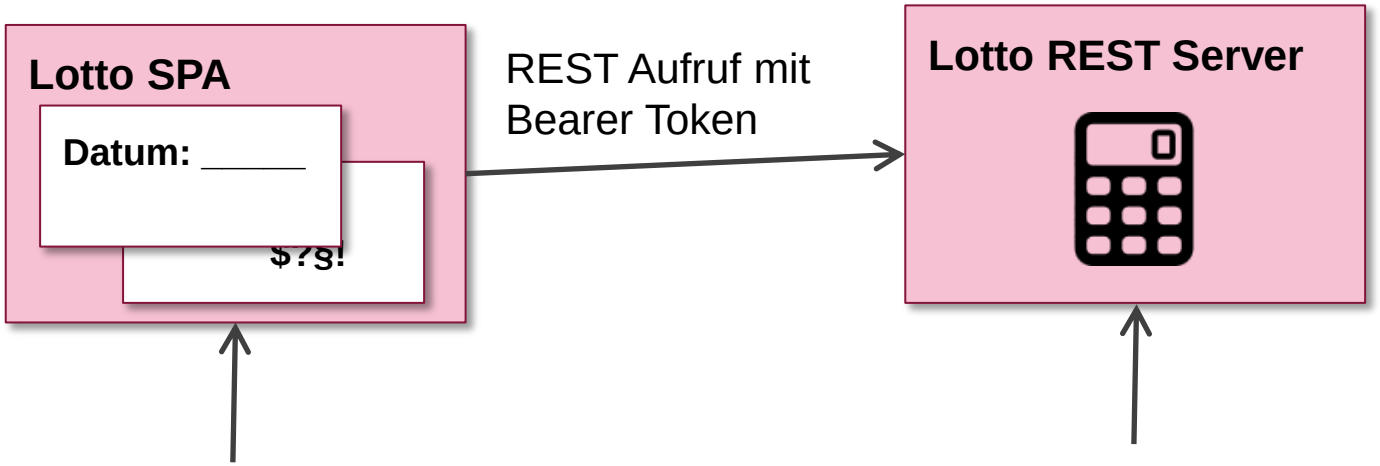
5 Absicherung einer JavaScript Single Page Application 18

