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 asymmetrische Verschlüsselungsverfahren.

CA certificate Authority

- Zertifizierungsinstanz
- Garantiert die Echtheit des Webserver und unverfälschte Übertragung des **public key** (Webserver)
- Das Zertifikat der CA wird in allen Browsern installiert und erscheint dort als «Vertrauenswürdige Stammzertifizierung»

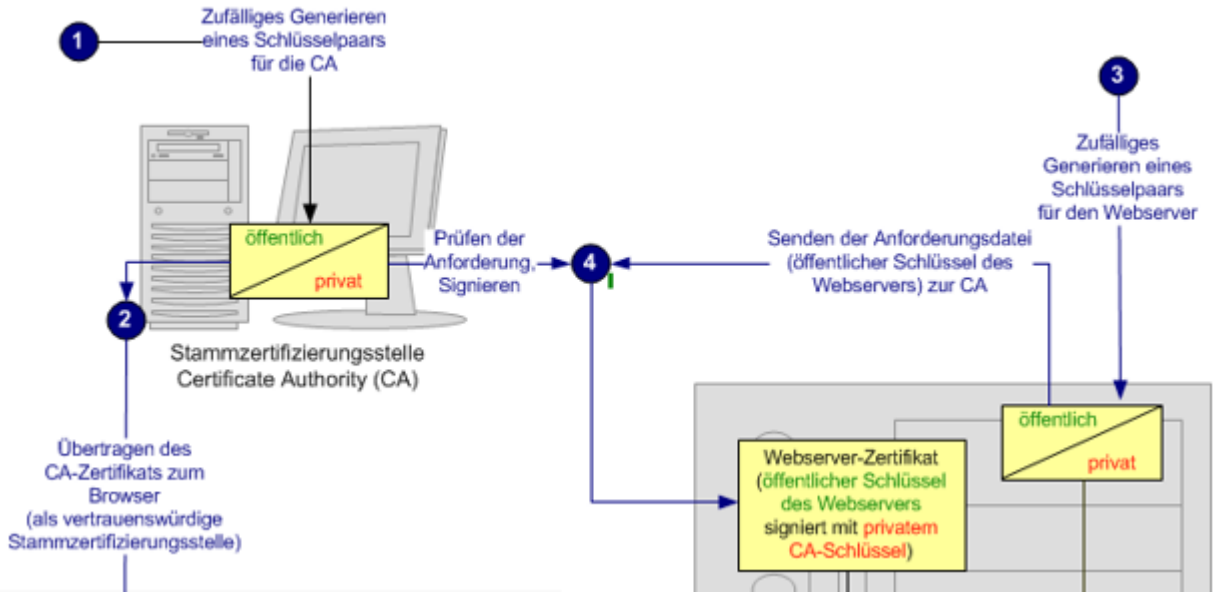
