Sertifikater og PKI

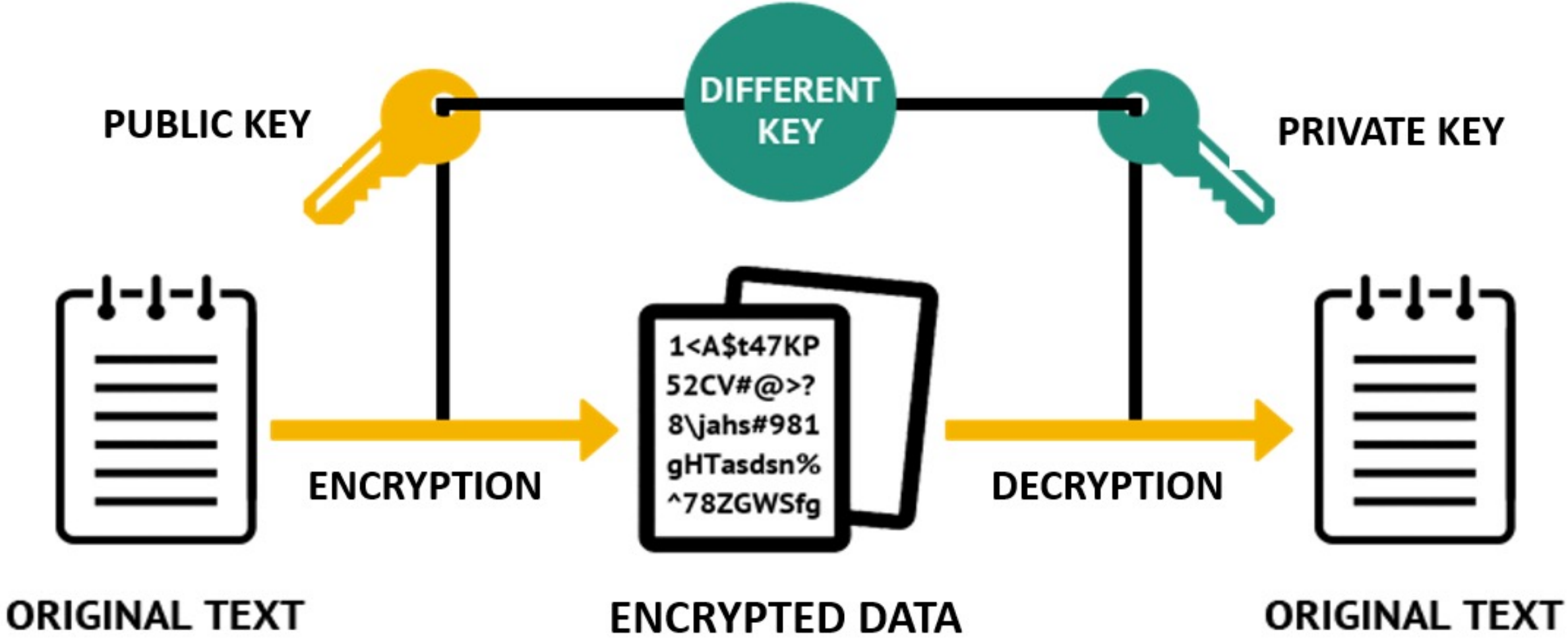
Sertifikater avmystifisert!

Agenda

- Kryptografi
- Nøkler
- Sertifikater
- SSH
- Demo SSH
- Public Key Infrastructure (PKI)

Kryptografi

- Offentlige nøkler -> kryptering
- Private nøkler -> dekryptering
- Kryptering != hashing
- Matematikk
  - Enkelt å kryptere, vanskelig å dekryptere uten nøkkel



Alice

"Call me today"

"dh12#djdi2+rg"

Using Bob's Public key to encrypt

Using Bob's Private key to decrypt

Bob

"dh12#djdi2+rg"

Call me today

Sertifikater

- Offentlige sertifikater
  - Pålitelighet i browsere
  - Root CA Utstedere (Mozilla sin sett på som golden standard)
    - https://wiki.mozilla.org/CA/Included_Certificates (52 unike utsdedere)
- Private sertifikater / Egensignerte sertifikater
- Domene navn (Common name)
- Https - SSL / TLS

