How to respond quantum computing threats and its standardization trend: Quantum Key Distribution and Post Quantum Cryptography

23 October 2024

Heung Youl Youm, Prof./Dr.

- **Soonchunhyang University, Korea (Republic of)**
- **Chair of ITU-T SG17 (former, 2017-2024)**
- **Commissioner, Personal Information Protection Commission in Korea**
- **Chair, Korea Chief Privacy Officer Council**

Keynote session

Introduction to ITU-T SG17

ITU-T Study Group 17: Security

ITU-T Study Group 17 (SG17) is responsible for **building confidence and security** in the use of information and communication technologies (ICTs). (Meets twice a year, normally for 8 - 9 working days)

SG17 is the lead Study Group for **security**, **identity management** and **Languages and description techniques**. Its work covers two main study areas:

- **providing security by ICTs** and
- **ensuring security for ICTs**.

ITU-T Study Group 17: Security

Areas of work in this study period (2022-2024) include:

- Application security
- Big Data analytics security
- Cybersecurity
- Countering spam
- Cloud computing security
- DLT security
- Fintech security
- Identity management
- Information security management
- IoT security
- ITS security
- Incubation (emerging technologies)
- Languages (ASN.1, SDL, MSC, TTCN-3 …)
- Mobile (5G) security
- PKI, PMI, Directory
- Quantum-based security - QKD
- SDN/NFV security
- Smart-grid security
- Telebiometrics

Security is Absolutely First Everywhere (SAFE)

ITU-T Study Group 17: Security

New and emerging area for next study period (2025-2028) include:

- Metaverse security
- 6G security
- SBOM
- DevSecOps
- Zero trust (ZT)
- SOAR (Security Orchestration, Automation, and Response)
- Use of cryptographic algorithms
- Data masking techniques
- Digital twin security
- Platform security
- Endpoint security
- Generative AI security
- Security for converged networks
- Autonomous driving security
- **Use of, migration to PQC**
- Operational aspects for data protection

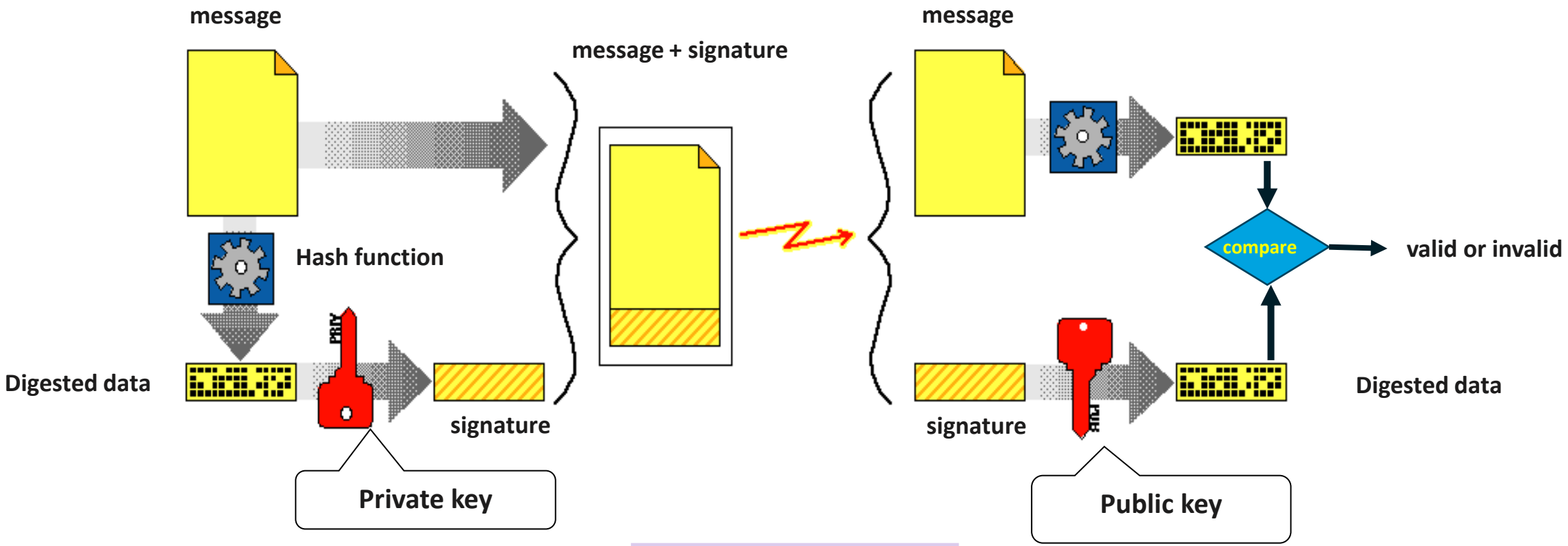
Security by design and privacy by design

