Blockveranstaltung Web-Technologien
Wintersemester 2005/06

SSL / Zertifikate

Peter Weckert

Lehr- und Forschungseinheit für Medieninformatik
am Institut für Informatik der Ludwig-Maximilians-Universität München

AGENDA

- Einführung: SSL
- Lokalisierung im Netzwerkprotokoll
- Einbindung in HTTP
- HTTPS über HTTP-Proxy: CONNECT-Methode
- OpenVPN
- PKI-Konzept: Zertifikate

- Blick in die Praxis

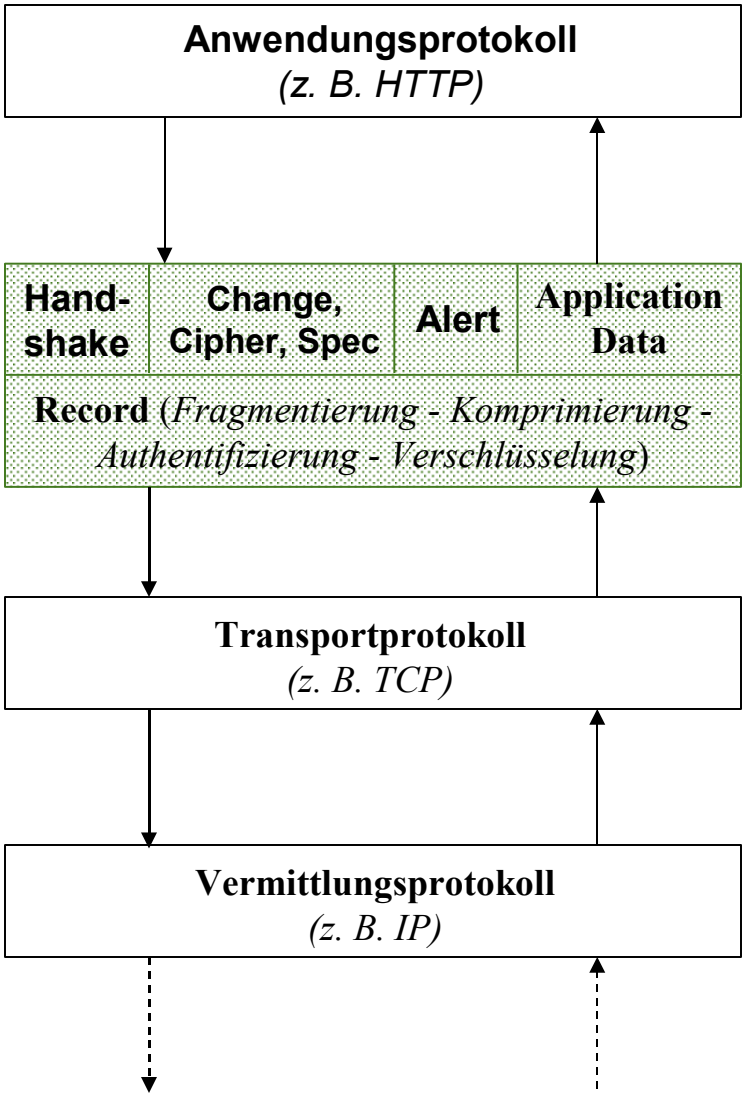
Einführung: SSL / TSL

- Def.: SSL - Secure Socket Layer
  - Erstmals November 1993 von National Center for Supercomputing Applications (NCSA)

- Versionen:
  - SSL 1.0 (November 1993)
  - SSL 2.0 (April 1994) in Netscape Navigator
  - Ende 1995 mit zusätzlichen Komponenten im Internet Explorer von Microsoft aufgenommen
  - Verbesserungen letzter Jahre in SSL 3.0 aufgenommen
  - TLS ≈ SSL 3.1 (Januar 1999)

