Current developments in Q.11/17

Jean-Paul Lemaire
Q.11/17 Rapporteur

ITU Workshop on "Improving the security of signalling protocols“

29 November 2021

Role of Q.11/17

Q.11/17, Generic technologies (such as Directory, PKI, Formal languages, Object Identifiers) to support secure applications is responsible of several series of Recommendations:

- X.500 series : Directory, Public Key Infrastructure (PKI), Privilege Management Infrastructure (PMI).
- X.660 and X.670 series (Registration).
- X.680 series (ASN.1 Language) and X.690 series (ASN.1 Encoding rules).
- Z.100 series (SDL and TTCN).

Recommendations related to security

- Two Recommendations related to security:
  - X.509 (10/2019): Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

  This Recommendation defines the following structures:
    - Public key certificate
    - Attribute certificate
    - Certificate revocation list
    - Authorization validation list
  - X.510 (08/2020: Information technology - Open Systems Interconnection - The Directory: Protocol specifications for secure operations.

  This Recommendation defines a wrapper protocol which provides authentication, integrity and optionally confidentiality (encryption).

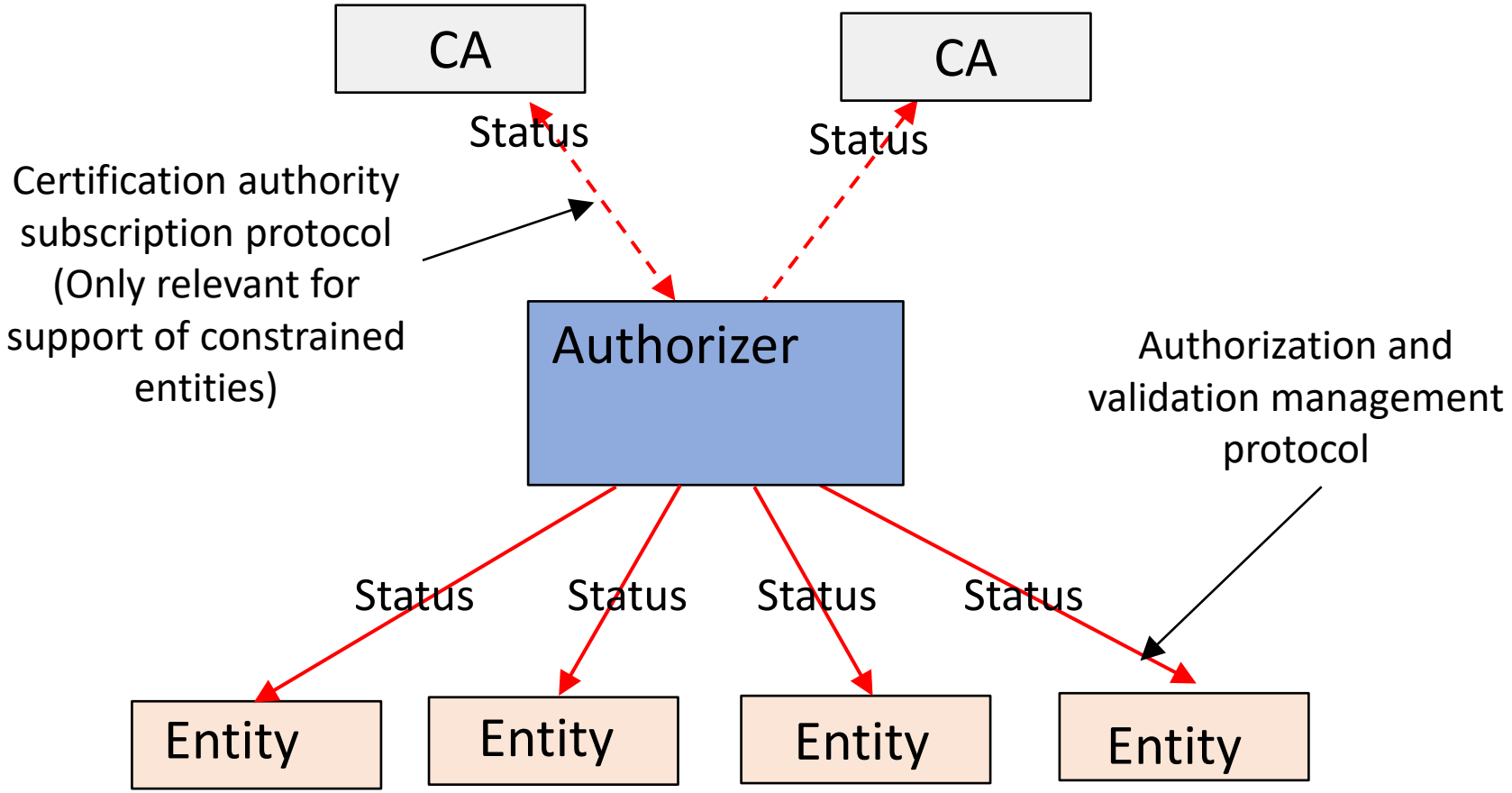
Recent developments in X.509

- Several feature have been added to cope with new requirements:
  - Authorization and validation list (AVL) to optimize validation of certificates including in constraint environments (power, storage or communication limits).
  - Migration to quantum resistant algorithms: definition of new extensions usable in public key or attribute certificates and also in certificate revocation lists and authorization and validation lists.

Authorization and validation list entity

- Authorization and validation list entities are usable in various environments:
  - No power or storage constraint: the AVL entity is used to restrict communications of the verifiers.
  - Power or storage constraint: the AVL entity shall keep locally information needed for validation and update them as needed.
  - No continuous access to revocation information: the AVL entity shall keep locally revocation information and update them when it is possible.
- The AVL entity uses a specific signed structure (AVL) to contain relevant information.

