

Secure Sockets Layer SSL

Thomas Feyerl


HTTP VS HTTPS



Was ist SSL?

- SSL steht für Secure Sockets Layer.
- Es ist ein Verschlüsselungsprotokoll, das die Sicherheit von Datenübertragungen über das Internet gewährleistet.
- SSL verschlüsselt die Kommunikation zwischen einem Webbrowser und einem Webserver.





Warum ist SSL wichtig?

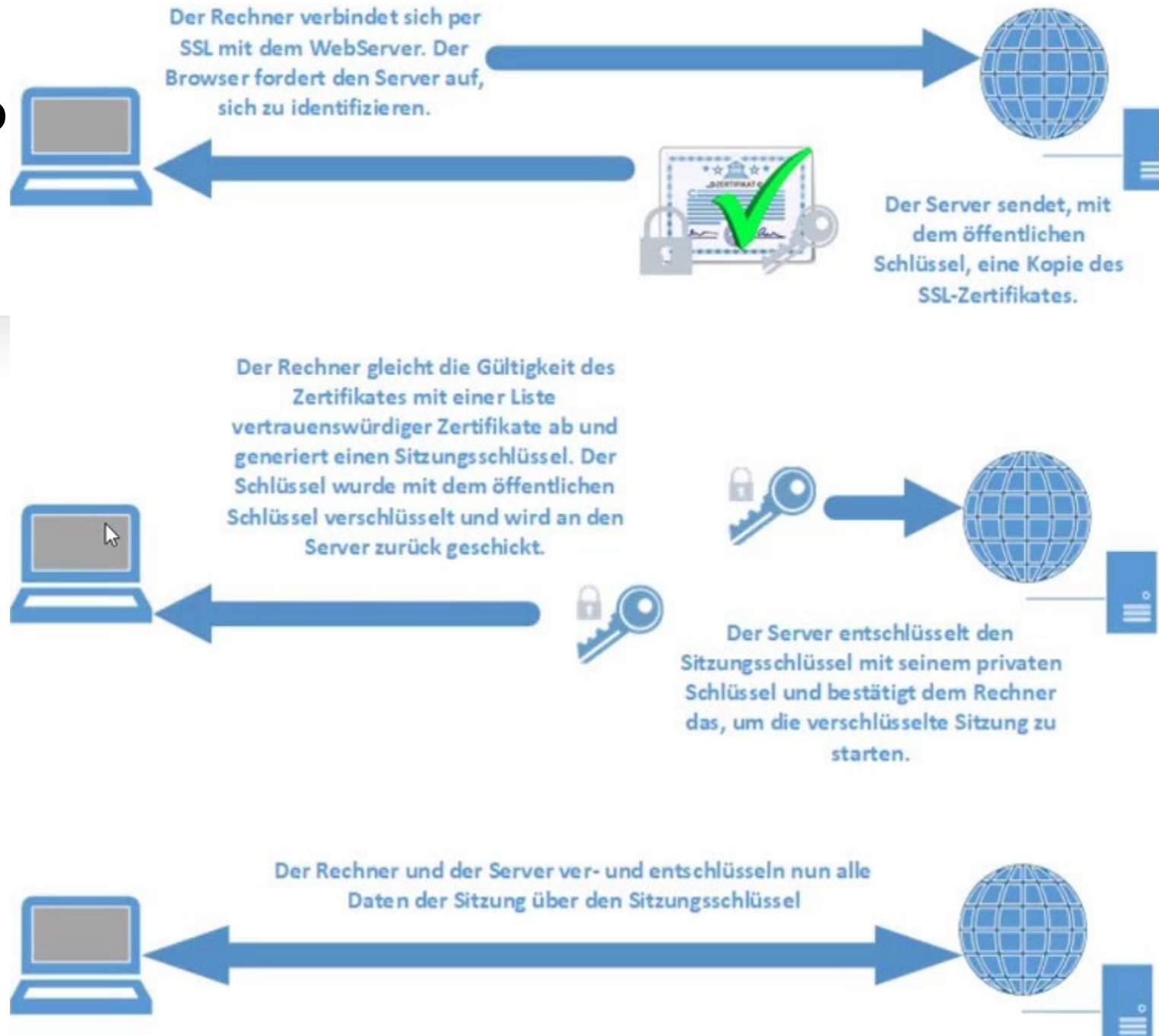
- Schutz sensibler Daten: SSL verschlüsselt vertrauliche Informationen wie Benutzernamen, Passwörter, Kreditkartennummern usw.
- Vertrauenswürdigkeit: SSL-Zertifikate bestätigen die Identität von Websites und ermöglichen es den Benutzern, sicher zu sein, dass sie mit der beabsichtigten Website kommunizieren und nicht mit einer gefälschten.



Wie funktioniert SSL?

- Handshake: Der Client und der Server führen einen Handshake durch, um sich auf die Verschlüsselungsmethoden zu einigen und die Identität zu überprüfen.
- Verschlüsselung: Nach dem Handshake verschlüsseln der Client und der Server die Daten, die zwischen ihnen ausgetauscht werden, mit einem gemeinsamen Schlüssel.
- Datenübertragung: Die verschlüsselten Daten werden sicher zwischen Client und Server übertragen.
- Entschlüsselung: Der Server entschlüsselt die empfangenen Daten, um sie zu verarbeiten.