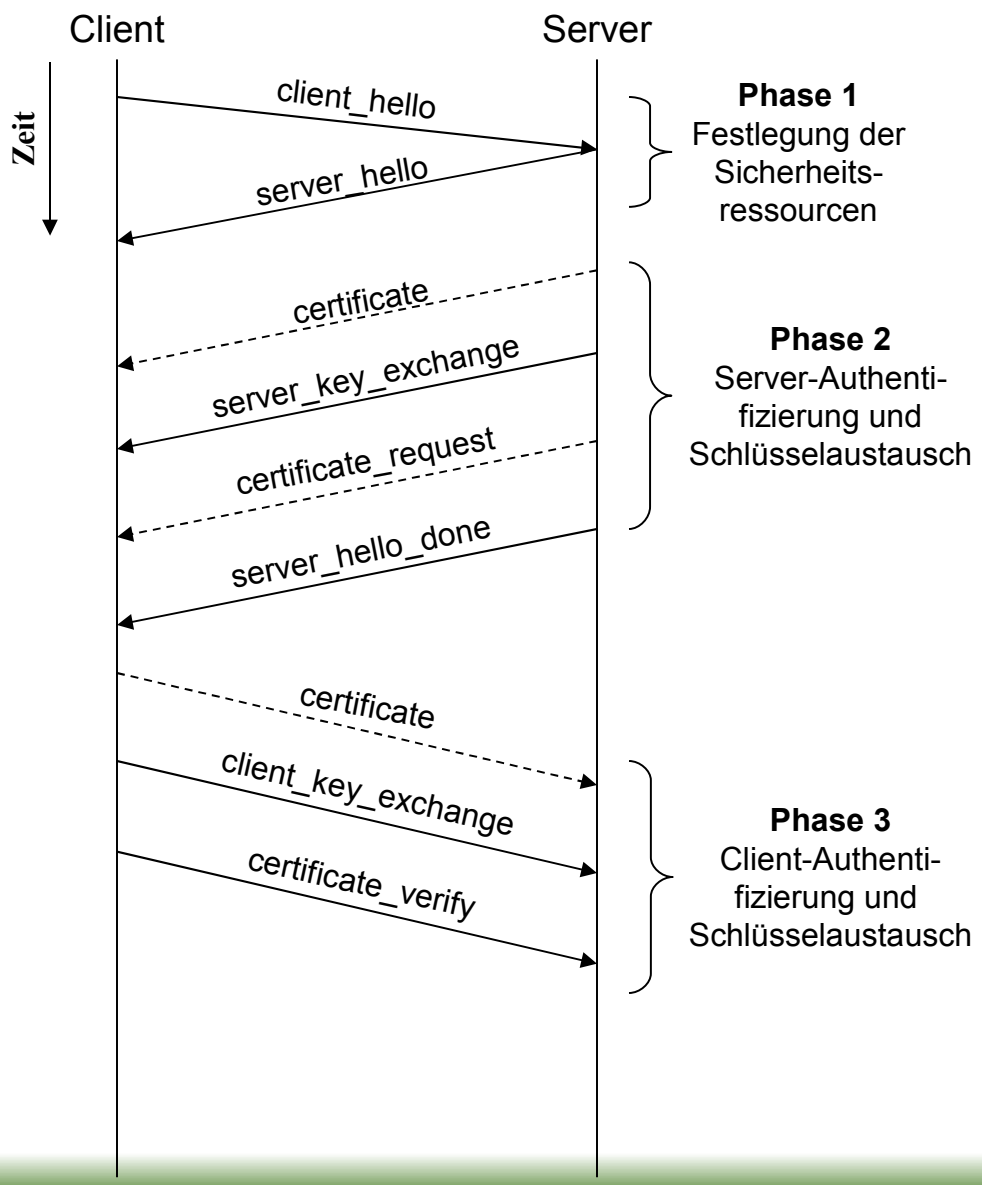
    [Transport Layer Security]

