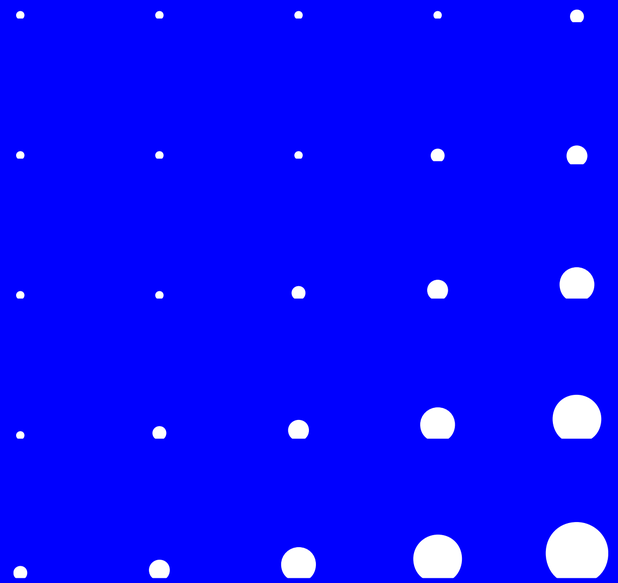
Technische Hochschule
mannheim

HTTP – Secure: HTTPS



Der Internet-Protokollstapel mit HTTPS

Technische Hochschule mannheim

OSI-Schicht	TCP/IP-Schicht	Beispiel
Anwendungen (7)	Anwendungen	HTTP, UDS, FTP, SMTP, POP, Telnet, OPC UA
Darstellung (6)		
Sitzung (5)		
		SOCKS
Transport (4)	Transport	TCP, UDP, SCTP
Vermittlung (3)	Internet	IP (IPv4, IPv6), ICMP (über IP)
Sicherung (2)	Netzzugang	Ethernet, Token Bus, Token Ring, FDDI, IPoAC
Bitübertragung (1)		

Zwischen Anwendungs- und Transportschicht wird ein weiteres Protokoll angewendet: SSL bzw. TLS

Was ist HTTPS?

Technische Hochschule mannheim

- HyperText Transfer Protocol Secure ist ein Kommunikationsprotokoll im World Wide Web, um Daten abhörsicher zu übertragen.
- Technisch definiert es als URI-Schema eine zusätzliche Schicht zwischen HTTP und TCP.
- HTTPS wurde von Netscape entwickelt und zusammen mit SSL 1.0 erstmals 1994 mit deren Browser veröffentlicht.
- Das HTTPS-Protokoll wird zur Verschlüsselung und zur Authentifizierung der Kommunikation zwischen Webserver und Browser im World Wide Web verwendet.
- Ohne eine solche Verschlüsselung sind Web-Daten für jeden als Klartext lesbar.
- Mittlerweile hat HTTPS das HTTP auf den meisten gängigen Webseiten abgelöst.

Was ist HTTPS?

Technische Hochschule mannheim

- Mit der zunehmenden Verbreitung von Funkverbindungen,
  die etwa an WLAN-Hotspots häufig unverschlüsselt ablaufen,
  nimmt die Bedeutung von HTTPS immer weiter zu,
  da damit die Inhalte unabhängig vom Netz verschlüsselt werden.
- Es stellt dabei das einzige Verschlüsselungsverfahren dar,
  das ohne gesonderte Softwareinstallation auf allen internet-fähigen Computern unterstützt wird.
- Die Authentifizierung dient dazu, dass sich jede Seite der Verbindung vor dem Aufbau der Kommunikation der Identität des Verbindungspartners vergewissern kann.
  - Dies ist ein Bedarf, der durch die steigende Zahl von Phishing-Angriffen ebenfalls wächst.

Was ist SSL/TLS?

Technische Hochschule mannheim

- Transport Layer Security (TLS), besser bekannt unter der Vorgängerbezeichnung Secure Sockets Layer (SSL), ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.
- Seit Version 3.0 wird das SSL-Protokoll unter dem neuen Namen TLS weiterentwickelt und standardisiert, wobei Version 1.0 von TLS der Version 3.1 von SSL entspricht.
- Bekannte Implementierungen des Protokolls sind OpenSSL und GnuTLS.

Was ist SSL/TLS?

Technische Hochschule mannheim

- TLS ist ohne eine zertifikatsbasierte Authentifizierung anfällig für Man-in-the-Middle-Angriffe:
  - Ist der Man-in-the-Middle vor der Übergabe des Schlüssels aktiv, kann er beiden Seiten seine Schlüssel vorgaukeln und so den gesamten Datenverkehr im Klartext aufzeichnen und unbemerkt manipulieren.
- Wegen der mangelnden Vertrauenswürdigkeit einiger Zertifizierungsstellen wird seit Anfang 2010 die Sicherheit von TLS grundsätzlich angezweifelt.

