#BaselOne18

CSS Versicherung

ELCA

Basel basel.ch

adesso business. people. technology.

JAVA USER GROUP CH

bluesky CONSIDER IT DONE

canoo [delivering end-user happiness]

Basler Versicherungen

Token statt Cookies

... dank JWT

#BaselOne18

Markus Schlichting

Senior Software Engineer Karakun.

[HACKERGARTEN] Basel
A COMPUTER PROGRAMMING CONTRIBUTOR GROUP

markus.schlichting@karakun.com

@madmas

#BaselOne18

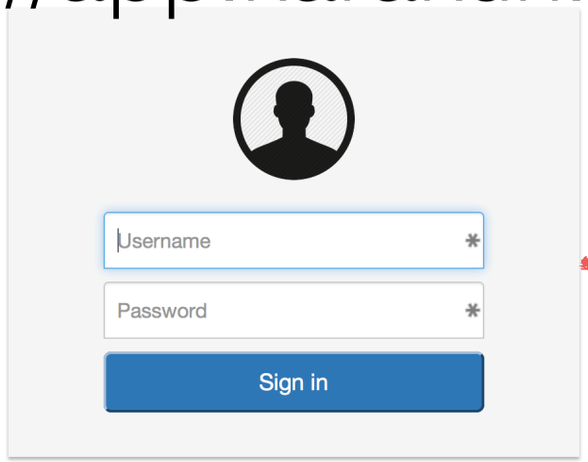
Warum?

- (REST) APIs
- Web Applications, Mobile Apps, *Multi-Channel*
- Microservices

Sessions & Cookies

http://app.karakun.com

http://app.karakun.com



Credentials validieren, Session erzeugen

Session Cookie

Session Store

Session validieren, Zugriff kontrollieren

#BaselOne18

Sessions & Cookies

Loadbalancing benötigt **geteilten Sessionpool**

Services werden **gekoppelt**

Cross Domain Authentifizierung: **CORS**

CSRF Verwundbarkeit

Andere Clients ausser Browser?

JSON Web Token

JSON Web Tokens are an open, industry standard method for representing claims securely between two parties.

(RFC 7519)

The suggested pronunciation of JWT is the same as the English word "jot".

JSON Web Token

basierend auf anderen JSON-Standards:

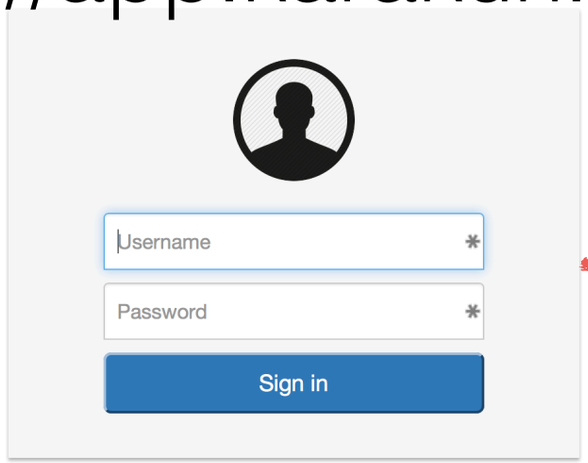
- JWS (JSON Web **Signature**)
- JWE (JSON Web **Encryption**)

Bibliotheken für..

JWT in Action

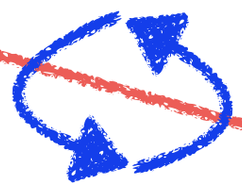
http://app.karakun.com

http://api.karakun.com



Credentials validieren,
Token erzeugen

Token speichern



Token validieren,
Zugriff kontrollieren

JWT - inside

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzd
WIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ik1hcmt1cyB
TYW1wbGUiLCJhZG1pbiI6dHJ1ZSwic2VjcmV0IjpmY
WxzZX0.XyIy2tfX_FxVcIpcqogtD6zyOfAfy1FeNAi
t_qO3Kwc
```

Decoded EDIT THE PAYLOAD AND SECRET (ONLY HS256 SUPPORTED)

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "Markus Sample",
  "admin": true,
  "secret": false
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  secret
) secret base64 encoded
```

jwt.io

#BaselOne18

JWT - inside: Payload

Registered Claims IANA JSON WebToken Register

Public Claims öffentl. lesbare Claims: Eindeutigkeit!

Private Claims private Claims: Freie Wahl!

JWT - in practice

Demo!

JWT Security Aspekte

immer verschlüsselt kommunizieren (HTTP**S**!)

URL Token vermeiden

https://yourpage.de/service/action?token=jwt.goes.here

Token Handling: Invalidation, Reset

JWT Überblick

basiert auf **JSON**

einfach zu nutzen**, einfach** zu implementieren

symmetrische und **asymmetrische** Crypto

reduziert Abhängigkeiten

Basisprinzip von REST: **State transfer**

Zusammenfassung

Cookies nicht obsolet, **Token** bieten jedoch **viele Vorteile**

JWT für **Skalierbarkeit** und **Flexibilität**

Cross Plattform

Cookies oder **Token?**

Anforderungen und Implikationen abwägen!

Demo Sources und Slides:

https://github.com/madmas/TokenVsCookies

#BaselOne18

CSS Versicherung

ELCA

Basel basel.ch

adesso business. people. technology.

JAVA USER GROUP CH

bluesky CONSIDER IT DONE

canoo [delivering end-user happiness]

Basler Versicherungen