zurück

Grundlagen zu TLS & SSL

Diese Seite erklärt die Grundlagen von SSL/TLS, deren Unterschiede, Einsatzbereiche und wie sie die Kommunikation im Internet absichern.

Was ist TLS/SSL?

SSL = Secure Sockets Layer (veraltet)

TLS = Transport Layer Security (aktueller Standard)

Ziel: Verschlüsselung und Authentifizierung von Verbindungen über unsichere Netzwerke

Hauptfunktionen

Verschlüsselung der Datenübertragung

Integritätsschutz (Daten wurden unterwegs nicht verändert)

Authentifizierung der Gegenstelle (Server, ggf. auch Client)

Unterschiede: SSL vs. TLS

Eigenschaft	**SSL (veraltet)**	**TLS (modern)**
Protokollversionen	SSLv2, SSLv3	TLS 1.0 – 1.3
Sicherheit	Schwachstellen in allen SSL-Versionen	TLS 1.2/1.3 sind sicher
Einsatz	**Nicht mehr empfohlen**	Industriestandard

Fazit: **SSL ist tot**. Verwende **immer** TLS!

Wie funktioniert TLS?

Client (Browser) stellt Verbindung zum Server her

TLS-Handshake beginnt → Aushandlung von:

unterstützten Versionen

Cipher Suites (Verschlüsselungsverfahren)

Zertifikat des Servers

Gemeinsamer Sitzungsschlüssel wird erzeugt (z. B. via Diffie-Hellman)

Danach: verschlüsselte Kommunikation mit symmetrischem Schlüssel

Was ist ein Zertifikat?

Digitale Bestätigung, dass ein öffentlicher Schlüssel zu einer bestimmten Domain gehört

Ausgestellt von einer vertrauenswürdigen Zertifizierungsstelle (CA)

Enthält:

Domainname

Öffentlicher Schlüssel

Ablaufdatum

Signatur der CA

Zertifikatstypen

Typ	Beschreibung	Beispiel
DV (Domain Validation)	Nur Domain wird validiert	Let's Encrypt
OV (Organisation Valid.)	Domain + Firmenname verifiziert	Unternehmen
EV (Extended Validation)	Strenge Prüfung, grünes Schloss	Banken, Behörden

Zertifikat anzeigen im Browser

Klick auf das Schloss-Symbol → Zertifikatsdetails anzeigen

Häufige Probleme

Zertifikat abgelaufen → Erneuern!

Falsche Domain im Zertifikat → Domain prüfen

Self-Signed ohne Vertrauen → Manuell bestätigen oder eigene CA einbinden

Siehe auch

Let's Encrypt + ACME mit Traefik

Certbot-Befehle und Beispiele