

Kryptografi og Tjenester i Internett

Gruppe 6

Kryptering

SSL -> TLS - > HTTPS

Applikasjonslaget
Transportlaget
IP/Internett
Linklaget
Fysiske lag

Secure Sockets Layer – (**https**) Kryptering for ende-til-ende Applikasjoner – f.eks. nettbank eller butikker.

VPN (IPSEC etc.) – Kobler to nettverk sammen så det fungerer som ett LAN selv om de er fysisk adskilt

WPA – WiFi Protected Access - Kryptering på trådløse nettverk, krypterer forbindelsen mellom deg og aksesspunkt/ruter.

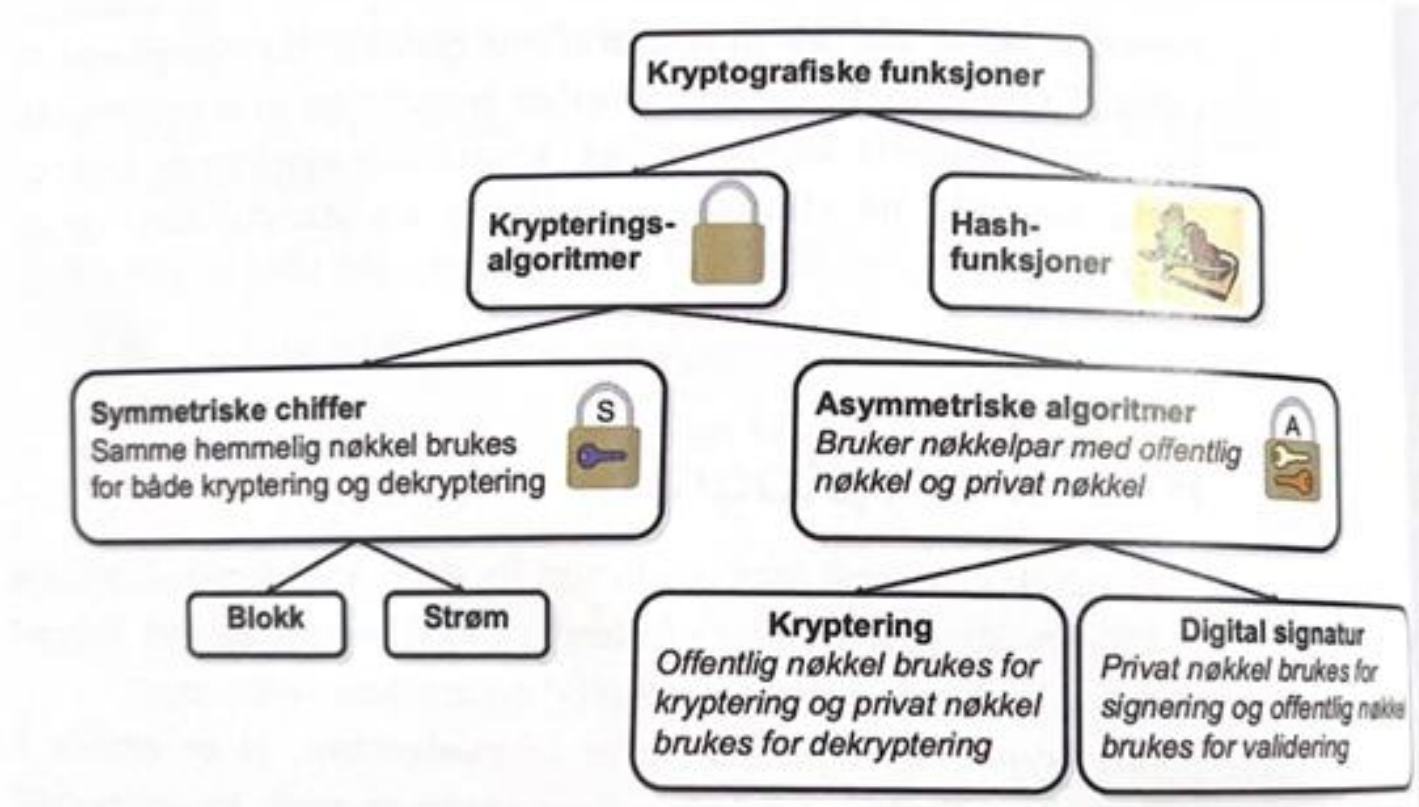
Kryptering på flere lag gjør det vanskeligere for uvedkomne å lytte til kommunikasjonen. Adressen (avsender / mottakeren) er vanskelig å kryptere, da router må vite hvor pakken skal leveres.

