Microprofile JWT im Detail

- Stateless Security für Microservices
- Spezifizierte Liste an Pflicht-Claims: typ, alg, kid, iss, sub, aud, iat, exp, jti, upn, groups
- Unterstützt ausschließlich RSA-SHA256 basierte digitale Signaturen
- Unterstützt JWTs als Bearer Tokens im Authorization HTTP Header
- JWTs werden als Authentication Token verwendet, via Issuer und Audience Claim.
- JWTs werden als Authorization Token verwendet, via Groups Claim.

Non-Goals of Microprofile JWT

- JWT Creation
  Nutzung von API Gateways oder Identity Provider Services (Okta, Auth0)
- RSA Public Key Distribution
  manuelle Verteilung oder Bereitstellung im Docker Image. Nutzung von JSON Web Key Sets.
- Automatic JWT Propagation
  Authorization Header wird nicht automatisch weitergeleitet. Nutzung von MP Rest-Client.

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
```