ITUWebinars

# Fourth ITU-T X.509 Day

5 September 2025
13:00-16:00 CEST

itu.int/go/X509_4

# Decentralized Public-Key infrastructure

# DPKI

Erik Andersen
era@x500.eu

# Two types of certificates in current ITU-T X.509

## Public-key infrastructure (PKI)

**Public-key certificate:**

Certification of identity

Issued by certification authority (CA)

## Privilege Management infrastructure (PMI)

**Attribute certificate:**

Certification of privileges

Issued by attribute authority (AA)

# Two types of certificates in DPKI & the future ITU-T X.509

## Public-key infrastructure (PKI)

**Public-key certificate:**

Certification of identity

Issued by certification authority (CA)

**Attribute certificate:**

Certification of privileges

Issued by attribute authority (AA)

# 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**

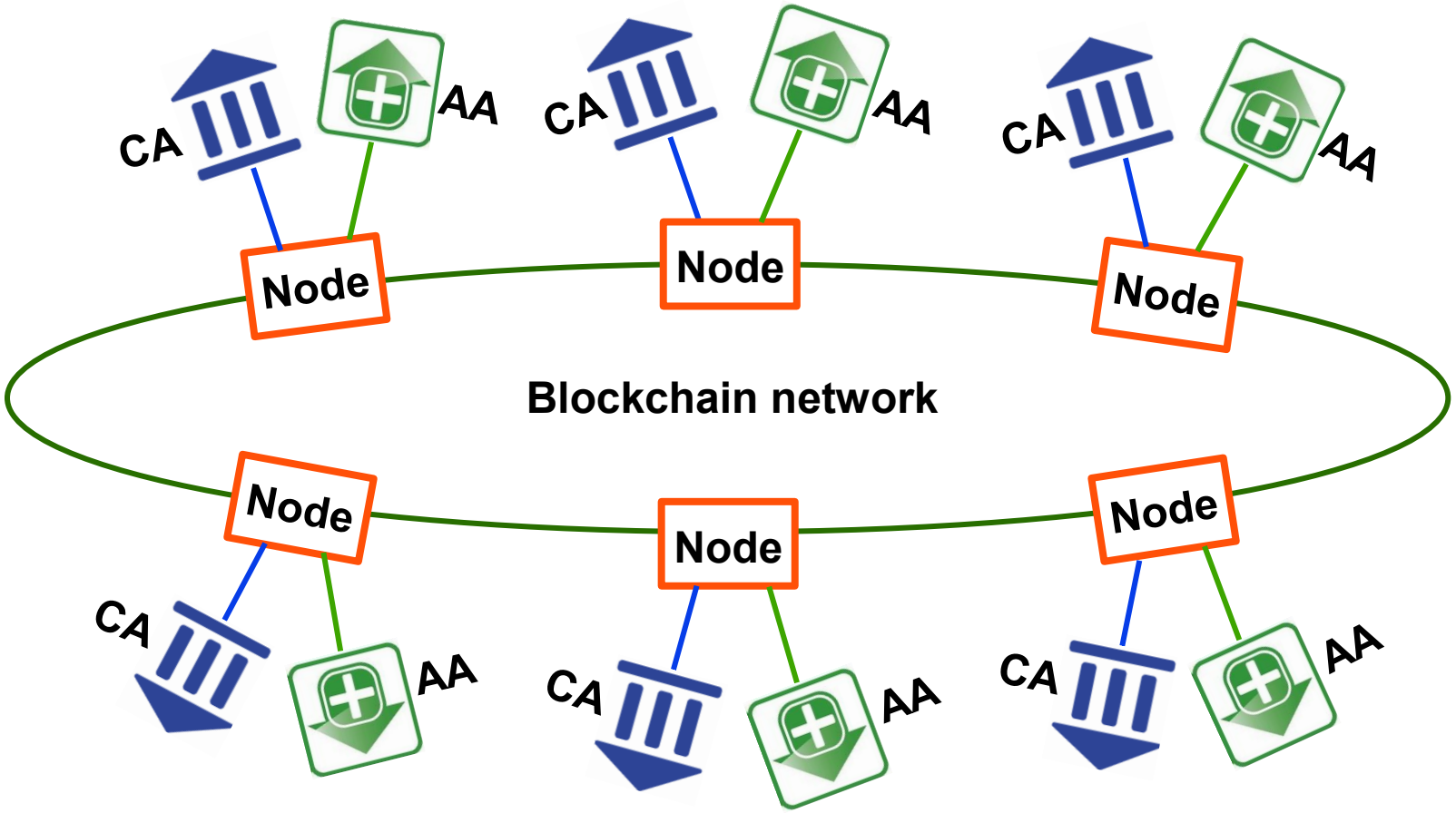
**PKI domains federated using blockchain technology**

