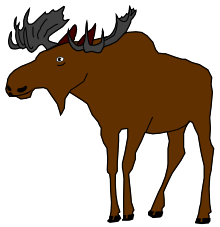


PKI & cybersecurity

ITUEvents

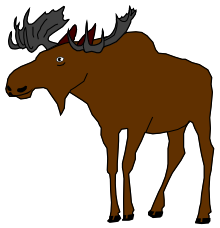
Fifth ITU-T X.509 Day

12 May 2026
Geneva, Switzerland

itu.int/go/X509_5

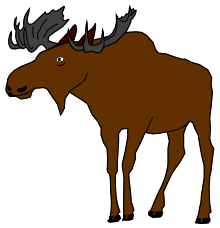
Towards decentralized PKI

Erik Andersen
era@x500.eu



Public-key infrastructure (PKI)

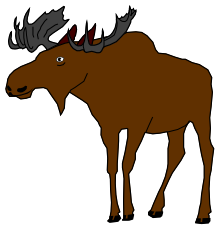
- **Since 1988 ITU-T X.509 has been:**
  - **Identity Management**
  - **The source of trust**
  - **Basis for protocol cybersecurity**
- **Since 1997 ITU-T X.509 has also been:**
  - **Privilege management (Authorization)**



Relationship between PKI and secure protocol design

PKI is the basis for establishing secure protocol design by secure use of cryptographic algorithm

- **Asymmetric algorithms:**
  - **Public-key algorithms**
  - **Digital signature algorithms'**
  - **Symmetric key establishment**
- **Symmetric algorithms**
  - **Symmetric key (encryption) algorithms**
  - **Integrity check value algorithms**
  - **Hash algorithms**



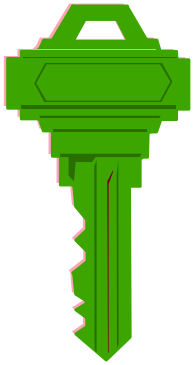
Public-key concept

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

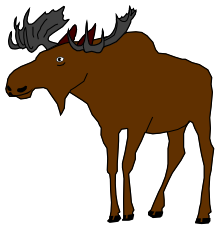
One key is the **private key** and has to be kept protected and secret by the owner.

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

Private key

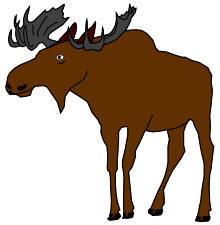


Public key



Three types standards

- **Procedure standards**
  - ISO/IEC 27001, *Information security management systems – Requirements*
  - ISO/IEC 27002, *Information security controls*
- **Requirement on cybersecurity in ICT products**
  - ETSI EN 303 645, *Cyber Security for Consumer Internet of Things: Baseline Requirements*
  - IEC 62443-3-3, *Systems security requirement and security levels*
  - IEC 62443-4-1, *Secure product development lifecycle requirements*
  - IEC 62443-4-2, *Technical security requirements for IACS components*
- **Fulfilling requirement on cybersecurity in ICT products**
  - ITU-T X.506 | ISO/IEC 9594-xx, *General methods for migration of cryptographic algorithms*
  - ITU-T X.508 | ISO/IEC 9594-12, *Key management and public-key infrastructure establishment and maintenance*
  - ITU-T X.509 | ISO/IEC 9594-8, *Public-key and attribute certificate frameworks*
  - ITU-T X.510 | ISO/IEC 9594-11, *Protocol specifications for secure operations*
  - IEC 62351 series



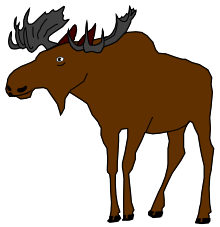
Inside or outside

It makes a difference whether you are outside or inside

Identifying security requirements →

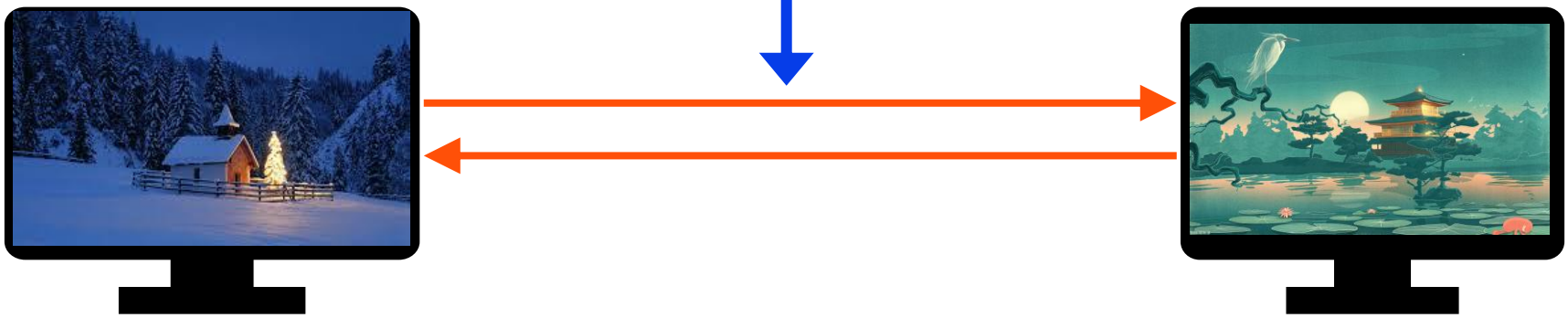
← Fulfilling security requirements

Identifying requirements is much easier than fulfilling requirements



Machine-to-Machine (M2M) communication

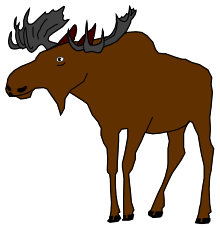
Securing this communication



Software built in Haparanda, Sweden

Software built in Kyoto, Japan

A digital signature generated in Haparanda shall be verifiable in Kyoto and visa verse



