

Token statt Cookies
... dank JWT



Markus Schlichting

Senior Software Engineer

canoo

[delivering end-user happiness]

Basel, Schweiz



Hackergarten Basel

[HACKERGARTEN]
A COMPUTER PROGRAMMING CONTRIBUTOR GROUP

markus.schlichting@canoo.com



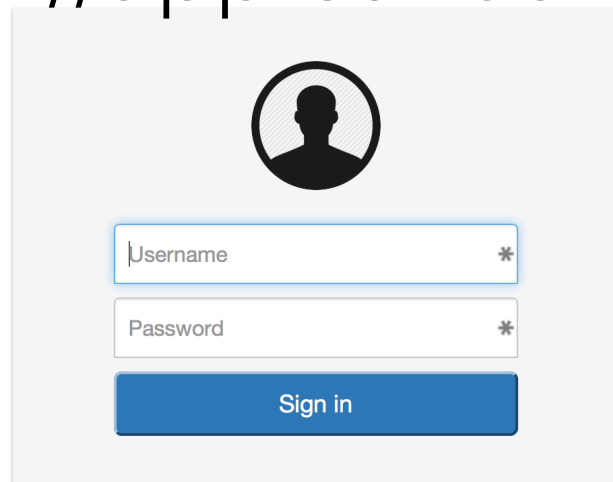
@madmas

Warum?

- REST APIs
- Single Page Applications
- Microservices

Sessions & Cookies

http://app.canoo.com



A login form with a user icon, a 'Username' input field with an asterisk, a 'Password' input field with an asterisk, and a blue 'Sign in' button.

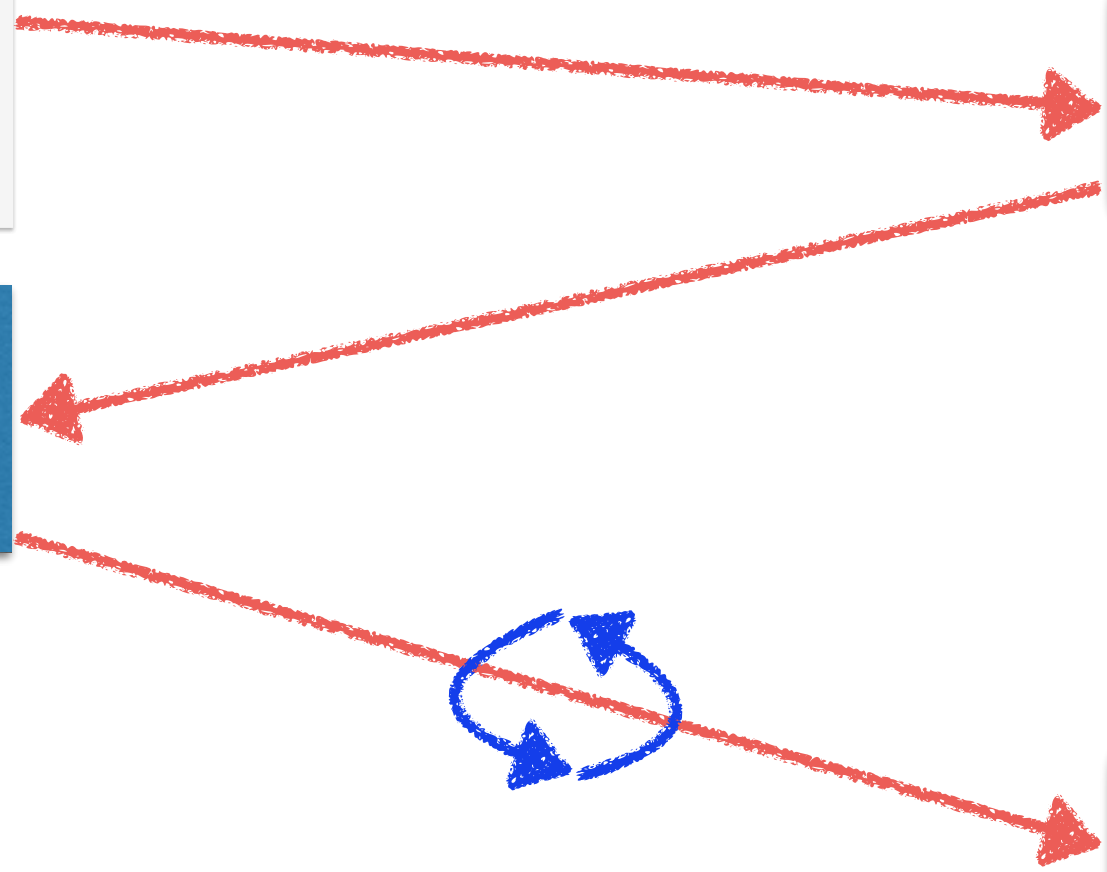
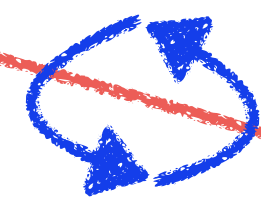
Session Cookie

http://app.canoo.com

Credentials validieren,
Session erzeugen

Session
Store

Session validieren,
Zugriff kontrollieren



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.canoo.com

Username *

Password *

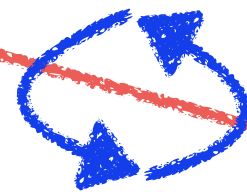
Sign in

http://api.canoo.com

Credentials validieren,
Token erzeugen

Token speichern

Token validieren,
Zugriff kontrollieren



JWT - inside

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpXVCJ9.t_q03Kwc
```

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 base64 encoded
```

jwt.io

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 (**HTTPS!**)

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>