PKI in global world

Securing telephone networks

17 November 2025

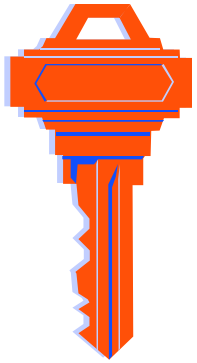
Erik Andersen
ITU-T Study Group 17
era@x500.eu

Public-key concept

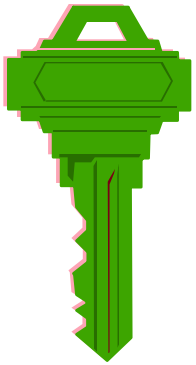
In asymmetric cryptography an entity has a mathematically related key pair, or several of such pairs.

One key is the **private key** and has to be kept protected and secret by the owner.

The other key is the **public key** and may be copied to other entities.



Private key

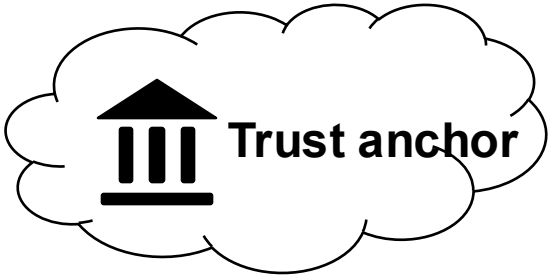


Public key

Public-key certificate

The certification authority (CA) as a trusted third party certifies by its digital signature that the public key and the corresponding private key belong to the subject (James Smidth)

Authenticated transfer with integrity



Alice
(Certificate owner)

CA certificate

Message, signature

Alice‘s public-key certificate

Bob
(Relying party)

What PKI is about (very simplified):

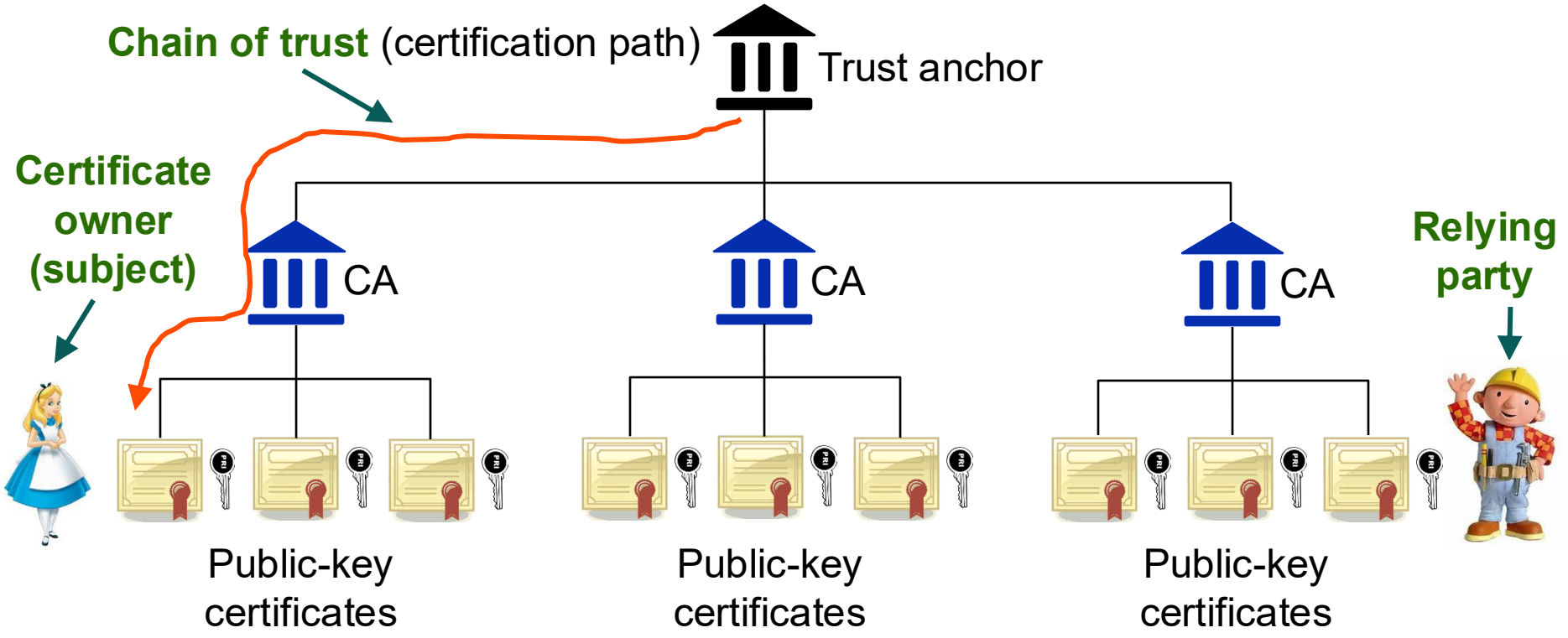
Message digitally signed by Alice and signature to be verified by relying party using the public key in Alice’s public-key certificate

