Hypertext Transfer Protocol | Transportlayer Security | Quic

IT-Technik - Netzwerkgrundlagen

Sebastian Meisel

5. März 2024

1 Hypertext Protocol (HTTP1/ HTTP2)

HTTP dient zum Abruf von Webseiten. Das Protokoll arbeitet auf dem *Presentation Layer (7)*. Es ist ein **zustandsloses** Protokoll, d. h. es gibt zunächst keine Möglichkeit Daten zu speichern. Dies kann durch **Cookies** umgangen werden, die im *HTML-Header* übertragen und vom Client gespeichert werden.
Neben dem Missbrauch von *Cookies* für Tracking, gibt es auch viele sinnvolle Nutzungsszenarien, z. B. für die Benutzerauthenfizierung.

2 Transport Layer Security (TLS) = Secure Socket Layer (SSL)

Die **HTTP**-Versionen 1 und 2 übertragen alle Information unverschlüsselt, sodass sie auf jedem Router, den sie passieren mitgelesen werden können.
Zur Verschlüsselung kann aber **TLS** verwendet werden.
Dabei identifizieren sich Server und Client zunächst im **TLS Handshake** mit Hilfe von **Zertifikaten**. Zugleich werden **Crypto-Schlüssel** ausgetauscht.
Dann werden im **TSL Record** sämtliche übertragenen Daten mit diesen **Schlüsseln** verschlüsselt.
Die Verschlüsselung des **Handshakes** ist **asymetrisch**, d. h. für der **Ver**schlüsselung wird ein anderer **Schlüssel** (öffentlicher Schlüssel / *public key*) als für die **Ent**schlüsselung (privater Schlüssel / *private key*).
Die Verschlüsselung des **Records** wiederum ist **symetrisch**. Zum Ver- und Entschlüsseln wird als von Client und Server jeweils **derselbe** Schlüssel verwendet.
So wird verhindert, dass Daten *beim Transport* **mitgelesen** (Vertraulichkeit) oder **manipuliert** (Integrität).

2.1 Zertifikate

Server Zertifikate werden von einer **Certificate Authority** (CA) ausgegeben und signiert.
Jeder Browser führt eine Liste vertrauenswürdiger **CAs**.
Das **Zertifikat** enthält Informationen über die **Organisation** für die es ausgestellt wurde.
Außerdem den **öffentlichen Schlüssel** der für die Verschlüsselung verwendet werden soll und eine **Signatur**, die die Echtheit des Zertifikats bestätigt.
Außerdem enthält es den Zeitraum der **Gültikeit** des Zertifikats.
Das **Clientzertifikat** wird vom Browser zur Verfügung gestellt.

2.2 TLS Handshake

3 QUIC

QUIC (Quick UDP Internet Connection) ist ein Protokoll, das entwickelt wurde, um herkömmliche *TCP* (Transmission Control Protocol) und *TLS* (Transport Layer Security) zu ersetzen, um eine schnellere und sicherere Kommunikation über das Internet zu ermöglichen. Im Gegensatz zu TCP, das auf einer Reihe von Hin- und Rücknachrichten zur Herstellung einer Verbindung beruht, arbeitet QUIC über UDP (User Datagram Protocol), was zu geringerer Latenz und verbesserte Leistung führt.
Bei QUIC können werden bereits mit dem 3. Paket Daten versandt - beim traditionellen TCP-TLS-Stack erst ab dem 8.