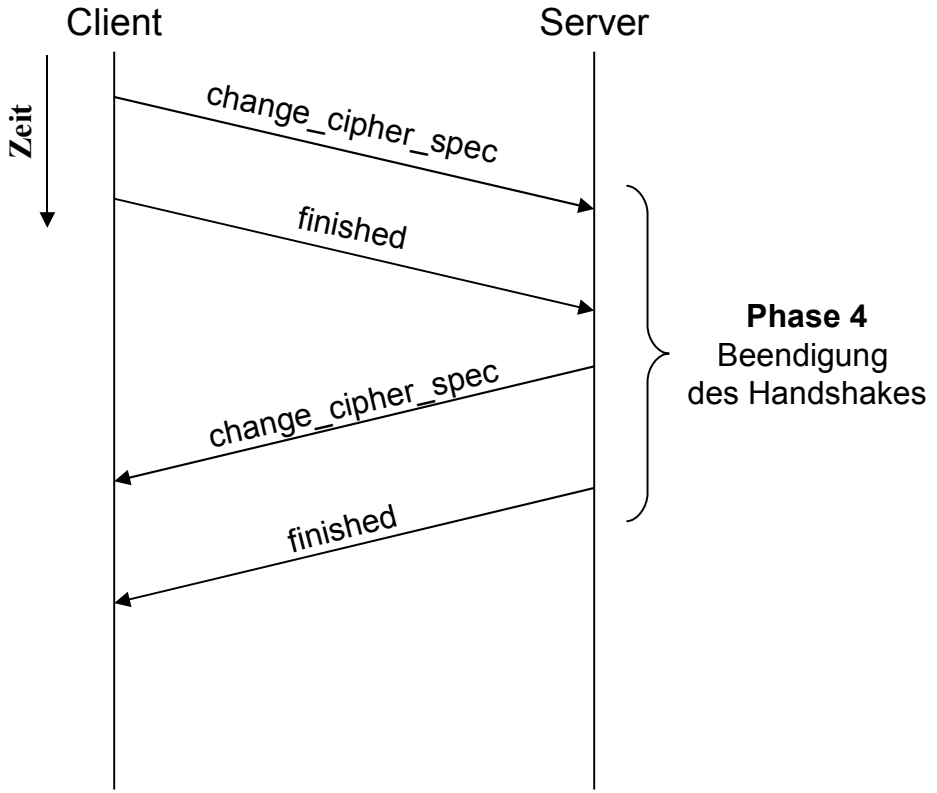
Lokalisierung im Netzwerkprotokoll



- Aufbau gesicherter TCP - Verbindung(en)
- Schutz von Datentransfer
- statt http://... https://...

