JWT

Inhaltsverzeichnis

JWT (JSON Web Token) transportiert signierte Aussagen über Identität und Rechte, oft für APIs und SSO. Der Empfänger prüft die Signatur und liest Claims ohne zentrale Session-Abfrage.

1 Funktionsweise

Ein Token besteht aus Header, Payload (Claims) und Signatur. Aussteller signieren es; Dienste validieren Algorithmus, Signatur, Audience und Ablauf.

- **Claims:** sub, exp, aud, roles …
- **Signatur/Encryption:** JWS/JWE
- **Bearer-Nutzung:** oft im Authorization-Header

2 Typische Einsatzbereiche

- API-Auth zwischen SPA/Mobile und Backend
- Microservices und Gateway-Flows
- Kurzlebige Access Tokens neben Refresh Tokens

3 Wichtige Hinweise

- „alg=none“ und schwache Keys sind klassische Fallen.
- Zu lange Lebensdauer erhöht Diebstahlrisiko.
- Revocation ist bei reinen JWTs begrenzt – kurz leben lassen.

4 Fazit

JWTs sind handlich für verteilte Auth – sicher nur mit strenger Validierung, kurzen Laufzeiten und sauberem Key-Management.