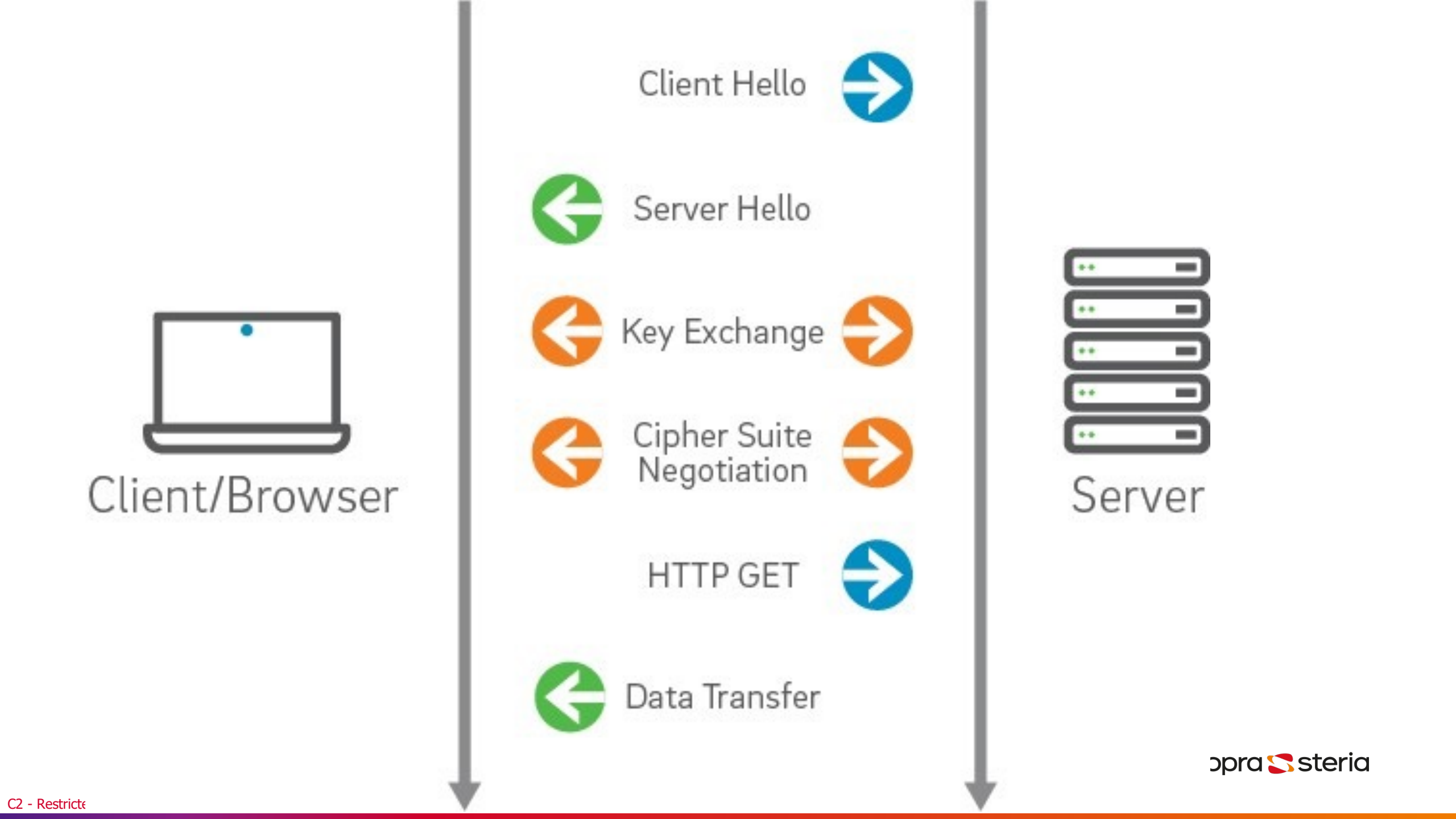
Sertifikater forskjeller

Offentlige sertifikater

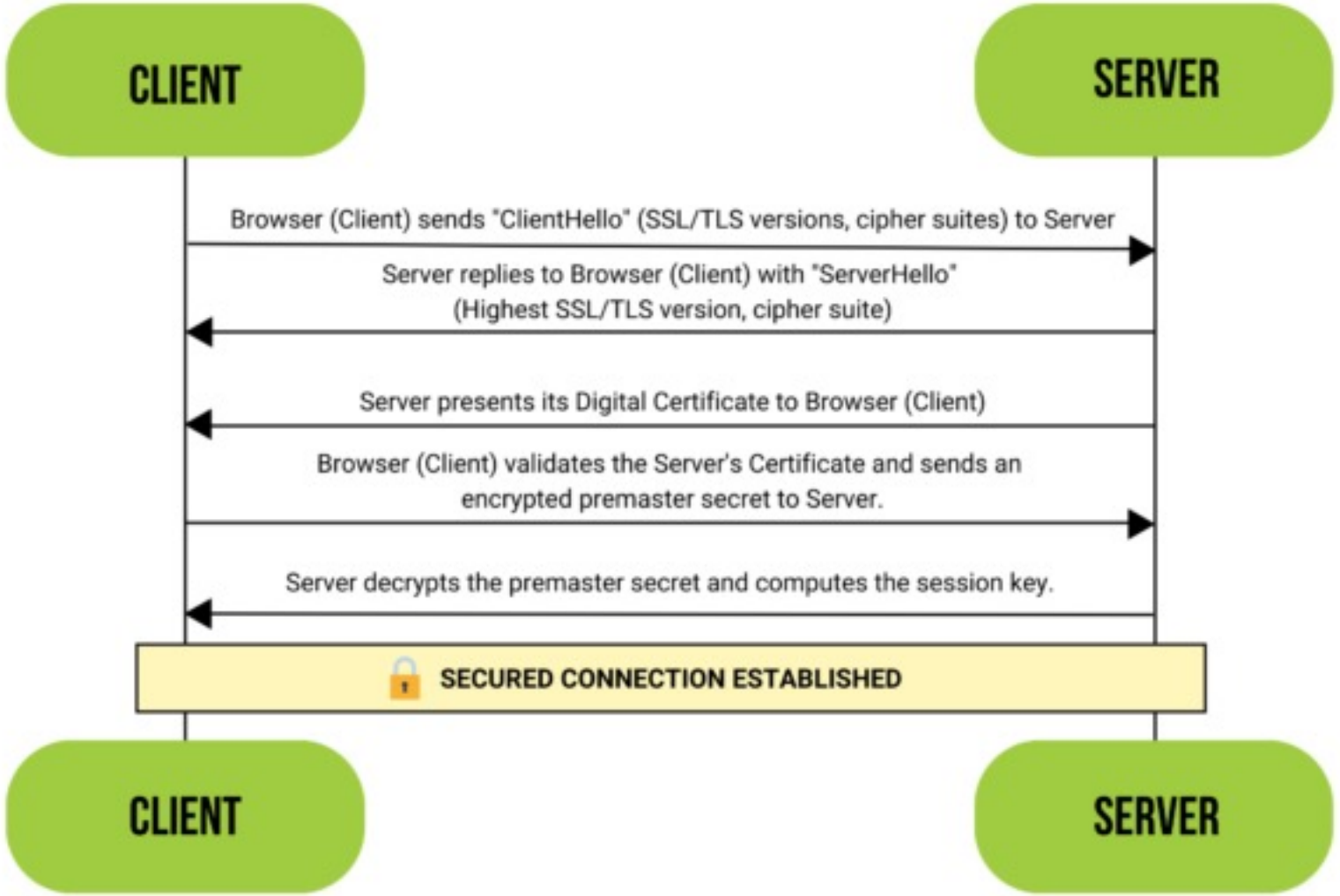
- Rotservere?
- Signering?
- Pålitelighet?
- Validering?

Private sertifikater

- Rotservere?
- Signering?
- Pålitelighet
- Validering?



SSL/TLS HANDSHAKE



Secure SHell (SSH)

- Privat og offentlig nøkkel (~/.ssh.)
- Server autentisert (known_host)
- Offentlig nøkkel på server
- Autentiser med privat nøkkel
- Frivillig passord på privat nøkkel
- Sesjon er kryptert

SSH Client

SSH Client
Secret Key

Encrypt message
with secret key

Client Initiates SSH Connection

Hello There

Generate random
message

$&#81 z3u%[>

Decrypted
the encrypted random message
using the client's public key

Authentication Passed

If random messages match, send a
affirmative response

Agree on Session Key

Encrypted Data (symmetrical algorithm)

