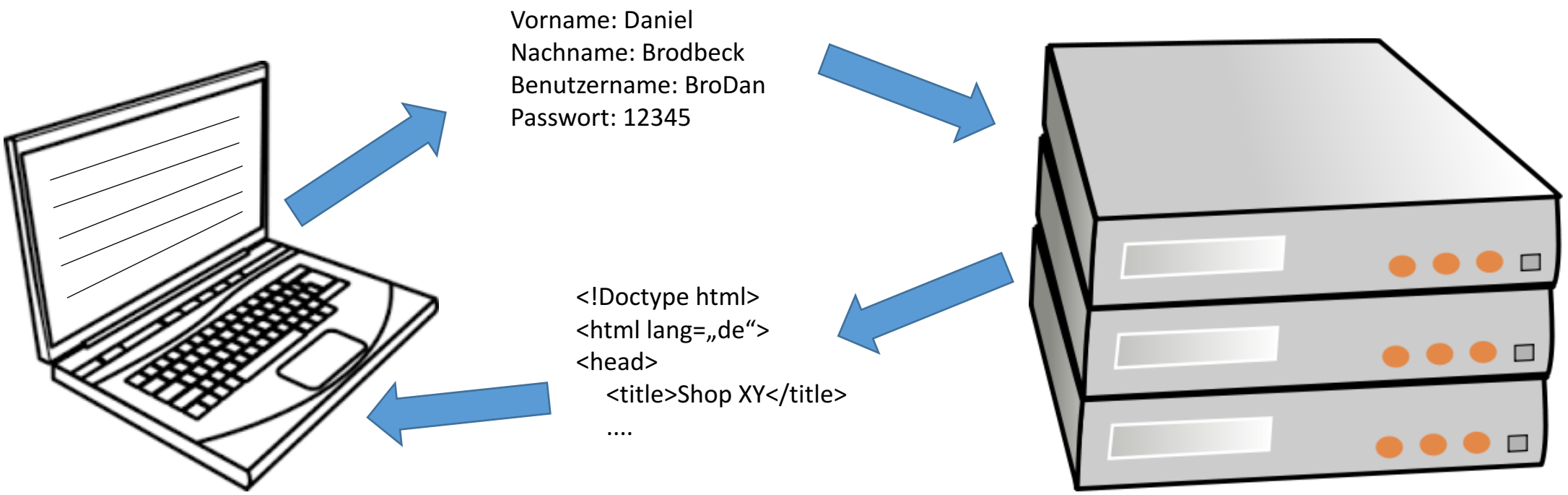
HTTPS / SSL / TLS

Sicher Datenübertragung zwischen Client und Server

Datenübertragung mit HTTP



Bei der Datenübertragung über HTTP (POST / GET) werden alle Daten unverschlüsselt übertragen.
Mit einem Sniffer können die Informationen mitgelesen, verändert und missbräuchlich verwendet werden.

Schutzziele der Informationssicherheit

Integrität der Daten

Die Integrität von Daten setzt voraus, dass diese nur von Berechtigten in beabsichtigter Weise verändert und nicht unzulässig modifiziert werden können. Bei der Integrität von Nachrichten kann davon ausgegangen werden, dass der Nachrichteninhalt auf der Sende- und Empfangsseite vollkommen identisch ist.

Mit HTTP ist die Integrität der Informationen nicht gegeben.

Schutzziele der Informationssicherheit

Vertraulichkeit

Unter Vertraulichkeit versteht man, dass Informationen nur für Befugte zugänglich sind.

So kann beispielsweise nur der Sender und Empfänger eine Nachricht im Klartext lesen. Um eine Vertraulichkeit zu gewährleisten, müssen die im System gespeicherten oder in den Kommunikationseinrichtungen übertragenen Informationen durch Verschlüsselung vor unberechtigtem Zugriff geschützt werden.

Mit HTTP ist die Vertraulichkeit der Informationen nicht gegeben.

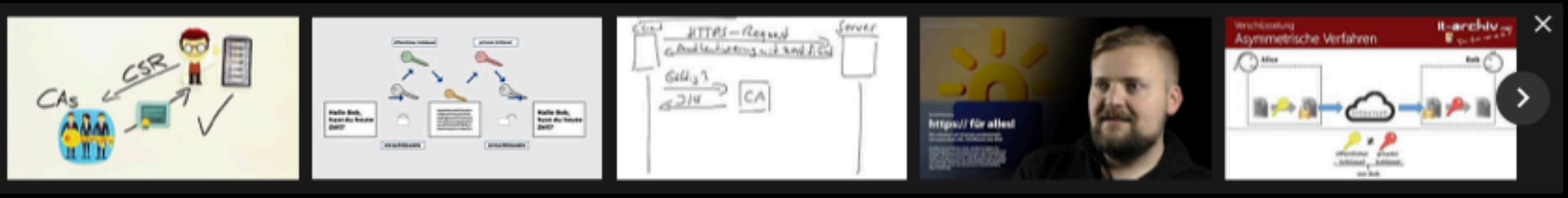
Schutzziele der Informationssicherheit

Authentizität

Durch die Authentizität muss sichergestellt werden, dass die Herkunft von Informationen zweifelsfrei nachgewiesen werden kann.

Mit HTTP ist die Authentizität der Informationen nicht gegeben.

Sichere Websiten (mit SSL), kurz erklärt.