PKI CHAIN OF TRUST

A problem for a federated PKI

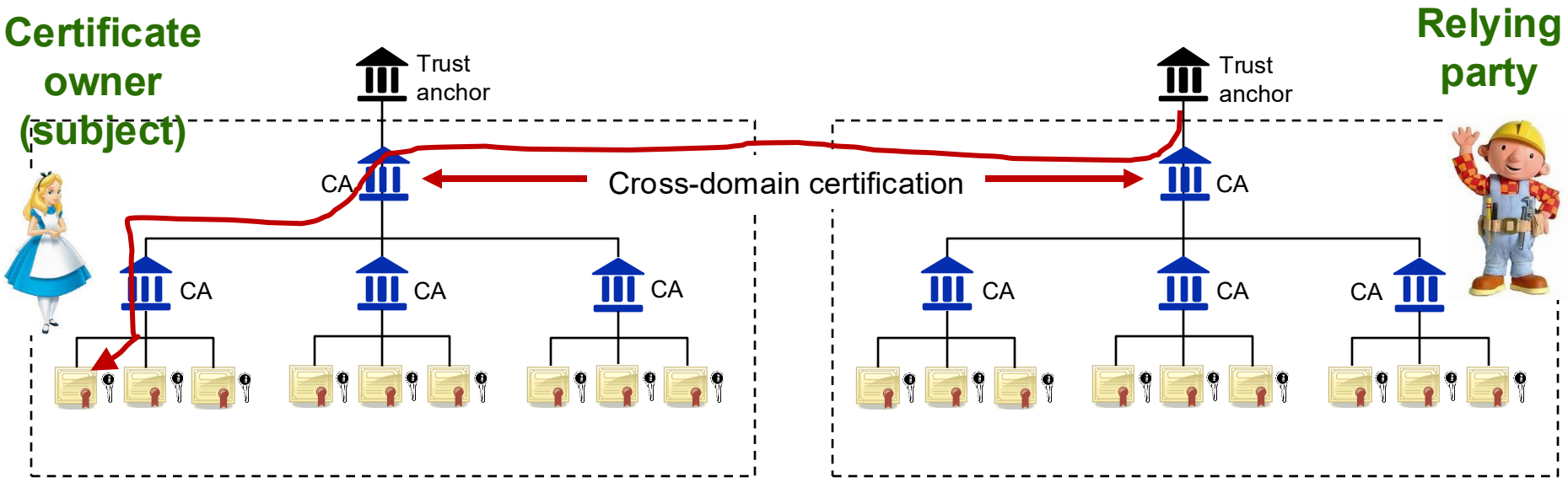
Chain of trust with traditional public-key infrastructure (PKI)

PKI Domain:

