#6 X.509 Certificates

SEGURANÇA NAS ORGANIZAÇÕES E INFORMÁTICA

deti universidade de aveiro
departamento de eletrónica, telecomunicações e informática

2024/2025

Asymmetric Cryptography

Recap

Private Key

- Sign data
- Decipher ciphered data

Public Key

- Verify signed data
- Cipher data

Asymmetric Cryptography

Recap

Private Key

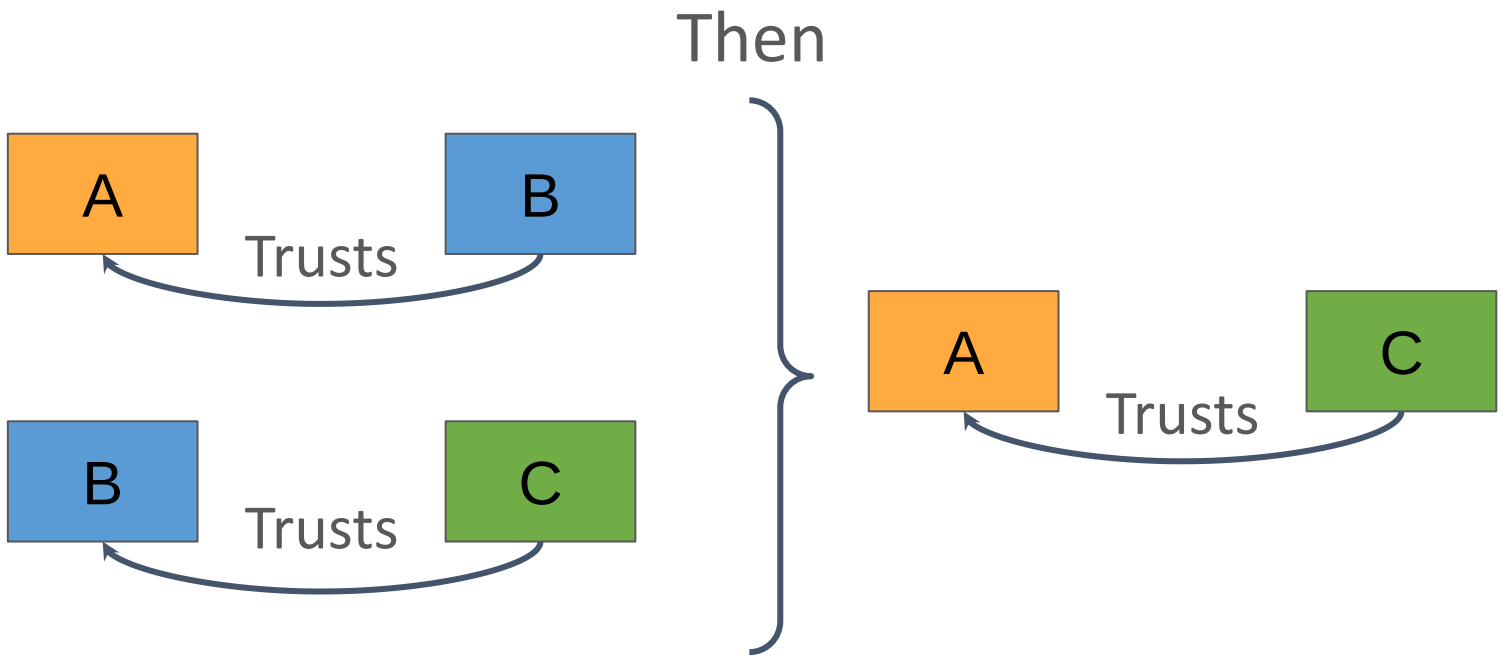
- Sign data
- Decipher ciphered data

Public Key

- Verify signed data
- Cipher data

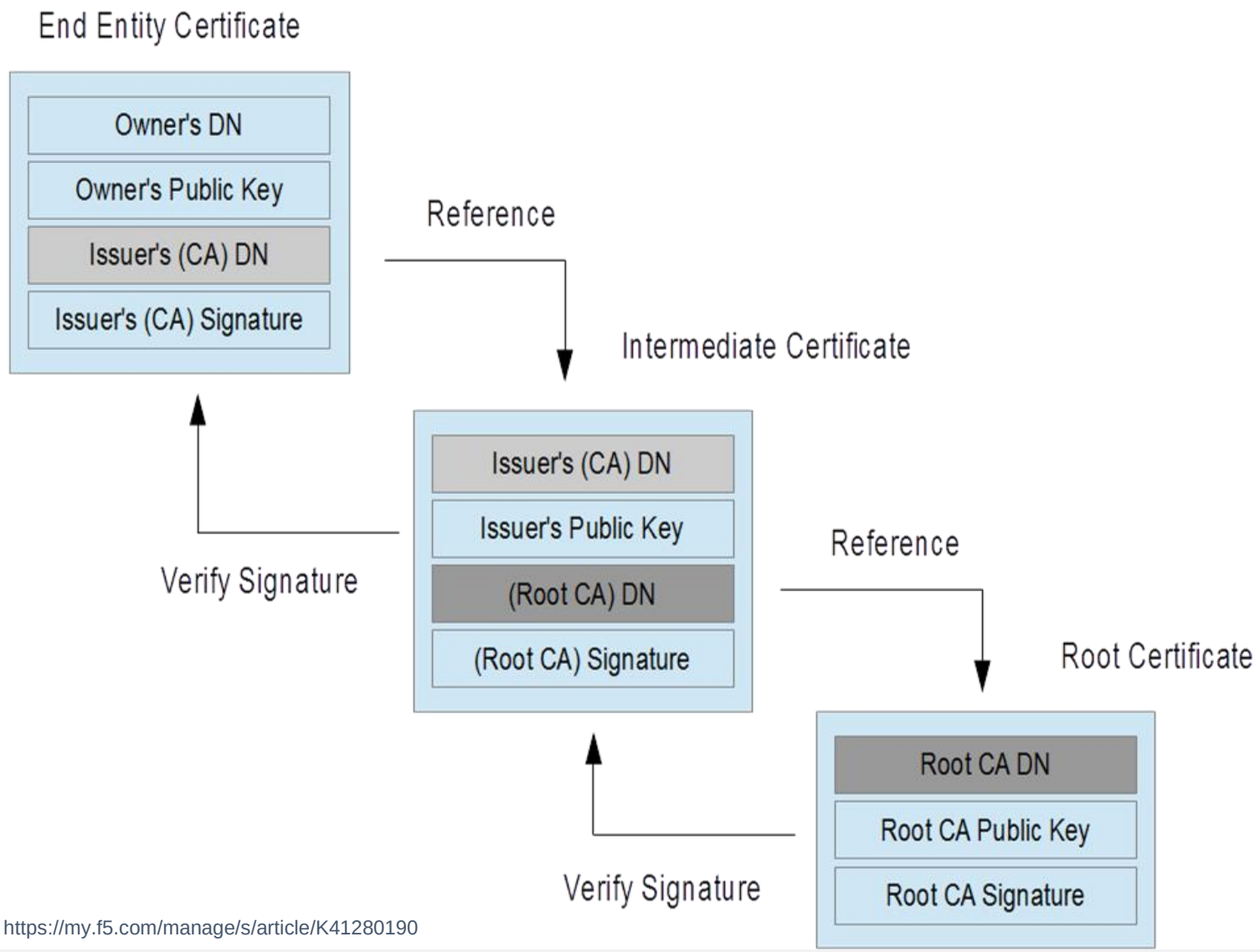
However, how can I trust a Public Key?