VPN /IPSEC -> krypterte forbindelsser gjennom åpne nett (internettet)



Kryptert forbindelse

Kryptografi = skjule betydningen av en tekst

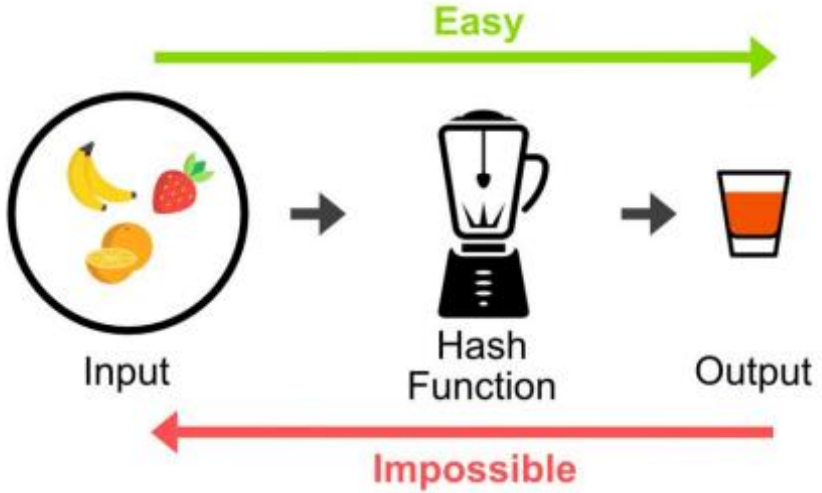


Kryptere: gjøre hemmelig

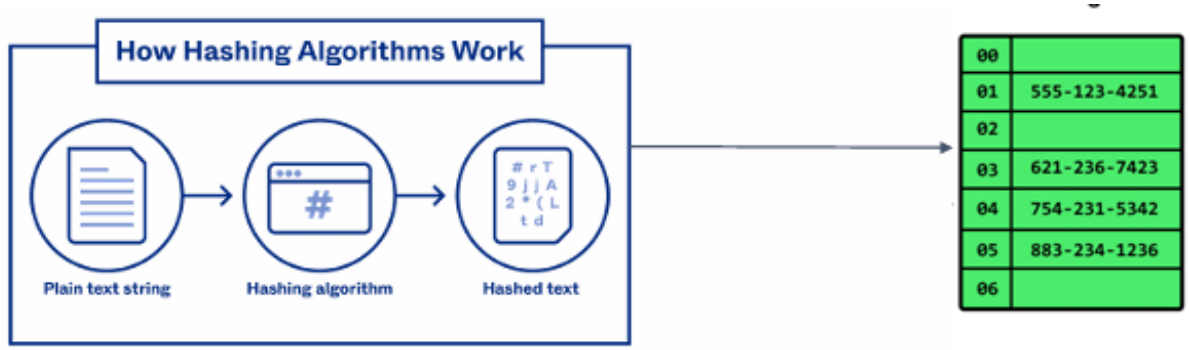
Dekryptere: Gjøre synlig

(*Chiffer = Krypteringsalgoritme*)