Strength of symmetric keys

A 64-bit symmetric encryption key is today considered week. A 64-bit key has the following number of combinations:

$$2^{64} = 18446744073709551616 \cong 1.84 \times 10^{19}$$

The Universe is considered 13.8 billion years old, which is

$$1.38 \times 10^{10}\ years$$

$$1\ year = 365 \times 24 \times 60 \times 60 = 31,536,000 \cong 3.15 \times 10^{7} seconds$$

$$Number\ of\ seconds\ elapsed\ since\ start\ of\ Universe =$$

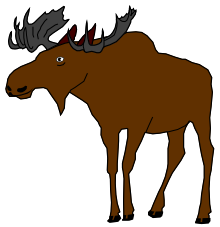
$$1.38 \times 10^{10} \times 3.15 \times 10^{7} \cong 4.35 \times 10^{17}$$

A 64-bit key has more combinations than seconds elapsed since start of Universe

Other values:

2^{128} = 340282366920938463463374607431768211456

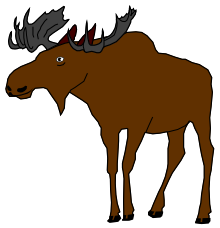
2^{256} = 115792089237316195423570985008687907853269984665640564039457584007913129639936



“Key under the mat”

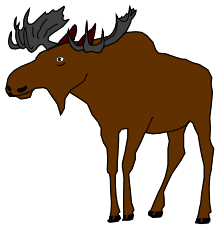
With the key under the mat, it becomes easy to break into the house

Instead of trying to break an encryption, try to find the symmetric key



How symmetric keys are established

- By key distribution from key distribution centre (KDC)
  - Risky if not implemented correctly
  - Using symmetric technique
  - Not scalable
- By communication between any two partners
  - Diffie-Hellman key agreement
  - Key encapsulation mechanism (KEM)
  - Using asymmetric technique



Diffie-Hellman key exchange

Discrete logarithm problem:
Find x if everything else is public

Public-key

Private key

$$y = g^x \pmod{p}$$

Generator

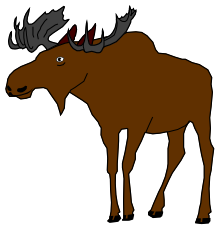
Large prime

Alice

Bob

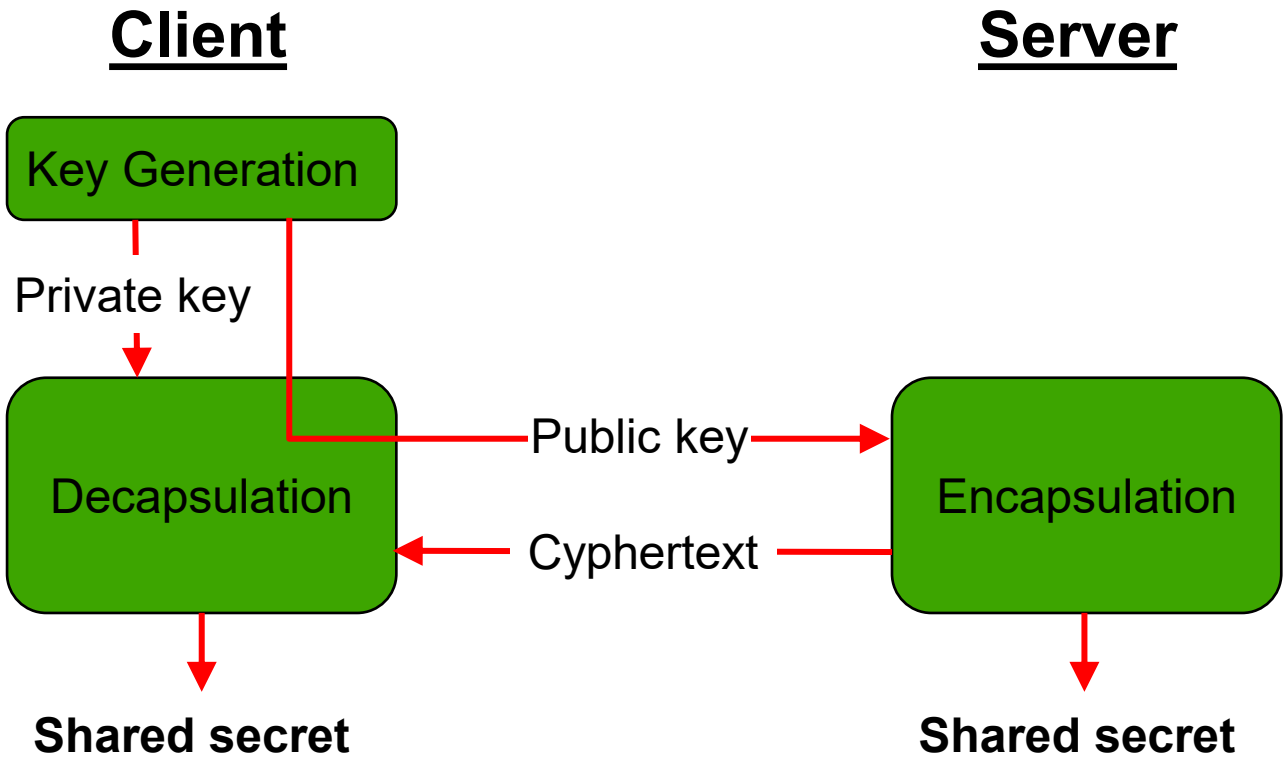
Alice's DH public key

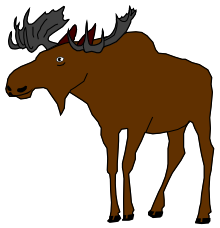
Bob's DH public key



Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)

