softed.de

# Wie funktioniert https? - SoftEd IT-Blog

· *Ulf Riechen*

5 Minuten

---

HTTPS ist der Standard für die verschlüsselte Übertragung von Daten zwischen Browser und Webserver. Er beruht auf X.509-Zertifikaten. Grundlage sind asymmetrische Verschlüsselungsverfahren. Diese erfordern einen hohen mathematischen Aufwand und
verursachen somit viel Prozessorlast. Dafür sind die übertragenen Schlüssel durch
einen Angreifer nicht abfangbar.

## Vorbereitung

Damit diese genutzt werden können, muss zunächst eine Zertifizierungsinstanz (Certificate
Authority – CA) eingerichtet werden. Diese garantiert die unverfälschte Übertragung
der öffentlichen Schlüssel und die Echtheit des Webservers. Das Zertifikat der CA
wird in allen Browsern installiert und erscheint dort als “Vertrauenswürdige
Stammzertifizierungsstelle”. Sollte das Zertifikat nicht installiert

sein,
erhält der Benutzer beim Öffnen der Webseite eine Fehlermeldung. Das Zertifikat
der SoftEd-Root-CA können Sie hier herunterladen.

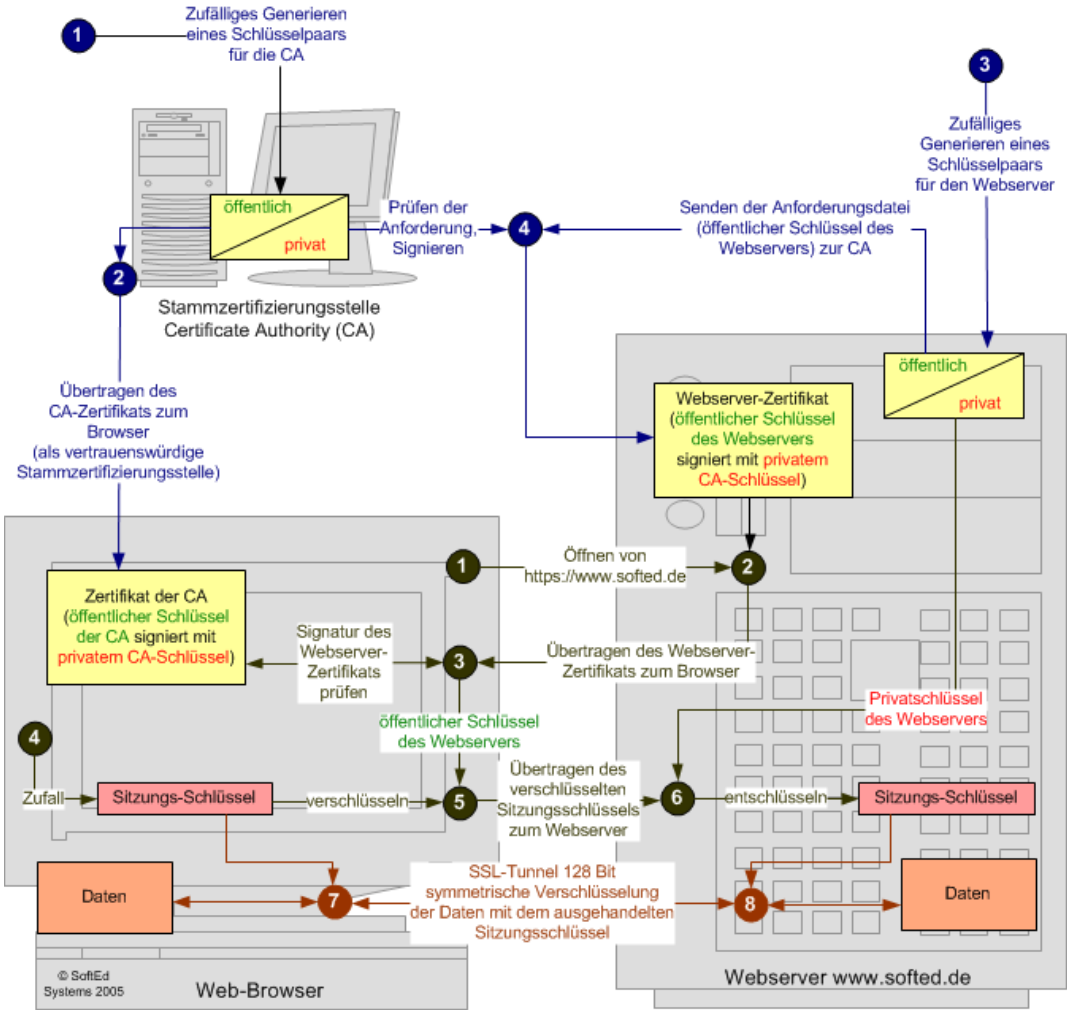
Der Webserver generiert ebenfalls ein Schlüsselpaar, dessen öffentlicher Teil zur
CA übertragen wird. Die CA prüft die Angaben des Webserverbetreibers und signiert
den Schlüssel. Das damit entstandene Webserver-Zertifikat garantiert die Echtheit
des Webservers und stellt eine Garantie für Clients dar, dass sie sich mit dem richtigen
Webserver verbunden haben.