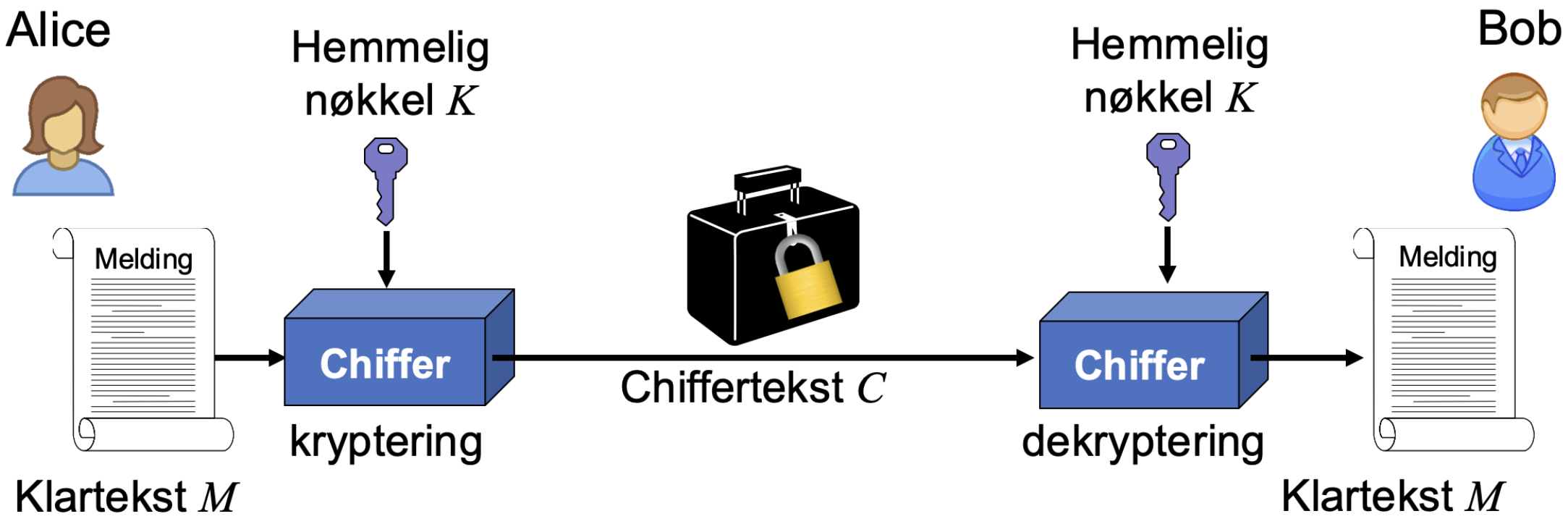
Hash-algoritmer



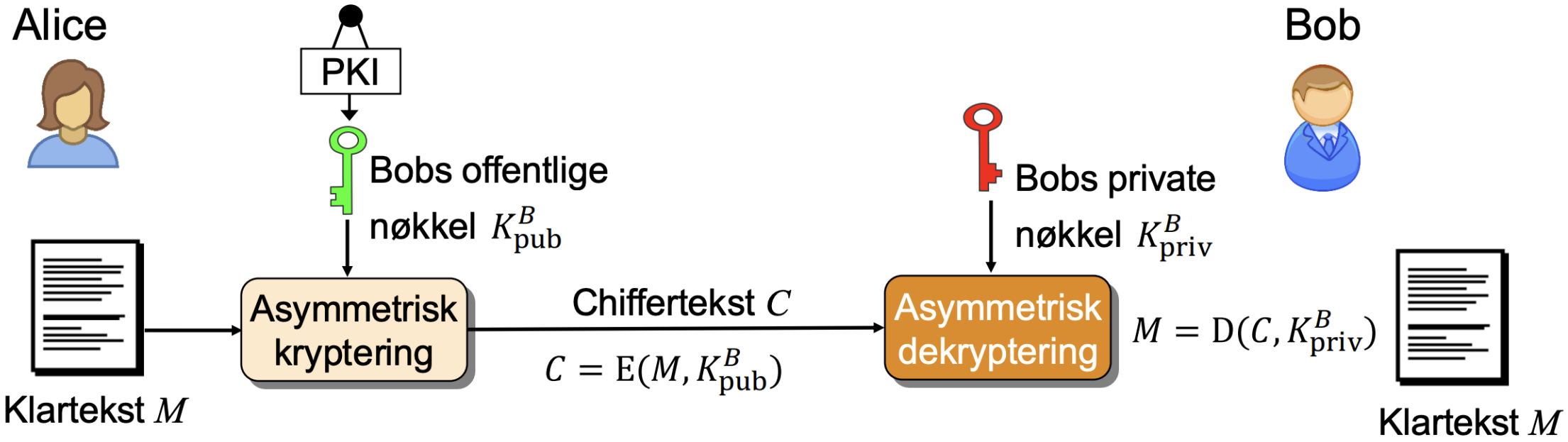
- Enveis identifikasjon – ingen nøkkel
- Konverterer data av en størrelse til en hash-verdi av fast størrelse
- Samme melding skal alltid produsere samme hash-verdi
- Brukes mye av for passordbeskyttelse
- En liten endring, endrer hele sjekksummen