**Decentralized public-key infrastructure (DPKI)**

# Design approach

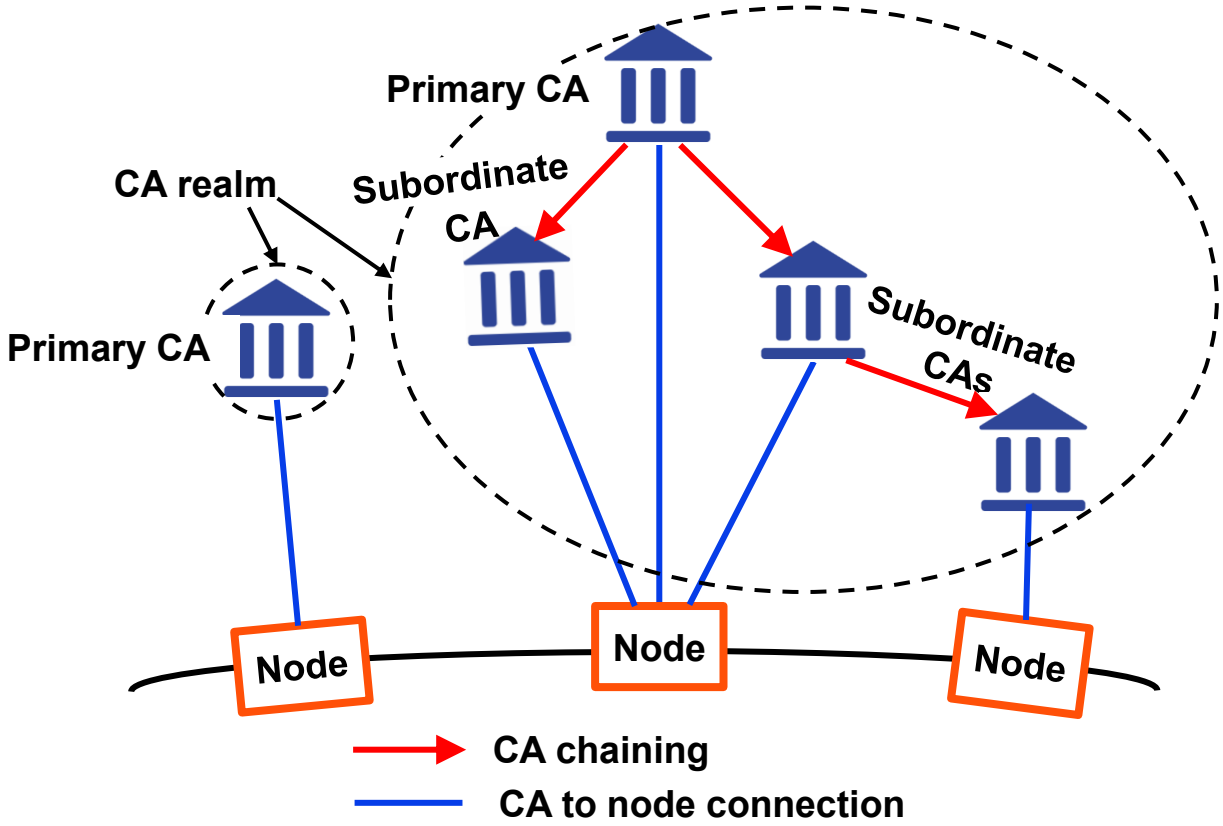
- Goal: ITU-T Recommendation | ISO/IEC International Standard
- Current blockchain platforms cannot be used as normative references
- Current blockchain platforms may be used as “inspirations” when specifying a standardized platform
- Hyperledger Fabric is a possible choice, but have more features than needed
  - Used by IBM for business support
  - Has extensive documentation
  - Proven technology
  - Pluckable consensus protocol
  - Includes a state database
- Stellar Consensus Protocol (SCP) possible “inspiration” for consensus protocol
- Much processing is PKI specific
- Ensure cryptographic algorithm migration capabilities