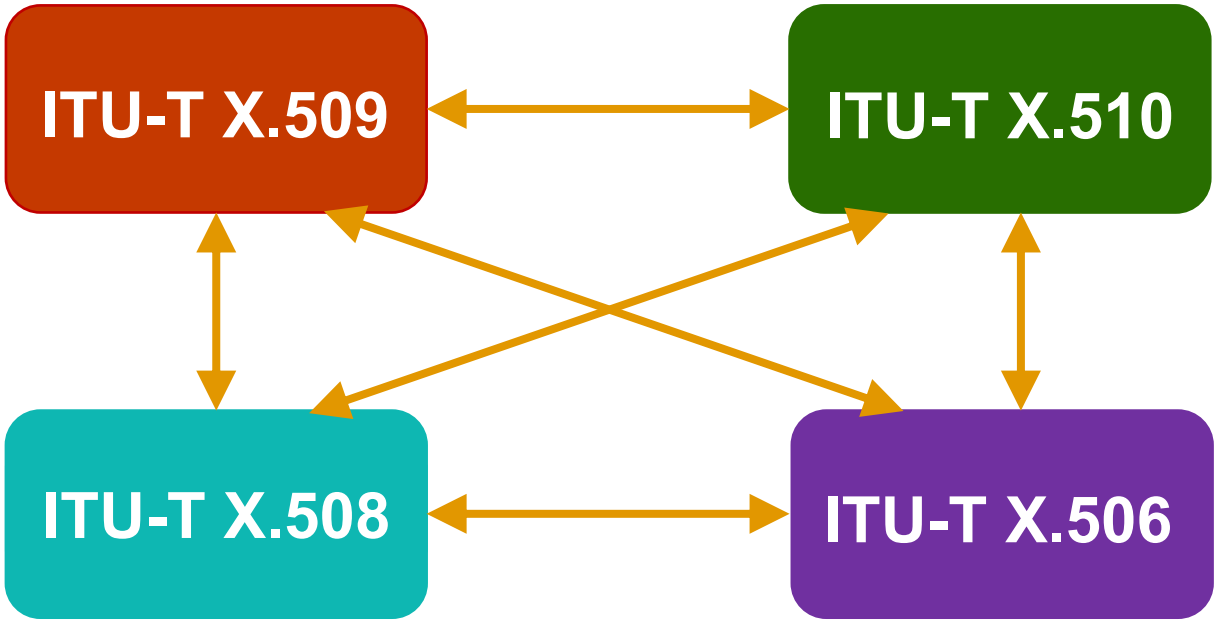
Encapsulation using public key of recipient;
decapsulation using private key of recipient



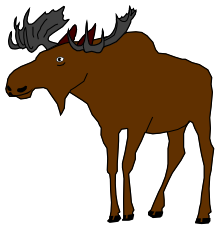


Four related specifications

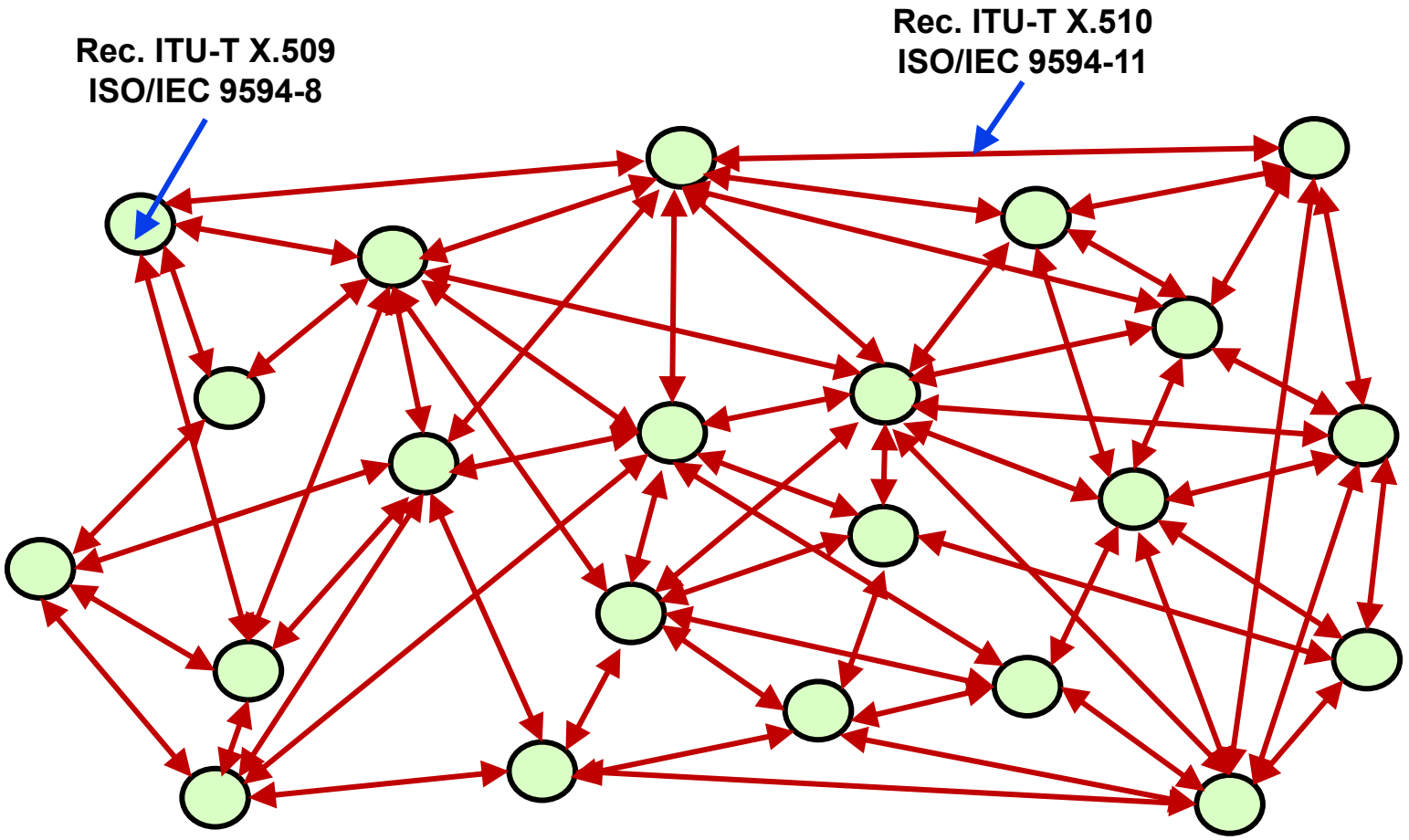
Four specifications complementing each other:

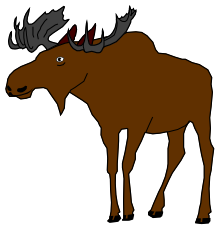


- Minimum overlap
- Mutual references
- DPKI to be added



Large interconnected ICT network





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

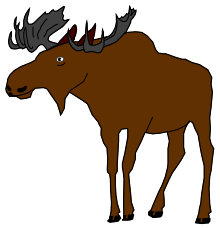
ITU-T X.509 | ISO/IEC 9594-8 is the framework for public-key certificates and attribute certificates

The European Commission (eDelivery) definition:

A Public Key Infrastructure (PKI) is a set of roles, policies, procedures and systems needed to create, manage, distribute, store and revoke ~~digital~~ public-key certificates.