Exchange Data using the Session Key
and a symmetrical crytographic algorithm

Secure SSH
Host Server

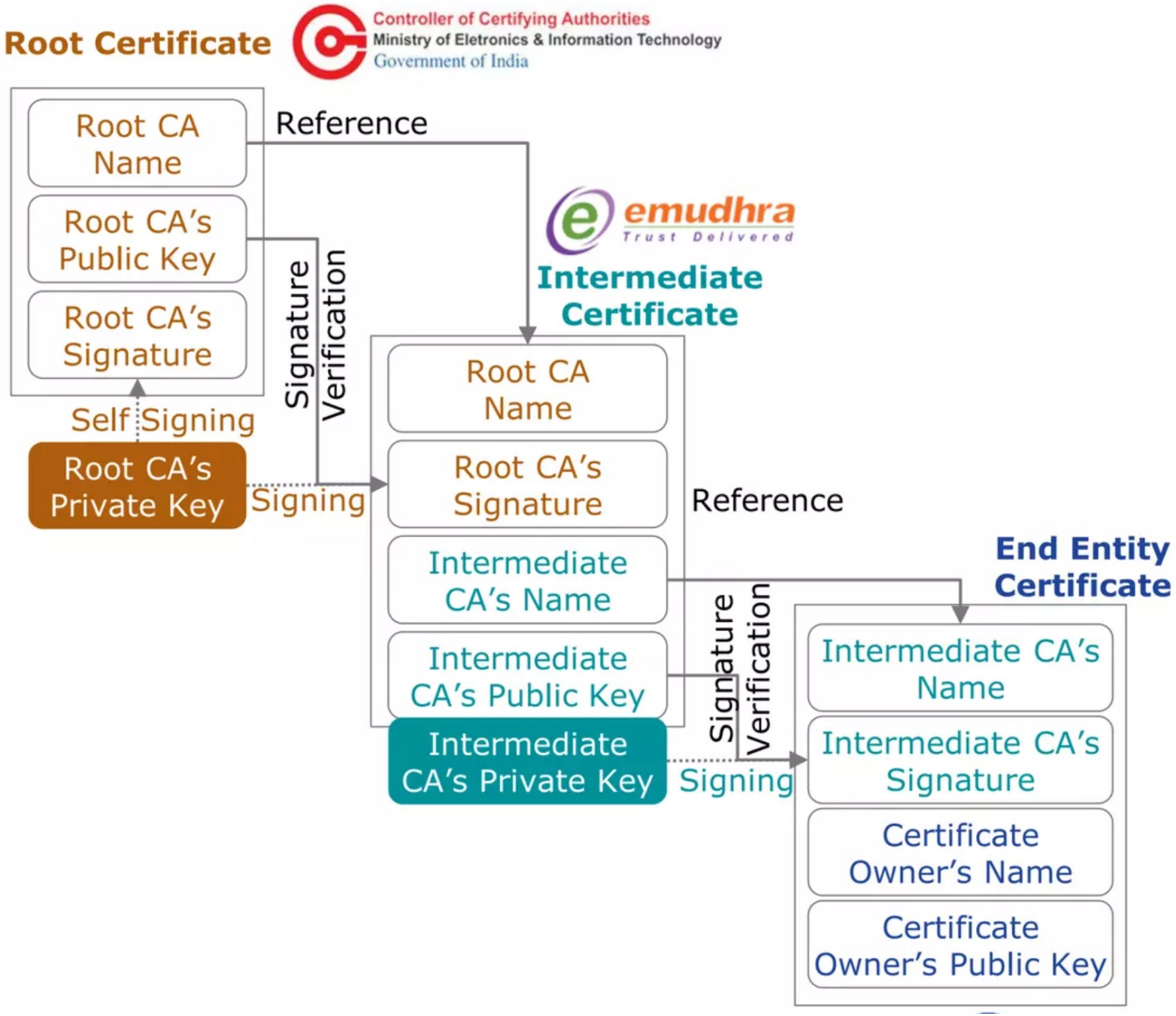
SSH Client
Public Key

Demo VM

- Generer lokalt SSH nøkkelpar
  - ssh-keygen -t ed25519 -C "your_email@example.com"
- Kopier offentlig nøkkel til VM i Azure
  - F.eks: `$ ssh-copy-id -i ~/.ssh/id_rsa.pub user@server.address.com`
- Logg på VM sikkert uten passord
  - ssh user@server.address.com

Public Key Infrastructure (PKI)

- Rotserver (Root Certification Authority)
- Offentlige rotservere
- Private rotservere
- Sertifikatkjede
- Windows / Linux




sopra steria