Was sind JSON Web Tokens?

- JWT ist in offener Standard der IETF spezifiziert unter RFC 7519
- Ein JWT beinhaltet Header, Claims und Signature
- Die Claims sind einfach Key/Value Paare. Es gibt Standard Claims.
- Die Signature ist zwar optional, sie ermöglicht aber die Verifikation und stellt Fälschungssicherheit sicher

```
eyJhbGciOiJIUzI1NiIsInR5cCI6
IkpXVCJ9.eyJzdWIiOiIxMjM0NTY
3ODkwIiwibmFtZSI6Ik1hcmlvLUx
lYW5kZXIgUmVpbWVyIiwidXBuIjo
ibWFyaW8tbGVhbmRlci5yZWltZXJ
AcWF3YXJlLmRlIiwiaWF0IjoxNTE
2MjM5MDIyLCJleHAiOjE1MTYyMzk
wMjIsImlzcyI6Ii9vYXV0aDIvdG9
rZW4iLCJncm91cHMiOlsiQWRtaW5
pc3RyYXRvciIsIkRldmVsb3BlciJ
dfQ.mFqC0QQCB3lNgrJ9KWBZi0le
OAxuKfy9qO_xCL4HWM4
```

Was sind JSON Web Keys?

- JWK ist in offener Standard der IETF spezifiziert unter RFC 7517
- JSON Datenstruktur zur Darstellung Kryptografischer Schlüssel
- Über JWK Thumbprint (RFC 7638) können Hashes von JWKs berechnet werden. Nutzung als JWT kid Claim
- JSON Web Key Sets sind eine Liste von (öffentlichen) JSON Web Keys, werden für die Verteilung genutzt


```
{
 "kty":"RSA",
 „use“:“sig",
 "alg":"RS256",
 "kid":"dfghj5678sdfadfasdf678asdfasfasdf",
 "n":"0vx7agoebGcQSuuPiLJXZptN9nndrQmbXEps2aiAFbWhM78LhWx4
     ...
     0Ls1jF44-csFCur-kEgU8awapJzKnqDKgw",
 "e":"AQAB",
 "d":"X4cTteJY_gn4FYPsXB8rdXix5vwsg1FLN5E3EaG6RJoVH-HLLKD9
     M7dx5oo7GURknchnrRweUkC7hT5fJLM0WbFAKNLWYSzUvxT0_YSfqij
     ...
     me1z0HbIkfz0Y6mqnOYtqc0X4jfcKoAC8Q",
 "p":"83i-7IvMGXoMXCskv73TKr8637FiO7Z27zv8oj6pbWUQyLPQBQxtPV
     ...
     WlWEh6dN36GVZYk93N8Bc9vY41xy8B9RzzOGVQzXvNEvn7O0nVbfs",
 "q":"3dfOR9cuYq-0S-mkFLzgItgMEfFzB2q3hWehMuG0oCuqnb3vobLyum
     ...
     kIdrecRezsZ-1kYd_s1qDbxtkDEgfAITAG9LUnADun4vIcb6yelxk",
 "dp":"G4sPXkc6Ya9y8oJW9_ILj4xuppu0lzi_H7VTkS8xj5SdX3coE0oim
     ...
     YZc3C3m3I24G2GvR5sSDxUyAN2zq8Lfn9EUms6rY3Ob8YeiKkTiBj0",
 "dq":"s9lAH9fggBsoFR8Oac2R_E2gw282rT2kGOAhvIllETE1efrA6huUU
     ...
     GF4Dh7e74WbRsobRonujTYN1xCaP6TO61jvWrX-L18txXw494Q_cgk",
 "qi":"GyM_p6JrXySiz1toFgKbWV-JdI3jQ4ypu9rbMWx3rQJBfmt0FoYzg
     ...
     yR8O55XLSe3SPmRfKwZI6yU24ZxvQKFYItdldUKGzO6Ia6zTKhAVRU"
}
```