Decentralized Public-Key Infrastrucure (DPKI) as it relates to Verifiable Health Credentials

Joint ITU/WHO Workshop on “Future of Verifiable Health Credentials Beyond COVID-19”
11 September 2023

Erik Andersen

Andersen's L-Service

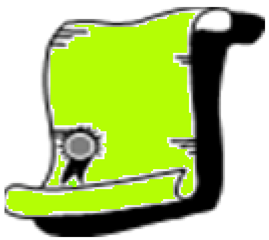
Danish representative in ITU-T Study Group 17, Question 11

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

era@x500.eu

Trust,
Identity
&
Privilege

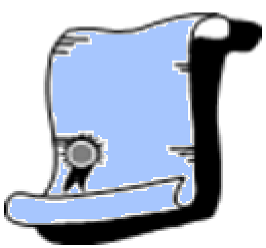
Certificate concept



Public-key certificate:

Certification of identity

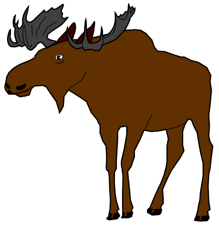
Issued by certification authority



Attribute certificate:

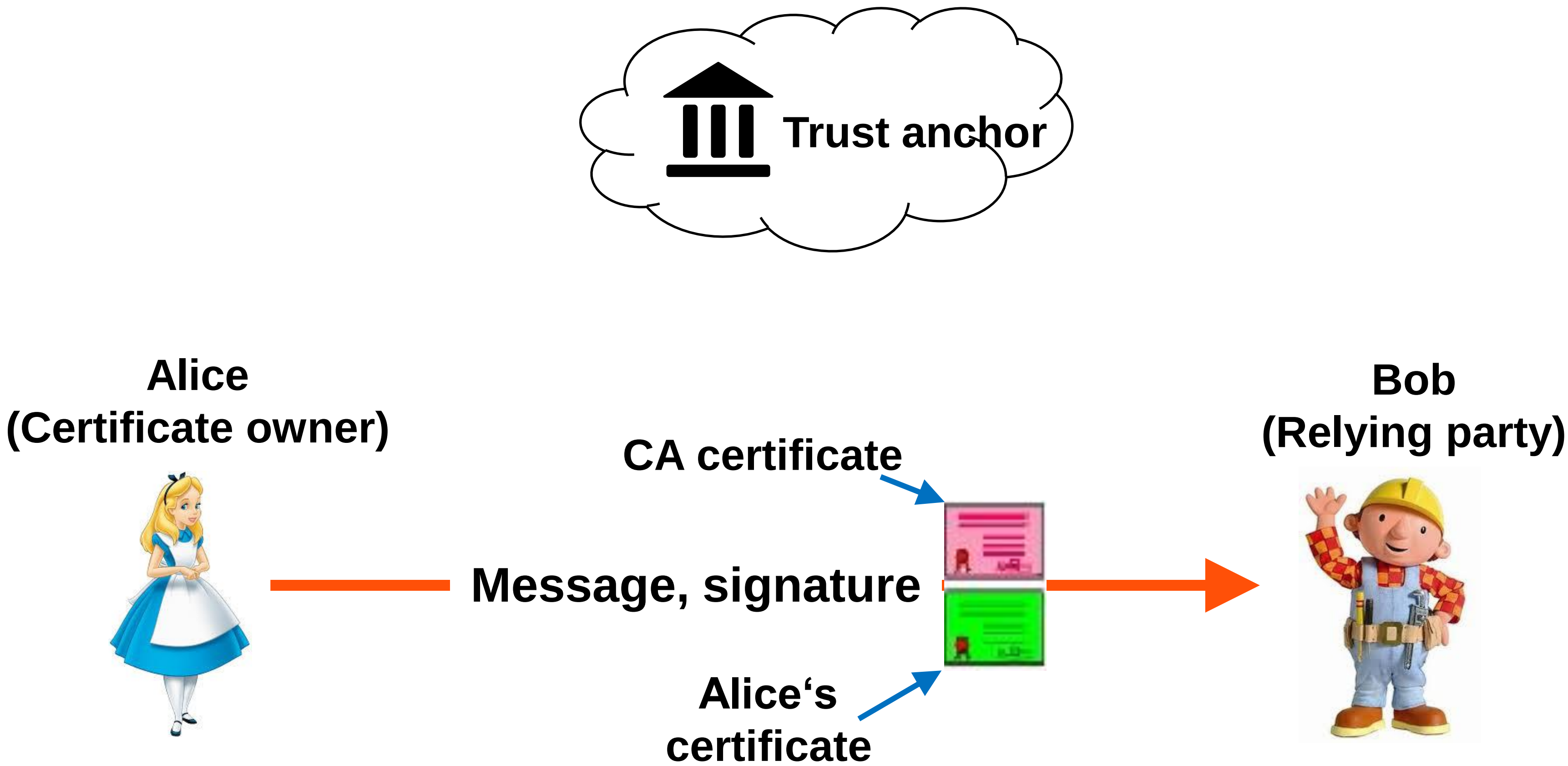
Certification of privileges

Issued by attribute authority



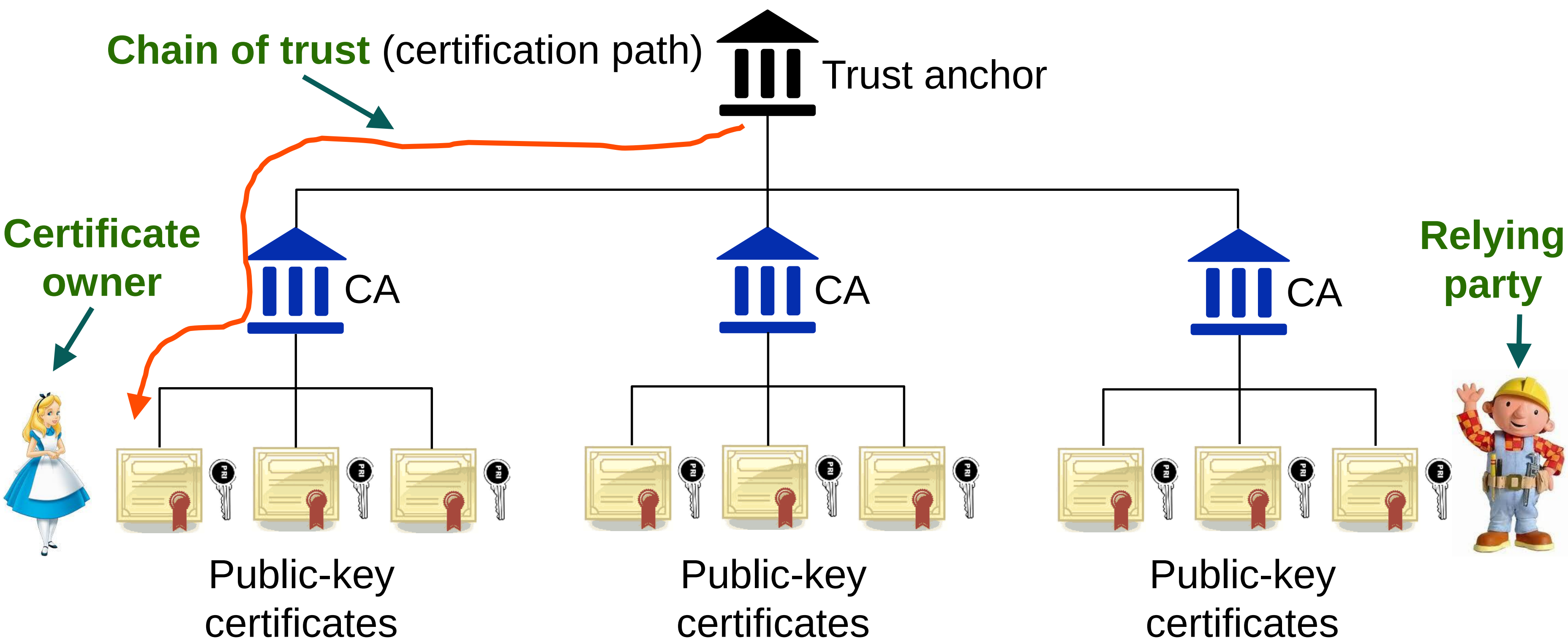
Trusted public-key certificate?