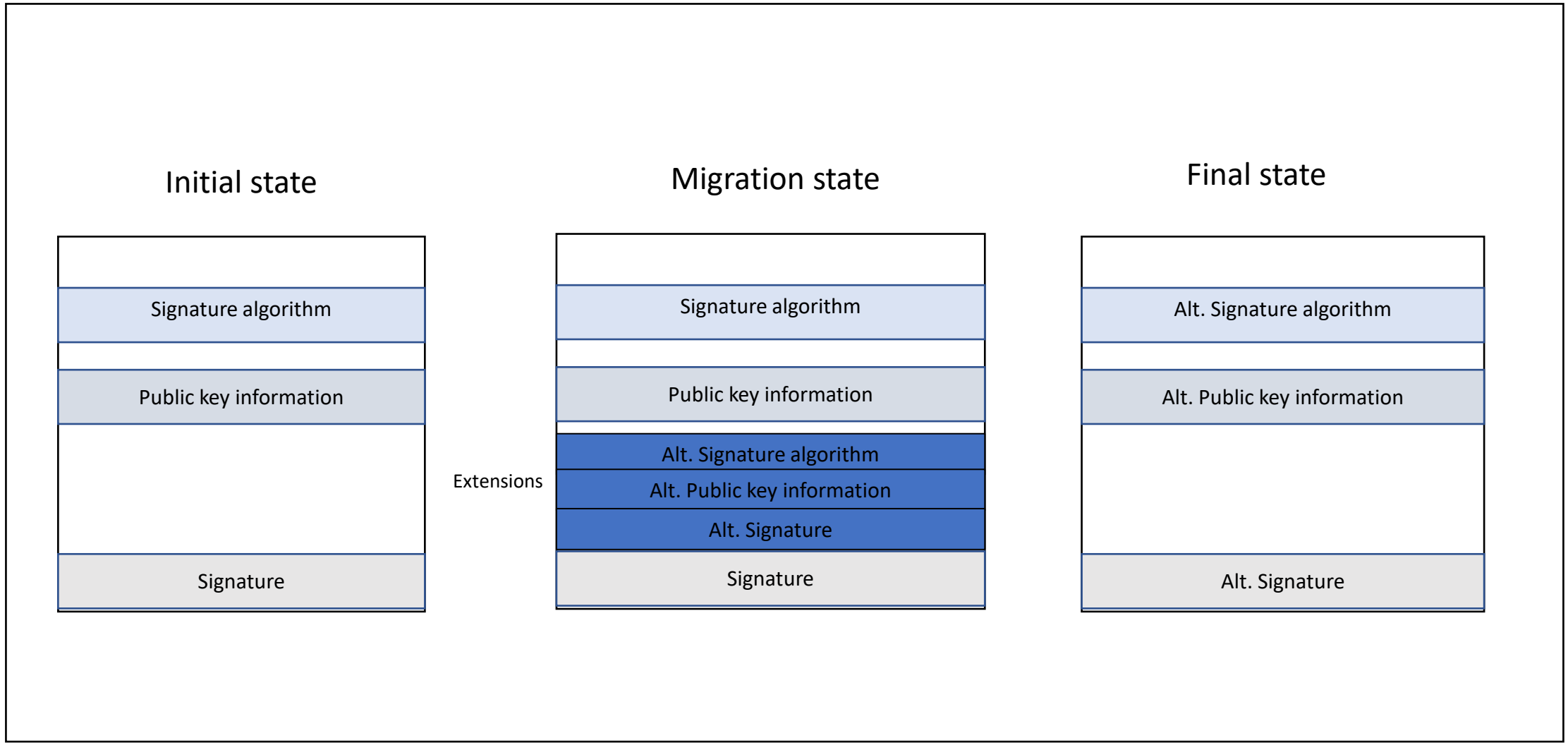
Authorizer in constraint environment



Migration to quantum-safe algorithms

- X.509 defines three new extensions:
  - *subjectAltPublicKeyInfo*: public key information using a quantum-safe algorithm (usable in public key certificates).
  - *altSignatureAlgorithm*: identification of the quantum-safe algorithm (usable in public key certificates, certificate revocation lists and authorization and validation lists).
  - *altSignatureValue* (usable in public key certificates, certificate revocation lists and authorization and validation lists).
- During migration, a signed structure can be validated by an entity supporting quantum-safe algorithms (using these extensions) and by other entities (using the signature algorithm and signature components).