Trust



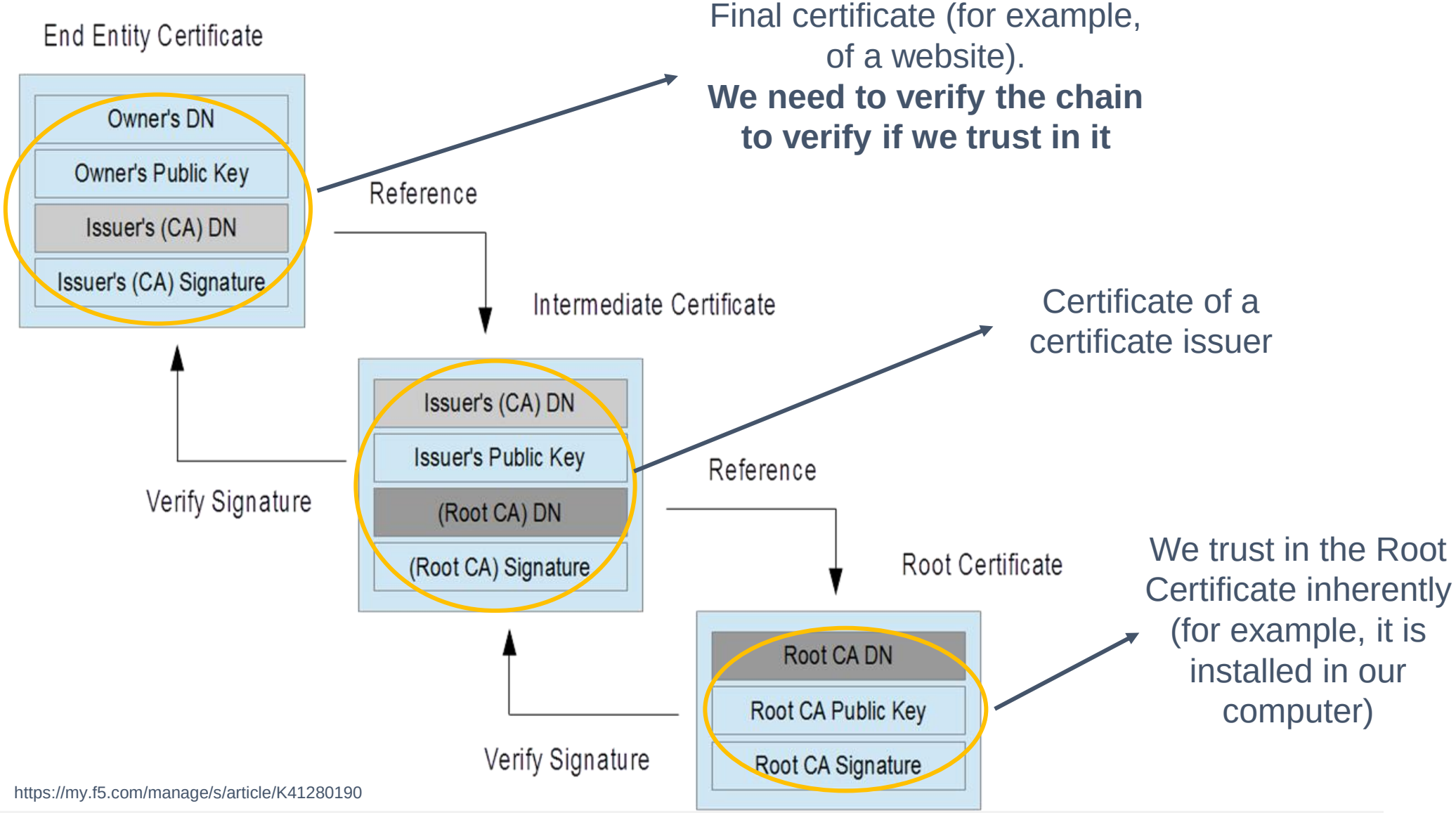
In certificates, trust is transitive

Chain of Trust



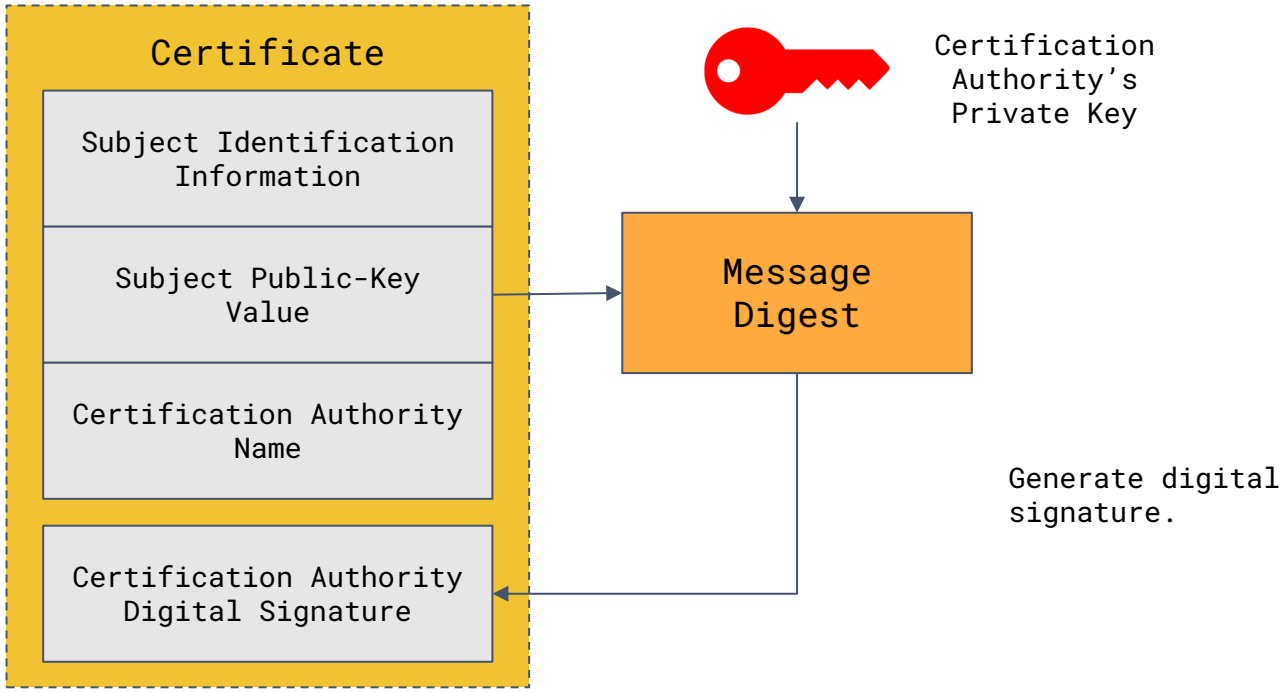
https://my.f5.com/manage/s/article/K41280190

Chain of Trust



https://my.f5.com/manage/s/article/K41280190

Trusting a public key



A certificate is just a format, to convey the trust of an authority on a specific key.