ITU-T X.509 PKI standard overview

What is PKI about?

- The infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.
- Trust (trust anchor concept) using the trusted third party called CA
- PKI provides functions:
  - Authenticity of data
  - Integrity of data
  - Confidentiality of data
  - Non-repudiation of data

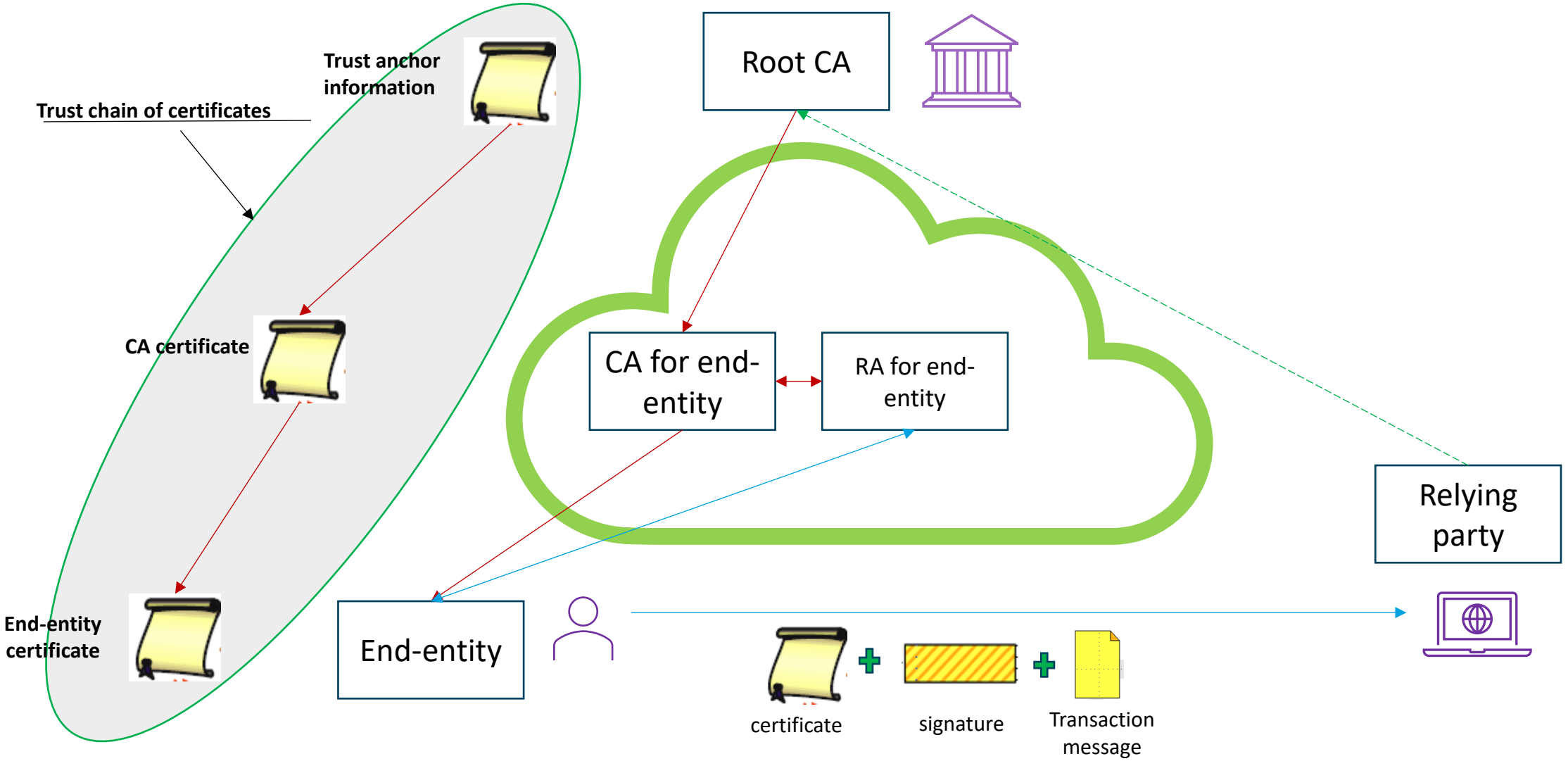
Digital signature generation and validation



