# Some thoughts on the future of ITU-T X.509 and related specifications

## First ITU-T X.509 day

**9 May 2022**


**Erik Andersen**

era@x500.eu

# ITU-T X.509 – a done deal?

**It is out there. It is working. Thousands of working systems are out there.**

**It is a done deal!**

**or is it?**

# Current status of ITU-T X.509

- Introducing authorization and validation lists (AVLs)
- Migration of cryptographic algorithms for
  - public-key certificates
  - attribute certificates
  - certificate revocation lists
  - authorization and validation list
- All non-PKI and all non PMI have been moved to other parts of the X.500 series
- A clear separation between PKI and PMI
- Unbundled from other parts of the X.500 series meaning fast progressing

# General challenges

- Requirement for lightweight, but strong cryptographic algorithms
- Lean and secure communication protocols
- Scalable specifications
- Adapting PKI to the new environments

# Challenge

## Two opposite trends:

- **Computers get faster - especially future quantum computers**
- **Devices get smaller and numerous**
  - **Constrained on processing power**
  - **Battery driven**
  - **Storage constraint**
  - **Stringent response requirements**
  - **Etc.**

**The bad guys get stronger**

**The good guys get weaker with large attack surface**

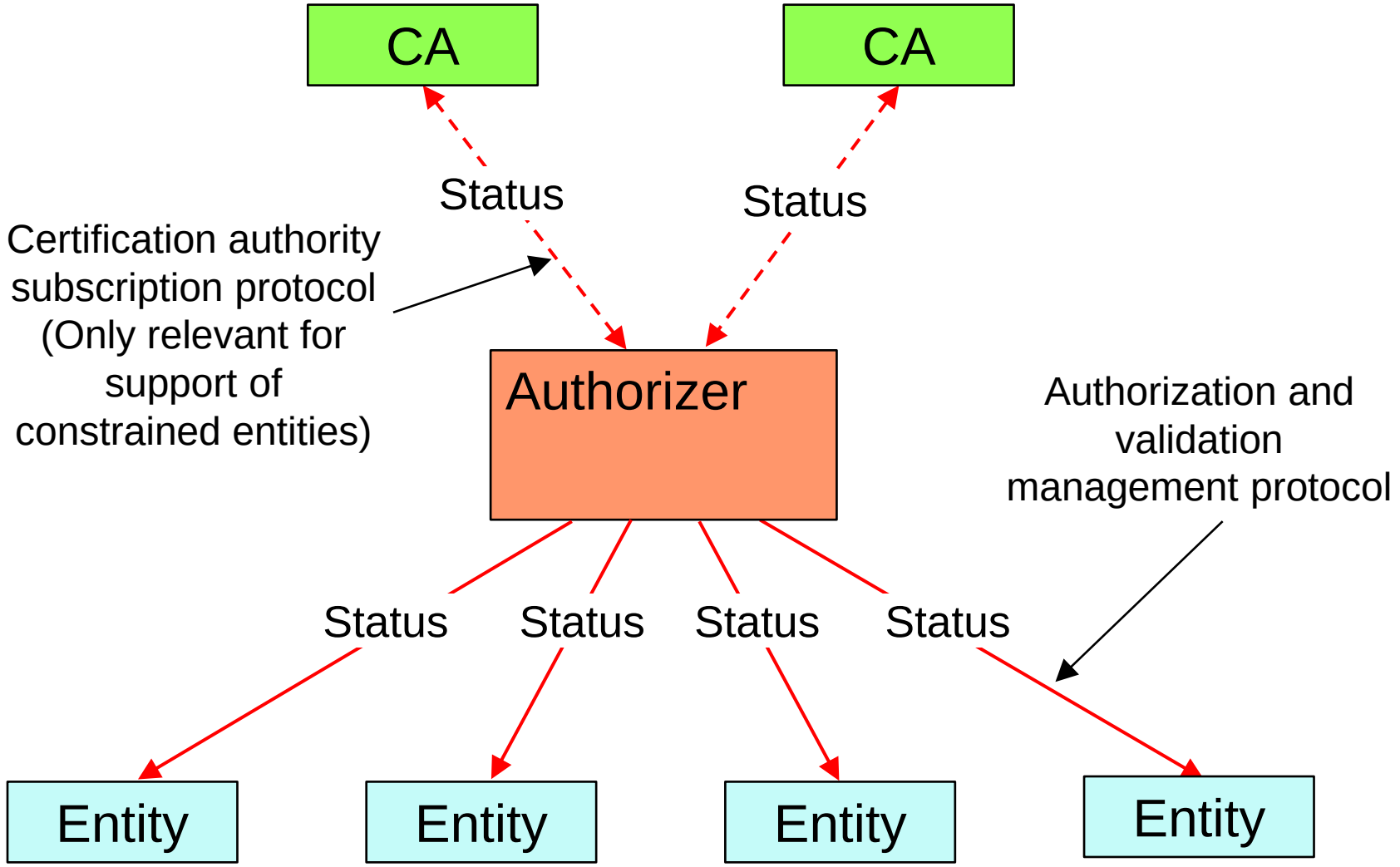
# Helping the small guys

- PKI puts several requirements on participating entities
- Offload some of these requirements to a stronger entity supporting constrained entities
- Facilitated using authorization and validation lists (AVLs) – An advanced whitelist

# Two modes of operation

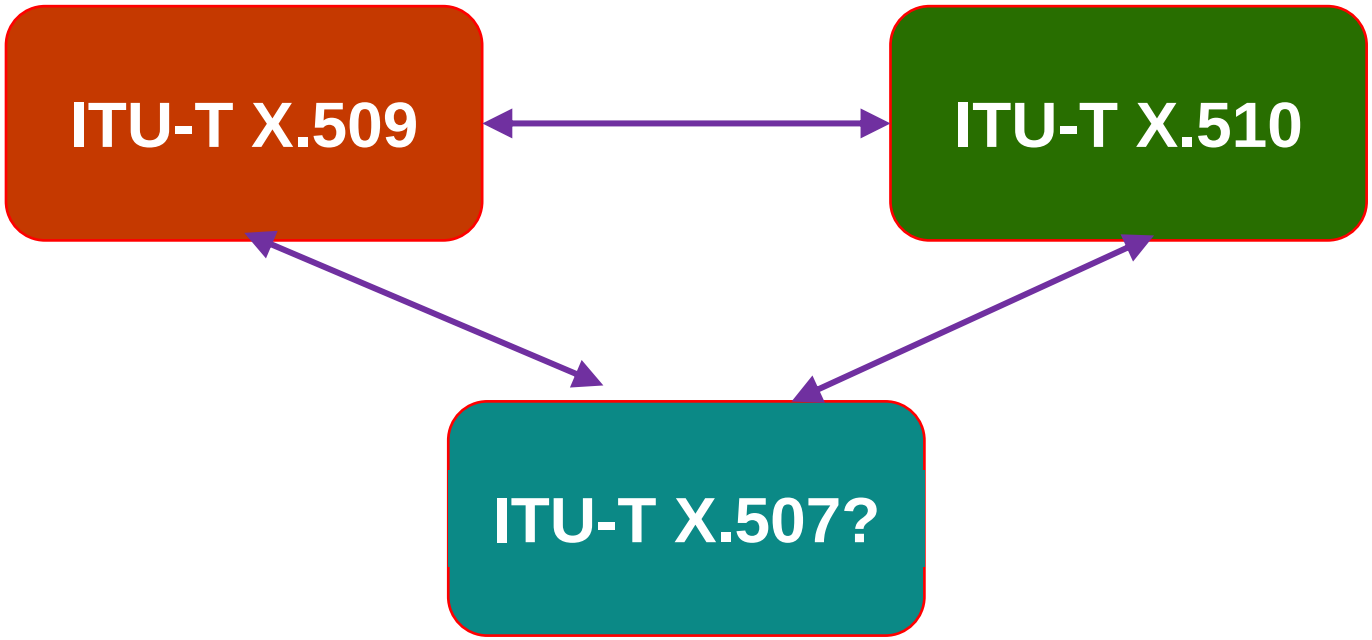
- Environments without resource constraints
- Environments with resource constraints:
  - Storage constrained
  - Processing constrained
  - Limited bandwidth
  - Time requirements, e.g., 1 ms validation time