Authenticated transfer with integrity



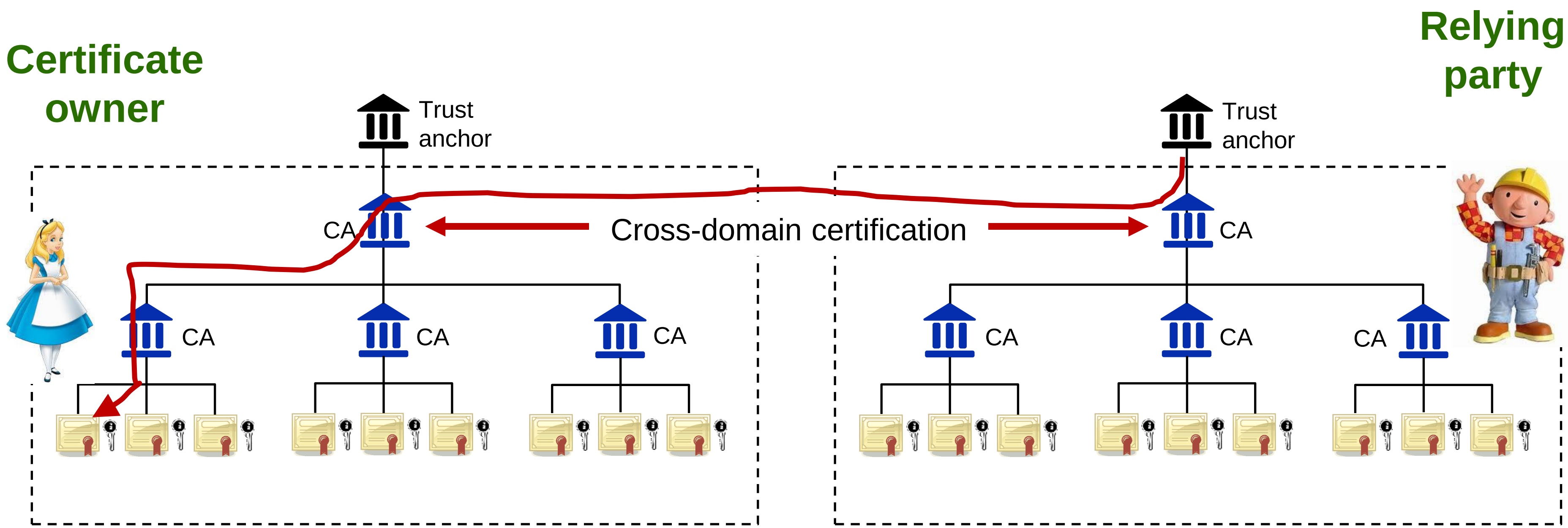
Chain of trust with traditional public-key infrastructure (PKI)

PKI Domain:



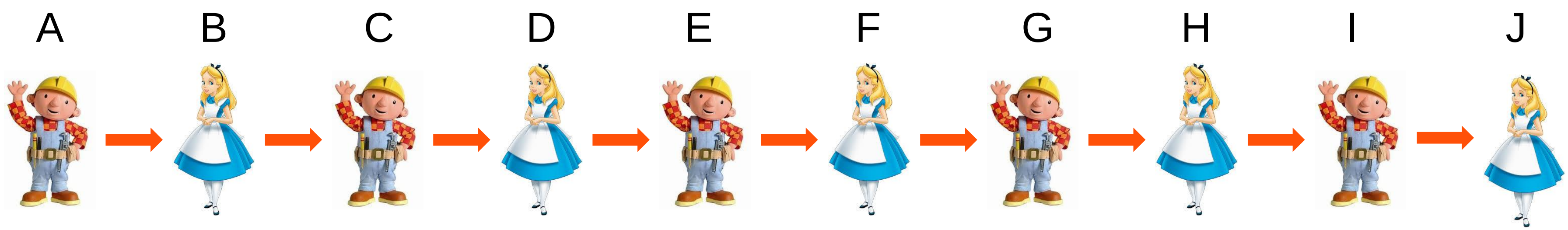
If the relying party and the certificate owner are far apart, then what?

