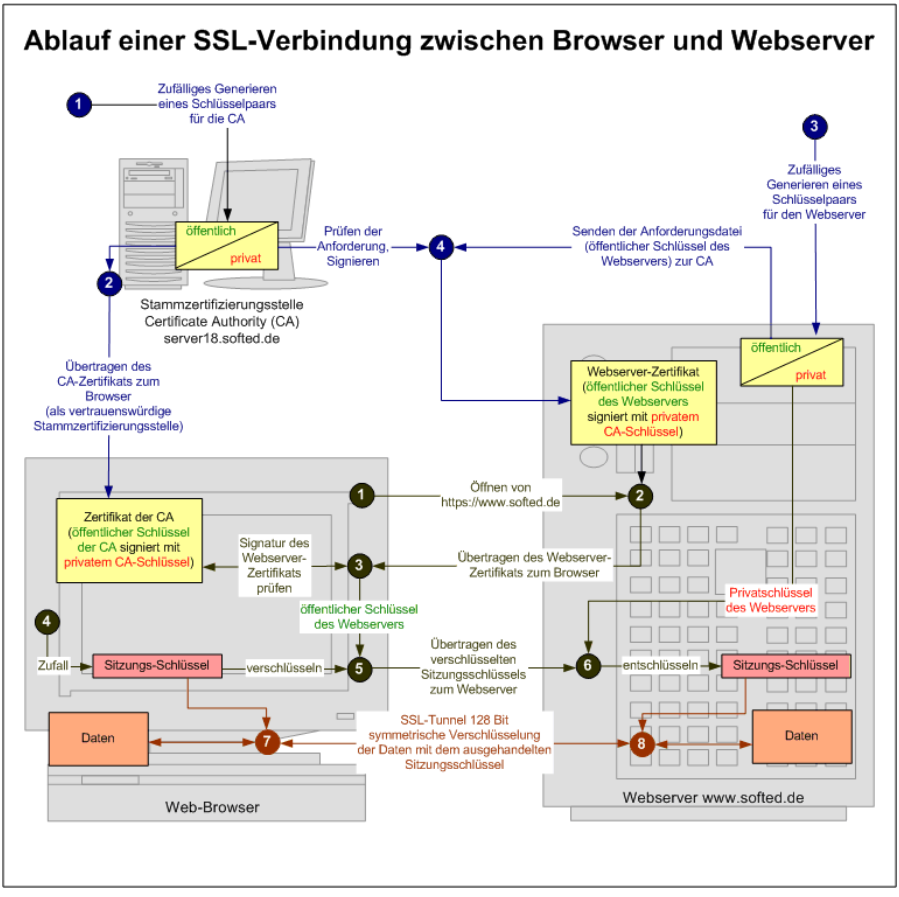
TS I	HTTPS	Name	Datum

Wie funktioniert HTTPS?

HTTPS ist der Standard für die verschlüsselte Übertragung von Daten zwischen Browser und Webserver. Er beruht auf X.509-Zertifikaten. Grundlage sind unsymmetrische Verschlüsselungsverfahren für den Schlüsselaustausch. Diese erfordern einen hohen mathematischen Aufwand und verursachen somit viel Prozessorlast. Dafür sind die übertragenen Schlüssel durch einen Angreifer nicht abzufangen. Der eigentliche Datenverkehr wird anschließend symmetrisch verschlüsselt à geringere Prozessorlast.

Vorbereitung
Damit Zertifikate genutzt werden können, muss zunächst eine Zertifizierungsstelle (Certificate Authority - CA) eingerichtet werden (1). 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" (2). Sollte das Zertifikat nicht installiert sein, erhält der Benutzer beim Öffnen der Webseite eine Fehlermeldung.
Der Webserver generiert ebenfalls ein Schlüsselpaar, dessen öffentlicher Teil zur CA übertragen wird (3). Die CA prüft die Angaben des Webserverbetreibers und signiert den Schlüssel (4). Das damit entstandene Webserver-Zertifikat bestätigt 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 (1). Der Webserver präsentiert sein Zertifikat (2), das der Client mit Hilfe des installierten CA-Zertifikats auf Echtheit überprüft (3). Danach erfolgt die nur für den Webserver lesbare Übertragung des zufällig (4) erzeugten Sitzungsschlüssels (5). Mit dem nun auf beiden Seiten vorhandenen Sitzungsschlüssel kann eine symmetrische Datenverschlüsselung beginnen (7,8). Diese symmetrische Verschlüsselung verursacht eine geringere Prozessorlast als die zum Übertragen der Schlüssel eingesetzten unsymmetrischen Verfahren.



Vorbereiten der CA

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

Vorbereiten des Webservers

3. Generieren eines Schlüsselpaares für den Webserver
4. Zertifizierung des Webservers nach Prüfung durch die CA

Unsymmetrischer 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. Symmetrische Ver- und Entschlüsselung beim Client
8. Symmetrische Ver- und Entschlüsselung beim Server