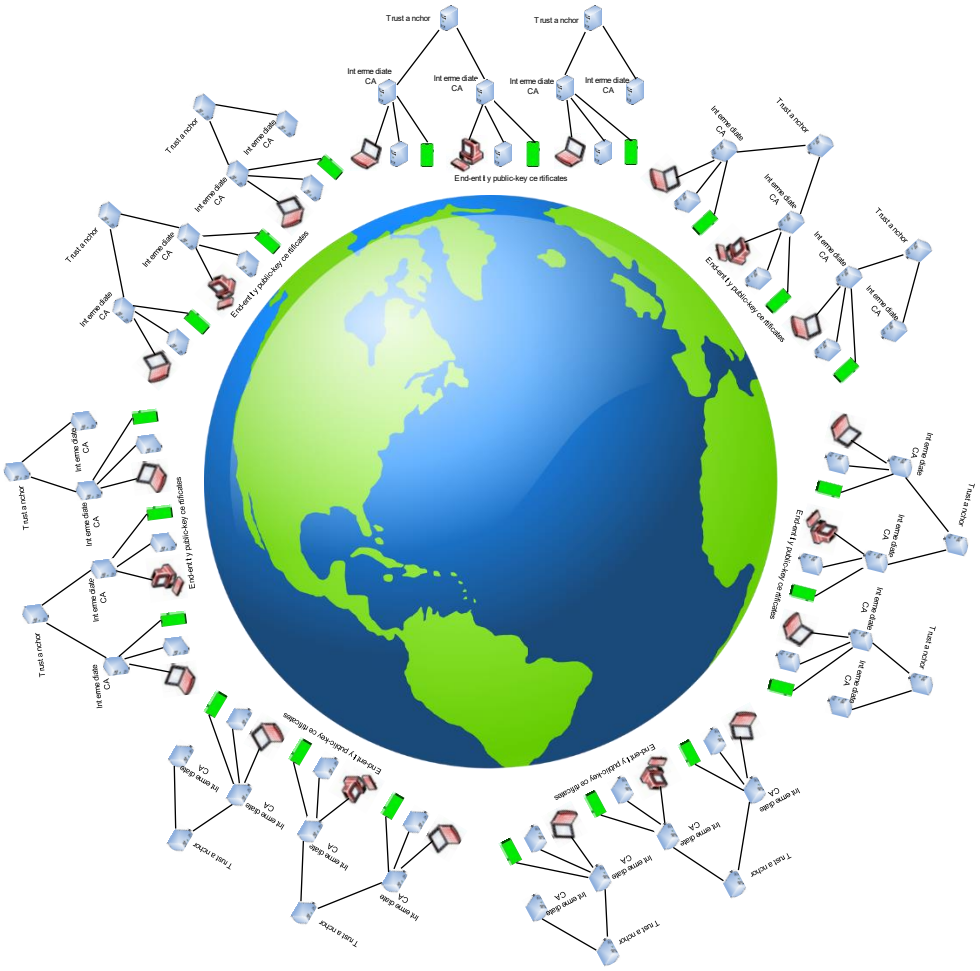


If the relying party and the certificate owner are far apart, then what?

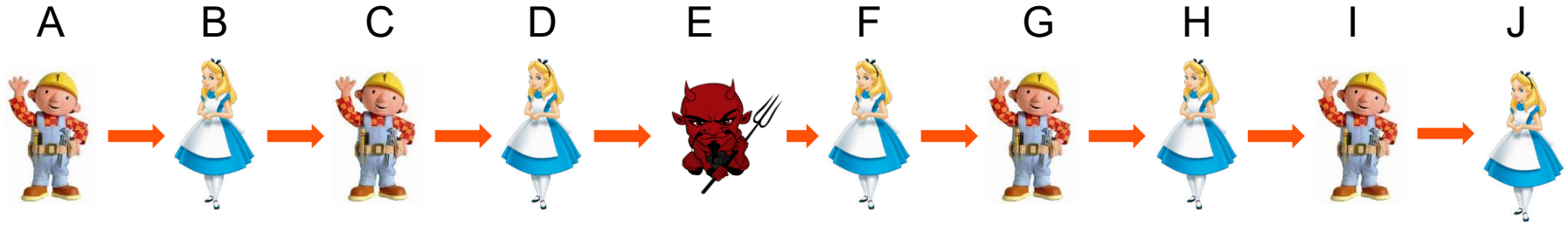
Interconnected Public-key infrastructure (PKI) domain



A world-wide federated PKI



Long chain of trust



A trust B, B trust C, ... , I trust J

Can A then trust J?