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

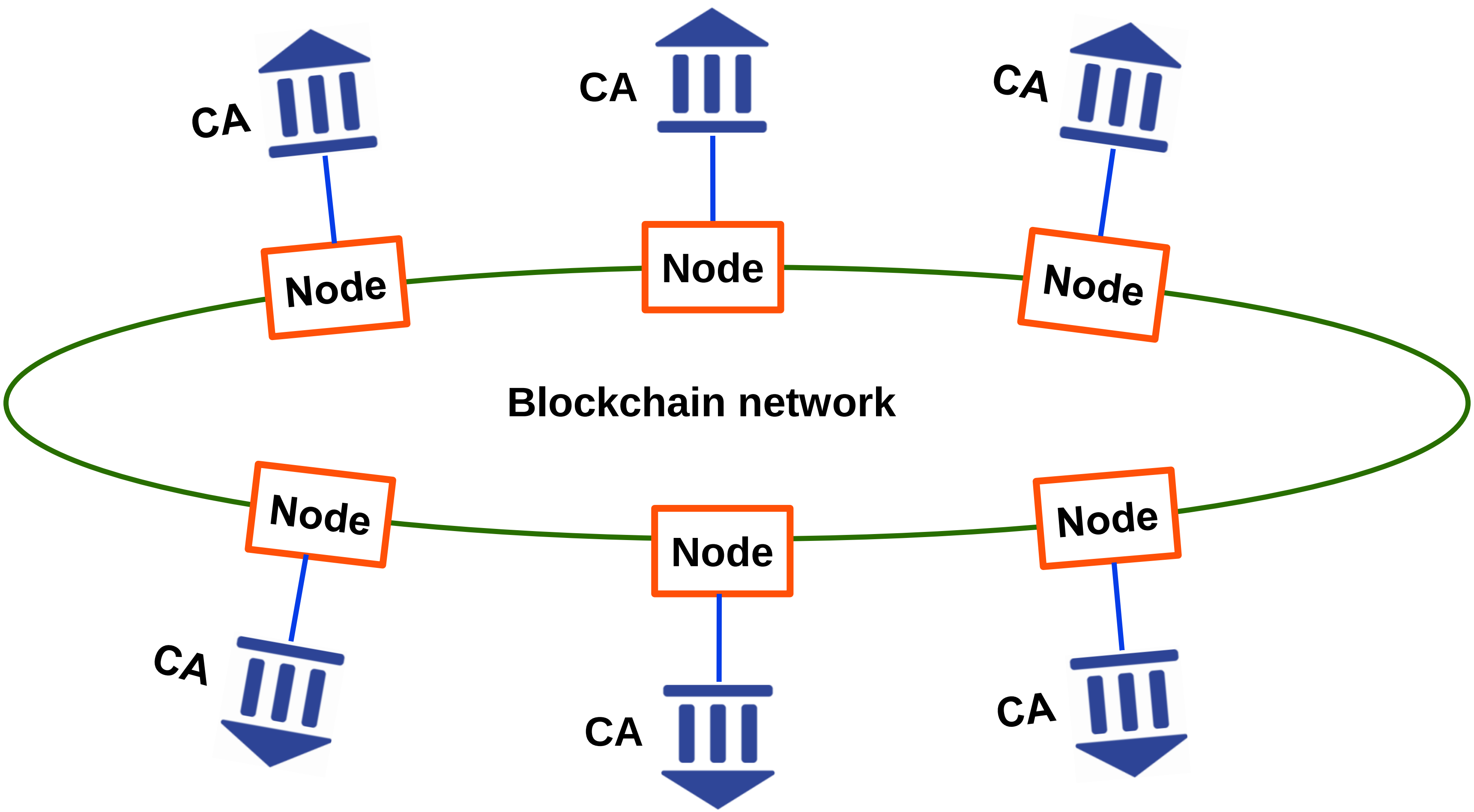
Trust by consensus