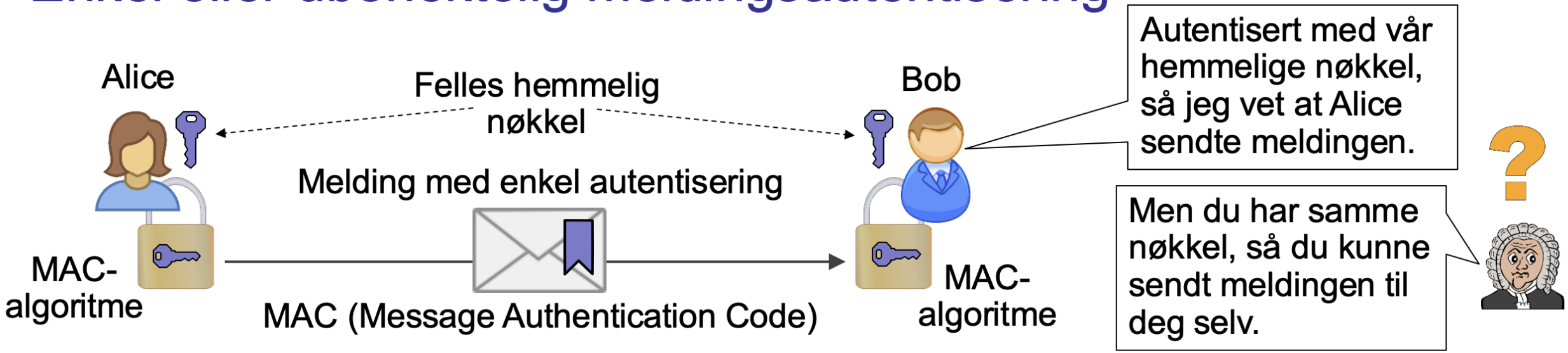
Symmetrisk kryptering

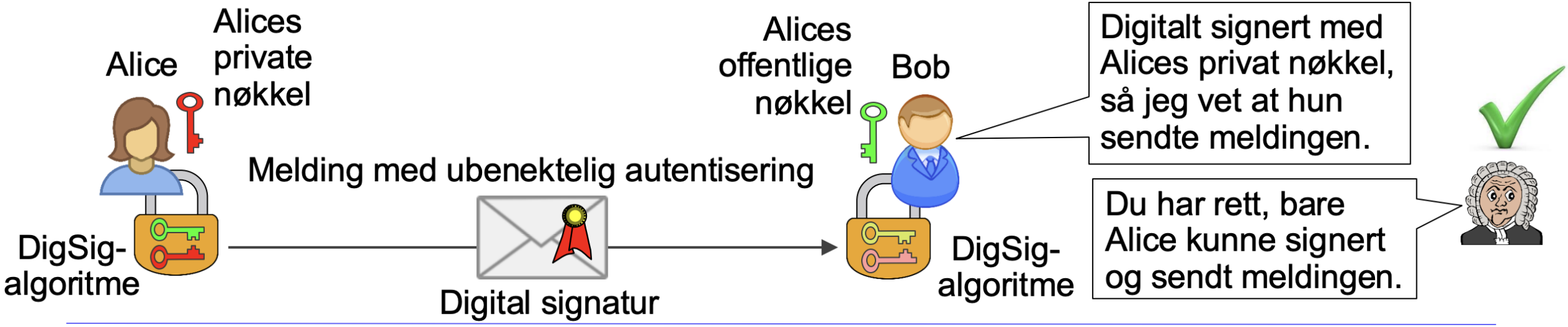


Asymmetrisk kryptering

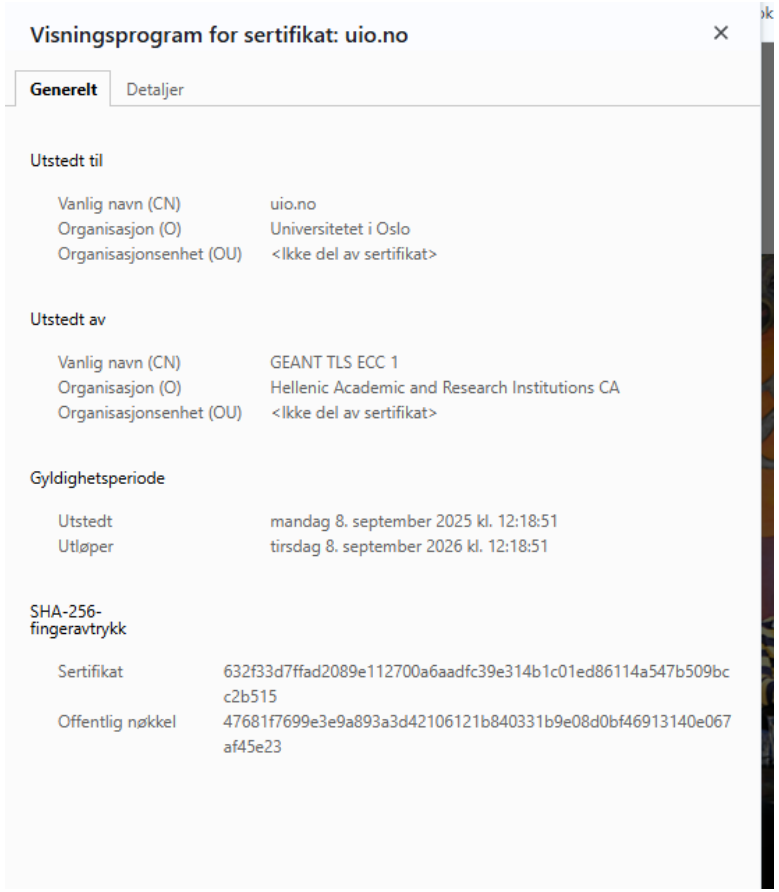


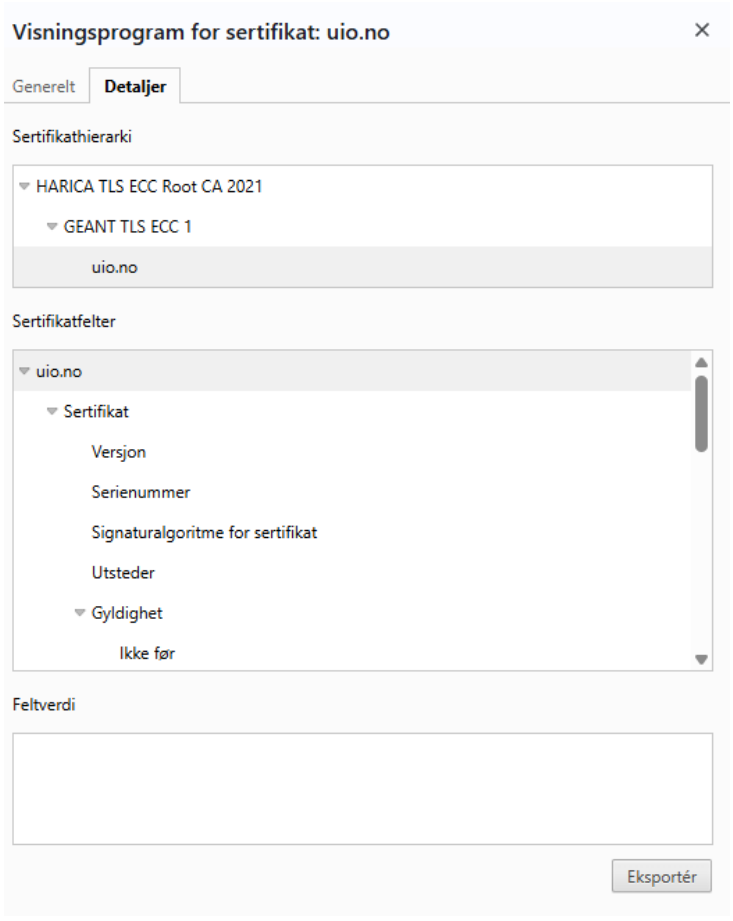
Enkel eller ubenektelig meldingsautentisering