- Unforgeable
- Authentic

- Not Reusable
- Unalterable
- Nonrepudiation

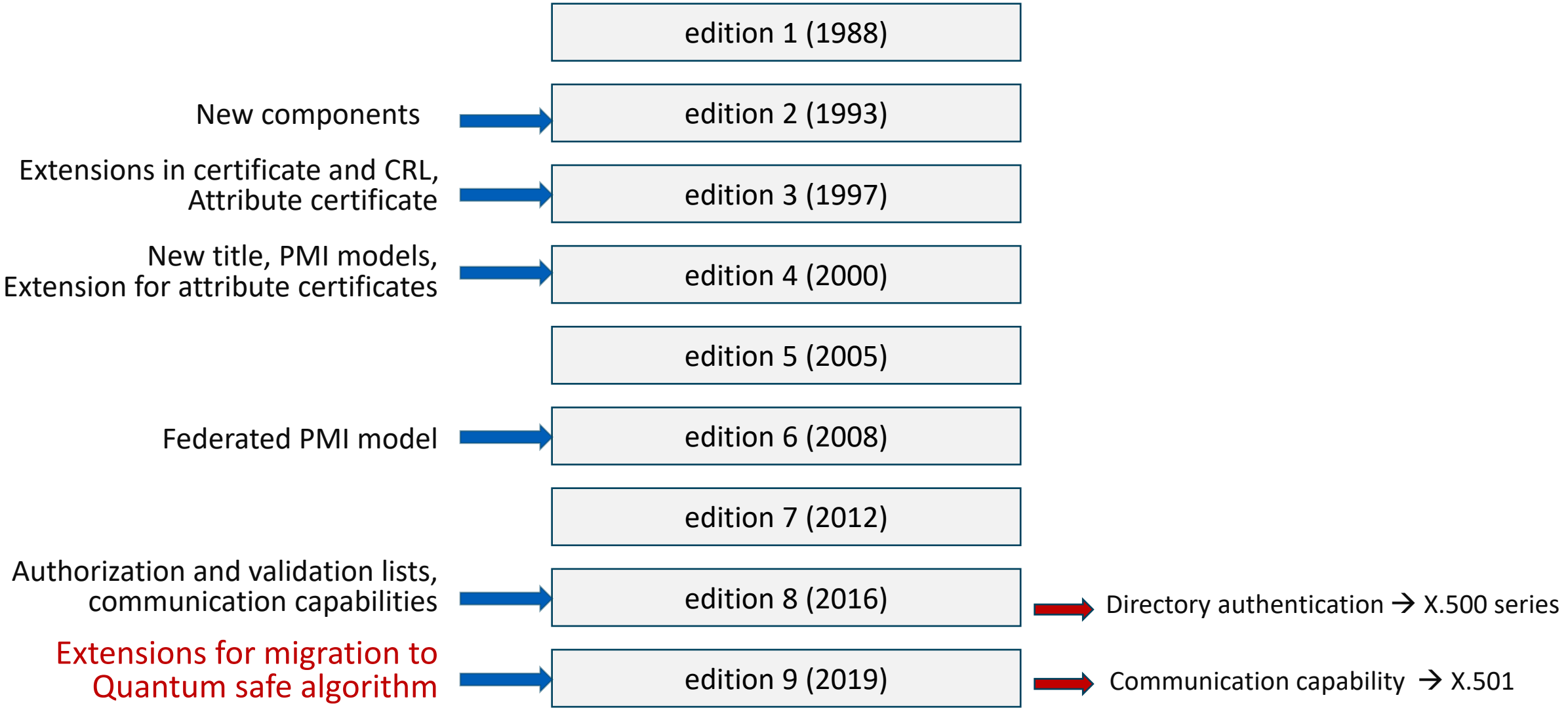
Components of PKI and trust chain of certificates