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

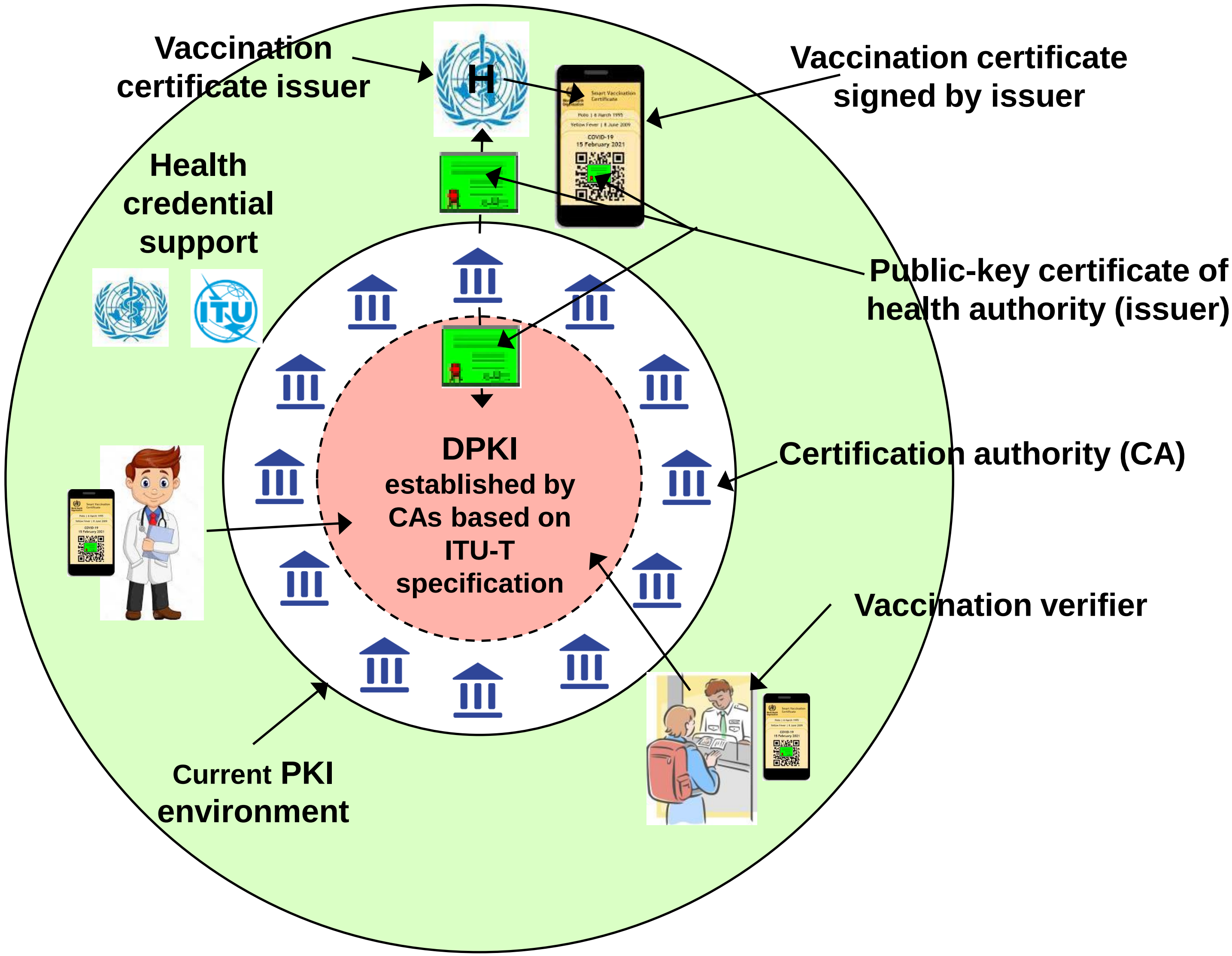
A PKI where trust is obtained by consensus