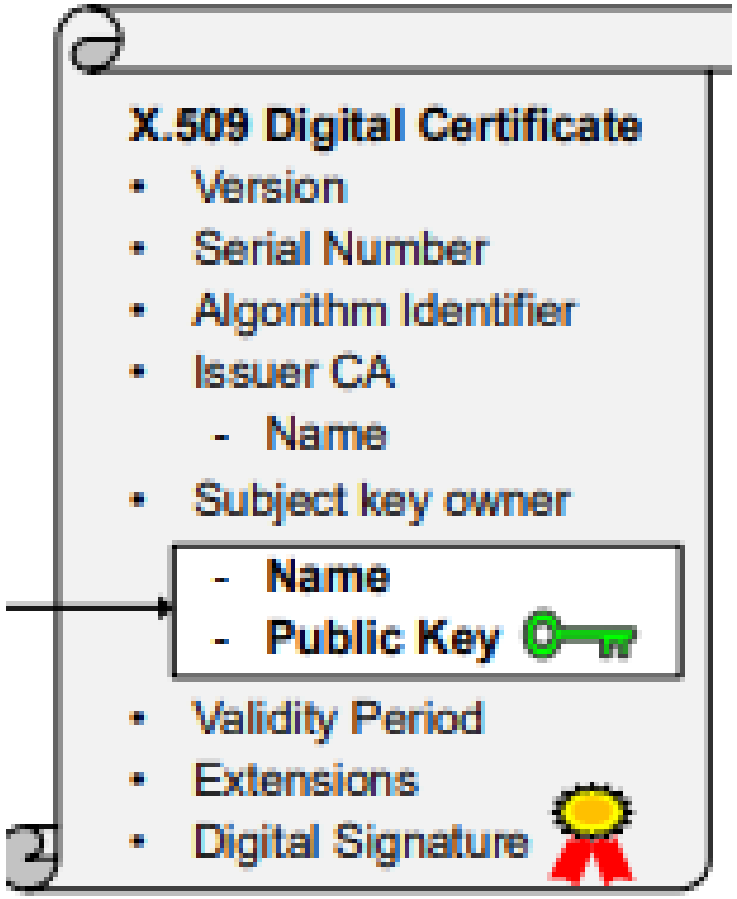




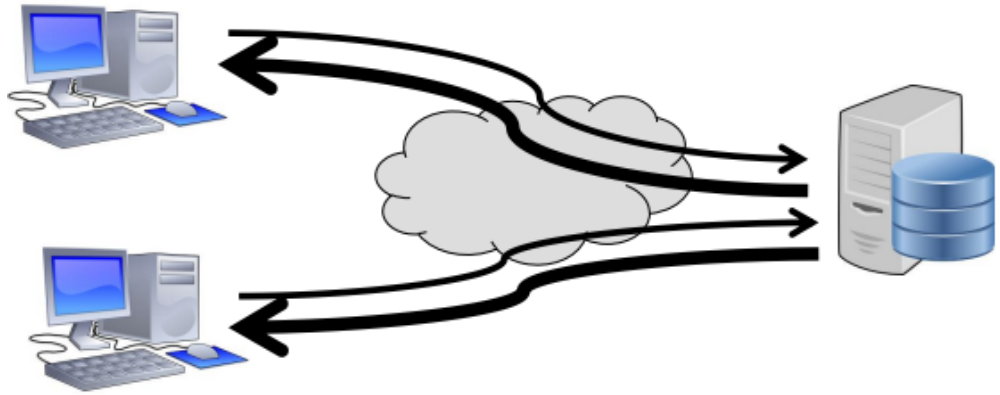
Offentlig nøkkel sertifikat







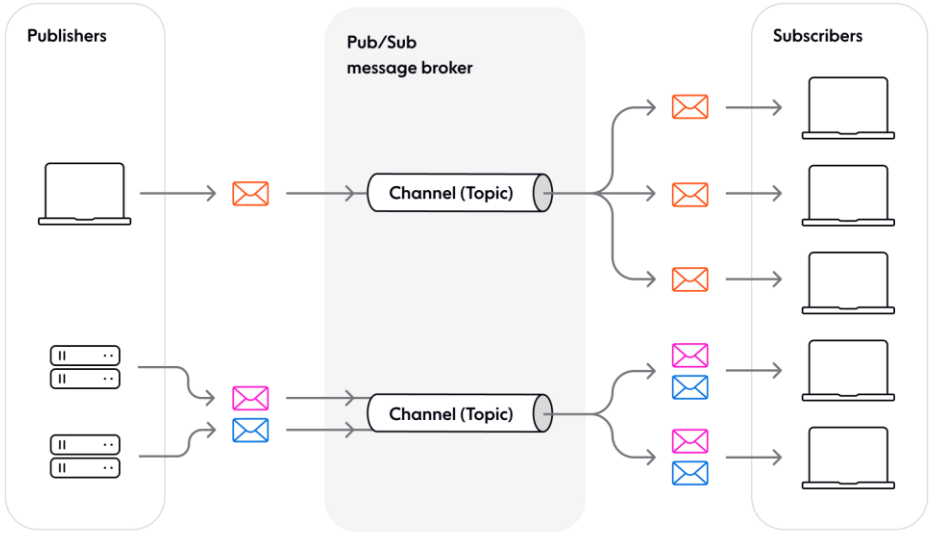