Rec. ITU-T X.509 until now

- The base specification for public-key infrastructure (PKI)
- The base specification for privilege management infrastructure (PMI)
- First edition in 1988
- Ninth edition in 2019
- PKI is widely deployed in the world:
  - Banking
  - E-government
  - Health
  - Etc.

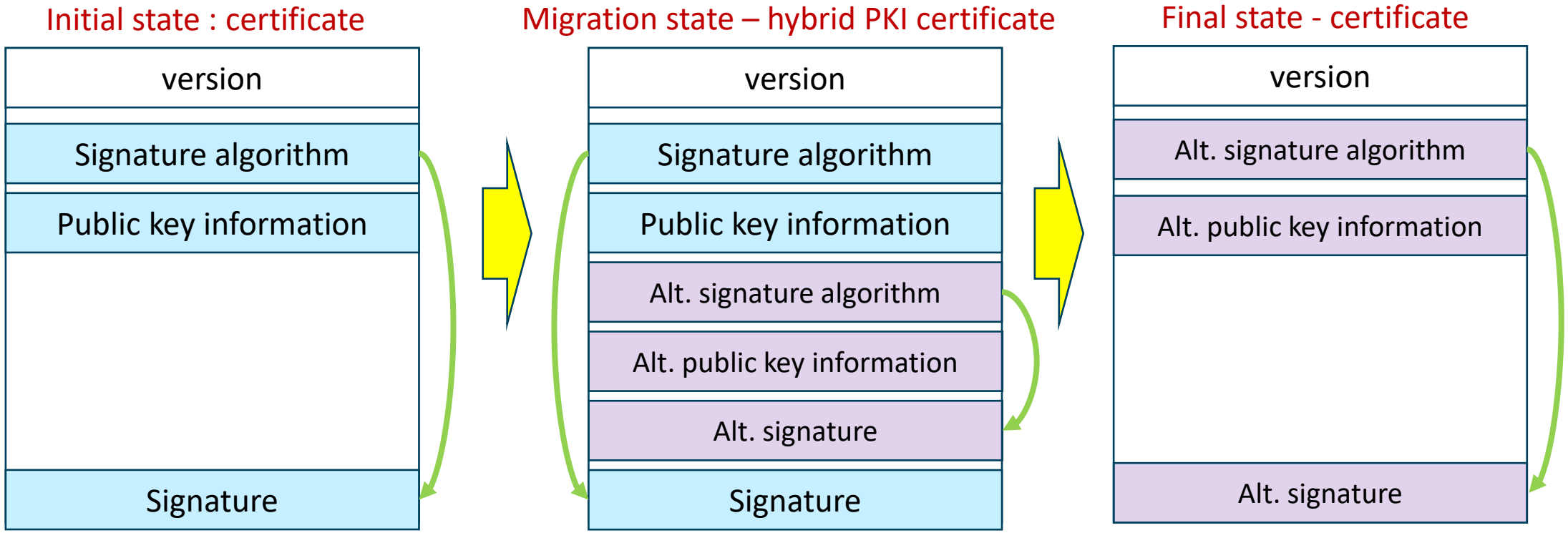
X.509 history



(Source: [13])

