Trust and identity by decentralized PKI and by data protection

2nd Joint ITU/WHO Workshop on
Digital COVID-19 Certificates
26 November 2021

Erik Andersen

Andersen's L-Service

Danish representative in ITU-T Study Group 17

Member of the IEC TC 57 WG 15 (smart grid security)

era@x500.eu

Trust & Identity

To trust or not to trust

CERTIFICATE AUTHORITY (CA): Also known as a "certification authority" in the context of a public key infastructure, is an entity or organization that issues digital certificates.

A rogue CA is a **certificate** authority

A sloppy CA is a **certificate** authority

A trustworthy CA is a **certification** authority

Trust in provided information

Trustworthy information and secure identification are crucial concepts!

A **certification authority** does not only issues public-key certificates, but with its digital signature **certifies** that the information provided is genuine.

and...

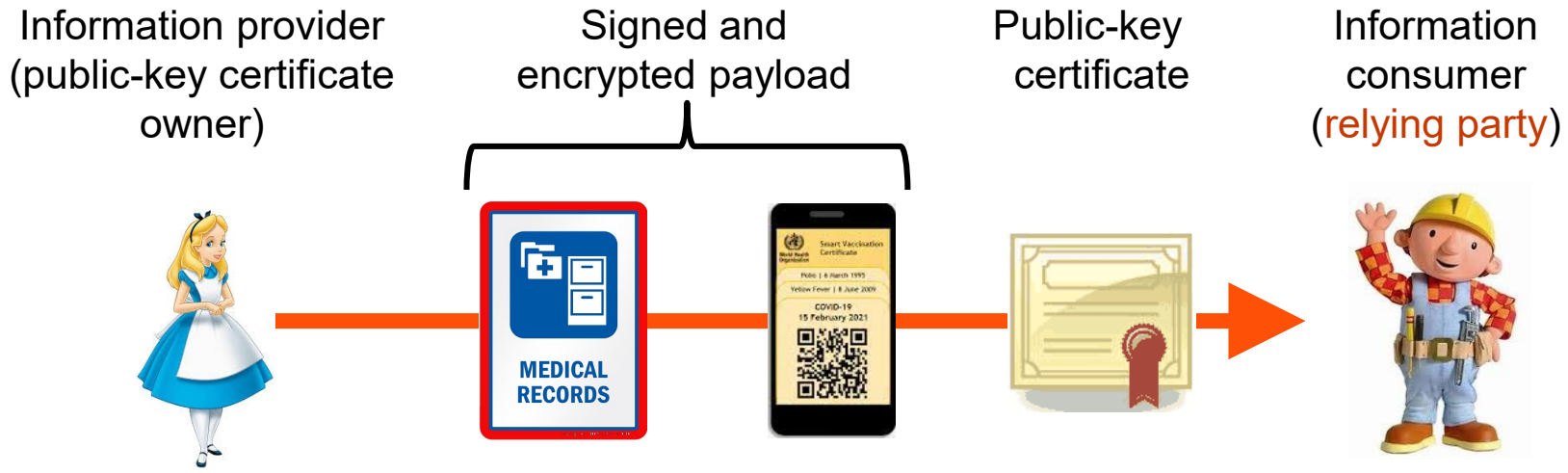
Identity!

what is crucial:

- The CA binds the identity of the owner of the public-key certificate to the public key
- Certifies that the owner is position of the corresponding private key

The public/private key pair is the identity associated with digital signature generation and verification.