The longer the chain of trust is, the more diluted trust becomes

Trust by consensus

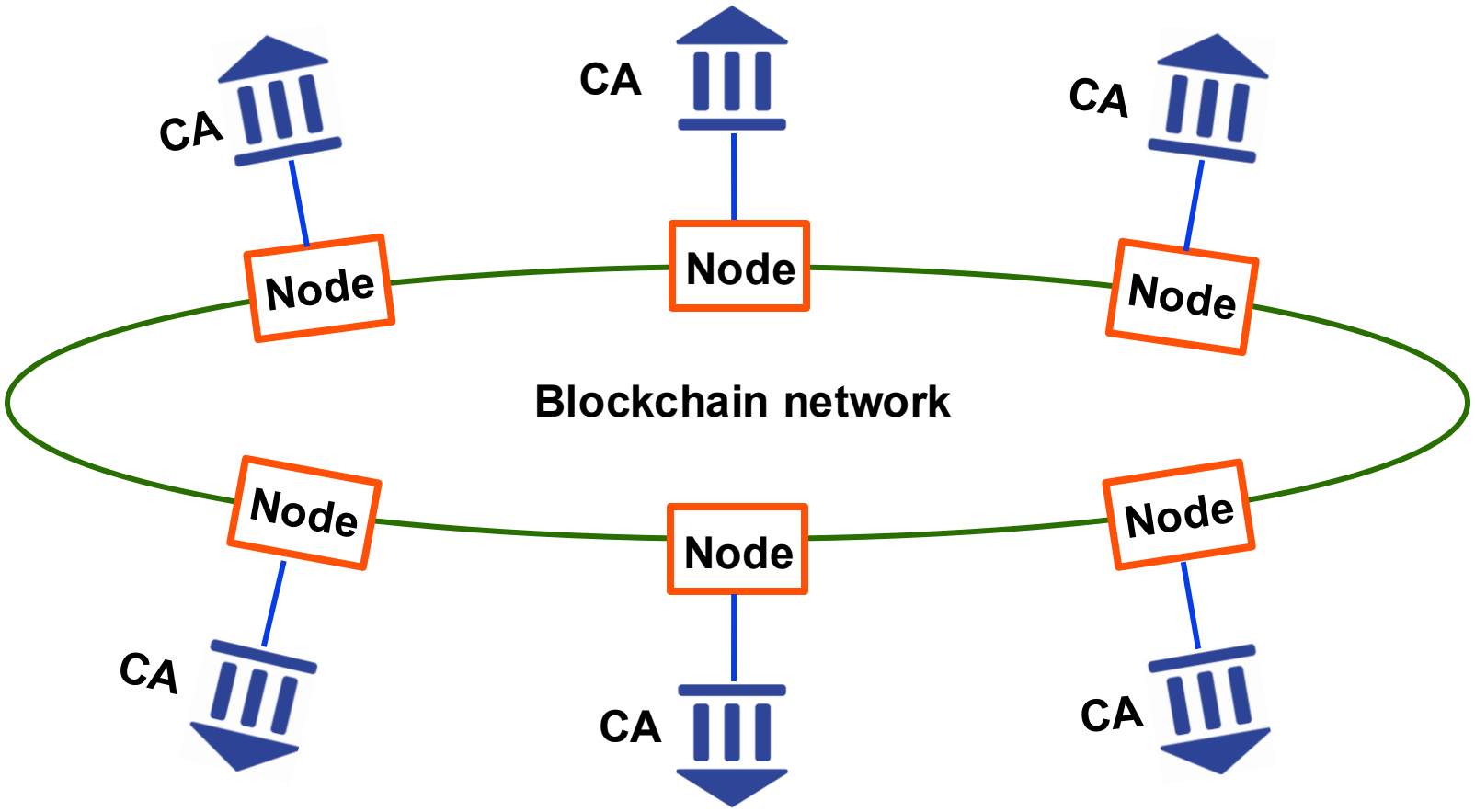
It seems problematic to create a world-wide federated PKI having world-wide trust using current PKI trust model.