Currently attribute certificate is part Privilege Management Infrastructure (PMI)

Plan to integrate attribute certificates into Public-Key Infrastructure (PKI)



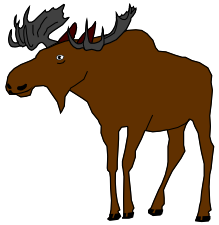
38 years with Zero Trust

Zero trust is an old ~~modern~~ security strategy based on the principle never trust, always verify. Instead of assuming everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an open network.

PKI has allowed for zero trust since 1988

The same for zero-knowledge proof (we call it proof of possession (PoP))

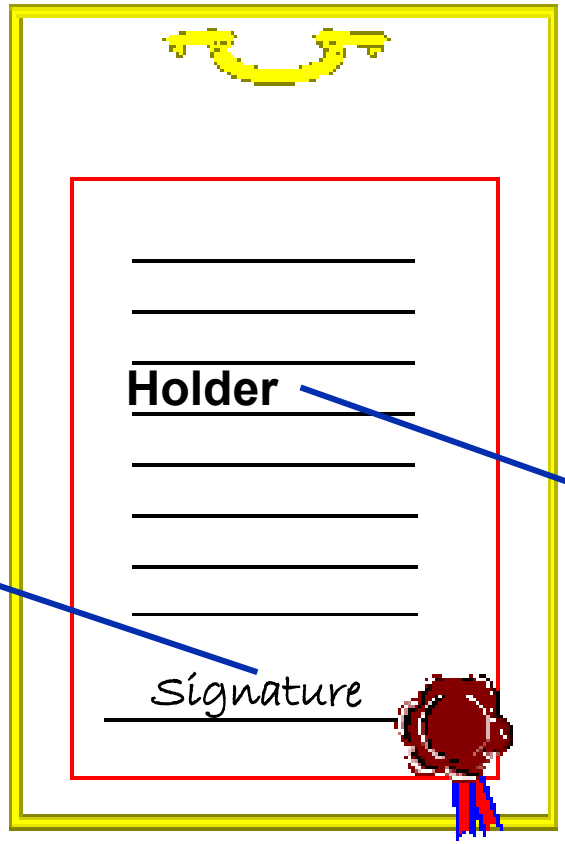
Old wine in a new bottle?



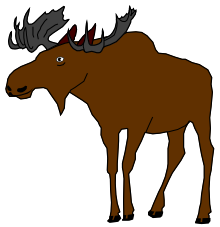
Relationship between attribute & public-key certificates

Attribute certificate

Signing public-key certificate

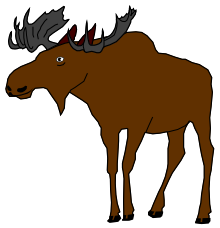


Holder public-key certificate



Crypto Agility

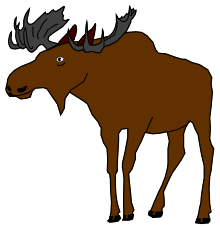
The ability to react quickly and appropriately to change



ITU-T X.506

General methods for migration of cryptographic algorithms

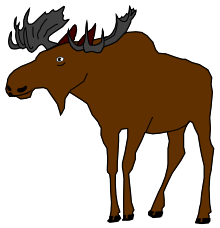
- Som basic ideas in ITU-T X.510 | ISO/IEC 9594-11 already in 2020 (6 years' head start)
- Migration consideration moved out of ITU-T X.510 | ISO/IEC 9594-11 to get visibility
- General on why
- Basic principle to avoid bulk migration
- Plug-in concept for cryptographic algorithms
- Tools for migration of certificates, etc. in 2019
- Tools for migrating protocols
- Overview of activities within IETF



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

Protocol specifications for secure operations

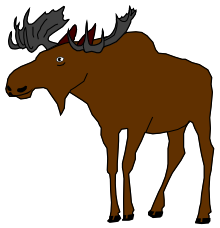
- General principles for secure protocol operation on the application layer
- Formal specification of cryptographic algorithms for inclusion in protocols including the new PQC algorithms
- Wrapper protocol allowing protection of other imbedded protocols
- Specification of utility applications protected by the Wrapper protocol
- Updated certificate signing request (CSR) to support migration