# Authorizer relationships



# A trilogy

**Three specifications complementing each other:**



# Standards activities

## Rec. ITU-T X.509 | ISO/IEC 9594-8:

- Extension of the AVL concept to have comprehensive support for IoT devices
- Refine the attribute specification
- Clearly define the relationship between PKI and PMI

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

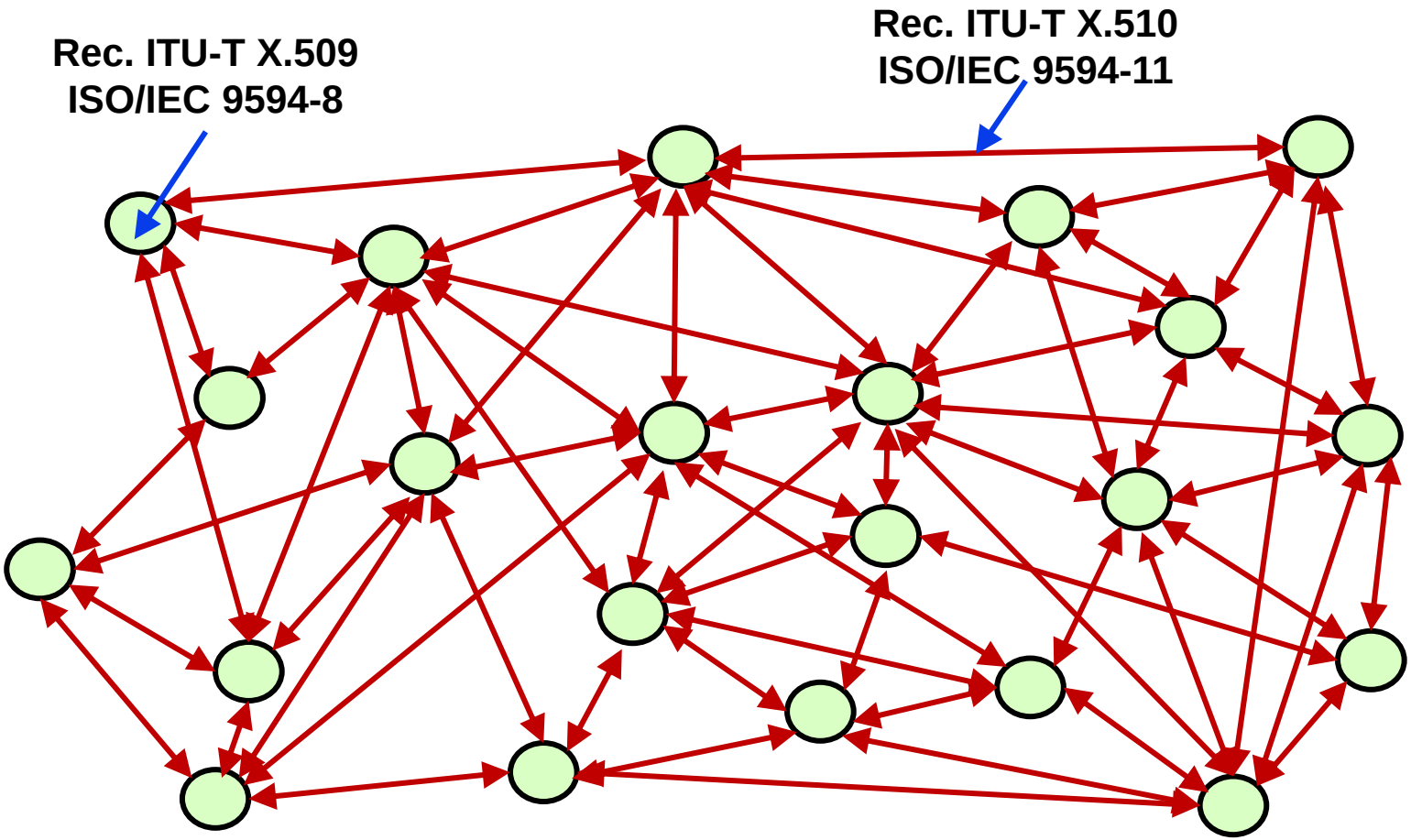
- Final specification exists
- Amendment in progress (key confirmation, cryptographic algorithm definitions, E2E support with intermediate systems, etc.)
- Protocol for protecting other protocols with migrating capabilities

