Zertifikate

Einsatzzweck

Zertifikate werden im Allgemeinen verwendet, um die Echtheit von Daten zu beweisen. Daten können hierbei E-Mails, Dokumente, Software / Updates, Webdaten oder gar ganze Verbindungen wie z. B. bei einem VPN sein.

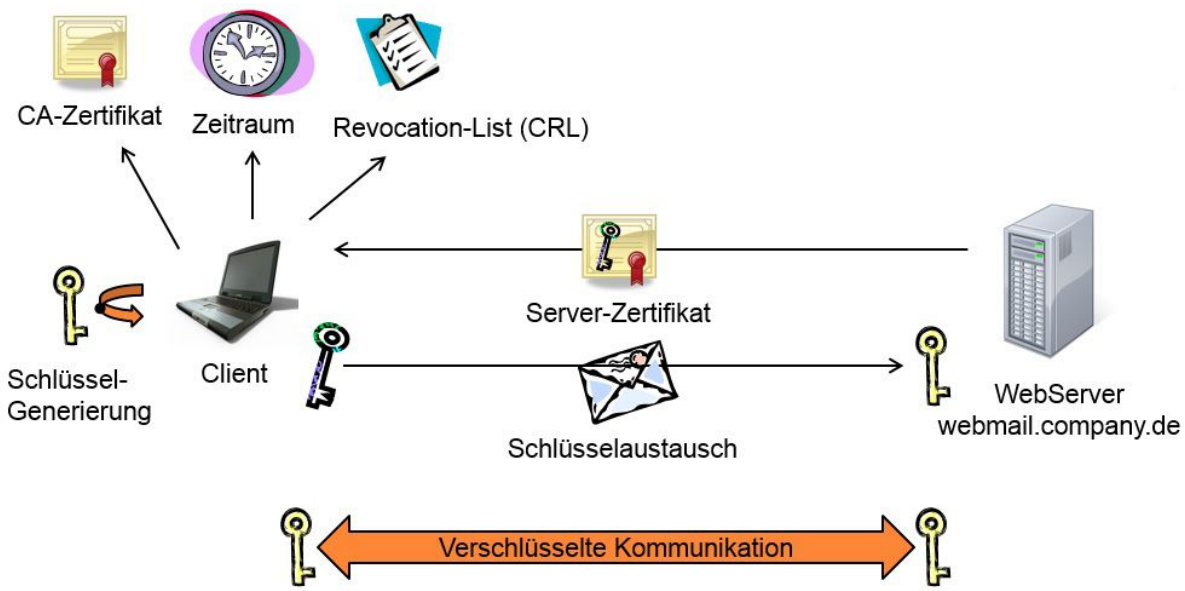
Funktionsweise

Damit Zertifikate funktionieren, sind in der Regel zwei Dinge notwendig. Zum einen wird eine Zertifizierungsstelle (Certification Authority oder auch CA) benötigt. Diese vergibt die Zertifikate und stellt sicher, dass derjenige der das Zertifikat beantragt auch der ist, der zu dem Zertifikat hinterlegt ist. Hierbei gibt es verschiedenste Stufen der Überprüfung, denn nicht jedes Zertifikat ist gleich vertrauenswürdig.

Des Weiteren ist, um die Zertifikate überprüfen zu können, eine sogenannte Public Key Infrastruktur, kurz PKI notwendig. Sie vereinfacht den Austausch von Zertifikaten dahingehend, dass es ein Root Zertifikat gibt, dem vertraut wird. Alle Zertifikate, die mit diesem signiert wurden, können als vertrauenswürdig betrachtet werden, da bei der Signierung der Zertifikate die Ansprüche der Root CA zu erfüllen sind.

Das gesamte System der Zertifikate basiert auf der asymmetrischen Verschlüsselung, wobei das Zertifikat immer nur den Public Key enthält. Der jeweilige Private Key bleibt bei den signierenden Parteien.

Der Ablauf einer mit Zertifikaten signierten Verbindung ist folgender Grafik zu entnehmen.



Revision #5
Created 2022-08-01 07:32:52 UTC by Joshua Lieder
Updated 2022-09-02 07:49:55 UTC by Joshua Lieder