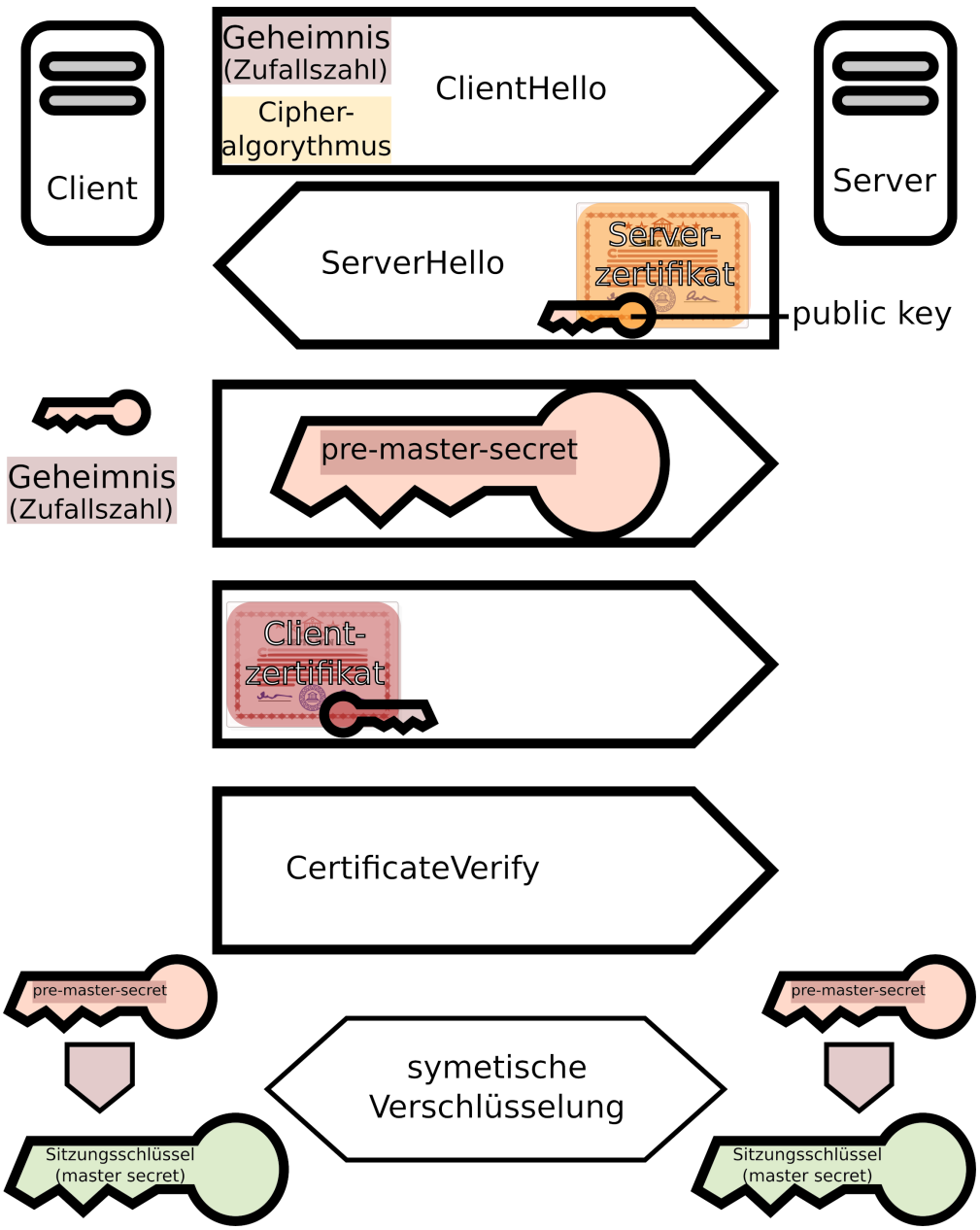

Abbildung 1: TLS Handshake

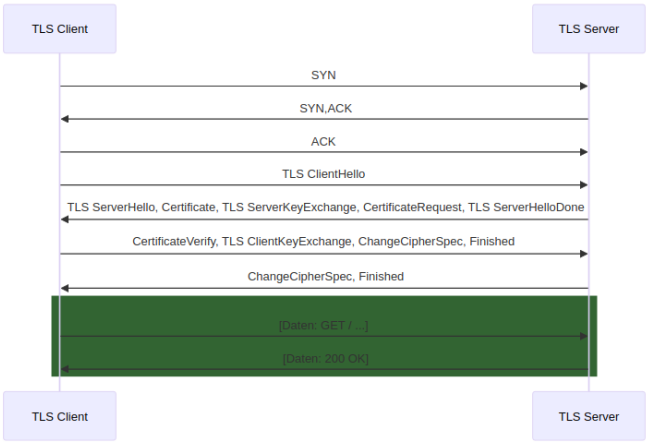

Abbildung 2: TCP/TLS Handshakes

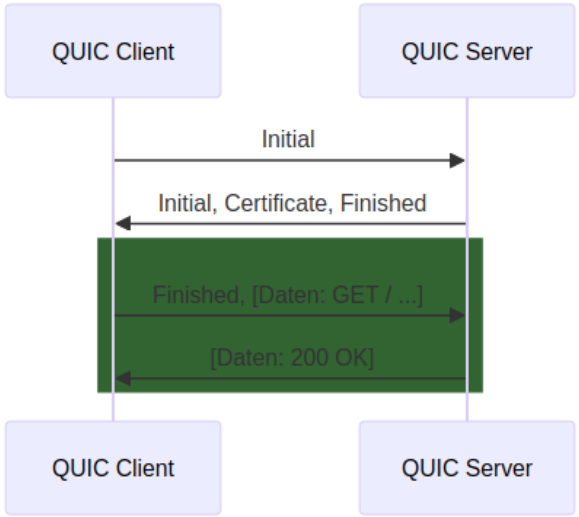

Abbildung 3: QUIC Handshake