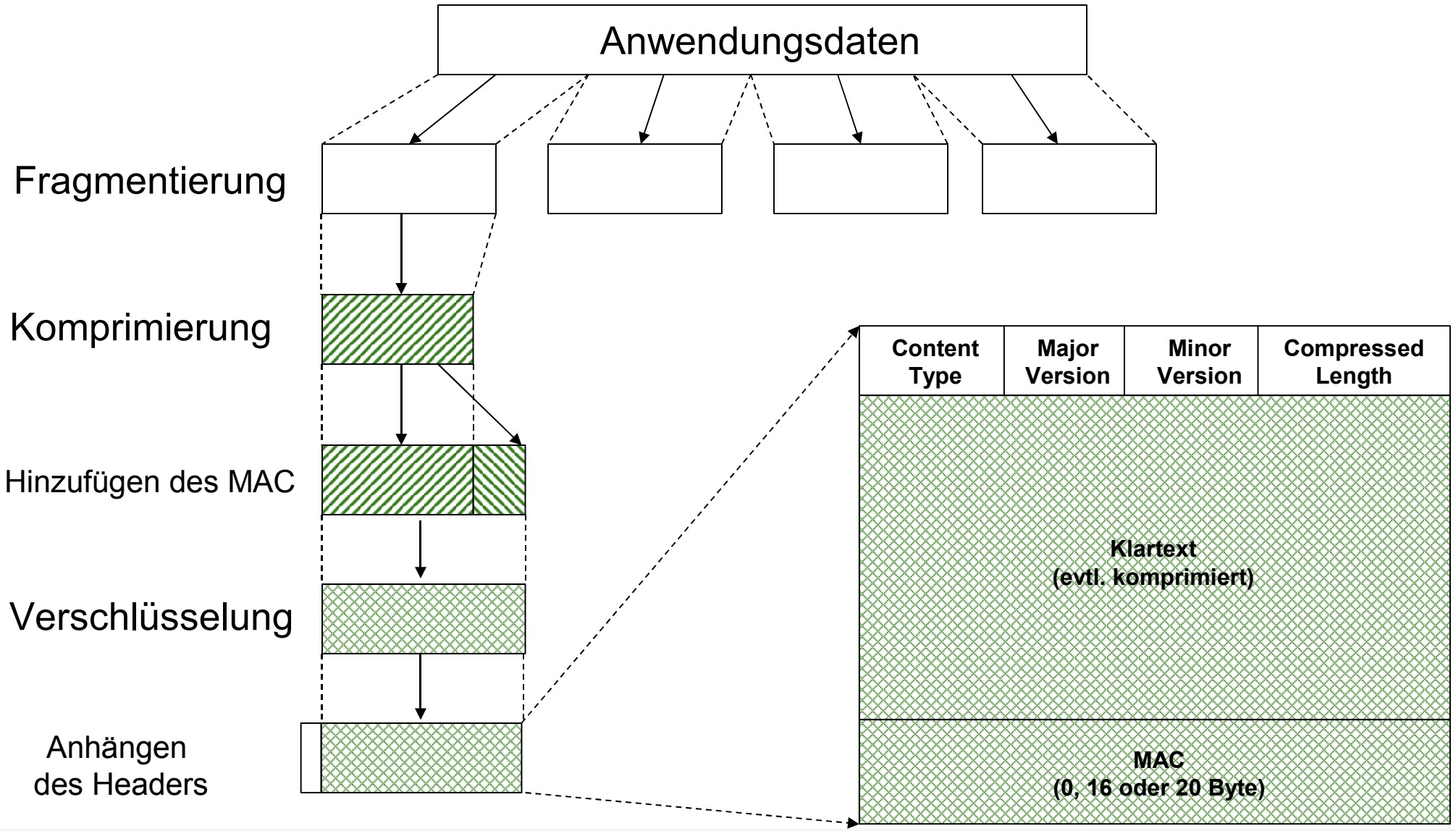
Exkurs: SSL - Handshake





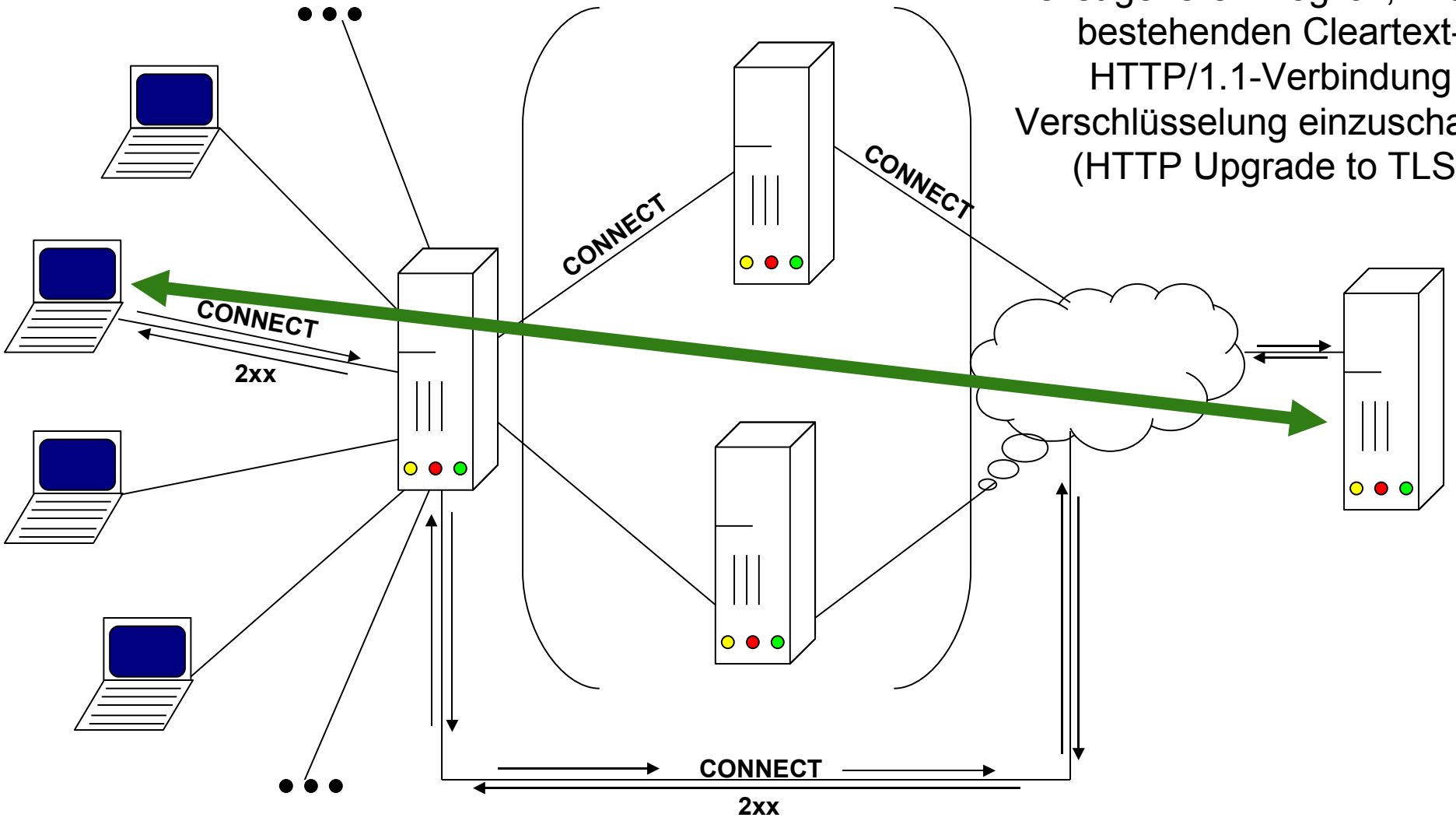
- Modus der Verschlüsselung
- Art der Nachrichtenauthentifizierung
- Geheimschlüssel
- bei Austausch von Zertifikaten: X.509v3-Standard

Einbindung in HTTP - Recordprotokoll



HTTPS über HTTP-Proxy: CONNECT-Methode

Es ist generell möglich, in einer bestehenden Cleartext-HTTP/1.1-Verbindung Verschlüsselung einzuschalten (HTTP Upgrade to TLS)