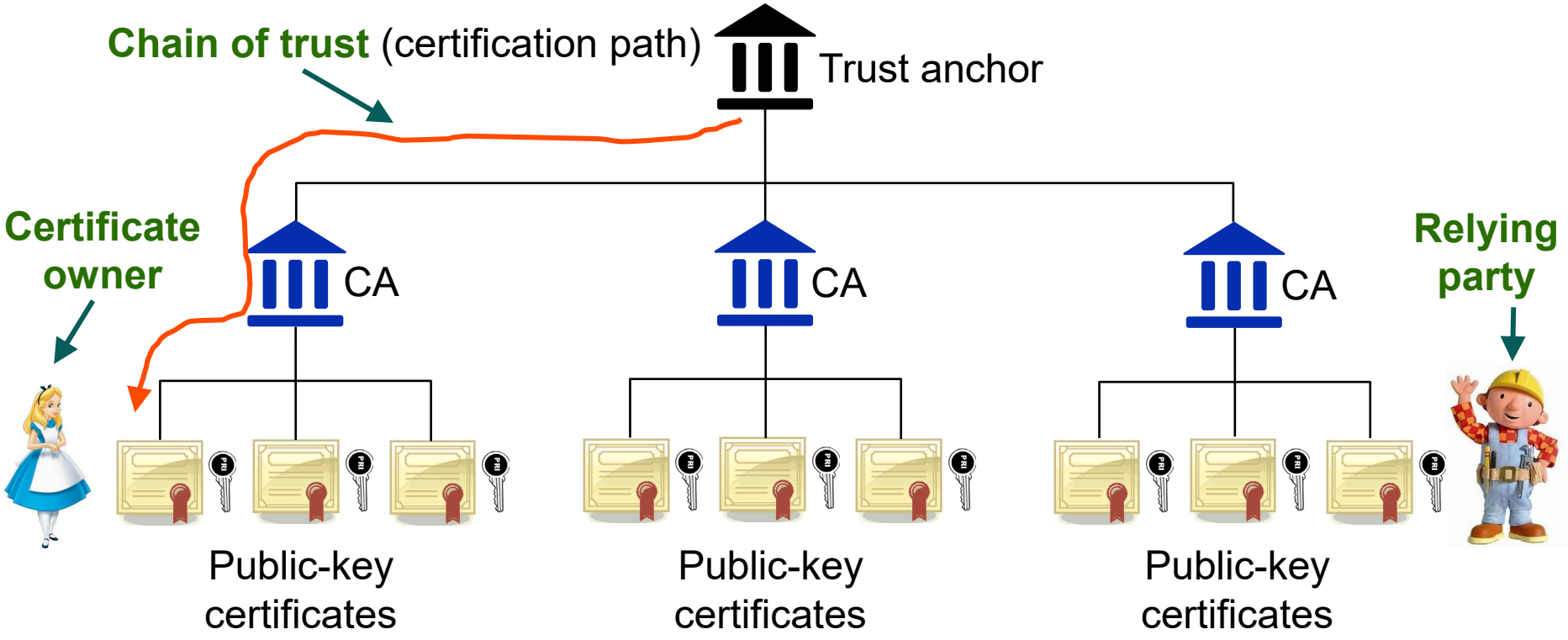
Integrity and confidentiality of information



The information consumer is relying on the information in the public-key certificate to make judgement on the integrity of the received information

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

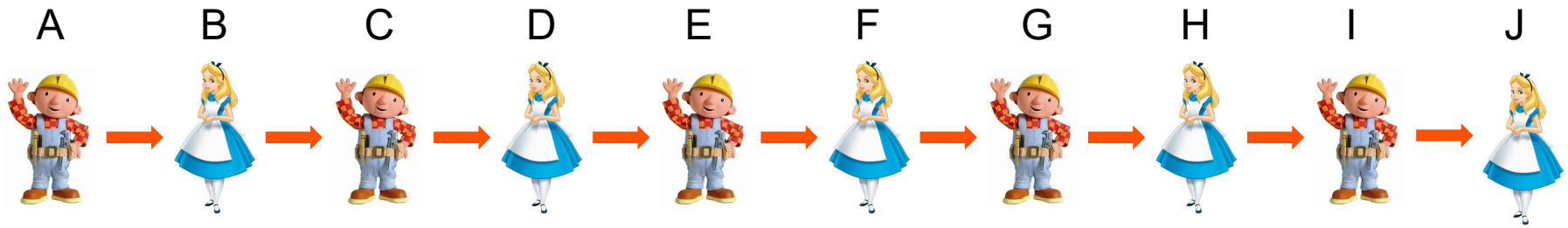
PKI Domain:



