JÖNKÖPING UNIVERSITY

School of Engineering

JSON WEB TOKENS

Peter Larsson-Green

Jönköping University

Autumn 2018

JSON WEB TOKENS

A simple and commonly used type of token.

- Specification: https://tools.ietf.org/html/rfc7519
- Abbreviated JWT (announced *jot*).
- Is Self-Contained.
  - The data is stored in the token (nothing is stored on the server).
  - The client can read the data, but not change it.
    - The server "signs" the data by hashing it with a secret (the hash is part of the token).
- The data is stored in JSON format.

JSON WEB TOKENS

Consists of three parts.

Same as "alg" in the header!

Header

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

base64UrlEncode( )

Payload

```
{
  "exp": 1472840818,
  "name": "Betty",
  "admin": true
}
```

base64UrlEncode( )

Signature

```
HMACSHA256(
  base64UrlEncode(header)
  +"."+
  base64UrlEncode(payload),
  "server-secret"
)
```

aaaaaaaaaaaaaaa.bbbbbbbbbbbbbbb.ccccccccccccccc

EXAMPLE

Playground: https://jwt.io

CLAIM NAMES

The payload/data in the token consists of claims (key-value pairs).

- Some *Registered Claim Names*:
  - `iss` - Issuer, identifies the one creating the token.
  - `sub` - Subject, identifies the user accepting the token to be created.
  - `aud` - Audience, identifies the client the token is intended for.
  - `iat` - Issued At, timestamp for when the token was created.
  - `exp` - Expired, timestamp for when the token expires.
- *Public Claim Names*:
  - Add to IANA JSON Web Token Registry.
  - Use a URI as name (your own domain).
- *Private Claim Names*:
  - Use any name you want (can collide with names others use).