Vorbereitungen

Vorbereiten der CA

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

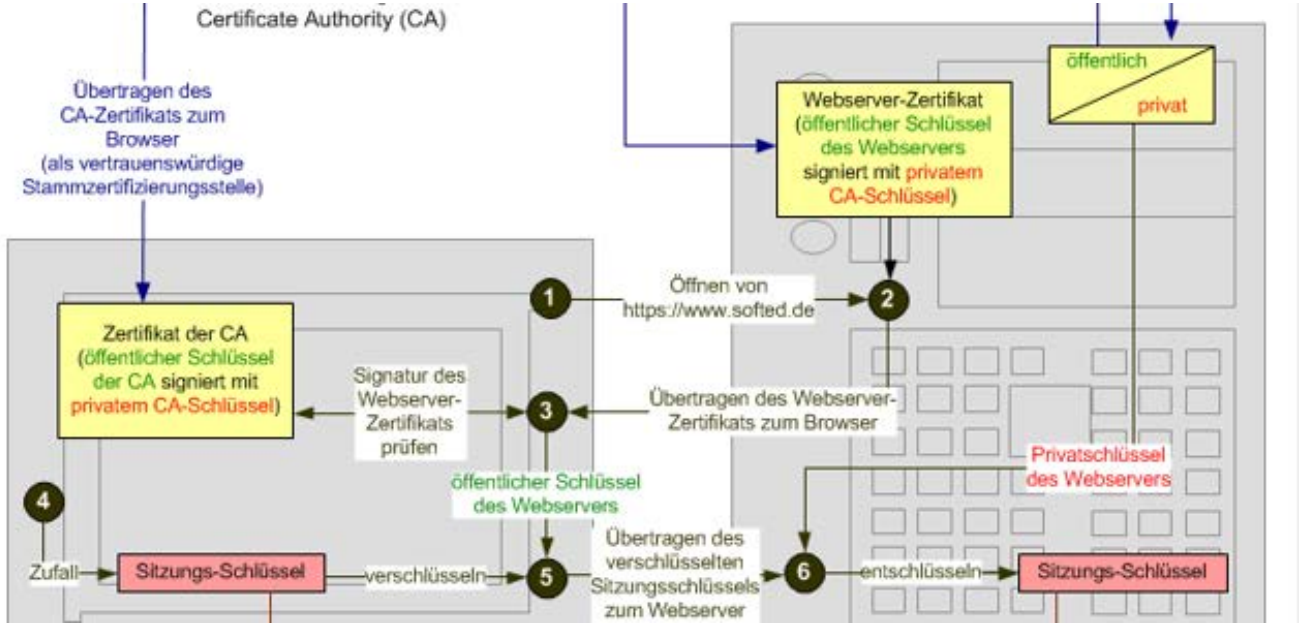
Vorbereiten des Webservers

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



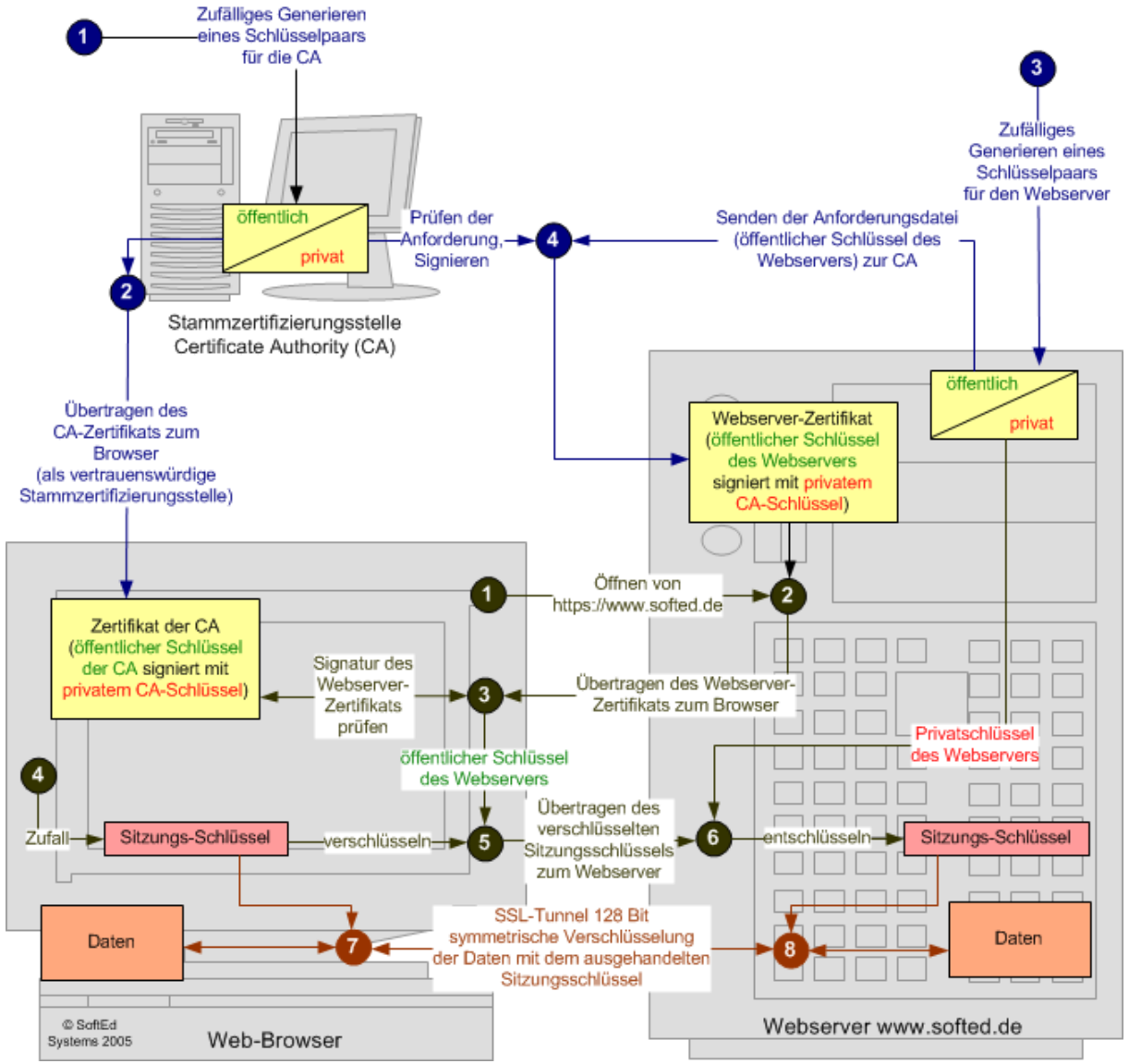
Asymmetrischer Sitzungsaufbau

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



Quellen: https://www.softed.de/blog/wie-funktioniert-https/?H=redir