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

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

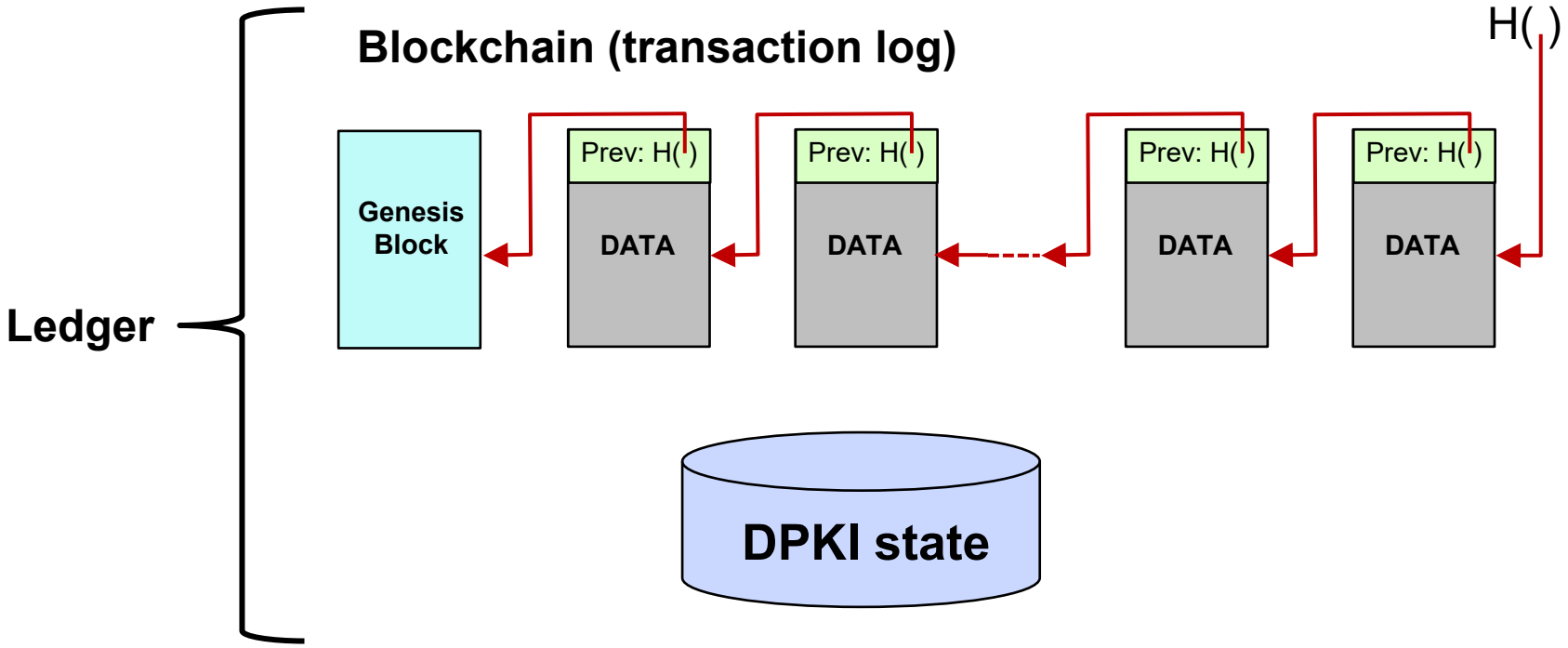
Trust by consensus

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

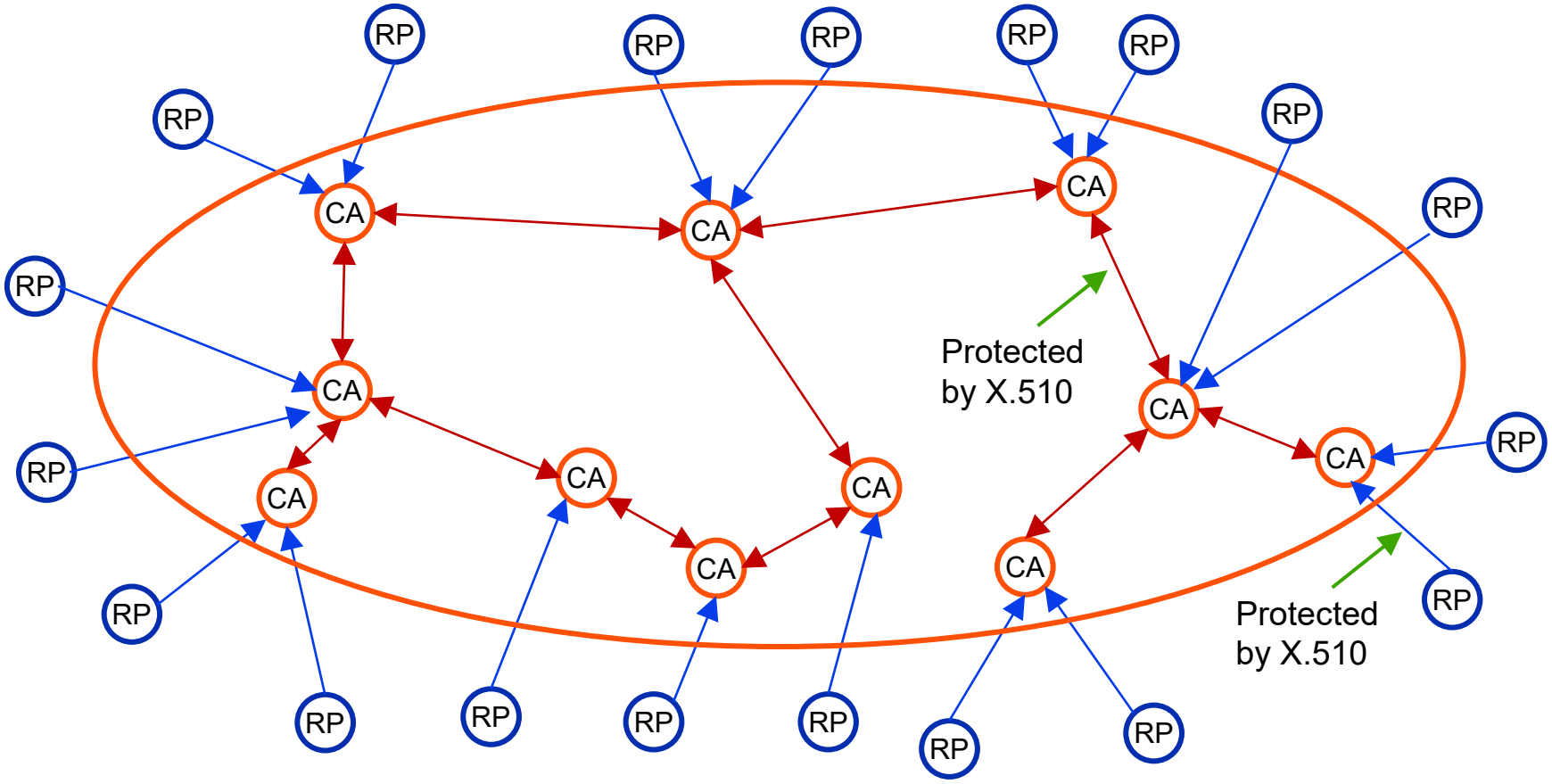
A PKI where trust is obtained by consensus

A decentralized PKI (DPKI) based on the blockchain technology

Distributed ledger



DPKI network



CA = certification authority
RP = relying party

Existing standards

For access control:

Rec. ITU-T X.1080.0, Telebiometrics, Access control for telebiometrics data protection

For cybersecurity:

Rec. ITU-T X.510 | ISO/IEC 9594-11, The Directory: Protocol specifications for secure operations

Access control

A need-to-know philosophy (right-to-now not sufficient)