OpenVPN

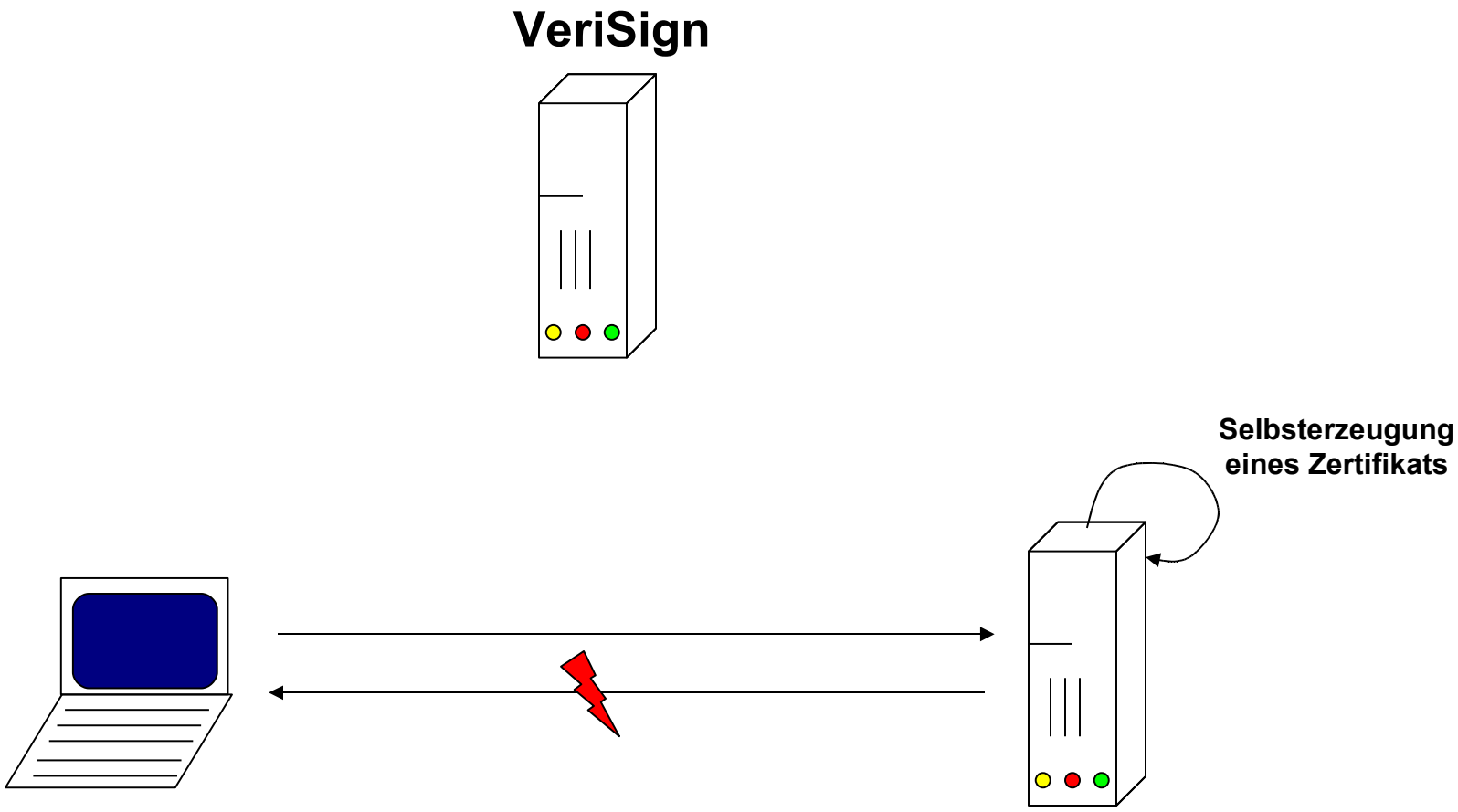
OpenVPN als Beispiel für einen verschlüsselten Einsatz außerhalb von HTTP - Anwendungen

- OpenVPN wird in jedem Wirtschaftsbetrieb eingesetzt
- Nur zertifizierte Zweigstellen (Filialen, Tochtergesellschaften, o. ä.) werden mit der Hauptgeschäftstelle vernetzt
- OpenVPN benutzt SSL/TLS zur Verschlüsselung beliebiger IP-Pakete
- Man-in-the-Middle Attacken können dadurch verhindert werden