X.509 - edition 9 (2019) of X.509 – PQC migration ready

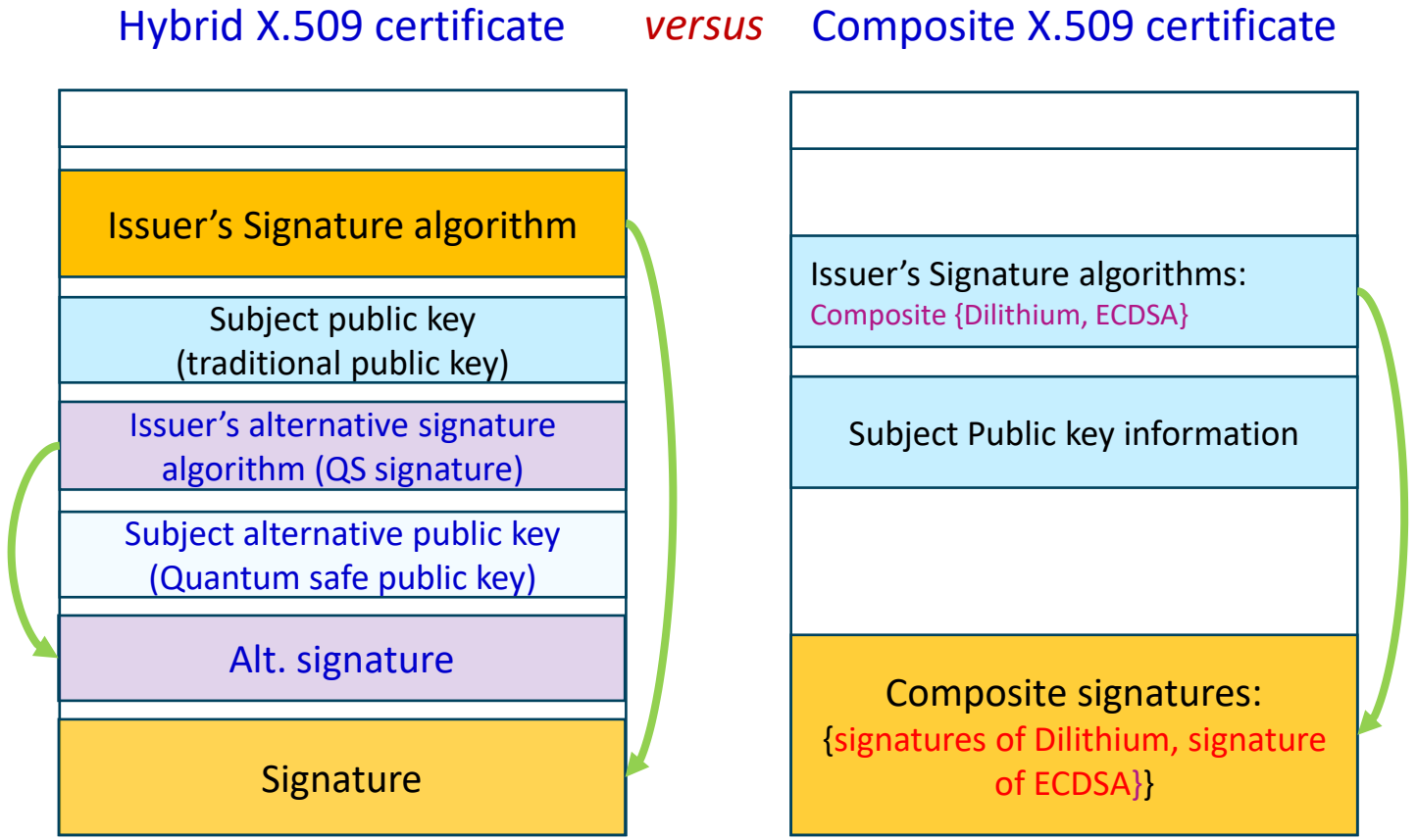
- The section related to protocols has been moved to a new part of X.500 series, X.510: Protocol specifications for secure operations.
- Hybrid PKI certificate - new extensions have been added to migrate to quantum safe algorithms.
  - Alternative signature algorithm
  - Alternative public key information
  - Alternative signature



Incorporation of Quantum safe algorithms into X.509 certificate

- End-entity certificate:
  - A public-key certificate issued to an entity, which then acts as an end entity within a public-key infrastructure.

- CA certificate
  - A public-key certificate for one certification authority (CA) issued by another CA or by the same CA.