Service oriented

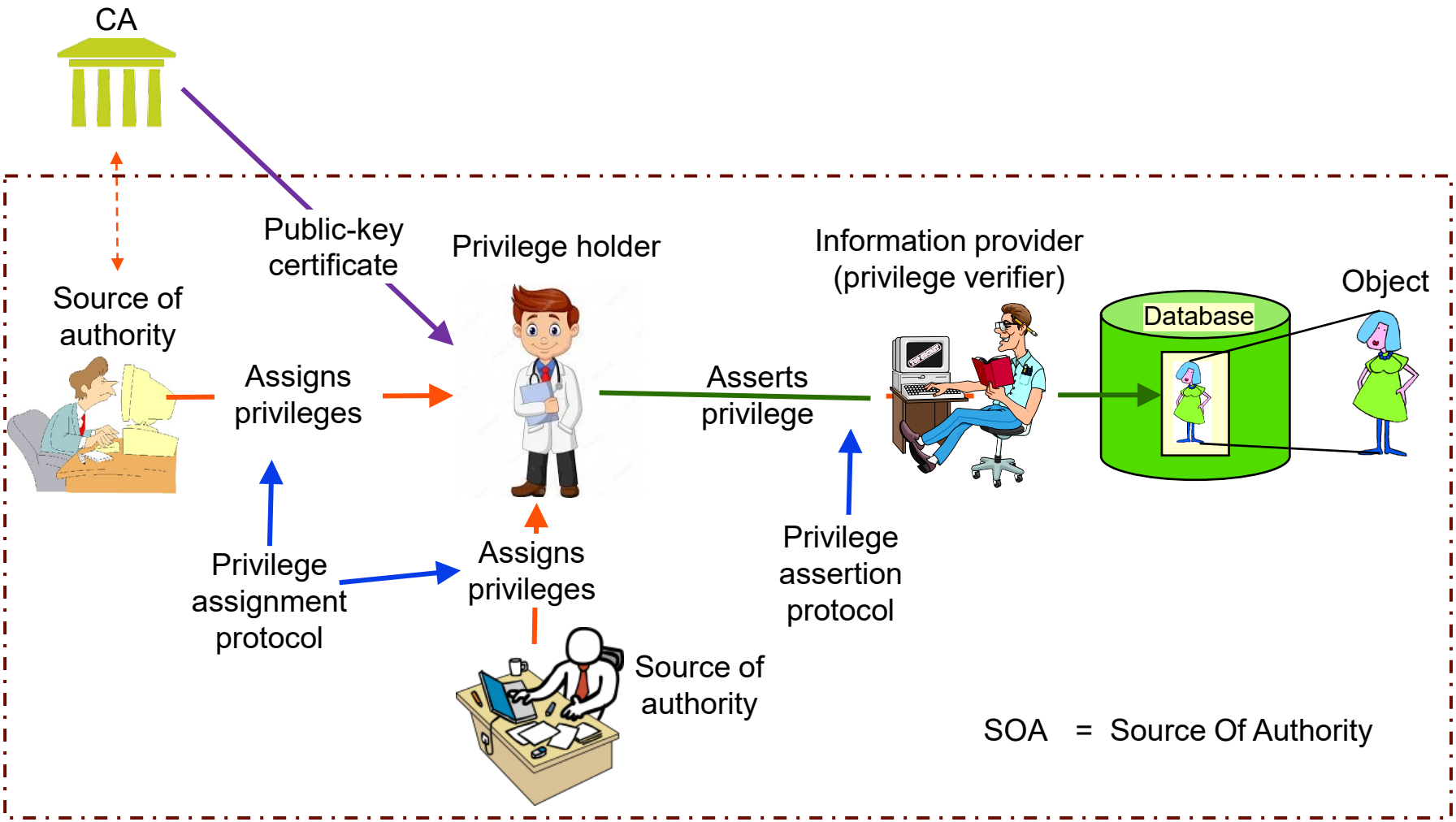
Fine granularity in privilege assignment

