

ZERTIFIKATE

Mariana Paradzik

Was sind SSL-Zertifikate

- SSL - Secure Socket Layer
- Datei, die auf Ursprungsserver einer Website installiert ist (nicht gleich sicher)
- Ausgestellt von Zertifizierungsstelle
- verschlüsselte Verbindung
- Schutz zw. Server und Website
- aktiviert Sicherheitsschloss und https-Protokoll

Was funktioniert ein SSL-Zertifikat

- Beginn mit SSL-Handshake: beide kommunizierende Parteien stellen sichere Verbindung her & tauschen Schlüssel aus
- während SSL-Handshake: beide Parteien generieren Sitzungsschlüssel (verschlüsselt & entschlüsselt gesamte Kommunikation)
- neue Sitzung -> neuer Schlüssel
- SSL stellt sicher, dass es die Partei ist, für die sie sich ausgibt und
- dass Daten nicht geändert wurden, da in Übertragungen ein Message Authentication Code (MAC) enthalten

Warum benötige ich Zertifikate?

- gewährleistet Geheimhalten von Online-Interaktionen
- Teil der SEO
- stärkt Vertrauen der Besucher
- Schutz der Kommunikation

Vorteile von Zertifikaten

- sichere Datenübertragung sensibler Daten (z.B. Login-Daten, Kreditkarteninformationen)
- stärkt Vertrauen der Besucher
- SEO - besseres Ranking

Arten von SSL-Zertifikaten

Extended Validation (EV SSL)	Organization Validated (OV SSL)	Domain Validated (DV SSL)
<ul style="list-style-type: none">• besonders hoher Schutz• 18 Überprüfungen• Unternehmen im Bank- und Finanzdienstleistungssektor, E-Commerce, große Konzerne, Fortune-500-Unternehmen, Global-2000-Unternehmen	<ul style="list-style-type: none">• Überprüfung: 9 Arten von Hintergrundinformationen• Mittelweg für Unternehmen• Anmeldebildschirme, Unternehmenswebsite, Webshop, Webmail	<ul style="list-style-type: none">• geringster Grad an Identitätsprüfung• bösartige Bots können schnell & einfach Zertifikat erhalten• oft verwendet von Websites ohne Zahlungstransaktionen• Blogs, persönliche Websites, Websites ohne Transaktionen und personenbezogene Daten

Wie erhält man ein SSL-Zertifikat?

- von einer Zertifizierungsstelle (CA - Certification Authorities)
- -> externe Partei, kann bestätigen, dass Webbesitzer der ist, der er vorgibt zu sein
- behält eine Kopie vom ausgestellten Zertifikat
- danach auf Webserver installieren

Anbieter:

Sectigo (ehemals Comodo)	DigiCert	GlobalSign
<ul style="list-style-type: none">• lange Zeit führendes Unternehmen• 2018 verkauft und umbenannt• breite Palette von Sicherheitsprodukten und Dienstleistungen	<ul style="list-style-type: none">• eine der führenden Zertifizierungsstellen weltweit• zentraler Akteur im Bereich der digitalen Zertifikate	<ul style="list-style-type: none">• Gründung: 1996• einer der ältesten aktiven Zertifizierungsstellen• breite Palette von digitalen Sicherheitsprodukten