A PKI where trust is obtained by **consensus**

PKI domains federated using blockchain technology

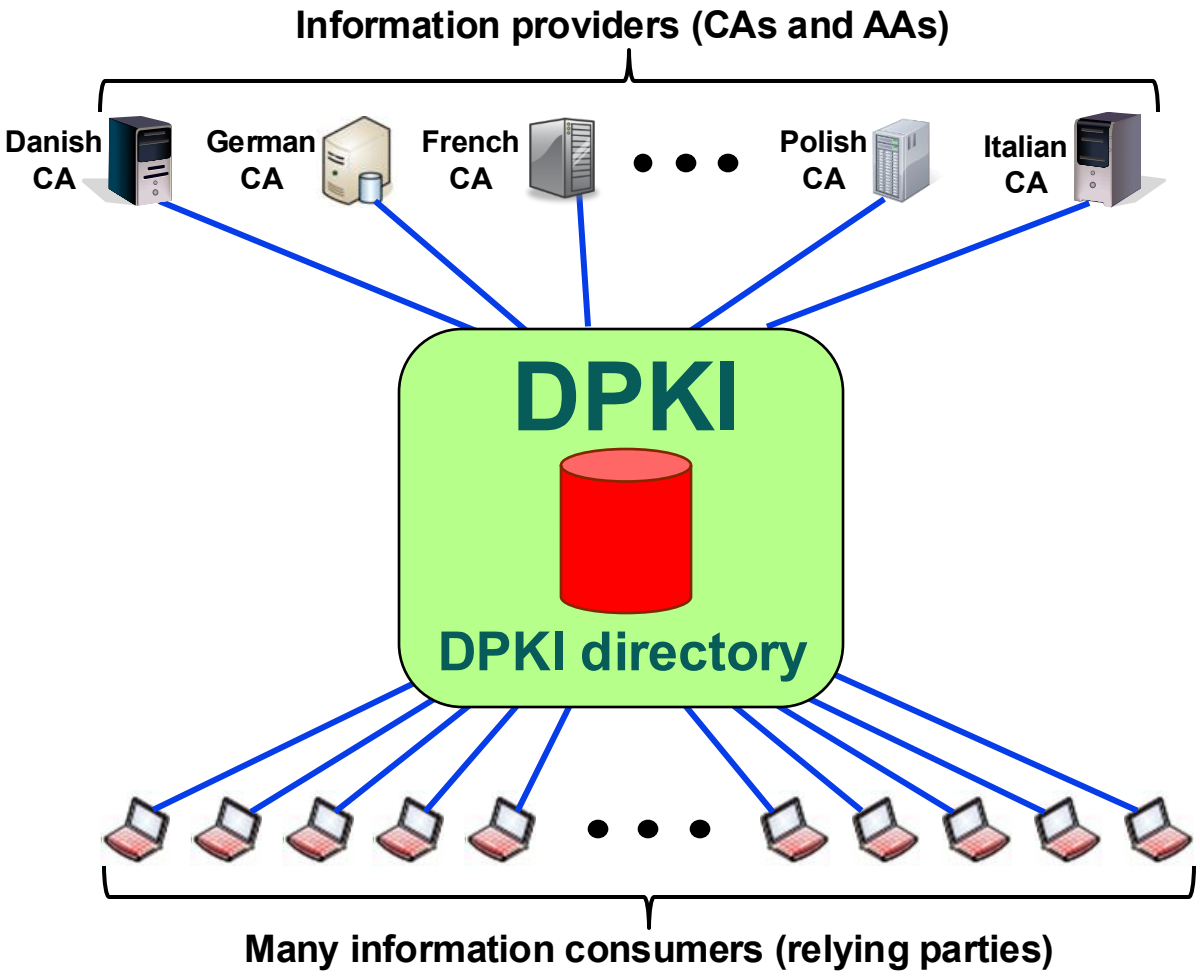
Decentralized public-key infrastructure (DPKI)

Positions of CAs the blockchain network



The CAs are outside the blockchain network

DPKI information providers and consumers



Different from other blockchain platforms: No interaction between service providers

END