ITU-T X.508 | ISO/IEC 9594-12

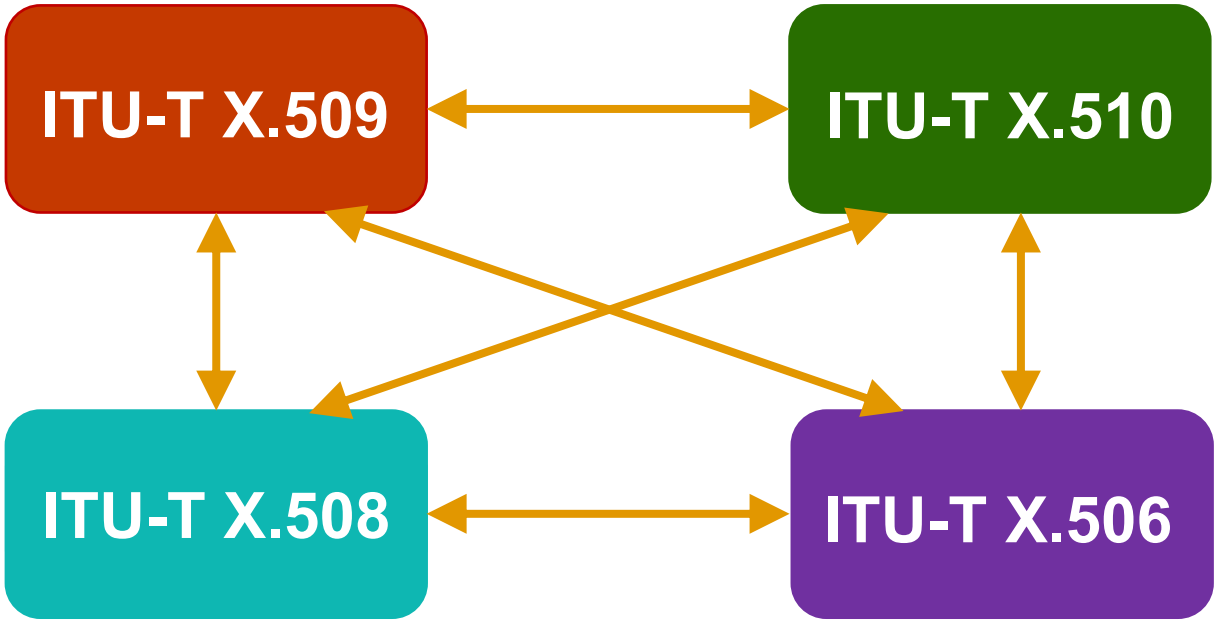
Key management and public-key infrastructure establishment and maintenance

- Comprehensive description of cryptographic algorithms (to be expanded with PQC algorithms)
- Mathematics behind cryptographic algorithms
- PKI establishment
- Certificate recommendations
- Certificate life management
- Trust establishment
- Etc.

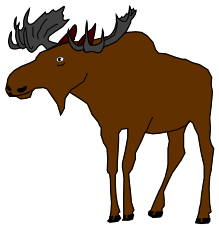


Four related specifications

Four specifications complementing each other:

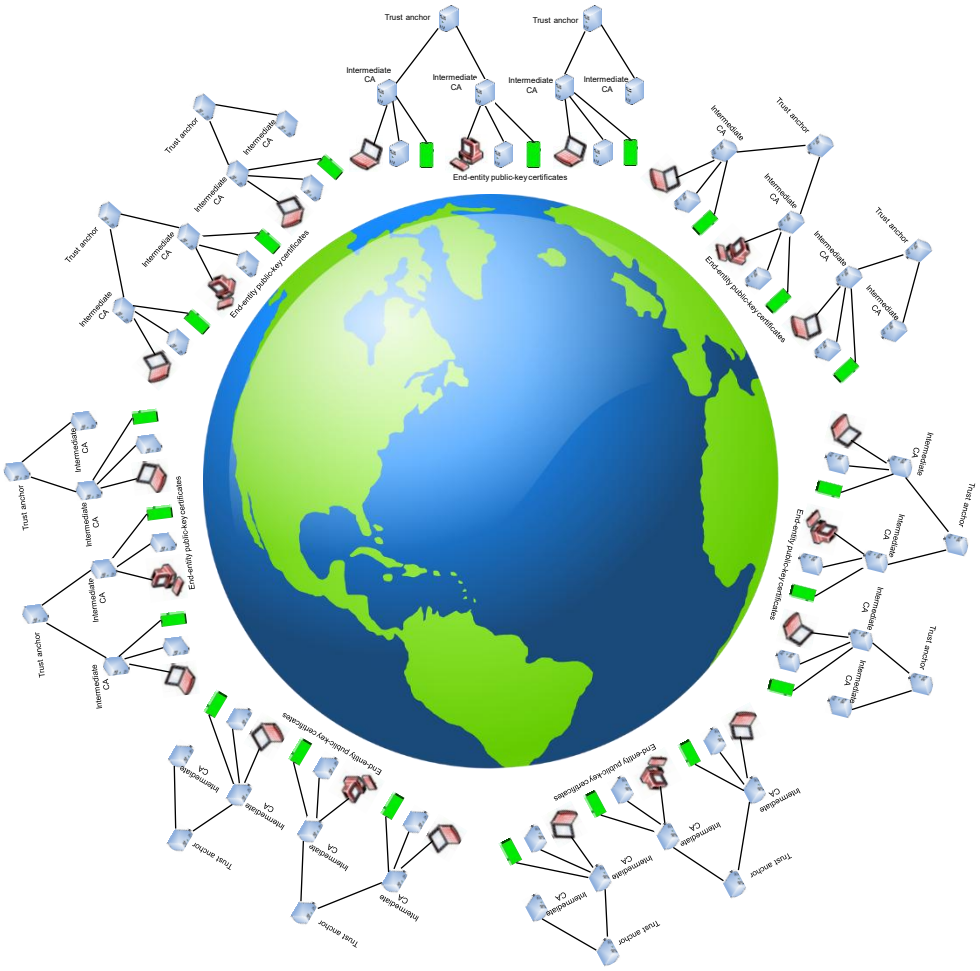


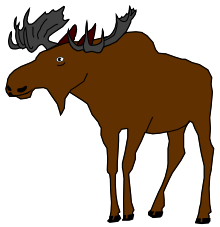
- Minimum overlap
- Mutual references
- DPKI to be added



Decentralized Public-Key Infrastructure (DPKI)

A world-wide federated PKI





Trust by consensus

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

↓

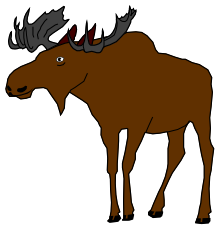
A PKI where trust is obtained by consensus