## Aufbau der HTTPS-Verbindung

Der Benutzer baut die Verbindung auf, indem er entweder auf einen Link mit https://…..
klickt, oder die URL im Browser einträgt. Der Browser baut daraufhin eine Verbindung
über Port 443 zum Webserver auf. Der Webserver präsentiert sein Zertifikat, das
der Client mit Hilfe des installierten CA-Zertifikats auf Echtheit überprüft. Danach
erfolgt die nur für den Webserver lesbare Übertragung des Sitzungsschlüssels. Mit
dem nun auf beiden Seiten vorhandenen Sitzungsschlüssel kann eine symmetrische Datenverschlüsselung
beginnen. Diese symmetische Verschlüsselung ist deutlich

einfacher als das Übertragen
der Schlüssel, weshalb hier auch nur eine geringe Prozessorlast verursacht wird.

Der Ablauf einer HTTPS-Verbindung wird in der folgenden Grafik dargestellt:




## Vorbereiten der CA

1. Generieren eines Schlüsselpaares für die CA
2. Verteilen des CA-Zertifikates auf alle browser

## Vorbereiten des Webservers

3. Generieren eines Schlüsselpaares für den Webserver

4. Zertifizierung des Webservers nach Prüfung durch die CA

**Asymmetrischer Sitzungsaufbau**

1. Aufbau der Verbindung https://www.softed.de auf Port 443
2. Übertragen des Webserver-Zertifikats zum Browser
3. Prüfen der Signatur des Zertifikats anhand des von der CA hinterlegten Schlüssels,
   bei Erfolg ist die Identität des Webservers festgestellt
4. Generieren eines temporären Sitzungsschlüssels
5. Senden des Schlüssels in einer nur für den Webserver lesbaren Art
6. Entschlüsseln des Sitzungsschlüssels

**Symmetrischer SSL-Tunnel**

7. Symmentrische Ver- und Entschlüsselung beim Client
8. Symmentrische Ver- und Entschlüsselung beim Server

## Fehlermeldungen beim Aufbau einer HTTPS-Verbindung

- Das Zertifikat ist abgelaufenJedes Zertifikat hat eine begrenzte Gültigkeitsdauer. So wird verhindert, dass ein
  “geknackter” Schlüssel lange verwendet wird. Die Gültigkeitsdauer sollte
  deutlich unter der Zeit liegen, die für einen Brute-Force-Angriff auf einen Verschlüsselungsalgorithmus
  benötigt wird. **Gefahr**: Ein Angreifer nutzt ein abgelaufenes

Zertifikat,
dessen Privatschlüssel er geknackt hat.

- Das Zertifikat wurde von einer nicht vertrauenswürdigen Zertifizierungsinstanz ausgestellt.Diese Meldung erhalten Sie, wenn Ihr Browser kein Zertifikat der Zertifizierungsinstanz installiert hat. Das kann über die Download-Seite der Zertifizierungsinstanz
  nachträglich erfolgen. **Gefahr**: Ein Angreifer stellt sich selber Zertifikate aus.
- Der auf dem Zertifikat angegebene Servername stimmt nicht mit dem Webserver überein.Hier wurde der Servername geändert, oder der Nutzer greift nicht über den Namen,
  sondern über “localhost” oder die IP-Adresse auf den Server zu.
  **Gefahr**:
  Ein Angreifer besorgt sich ein für einen fremden Webserver ausgestelltes Zertifikat.

## SoftEd unterstützt Sie mit

**Know-how:**

Beratung zur IT-Security

**Seminaren:**

IT-Sicherheit – Firewall, Verschlüsselung,IDS