Was sind X.509 Zertifikate?

Technische Hochschule mannheim

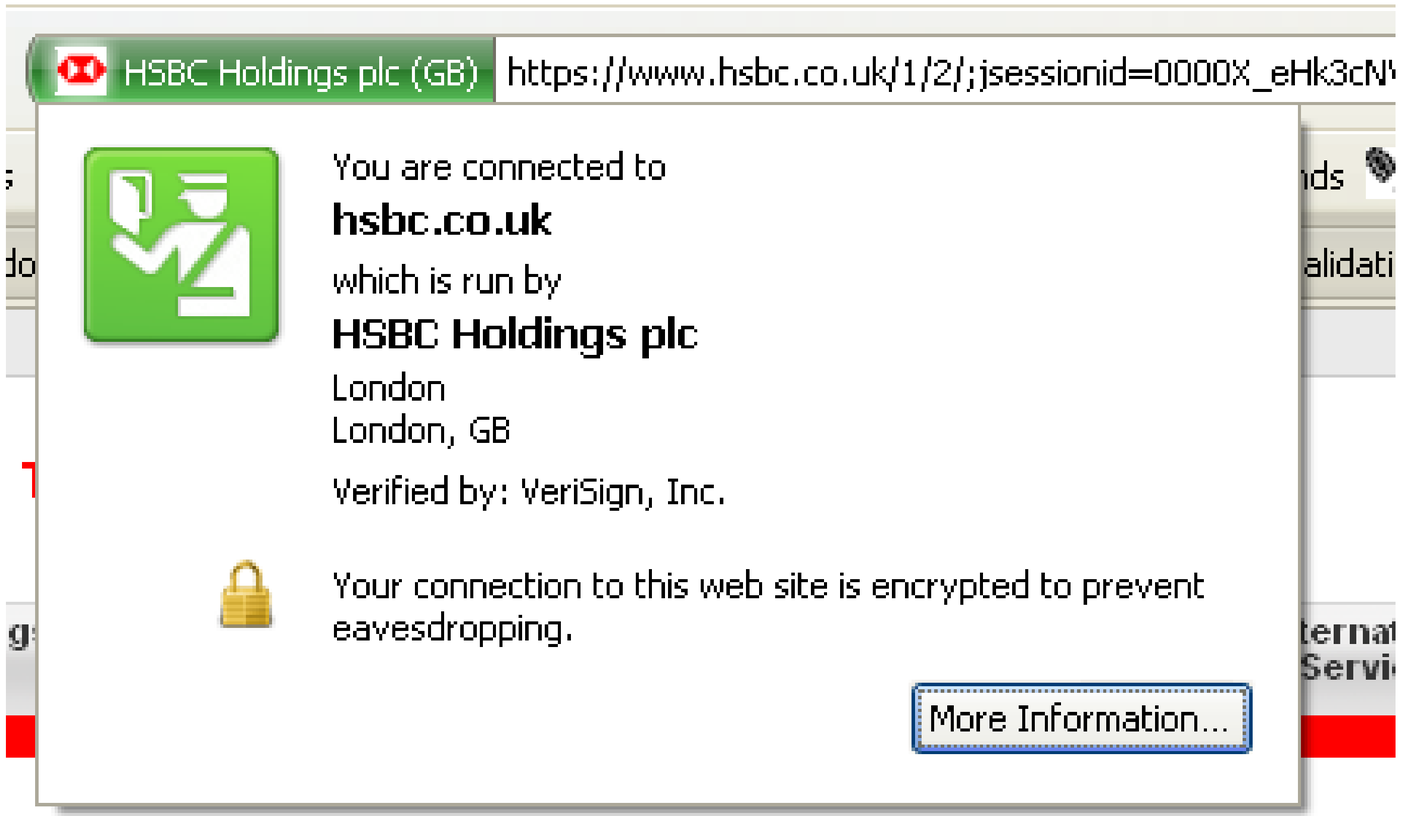
- X.509 ist ein ITU-T-Standard für eine Public-Key-Infrastruktur zum Erstellen digitaler Zertifikate.
- Die Entwicklung von X.509 setzt ein striktes hierarchisches System von vertrauenswürdigen Zertifizierungsstellen (certificate authority, CA) voraus, die Zertifikate erteilen können.
- Dieses Prinzip steht im Gegensatz zum Web-of-Trust-Modell, welches einen Graphen und nicht nur einen Baum darstellt und bei dem jeder ein Zertifikat „unterschreiben“ und damit seine Echtheit beglaubigen kann (vgl. OpenPGP).
- Ein von einer Zertifizierungsstelle ausgestelltes digitales Zertifikat wird im X.509-System immer an einen „Distinguished Name“ oder einen „Alternative Name“ wie eine E-Mail-Adresse oder einen DNS-Eintrag gebunden.

Was sind X.509 Zertifikate?