PKI domains federated using blockchain technology

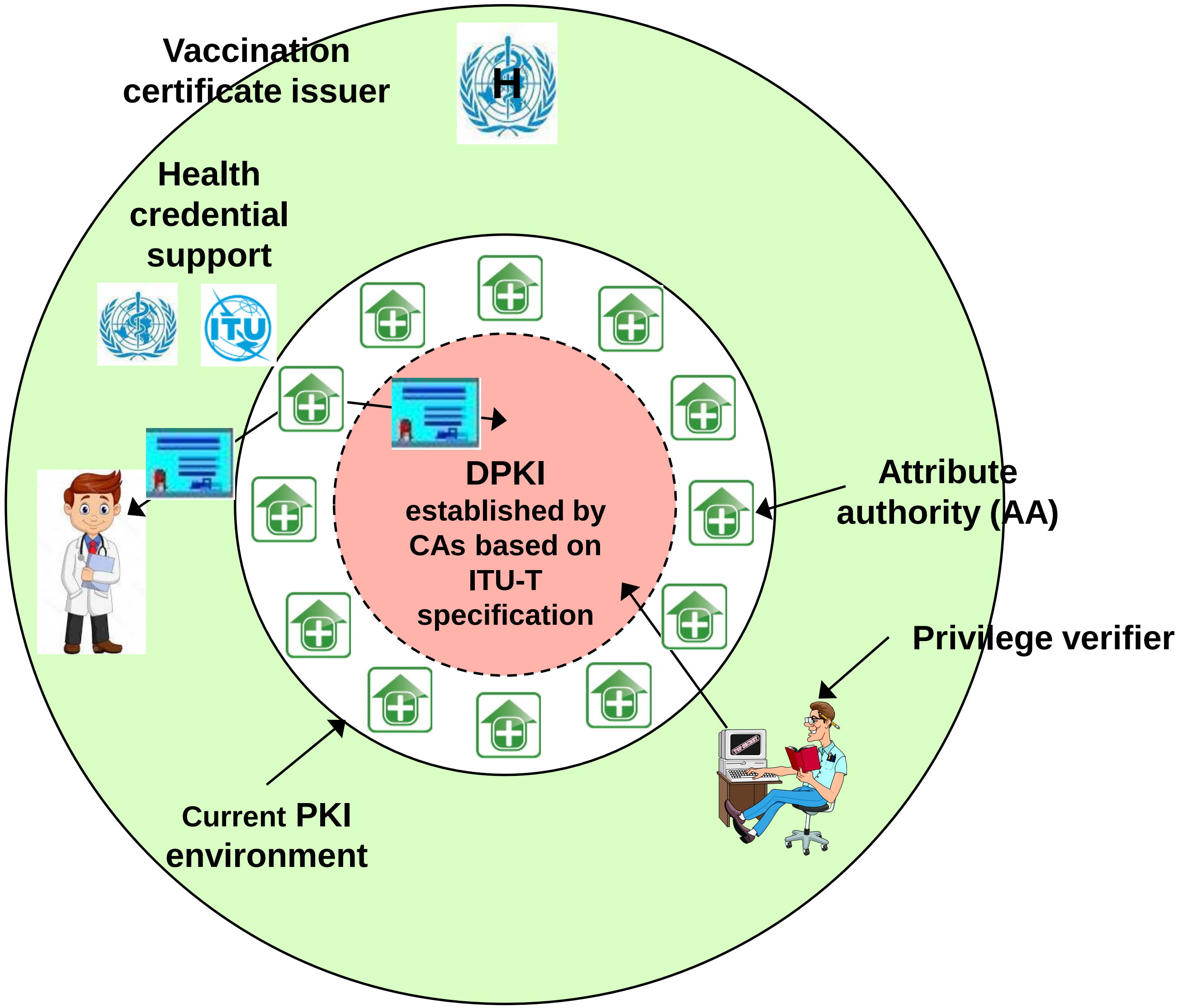
A figurative representation of the underlying network



Components of health credential support



Health credential access control



Standards support

- **Rec. ITU-T X.50x | ISO/IEC 9594-13, *Decentralized public-key infrastructure***
- **Rec. ITU-T X.510 | ISO/IEC 9594-11, *Protocol specifications for secure operations***
- **Rec. IT*U*-T X.1080.0, *Access control for telebiometrics data protection***
- **Plus, what communication protocol support is needed for the health credential support**