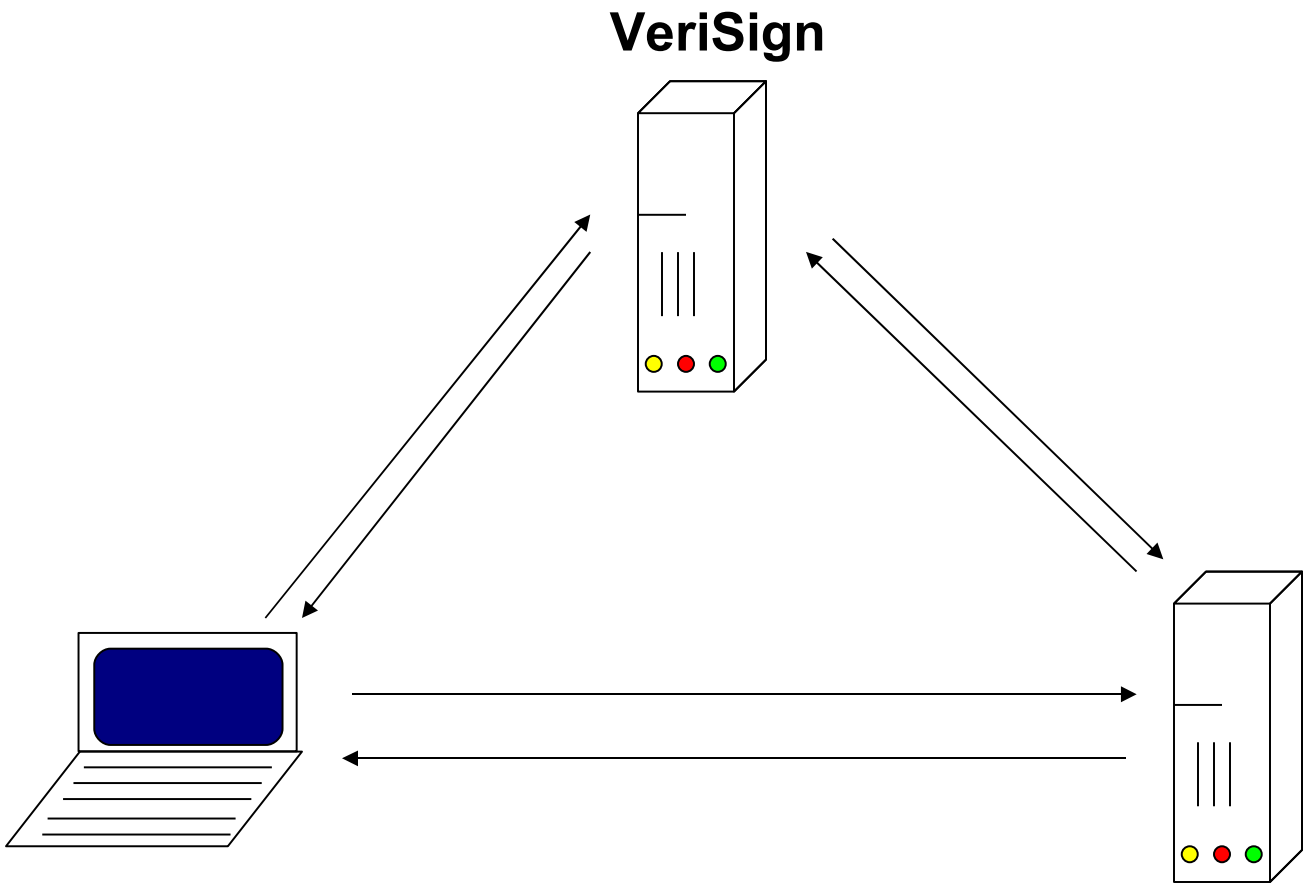
PKI-Konzept: Zertifikate

- PKI: Public Key Infrastructure
- Zertifikate werden von einer CA (Certificate Authority, es gibt mehrere davon, z. B. VeriSign Deutschland http://www.verisign.de) ausgestellt
- Kommunikationspartner können sich dadurch gegenseitig ausweisen in Form von Überprüfung und Bestätigung
- Ferner werden u. a. mittels Zertifikate die Transferdaten ver- und entschlüsselt > hoher Grad an Vertraulichkeit & Nachrichtenintegrität
- Standardformat für Zertifikate: X.509v3
- Auch in Hardware zu finden: z. B. Smart Card

Praxis: HTTPS auf einem Server

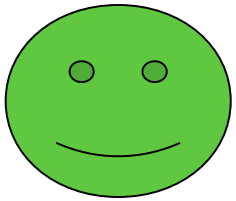


Praxis: HTTPS auf einem Server



Ich bedanke mich

für Ihre Aufmerksamkeit !!!



... noch Fragen...?