6 **Absicherung von REST Services** **20**

7 Ausblick 23

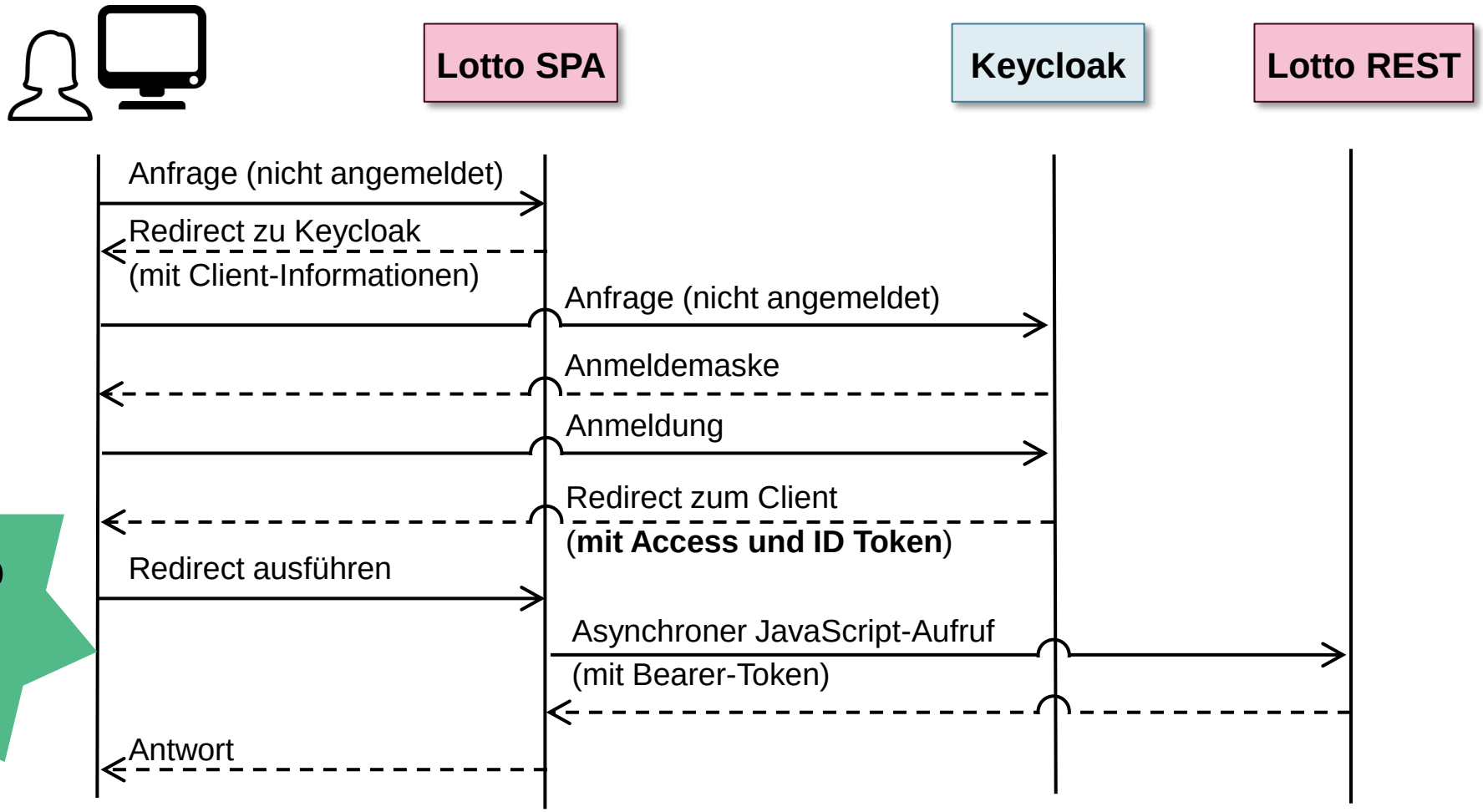
8 Secure all the things! 25

Bearer Tokens werden bei jedem Aufruf mitgeschickt



- Schickt Bearer-Token bei jedem Aufruf mit
- Server ist stateless, da alle Informationen im Token in signierter Form vorhanden sind

Ablauf Bearer Token



Plug & Play Benutzerverwaltung mit JBoss Keycloak

1 Die Killerapplikation 4

2 Vorstellung von JBoss Keycloak 8

3 Absicherung einer JEE Webanwendung 13

4 Integration externer Authentifizierungsquellen 16

5 Absicherung einer JavaScript Single Page Application 18

6 Absicherung von REST Services 20

7 **Ausblick** **23**

8 Secure all the things! 25

Sicherheitsmaßnahmen im Hintergrund

- Aktualisierung von Tokens bei Bedarf
- Rückruf von bereits ausgegebenen Token über „not valid before“
- Single-Sign-Out (Serverseitig über Aufruf des Backends von Keycloak aus, beim Single Page Application Frontend über iFrame)
- Erkennung von Brute-Force-Attacken auf dem Keycloak-Server

Plug & Play Benutzerverwaltung mit JBoss Keycloak

1 Die Killerapplikation 4

2 Vorstellung von JBoss Keycloak 8

3 Absicherung einer JEE Webanwendung 13

4 Integration externer Authentifizierungsquellen 16

5 Absicherung einer JavaScript Single Page Application 18

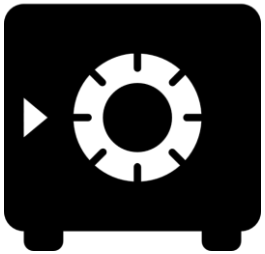
6 Absicherung von REST Services 20

7 Ausblick 23

8 **Secure all the things!** **25**

Secure all the things!

- Keycloak bietet alle Funktionen einer Benutzerverwaltung
- Schnittstelle zur Anwendung ist über OAuth 2.0 und Open ID Connect standardisiert
- Verschiedene Integrationen sind vorhanden, eigene Integrationen sind möglich
- Funktionalität der Benutzerverwaltung wird unabhängig von der Anwendung konfiguriert



http://keycloak.org/

ahus1/keycloak-dropwizard-integration

@ahus1de

Alexander Schwartz
Principal IT Consultant

+49 171 5625767
alexander.schwartz@msg-systems.com

@ahus1de

msg systems ag
Mergenthalerallee 73-75
65760 Eschborn
Deutschland

www.msg-systems.com

.msg .consulting .solutions .partnership