mTLS (Mutual TLS)

Inhaltsverzeichnis

Bei mTLS authentifizieren sich Client und Server gegenseitig per Zertifikat. So wird nicht nur die Verbindung verschlüsselt, sondern auch die Identität beider Seiten kryptografisch geprüft.

1 Funktionsweise

Zusätzlich zur Server-Zertifikatsprüfung legt der Client ein eigenes Zertifikat vor. Der Server akzeptiert nur Clients mit gültiger, vertrauenswürdiger Identität.

- **Server-Auth:** wie bei klassischem HTTPS
- **Client-Auth:** Zertifikatspflicht auf Client-Seite
- **Trust Store:** welche CAs bzw. Zertifikate gelten

2 Typische Einsatzbereiche

- Service-zu-Service-Kommunikation und interne APIs
- Hochsicherheitszugänge und Maschinenidentitäten
- Zero-Trust- und Service-Mesh-Szenarien

3 Wichtige Hinweise

- Zertifikatsverwaltung (Ausstellung, Rotation, Widerruf) ist der kritische Teil.
- Fehlerhafte Trust Stores führen schnell zu Ausfällen.
- mTLS ersetzt nicht Autorisierung innerhalb der Anwendung.

4 Fazit

mTLS stärkt Maschinen- und Service-Identitäten deutlich – ideal, wenn „wer spricht mit wem?“ genauso wichtig ist wie Verschlüsselung.