↓

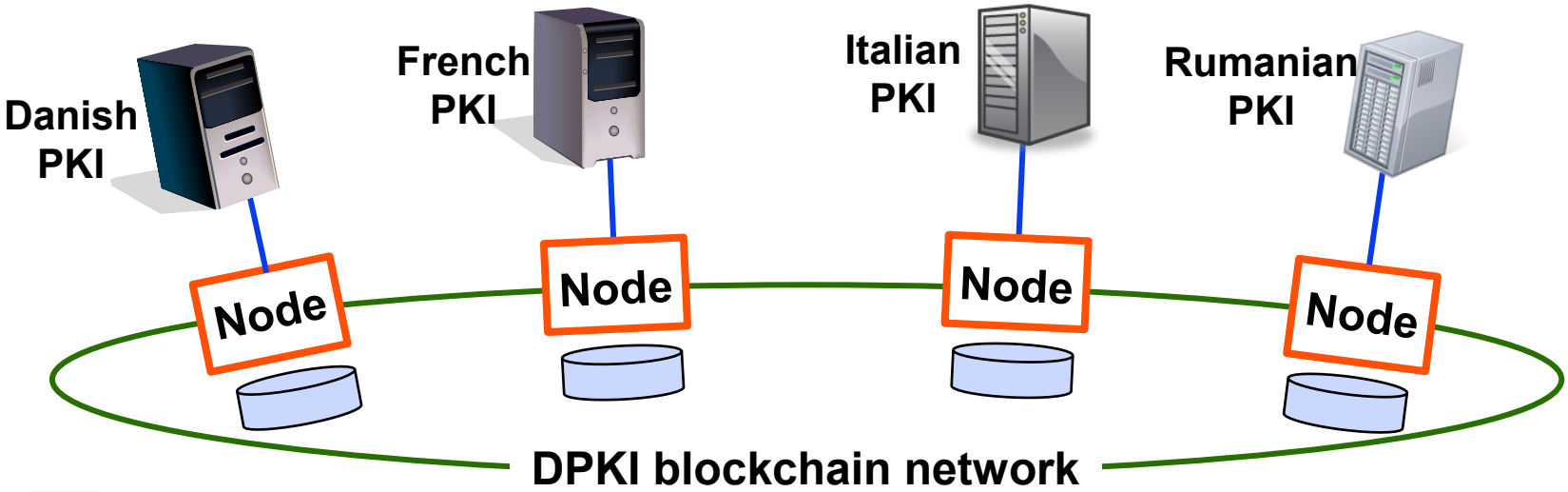
PKI domains federated using blockchain technology

↓

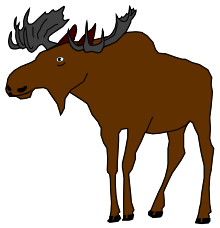
Decentralized public-key infrastructure (DPKI)



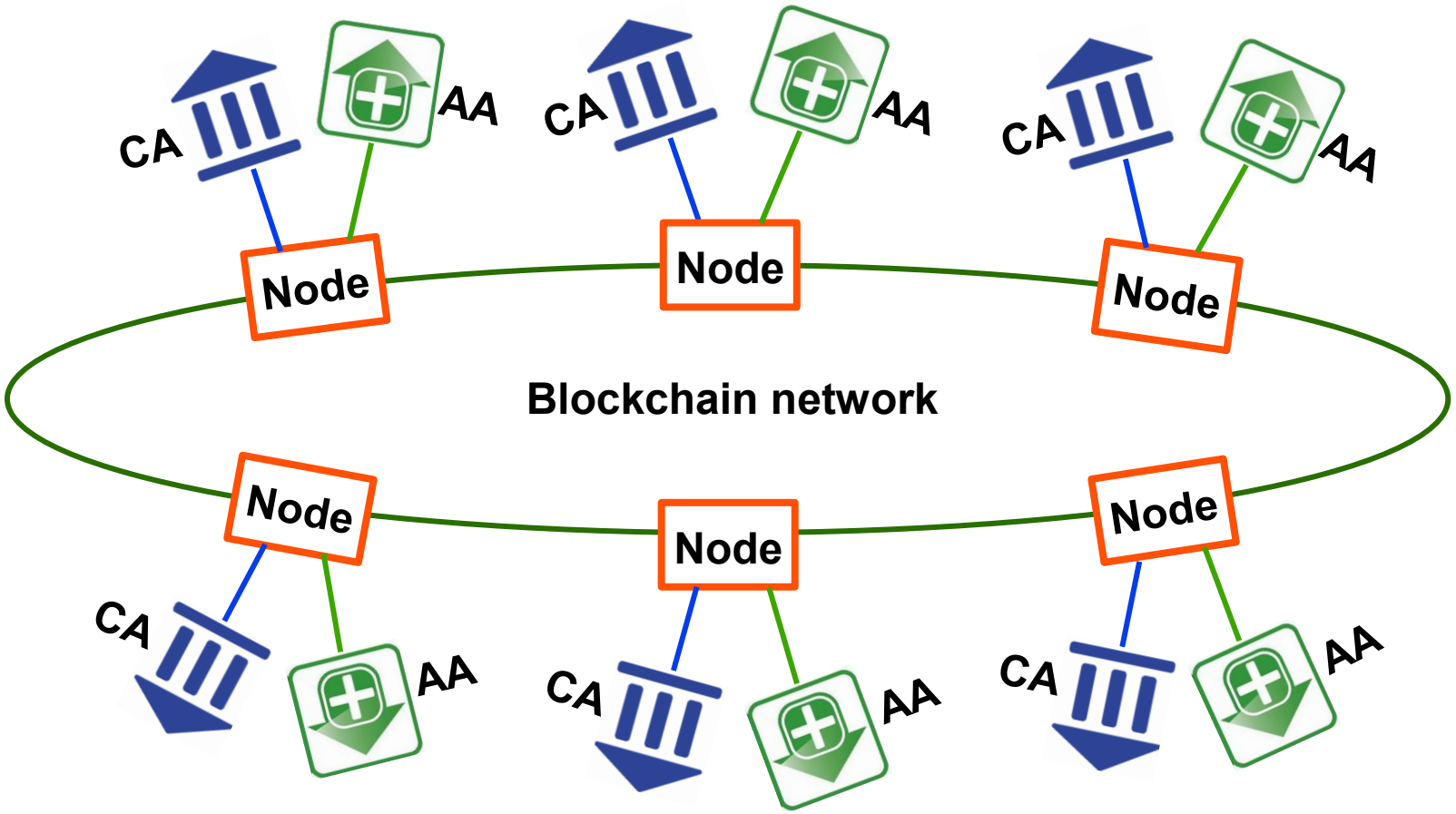
Decentralized Public-Key Infrastructure interconnecting PKI domains