# Positions of CAs & AAs vs the blockchain network




**The CAs & AAs are outside the blockchain network**

# Hierarchy of CAs




**CA realm: A primary CA with all its subordinate CAs (if any)**

**Different CA realms cannot connect to the same node**

# Two types of DPKI

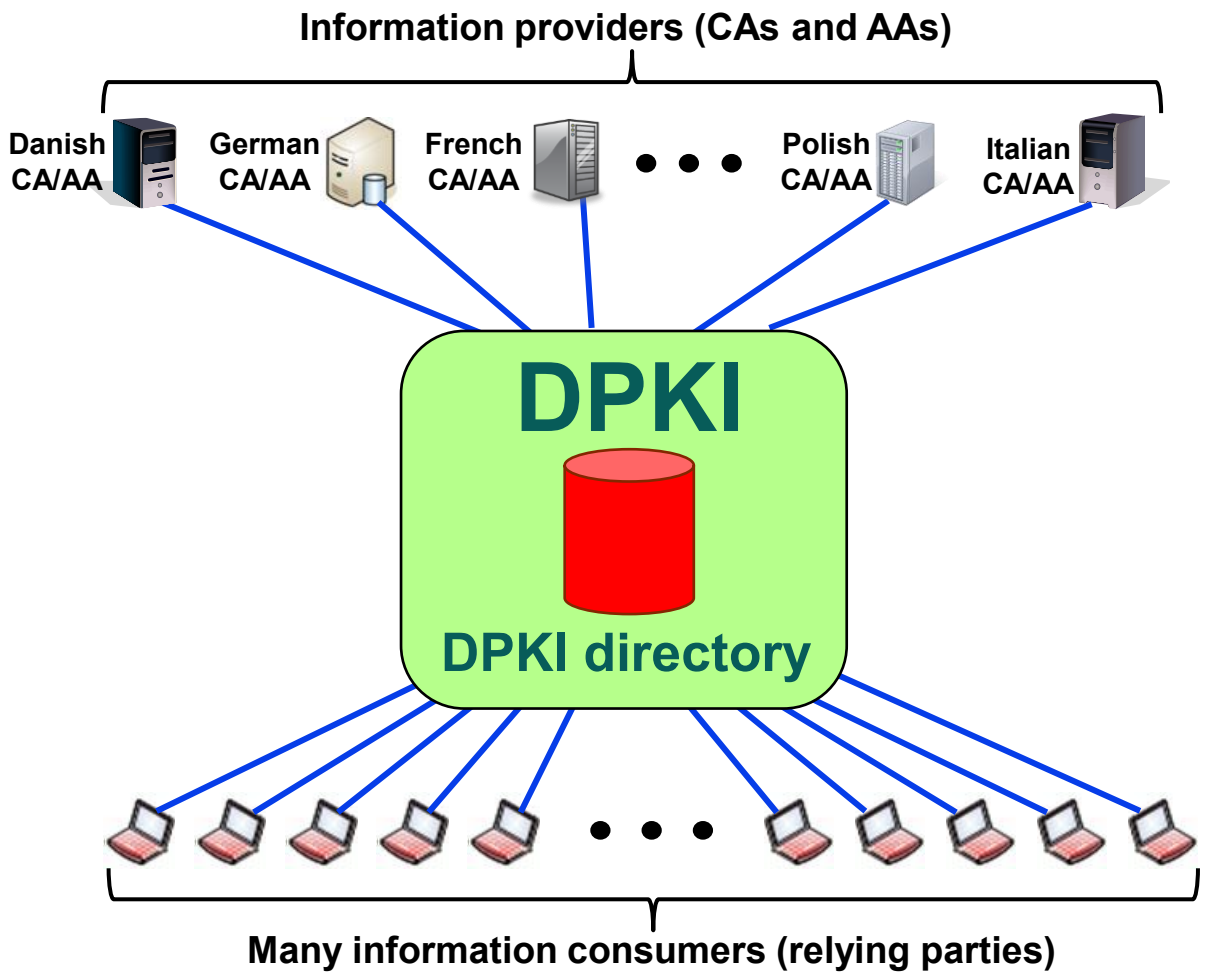
- Authority DPKI
  - Controle of participation by country authorities
- Private PKI
  - By request from China
  - Control of participants by organisation