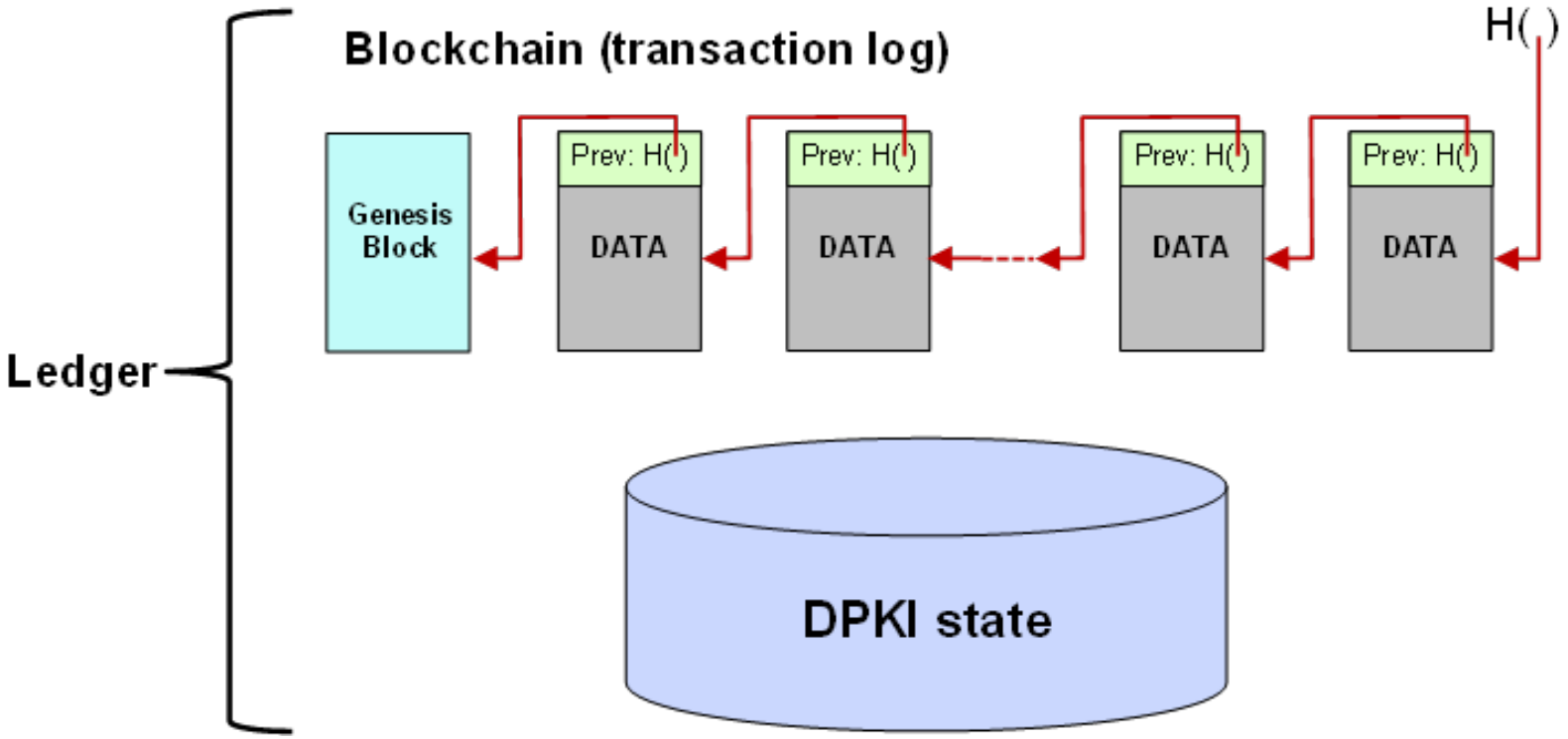
Migration to quantum safe algorithms



Decentralized Public key infrastructure

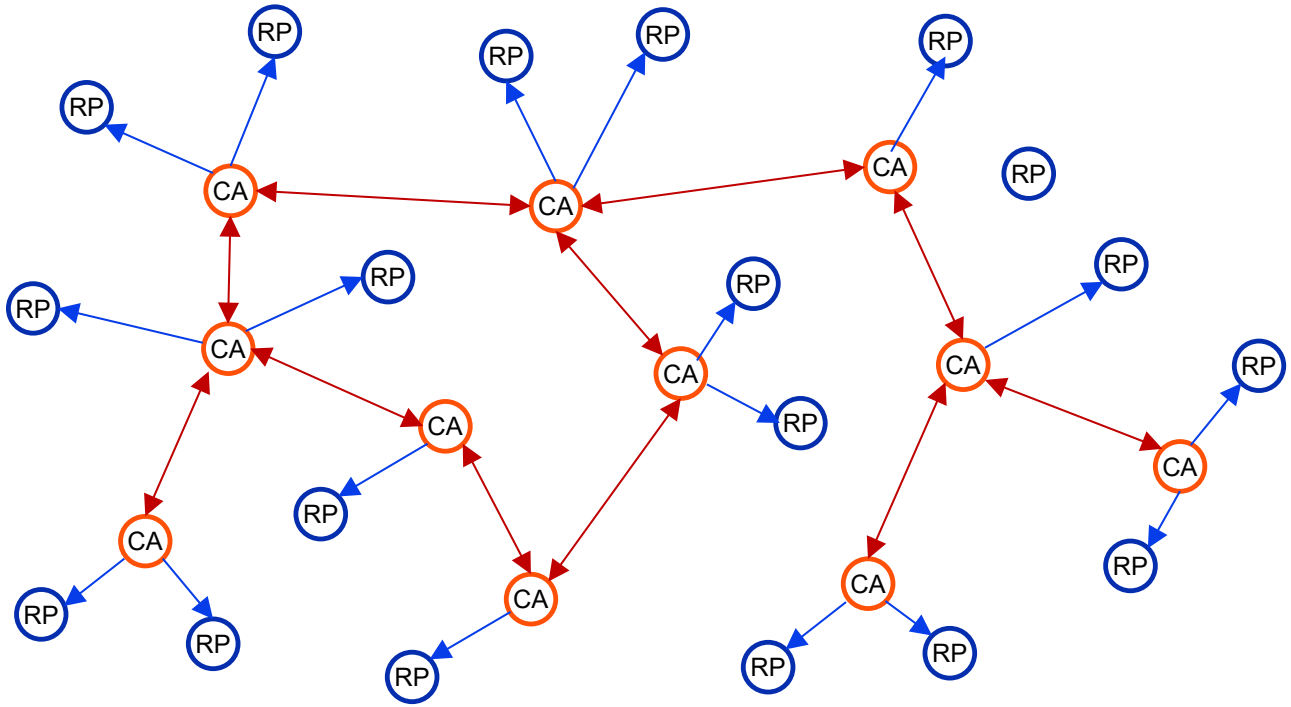
- Q11/17 is working in coordination with Q14/17 (Distributed Ledger Technology (DLT) security) on decentralized PKI.
  - A decentralized PKI structure has been defined to reduce the size the certificate.
  - The ledger has two components:
    - The ledger state which holds the state of the ledger.
    - The transaction log (blockchain).
  - Each participant has a copy of the ledger.

The ledger in decentralized PKI



The blockchain network in DPKI

- The blockchain network contains two types of nodes:
  - Certification Authority (CA) nodes: these nodes can generate blocks and update the DPKI state.
  - Relaying Party (RP) nodes have only read access.



New X.510 recommendation

- X.510 specifies a general wrapper protocol that provides authentication, integrity and confidentiality (encryption) protection for other protocols.
- As X.509 the wrapper protocol includes a migration method to quantum-safe cryptographic algorithms.

The wrapper protocol

- The wrapper protocol establishes an association between to entities. The protocol has several phases:
  - Association establishment phase: the handshake step try to establish a secure association with the remove entity using key establishment method.
  - Data transfer phase: this phase is used to transfer encrypted data, non encrypted data and also for key renewal.
  - Association release phase: this phase in uses to terminate the association.
  - An abort mechanism is also provided for error detection.