de.KCD summer school

Day 4

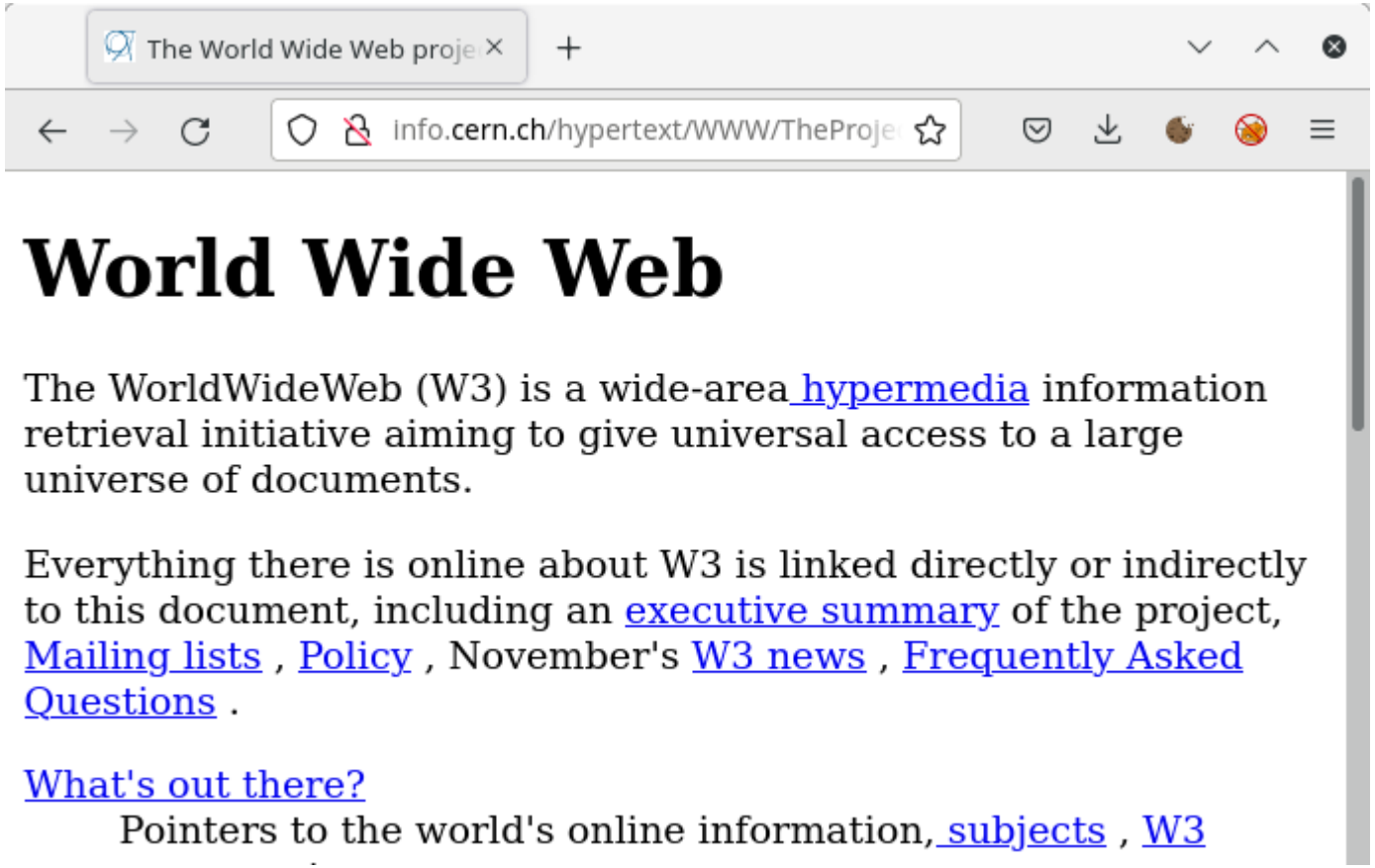
Technical introduction

Berlin Institute of Health
Charité - Universitätsmedizin Berlin

Schedule

Image by vectorjuice on Freepik

- Internet security
- Certificates
- Certificate architecture