# CA registration

- Primary CAs have self-signed CA certificates
- Only “authorized” CAs should be accepted as primary CA and thereby be trusted as being well-behaving
- A primary CA in authority DPKI is authorized by the country Registration Authority (RA) and given an object identifier easy to check
- For establishment of country RA see:

  https://oid-rep.orange-labs.fr/doc/country-OIDs.htm

# DPKI information providers and consumers




**Different from other blockchain platforms: No interaction between service providers**

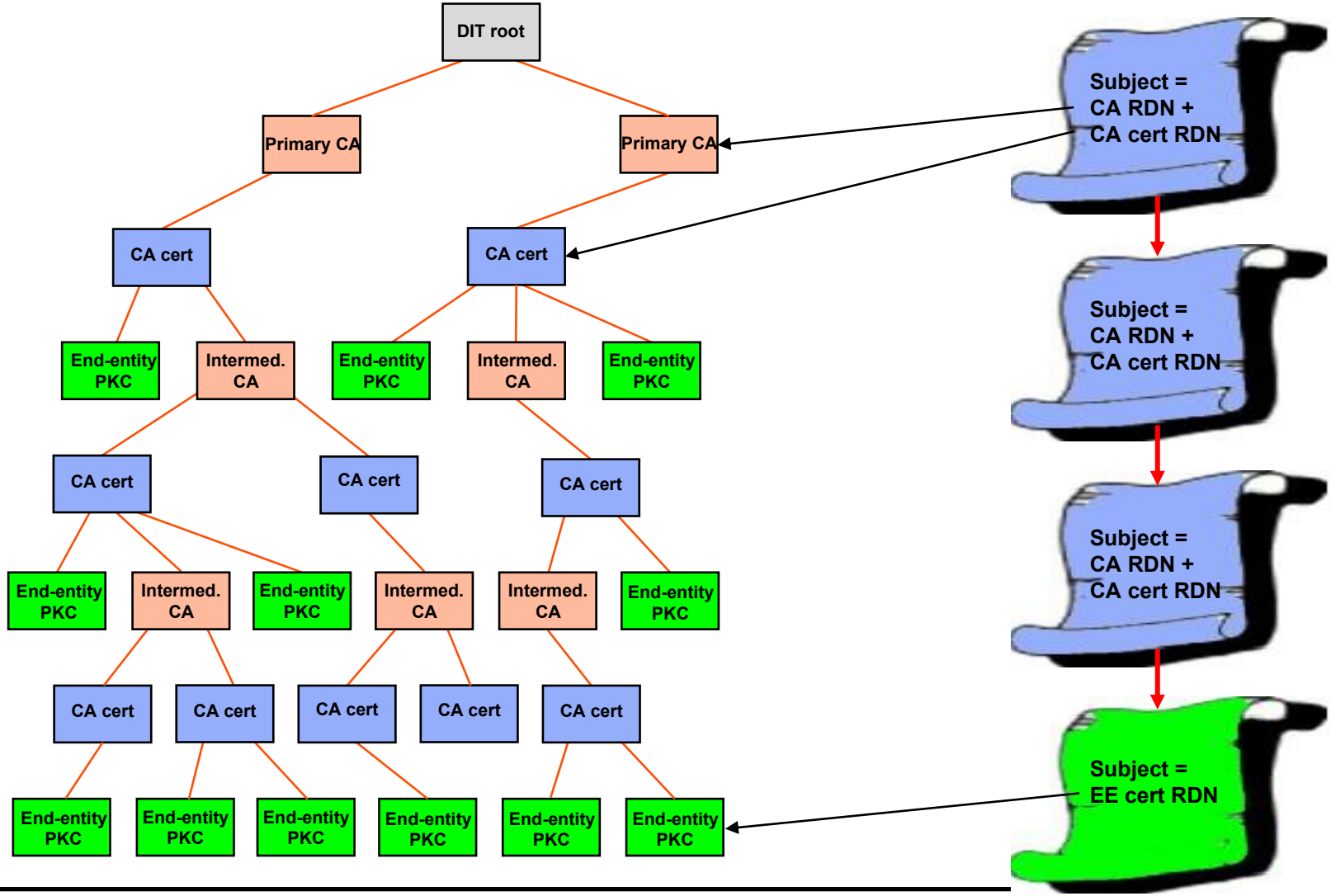
# Authority relationship

- Certification authorities (CAs) and attribute (AAs) authorities are “outside” the blockchain
- CAs and AAs unmodified except for interface to local blockchain node
- Only certificates of interest outside the local PKI domain should be inserted in the DPKI
- Short lived certificates should not be inserted in the DPKI
- That status information (revocation information) is available in a DPKI is signalled in an extension

