**Zertifikate und Verschlüsselung**

* Verschlüsselung – damit niemand fremder mitlesen kann.
  + **Leitungsverschlüsselung:**  
    Rechner gibt nur verschlüsselte Daten an den nächsten Rechner, welcher die Daten entschlüsselt wieder verschlüsselt weitergibt
  + **Ende-zu-Ende-Verschlüsselung:**Rechner schickt Nachricht verschlüsselt weg, die Nachricht wird dann erst beim geforderten Empfänger entschlüsselt
* Zertifikate ausstellen erfolgt durch offizielle Zertifizierungsstelle
* Bestätigt Authentizität und Integrität d. kryptographische Verfahren
* Website/Anbieter ist vertrauenswürdig

**Verschlüsselung bei der Datenübertragung mit Zertifikaten im öffentl. Netzwerk (OSI-Layer 4)**

– seit DSGVO Pflicht (f. Unternehmen, Organisationen)

– https:// (hyper text transfer protocoll security)

- für Websites – Verschlüsslung der Übertragung

- TLS (neu) Transport Layer Security

- SSL (veraltet)= Secure Socket Layer - bei LetsEncrypt (gratis) kann man Zertifikate anfertigen lassen

TLS E-Mail

POP3s Port 110

IMAPs Port 143

SMTPs Port 25 oder 587

SSL E-Mail

POP3s Port 995

IMAPs Port 993

SMTPs Port 25

**SSH (Secure Shell)**

Zur Datenübertragung zb. Vom Entwicklungsrechner zum Webserver oder von Cl. Zu Cl.

OSI Layer 5-7

Port 22

Nutzt meist AES Advanced Encryption Standard (bis zu 256 Bit Verschlüsselung (Blockgröße 128 Bit))