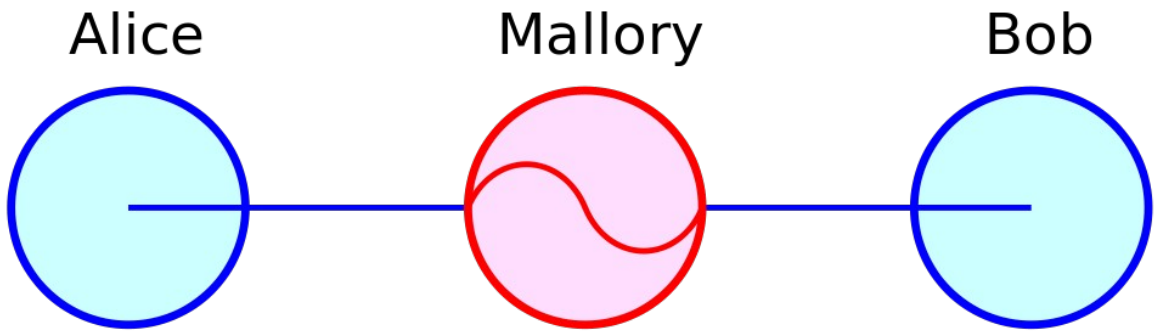


Quelle:
http://info.cern.ch/hypertext/WWW/TheProject.html

Internet security

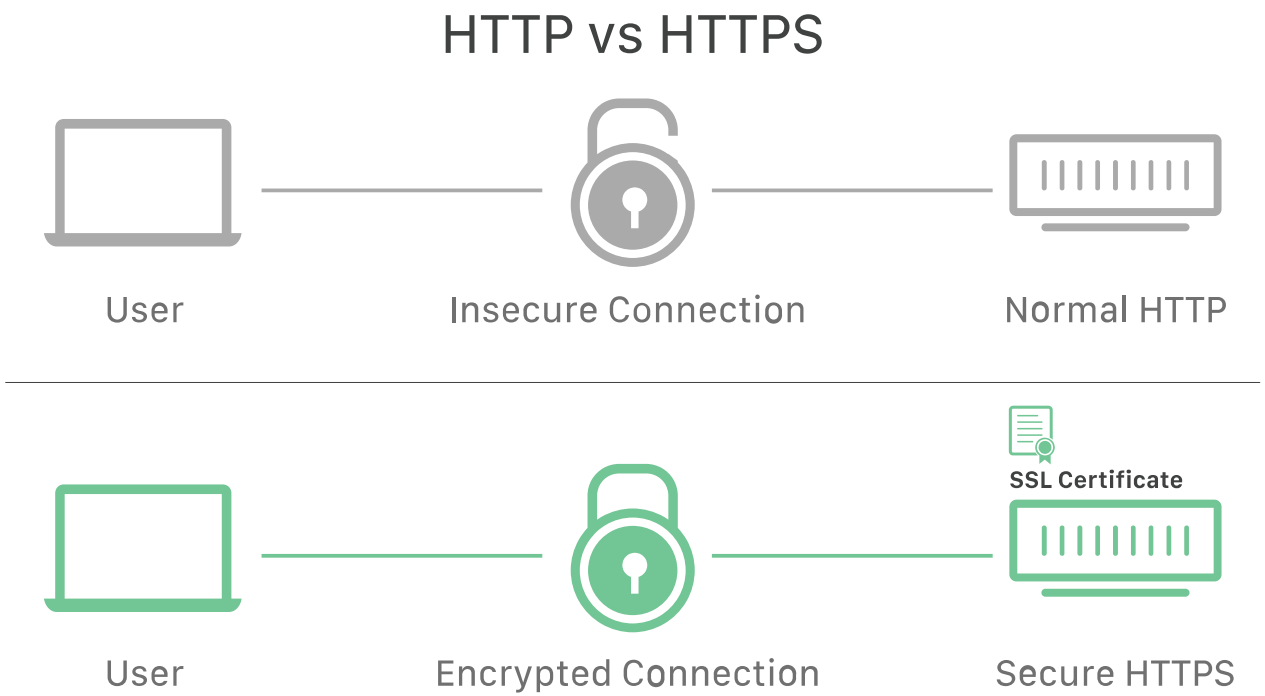
- Online services are reachable over the internet
- Default connection protocol is http
- Data is transferred in plain text