# DPKI directory

- Directory described in terms of the X.500 directory specifications
- Easy locally mapping to LDAP
- Holds information about certificates (public-key and attribute certificates) and their status
- Tight specifications to ensure that the directory information tree (DIT) has exactly the same structure in all nodes

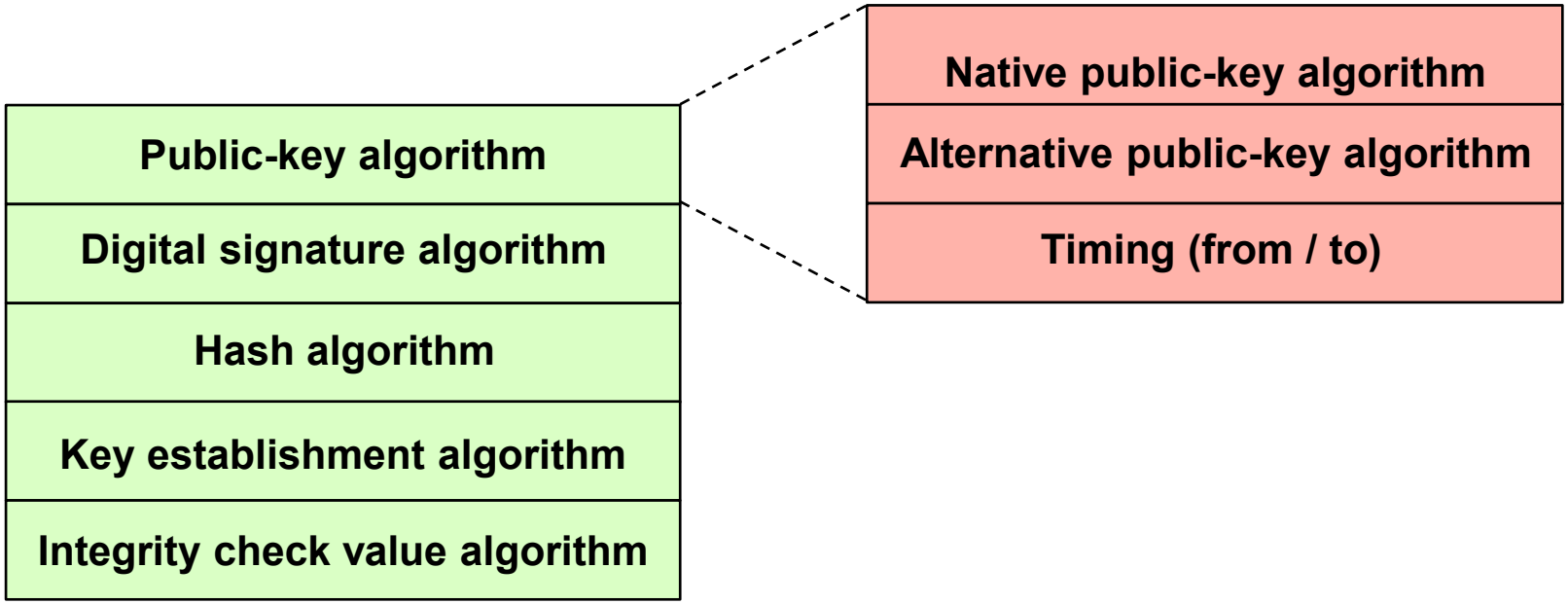
# DIT structure vs. certification path



# Checking of input to DPKI

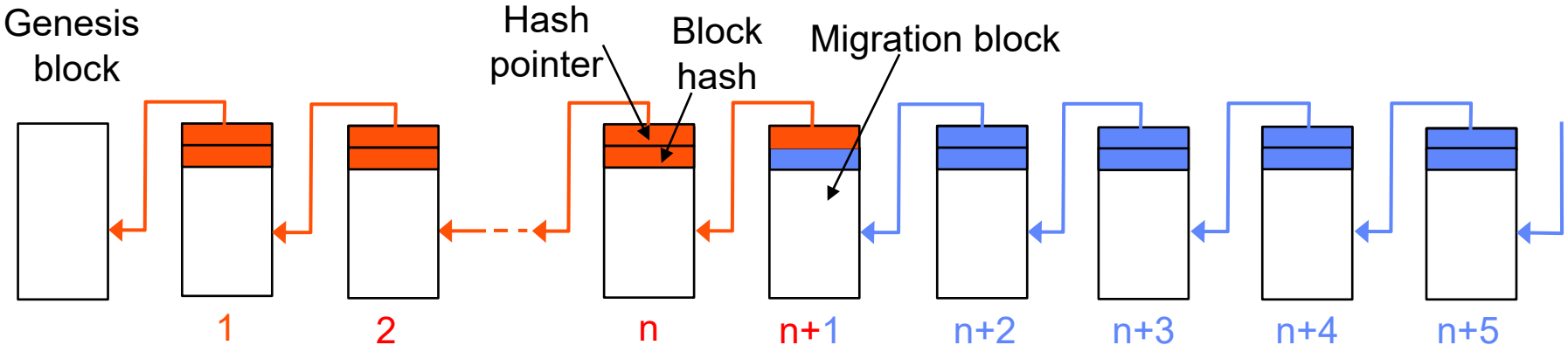
- Ensure that when a certificate or certificate status information has passed successfully through the consensus process, it will then not fail the final update to the DPKI directory
- Ensure the operation between a CA/AA and a node is valid