Semi-permanent or time limited privileges

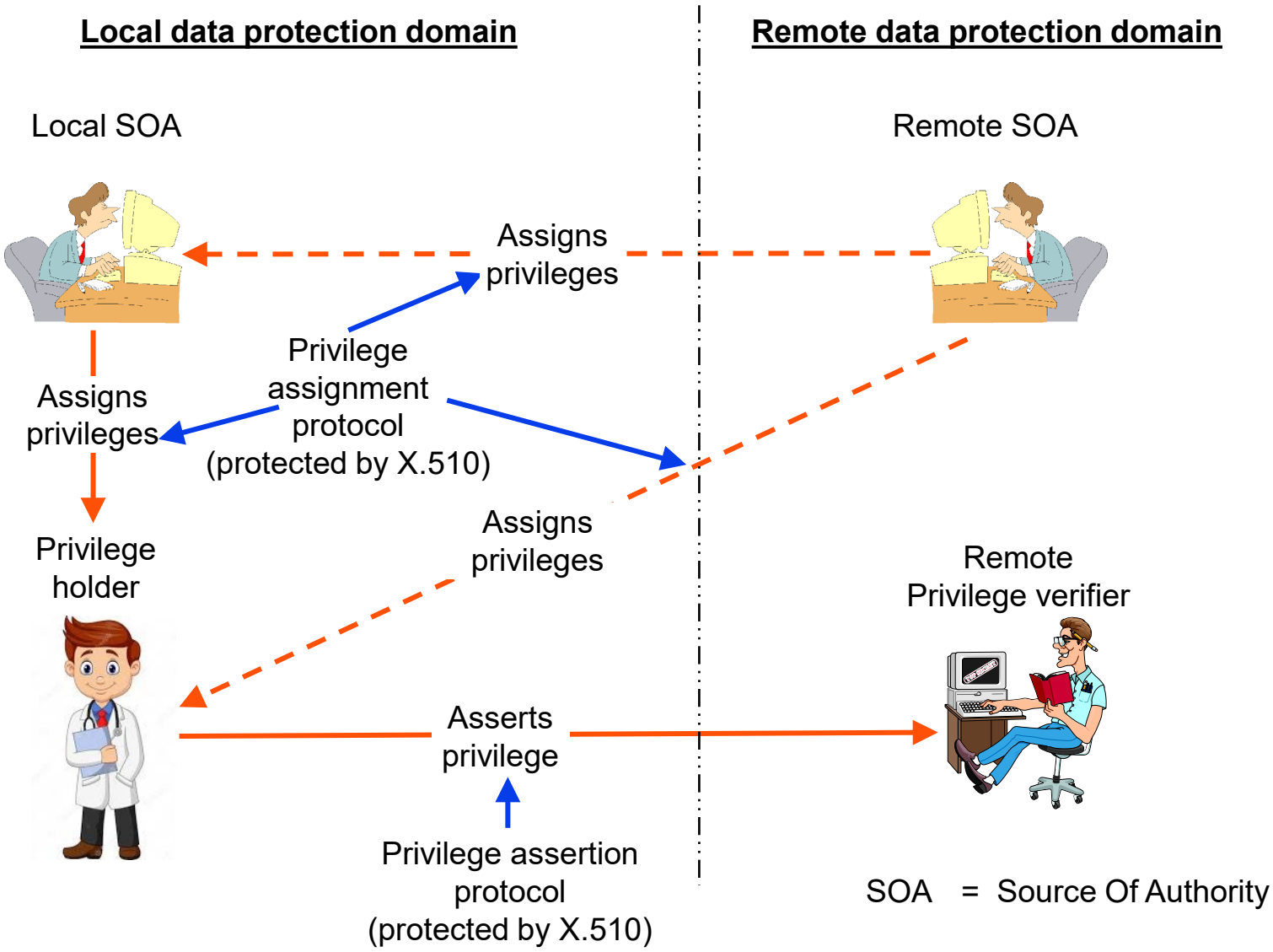
Large number of defined operations

Protected by X.510 (in progress)

Single privacy protection domain



Cross-domain privileges



Standards activities

Decentralized public-key infrastructure (DPKI):

- Work in progress
- Still some way to go
- Contributions required

Access control – Rec. ITU-T X.1080.0:

- Final specification exists
- May need some extensions
- A manageable activity

Cybersecurity - Rec. ITU-T X.510 | ISO/IEC 9594-11:

- Final specification exists
- Amendment in progress
- A manageable activity