Man in the middle attack



Quelle: https://en.wikipedia.org/wiki/Man-in-the-middle_attack

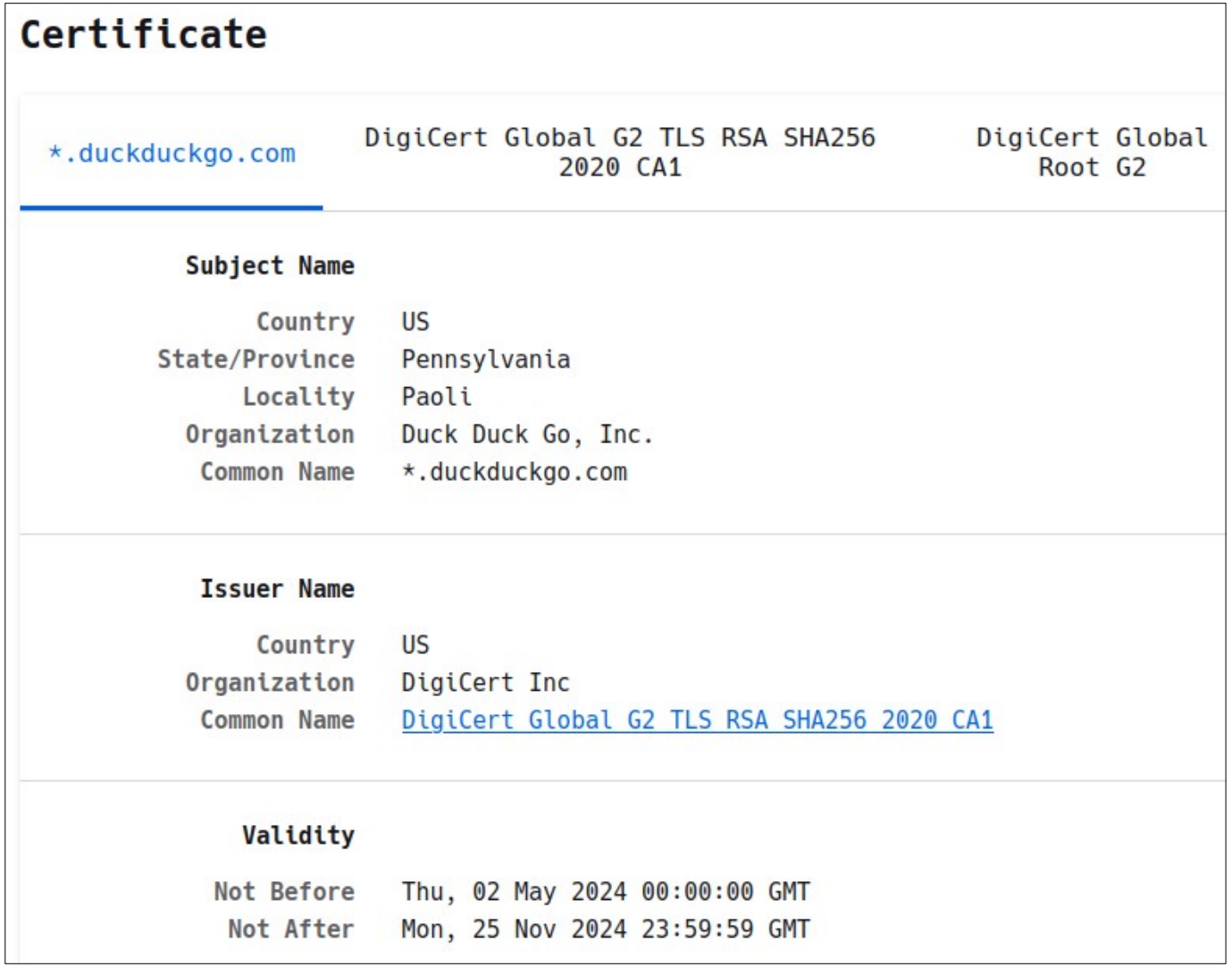
- An attacker can intersect the plain text communication
- The data can be read and changed by the attacker



Quelle: https://www.cloudflare.com/de-de/ssl/

Https with TLS

- Connection between server and browser is encrypted
- Received data must be encrypted before they can be read
- The encryption is done via x509 certificates



Digital certificates

- The public key certificate (x509) proofs the validity of the public key
- Certificate contains:
  - Public key
  - Owners identity
  - Issuer (Certificate Authority or CA)
  - Expiring date

Certificate Authorities (CAs)

- Certificate Authorities (CAs): Trusted entities that issue digital certificates to verify online identities.
- Certificate Chain: A hierarchy of trust from end-entity certificates up to root CAs, used by browsers to authenticate identities.
- Public Key Infrastructure (PKI): Manages certificates and encryption, involving CAs, Registration Authorities, and validation mechanisms like CRLs and OCSP.