SSL Verschlüsselung im Detail



Arten von SSL-Zertifikaten

- Domain Validated (DV): Bestätigt die Inhaberschaft der Domain.
- Organization Validated (OV): Bestätigt die Identität des Unternehmens.
- Extended Validation (EV): Bietet die höchste Stufe der Validierung und zeigt den grünen Balken im Browser an.

Vorteile von SSL

Datenschutz: Schutz sensibler Daten vor unbefugtem Zugriff.

Vertrauen: Zeigt den Benutzern, dass die Website sicher ist.

Suchmaschinen-Ranking: Google bevorzugt Websites mit SSL-Verschlüsselung in den Suchergebnissen.



Wie implementiert man SSL?

SSL-Zertifikat erwerben: Ein SSL-Zertifikat von einer Zertifizierungsstelle (Certificate Authority, CA) erwerben.

Installation auf dem Server: Das SSL-Zertifikat auf dem Webserver installieren und konfigurieren.

Überprüfung: Sicherstellen, dass die SSL-Konfiguration ordnungsgemäß funktioniert und das HTTPS-Protokoll aktiviert ist.

SSL- Zertifikatsvalidierung

- Beim Handshake überprüft der Client das SSL-Zertifikat des Servers, um sicherzustellen, dass es gültig ist.
- Die Validierung umfasst:
- Gültigkeit des Zertifikats: Überprüfung des Ablaufdatums.
- Signaturprüfung: Überprüfung, ob das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde.
- Domainüberprüfung: Überprüfung, ob das Zertifikat zur Domain des Servers passt.

SSL- Verschlüsselungsstärken

- SSL bietet verschiedene Verschlüsselungsstärken, die die Sicherheit der Kommunikation beeinflussen.
- Die gängigsten Verschlüsselungsalgorithmen sind RSA (Rivest-Shamir-Adleman) und ECC (Elliptic Curve Cryptography).
- Die Verschlüsselungsstärke wird durch die Länge des verwendeten Schlüssels bestimmt, z.B. 128-Bit oder 256-Bit-Verschlüsselung.

Risiken und Herausforderungen

- Fehlkonfigurationen: Falsch konfigurierte SSL-Implementierungen können Sicherheitsrisiken darstellen und Angriffe ermöglichen.
- Schwache Verschlüsselung: Veraltete oder unsichere Verschlüsselungsalgorithmen können von Angreifern geknackt werden.
- Zertifikatsmissbrauch: Gefälschte oder gestohlene SSL-Zertifikate können verwendet werden, um Phishing-Angriffe durchzuführen oder Benutzer zu täuschen.
- Man-in-the-Middle-Angriffe: Angreifer könnten versuchen, die Kommunikation zwischen Client und Server abzufangen oder zu manipulieren, indem sie sich als vertrauenswürdiger Server ausgeben.

SSL in der Praxis



SSL wird in verschiedenen Bereichen eingesetzt, darunter:



E-Commerce: Schutz von Online-Zahlungen und Transaktionen.



Online-Banking: Sicherstellung der Vertraulichkeit von Bankgeschäften.



Soziale Medien: Verschlüsselung von Benutzerdaten und -kommunikation.



Viele moderne Webbrowser und Apps unterstützen automatisch SSL und zeigen eine sichere Verbindung durch das Schlosssymbol in der Adressleiste an.

Transport Layer Security (TLS)

- Entwicklung aus SSL: TLS ist die Weiterentwicklung von SSL und bietet verbesserte Sicherheit und Zuverlässigkeit.
- Ziele von TLS:
 - Sicherstellung der Vertraulichkeit: Verschlüsselung der Datenübertragung zwischen Client und Server.
 - Gewährleistung der Integrität: Schutz vor Datenmanipulation während der Übertragung.
 - Authentifizierung: Überprüfung der Identität des Servers und manchmal auch des Clients.
- Versionsgeschichte:
 - TLS 1.0, 1.1, 1.2, 1.3: Jede Version bringt Verbesserungen in Bezug auf Sicherheit und Effizienz.

Unterschiede zwischen SSL und TLS

- Protokollversionen:
 - SSL hat verschiedene Versionen, darunter SSL 2.0 und SSL 3.0.
 - TLS hat seine eigene Versionierung, beginnend mit TLS 1.0 bis hin zu TLS 1.....
- Sicherheit:
 - TLS bietet verbesserte Sicherheitsfunktionen im Vergleich zu SSL, einschließlich stärkerer Verschlüsselungsalgorithmen und sichererer Handshake-Protokolle.
- Flexibilität:
 - TLS ermöglicht eine größere Flexibilität bei der Unterstützung verschiedener Verschlüsselungsalgorithmen und kryptographischer Techniken.
- Rückwärtskompatibilität:
 - TLS-Versionen sind oft rückwärtskompatibel mit älteren SSL-Versionen, was die Migration erleichtert.

Fazit

- SSL früher, TLS heute ist ein wesentlicher Bestandteil der Internet-Sicherheit, der die Vertraulichkeit und Integrität von Datenübertragungen gewährleistet.
- Die Implementierung von SSL/TLS schützt nicht nur sensible Daten, sondern verbessert auch das Vertrauen der Benutzer und das Suchmaschinenranking der Website.