Forbindelsesstrategier

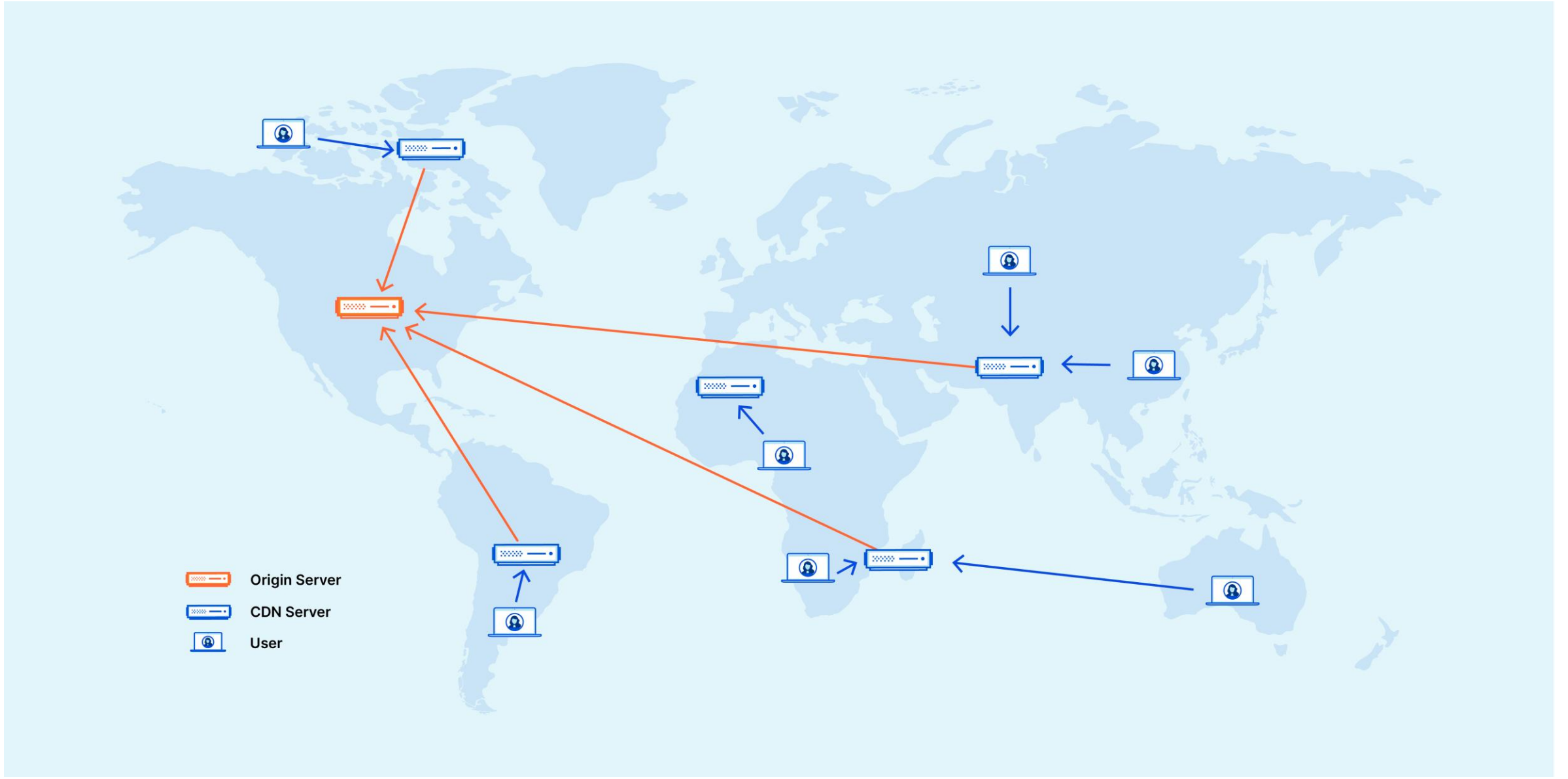


- Pull: Klienten ber om en tjeneste (vanligste metoden)
- Push: Tjeneren «dytter» en tjeneste (beskjed) til klienten

