

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
    ...
    me1z0HbIkfz0Y6mqn0Ytqc0X4jfcKoAC8Q",
  "p": "83i-7IvMGXoMXCskv73TKr8637Fi07Z27zv8oj6pbWUQyLPQBQxtPV
    ...
    WlWEh6dN36GVZYk93N8Bc9vY41xy8B9Rzz0GVQzXvNEvn700nVbfs",
  "q": "3df0R9cuYq-0S-mkFLzgItgMEfFzB2q3hWehMuG0oCuqnb3vobLyum
    ...
    kIdrecRezsZ-1kYd_s1qDbxtkDEgfAITAG9LUnADun4vIcb6yelxk",
  "dp": "G4sPXkc6Ya9y8oJW9_ILj4xuppu0lzi_H7VTkS8xj5SdX3coE0oim
    ...
    YZc3C3m3I24G2GvR5sSDxUyAN2zq8Lfn9EUms6rY30b8YeiKkTiBj0",
  "dq": "s9lAH9fggBsoFR80ac2R_E2gw282rT2kG0AhvI1lETE1efrA6huUU
    ...
    GF4Dh7e74WbRsobRonujTYN1xCaP6T061jvWrX-L18txXw494Q_cgk",
  "qi": "GyM_p6JrXySiz1toFgKbWV-JdI3jQ4ypu9rbMWx3rQJBfmt0FoYzg
    ...
    yR8055XLSe3SPmRfKwZI6yU24ZxvQKFYItldldUKGz06Ia6zTKhAVRU"
}
```