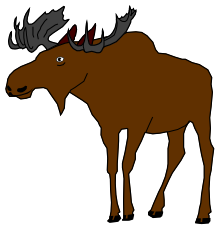
- Trust by consensus
- DPKI interconnect national PKIs e.g., for support of single market
- The concept of PKI is not changed
- PKI information (certificates and status) globally available by a DPKI directory part beginning of the ledger
- All PKI information in the DPKI directory validated and genuine
- Migration tools for cryptographic algorithm
- Some harmonisation of participating PKIs may be necessary



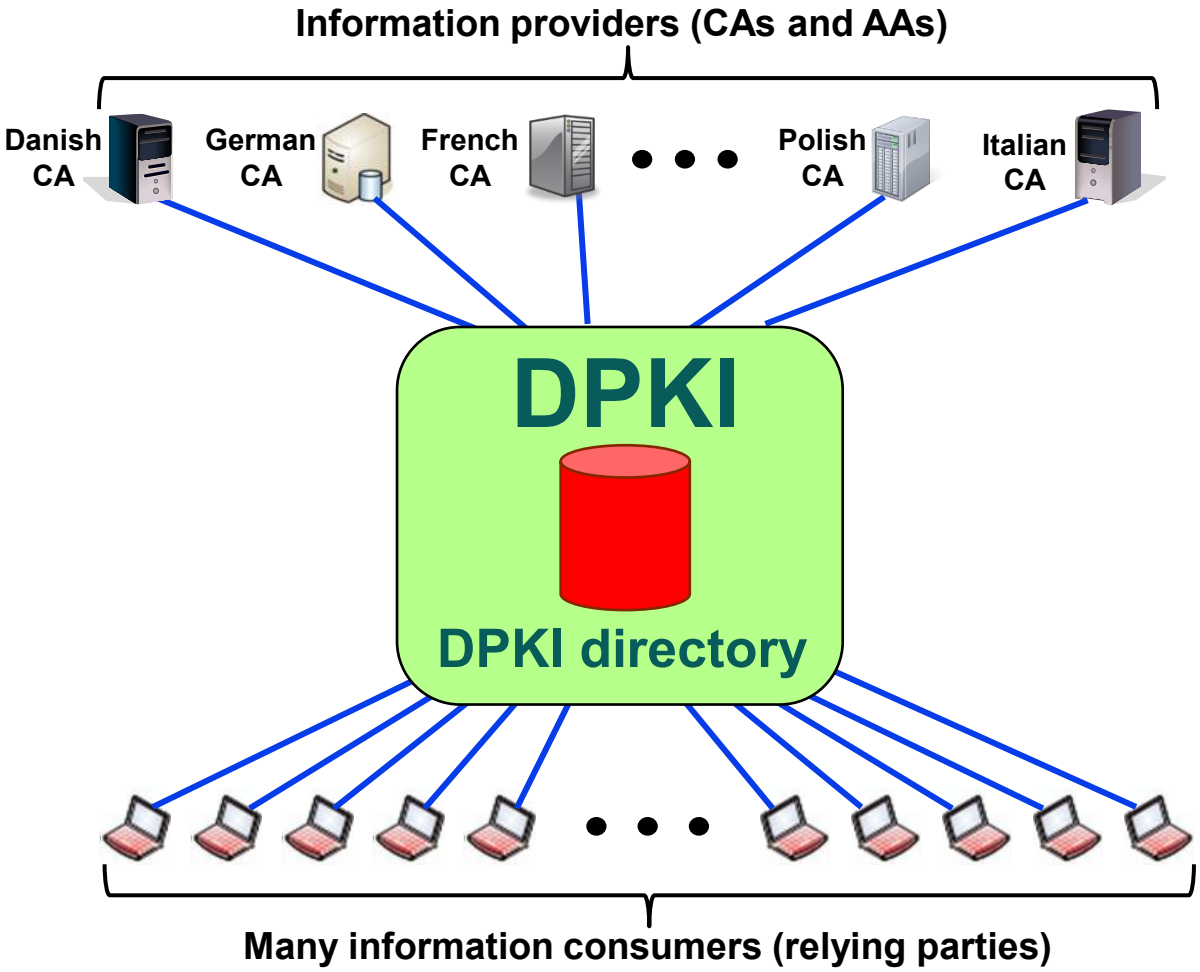
Positions of CAs & AAs vs the blockchain network



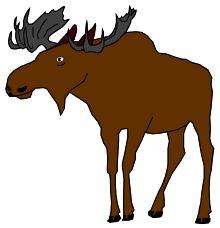
The CAs & AAs are outside the blockchain network



DPKI information providers and consumers

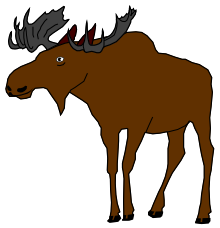


Different from other blockchain platforms: No interaction between service providers



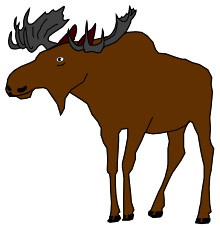
DPKI directory

- Directory described in terms of the X.500 directory specifications
- Easy local 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