# Standards activities

## Rec. ITU-T X.507(?) | ISO/IEC 9594-12:

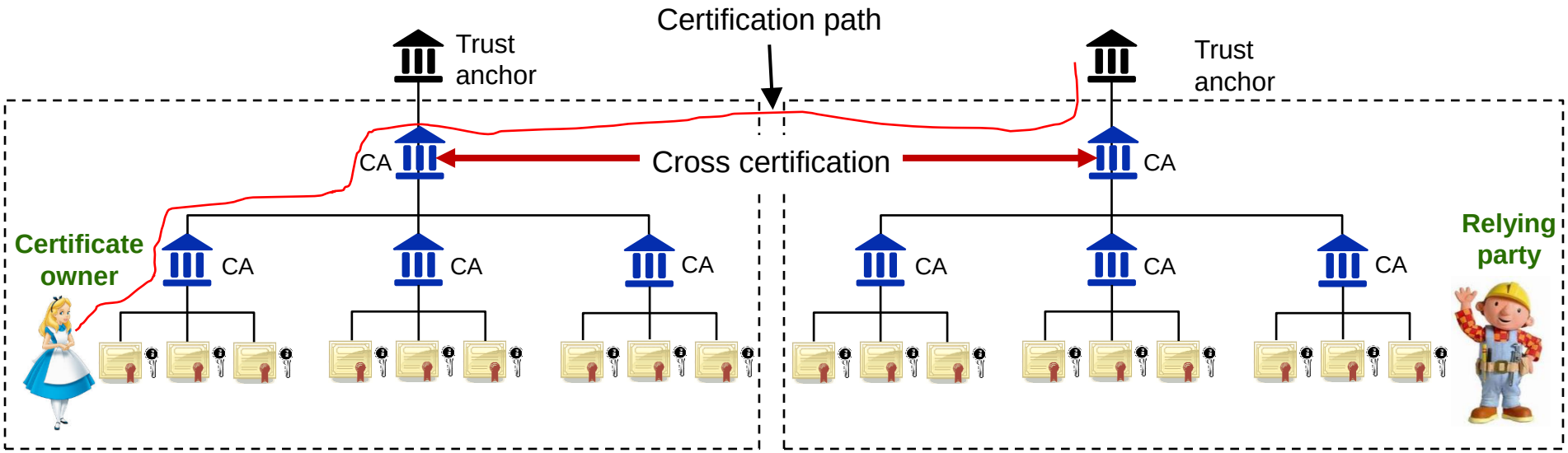
- Expect approval September 2022
- Somewhat detailed tutorial type of description of cryptographic algorithms with reference to relevant NIST and IETF specifications
- Future version to include post-quantum algorithms
- Some mathematics behind cryptographic algorithms
- PKI best practice

# Key management



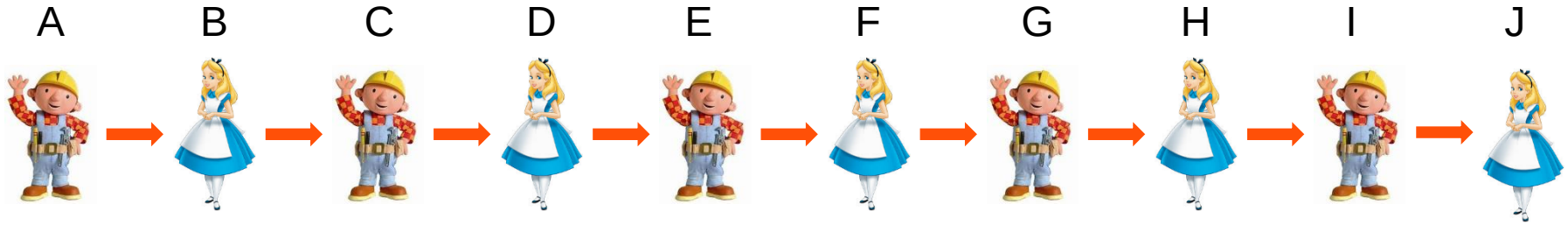
# Decentralized public-key infrastructure
# DPKI
# (ITU-T X.508?)

# Public-key infrastructure (PKI) long certification path



# 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**