Technische Hochschule mannheim

- Nahezu alle Webbrowser beinhalten eine vorkonfigurierte Liste vertrauenswürdiger Zertifizierungsstellen, deren ausgestellten SSL-Zertifikaten der Browser vertraut.
- X.509 beinhaltet außerdem einen Standard, mittels dessen Zertifikate seitens der Zertifizierungsstelle wieder ungültig gemacht werden können, wenn deren Sicherheit nicht mehr gegeben ist, z. B. nach dem öffentlichen Bekanntwerden des Private Keys für das Signieren von E-Mails.
- Die Zertifizierungsstelle kann hierfür ungültige Zertifikate in Zertifikatsperrlisten führen.

Ein X.509 Zertifikat von VeriSign

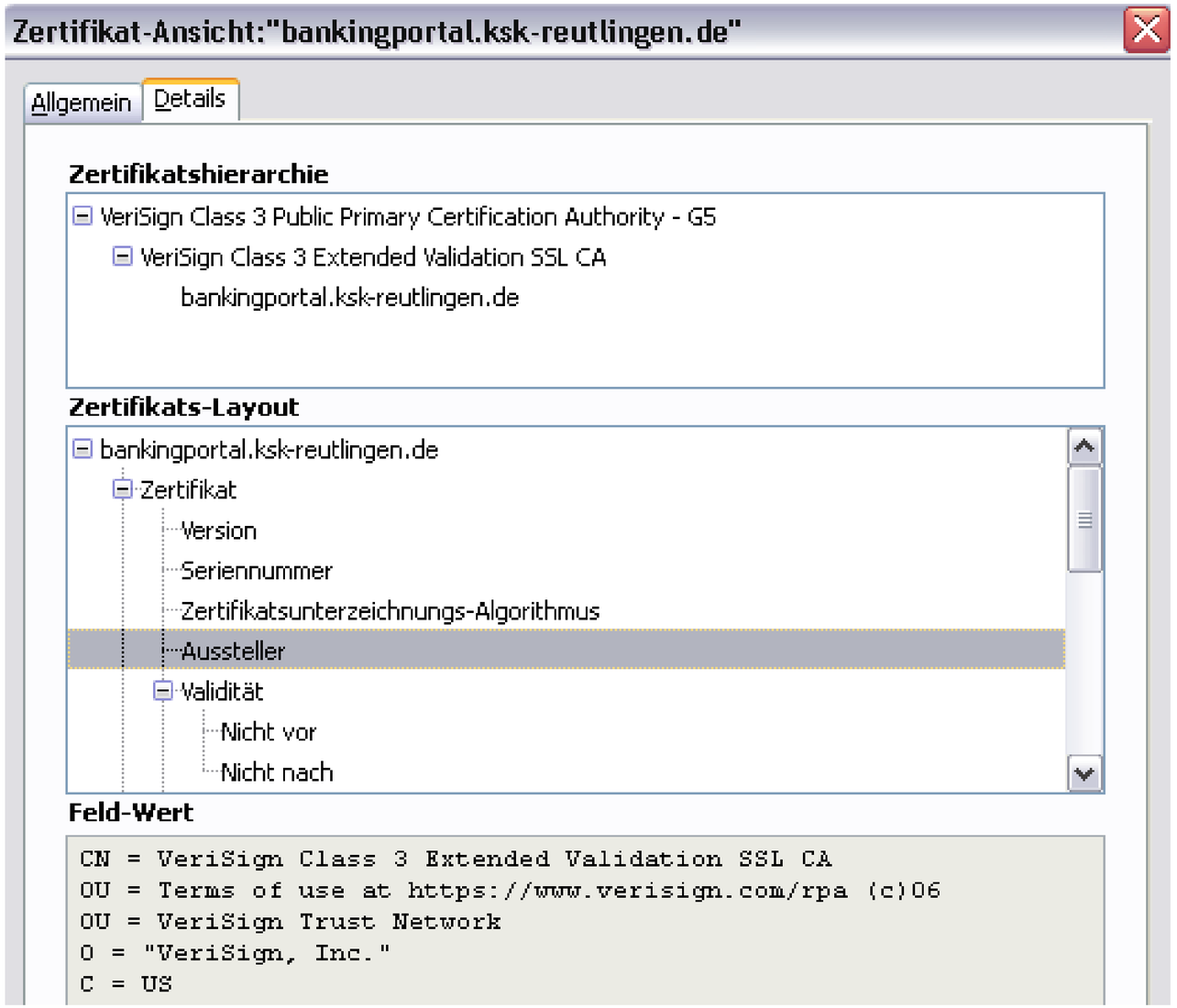


Zertifikat der ksk-reutlingen.de

Technische Hochschule mannheim

Zertifikat der ksk-reutlingen.de

Technische Hochschule mannheim



Zertifikat von frank-dopatka.de

Technische Hochschule mannheim