  - Krever en forbindelse fra før mellom tjener-klient

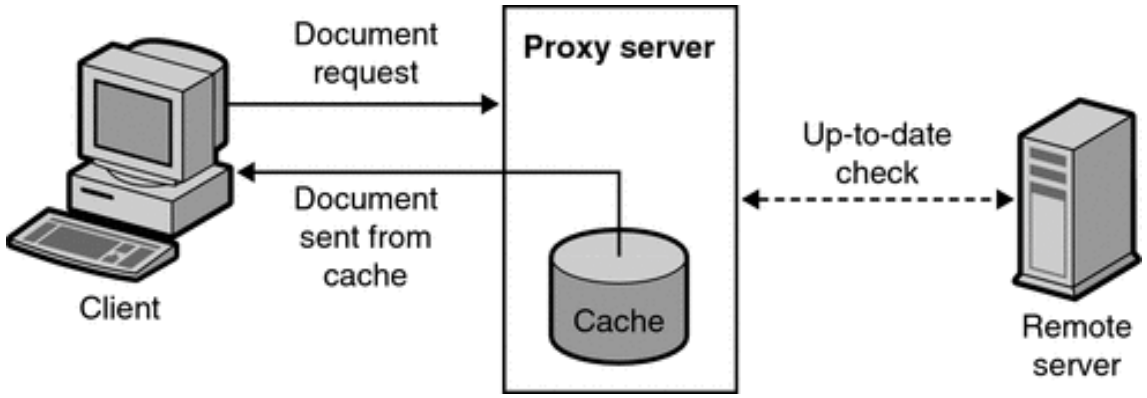
- Publish-subscribe: Push, tjeneren dytter ut beskjeder til en gruppe av abonnenter




Origin Server
CDN Server
User

Proxy – cache

- Lar servere fungere som mellomledd mellom bruker og leverandør av nettinnhold
- Forward Proxy: Står nær klienten og mellomlagrer data for klientene, slik at de ikke trenger å gå helt til kilden.
- Reverse Proxy: Står nær tjener og mellomlagrer data fra én eller flere tjenere, slik at klienten slipper å gå helt til kilden.



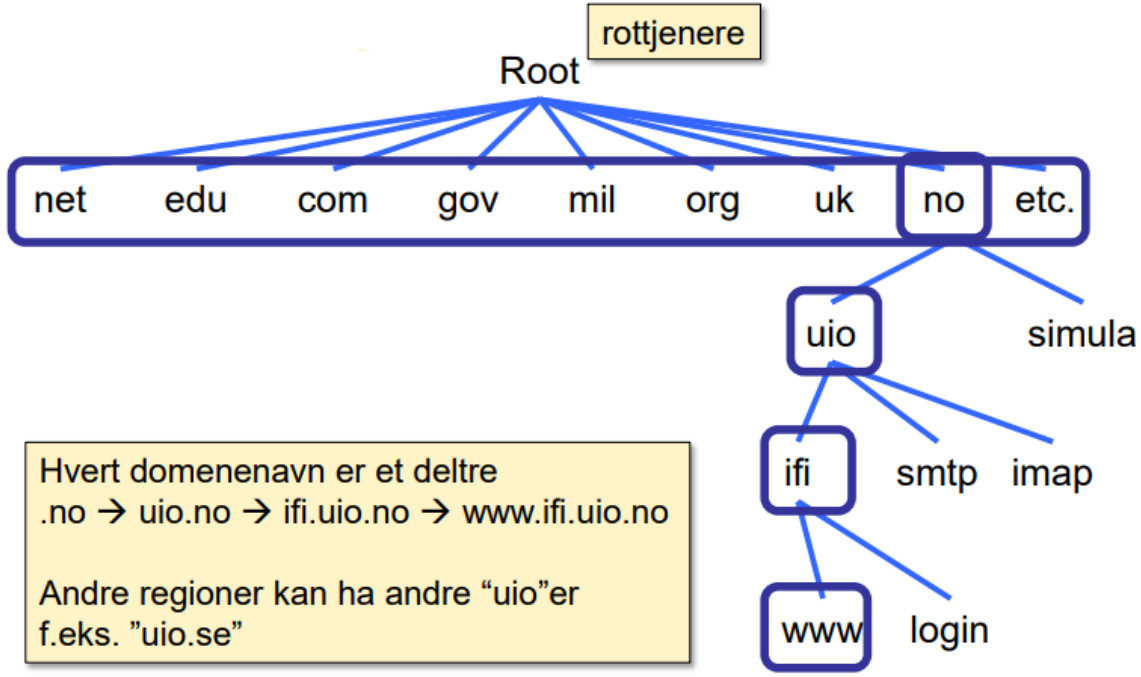
Koble til en annen maskin

- Bruk av DNS (Domain Name System)
- Nettadresser f.eks. www.google.com
- Bak navnet ligger det en IP-adresse
- Strukturen begynner fra enden.

f.eks.: .com → google.com → mail.google.com

- Deler i soner,

  der hver sone har en ansvarlig



HTTP Responsstatus

200 OK

- Forespørselen var vellykket, objektet kommer senere i meldingen

301 Moved Permanently

- Objektet har byttet plassering. Referanse til ny plassering kommer senere I meldingen.