- Ensure a (public-key or attribute) certificate has the right content
- Ensure the appropriate certificate extensions are present, and unwanted extensions are absent

# Configuration file

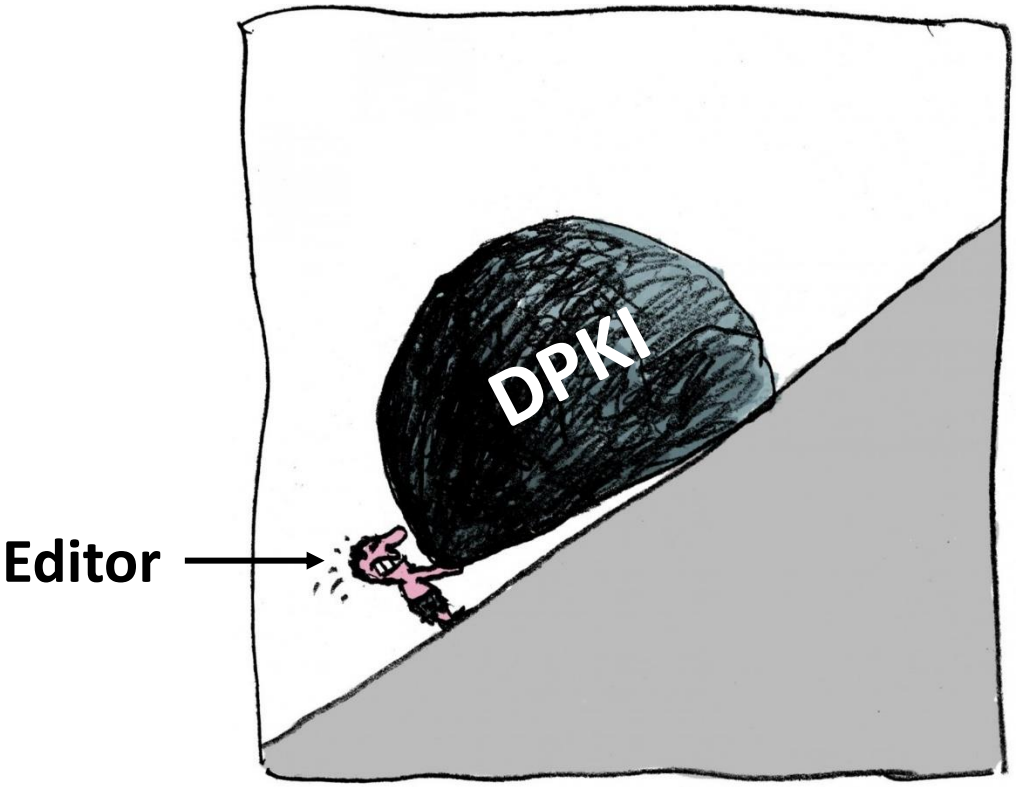



- Holds information about cryptographic algorithms used by DPKI
- During migration period, two algorithm are specified for each type of algorithm
- Start and stop of migration period.
- Updated by management operations

# Migration of hash chain




- **Nodes not migrating at the same time**
- **The migration block may be different for different nodes**
- **The migration block holds information about the previously used hash algorithm**




# END