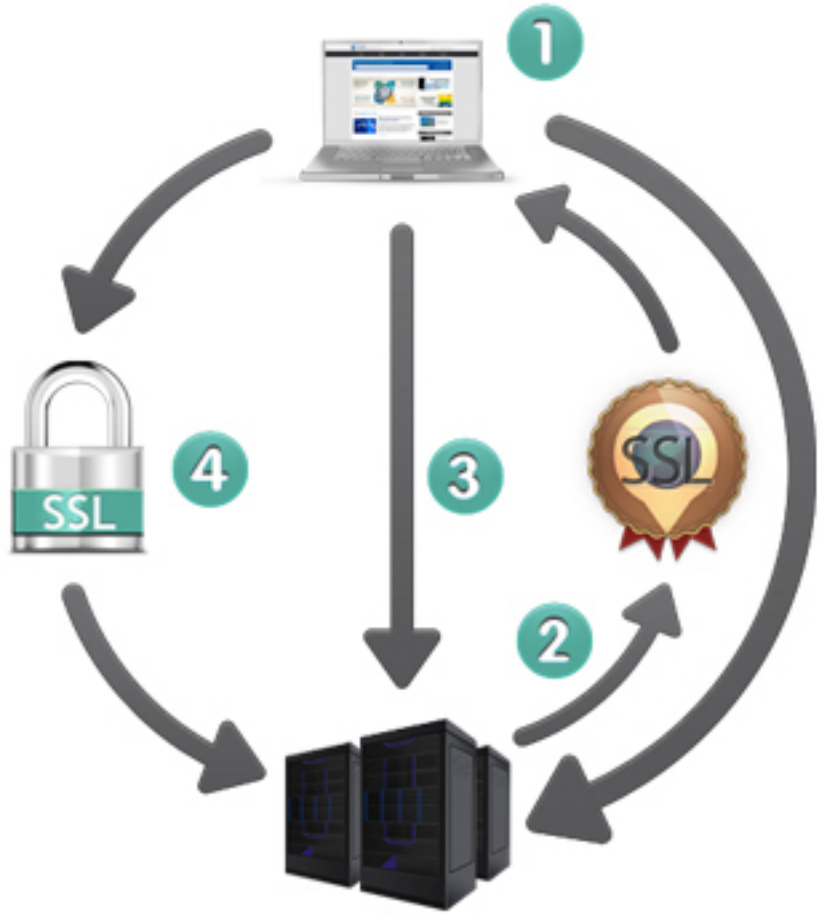


0:14 / 3:09

Verschlüsselungsverfahren (symmetrisch, asymmetrisch, hybrid) - it-archiv.net

1:05 / 5:15

Ablauf einer SSL/TLS Verbindung



1. Anfrage zum Aufbau einer SSL/TLS gesicherten Verbindung
2. Anzeigen des Zertifikates
   In diesem Schritt werden folgende Informationen des Zertifikates überprüft:
   1. Gültigkeit
   2. Signatur durch eine vertrauenswürdige Dritt-Instanz
3. Übertragung eines eindeutigen Session-Schlüssels (mit dem öffentlichen Schlüssel des Servers verschlüsselt)
4. Entschlüsselung des Session-Schlüssels durch den Server mit Hilfe des privaten Schlüssels
   Aufbau der sicheren Verbindung

Arten von SSL/TLS-Zertifikaten

- **Domain SSL-Zertifikat**
  (die Domain des Antragsstellers wird geprüft)
- **Organisation SSL-Zertifikat**
  (die Domain und der Handelsregistereintrag des Antragstellers werden geprüft)
- **Extended Validation SSL-Zertifikat**
  (die Domain, Handelsregistereintrag und weitere Angaben zum Antragssteller wie z.B. der Unternehmenssitz werden geprüft)
  Extended validierte Webseiten werden deutlich sichtbar durch eine grüne Adresszeile im Browserfenster angezeigt.

Beantragen eines SSL/TLS-Zertifikates

Ein SSL/TLS Zertifikat kann bei unterschiedlichsten Zertifizierungsstellen (**CA** *certification authority*) beantragt werden.

Für die Zertifizierung benötigt man einen serverseitigen Schlüssel für die asynchrone Verschlüsselung (privat/öffentlich) und eine Zertifizierungsanforderung (**CSR** *cerificate signing request*). Schlüssel und Zertifizierungsanforderung werden auf dem Webserver erstellt und an die Zertifizierungsstelle übermittelt.

Die Preise unterscheiden sich nach Art des Zertifikates und der Zertifizierungsstelle.

Let‘s Encrypt

Im Jahr 2015 wurde durch verschiedene grosse Player aus dem Internet- und Netzwerkbereich (Google / Cisco / Mozilla Foundation) Let‘s Encrypt ins Leben gerufen.

Let‘s Encrypt ist eine Zertifizierungsstelle mit dem Ziel, einfach kostenlose Domain SSL/TLS-Zertifikate zur Verfügung zu stellen um das Internet sicherer zu machen.

https://letsencrypt.org/

Self Signed SSL/TLS-Zertifikate

Für Testzwecke kann auf der eigenen Entwicklungsumgebung ein Self Signed SSL-Zertifikat erstellt und installiert werden. Wie der Name bereits sagt, wird dieses Zertifikat von keiner Zertifizierungsstelle beglaubigt.

Eine Anleitung dazu finden Sie auf:
BSCW > M133 > Zertifikat_Apache

Weiterführende Informationen

- Informationen zu HTTPS
  https://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure
- Informationen zu SSL/TLS
  https://de.wikipedia.org/wiki/Transport_Layer_Security
- CSR für Apache erstellen
  https://search.thawte.de/support/ssl-digital-certificates/index?page=content&actp=CROSSLINK&id=SO2614