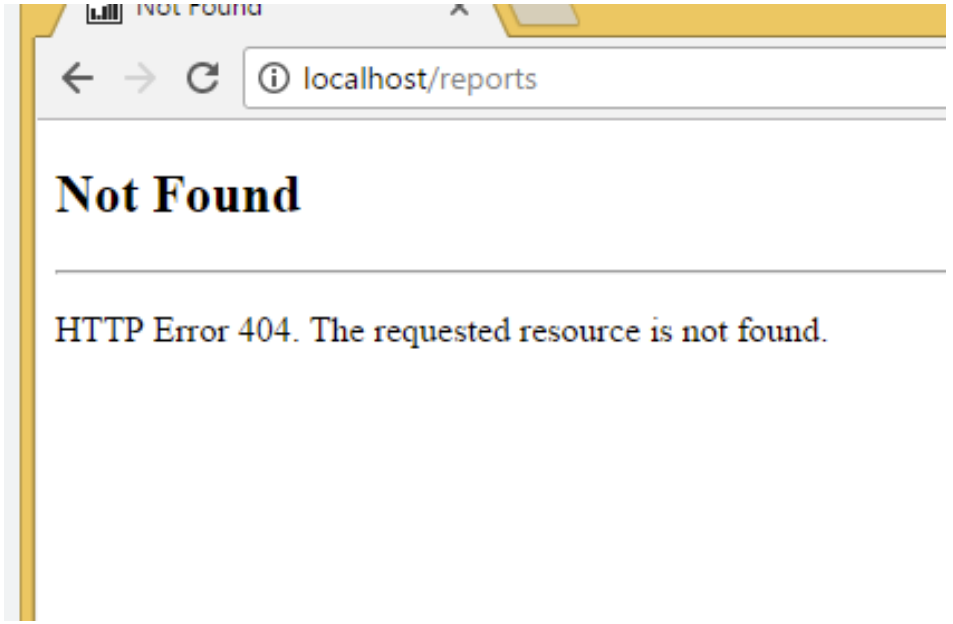
400 Bad Request

- Forespørselen var uforståelig for tjeneren

404 Not Found

- Dokumentet ble ikke funnet på tjeneren

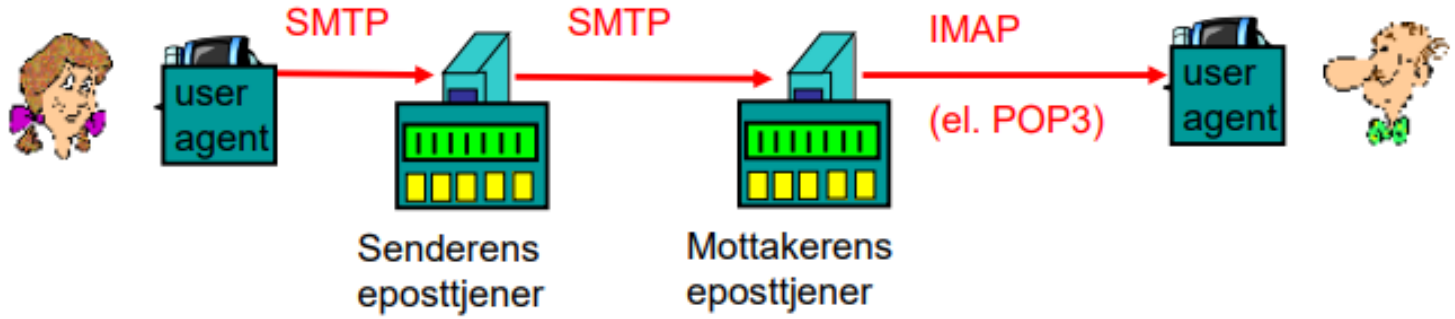
505 HTTP Version Not Supported



Epost

- Mailtjenere inneholder innkommende meldinger til brukeren og meldingskø
- SMTP – Simple Mail Transfer Protocol
  - Et sett med kommandoer for overføring
  - Klient: sender en epost
  - Tjener: Mottar

Bruker TCP



Videostreaming

- Konstant strøm av data.
- Bruker vi TCP eller UDP?
- Deler videoene i segmenter (2-10 sekunder)
- Sender de som pakker
- Klienten velger kvalitet på videoen