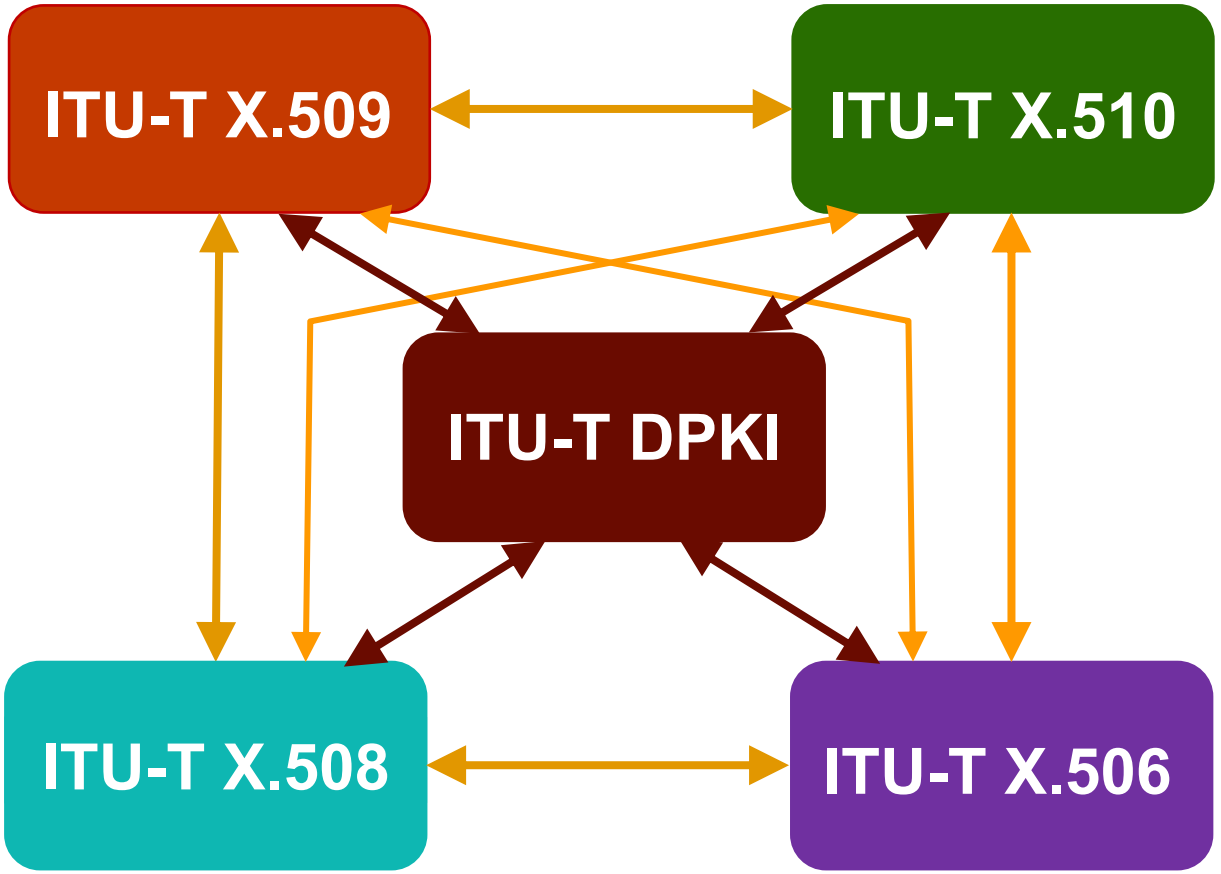
Checking of input to DPKI

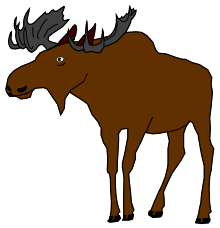
- Ensure that when a certificate or certificate status information has passed successfully through the consensus process, it will then not fail the final update to the DPKI directory
- Ensure the operation between a CA/AA and a node is valid
- Ensure a (public-key or attribute) certificate has the right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



Five related specifications

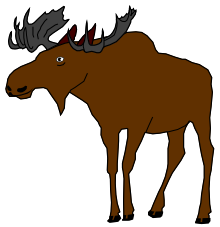
Five specifications complementing each other:

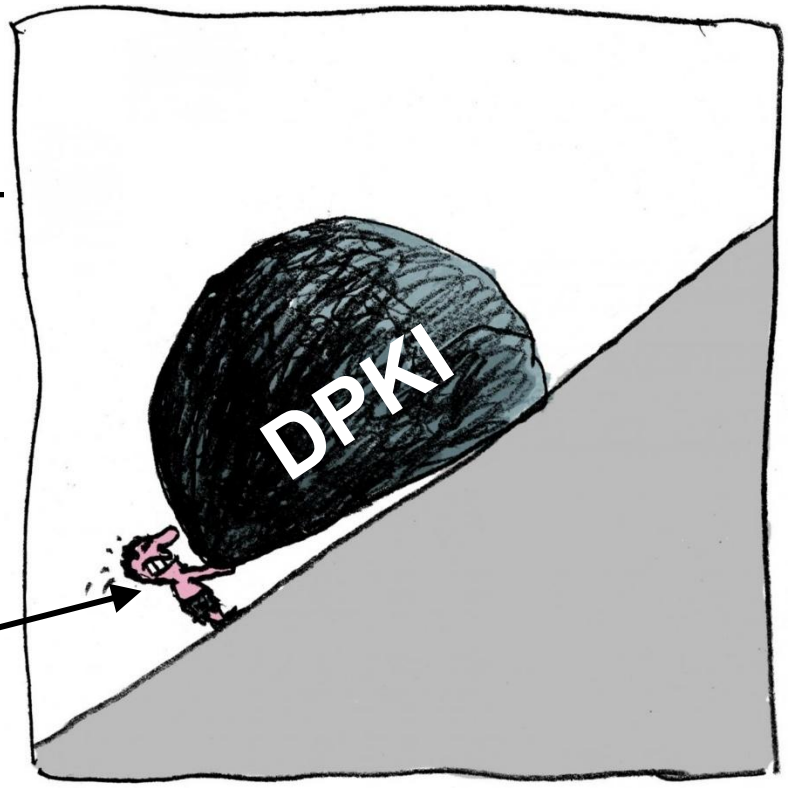




DPKI interactions

- **ITU-T DPKI interacts with:**
  - **ITU-T X.509 for PKI related specifications**
  - **ITU-T X.510 for secure protocol support**
  - **ITU-T X.508 for cryptographic algorithm support**
  - **ITU-T X.506 for cryptographic algorithm migration support**





Korea
China
Editor

END