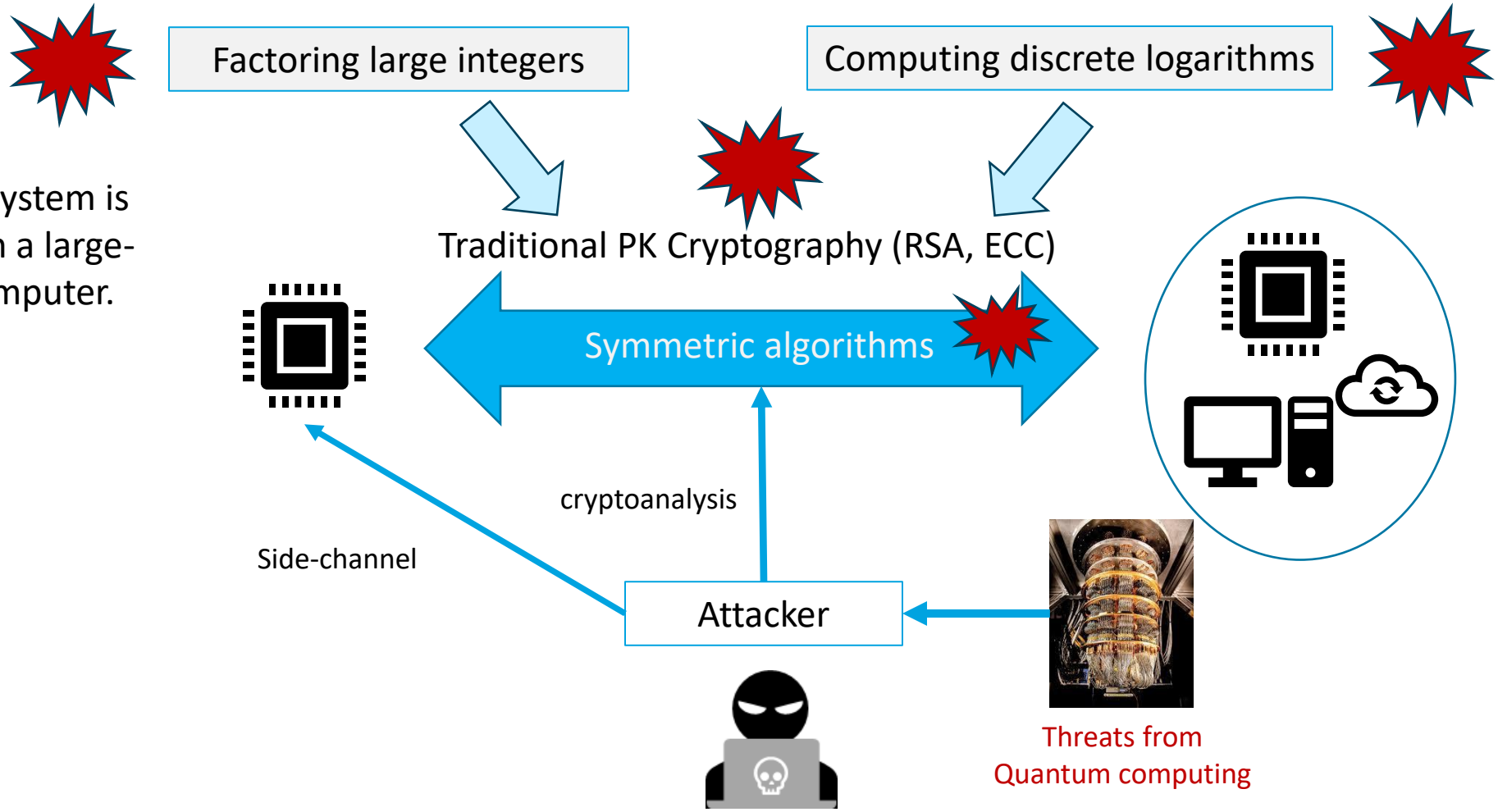
(Source: edition 9 of ITU-T X.509)

(Source: Composite Signatures For Use In Internet PKI, IETF RFC draft)

Responding to threats from Quantum computers

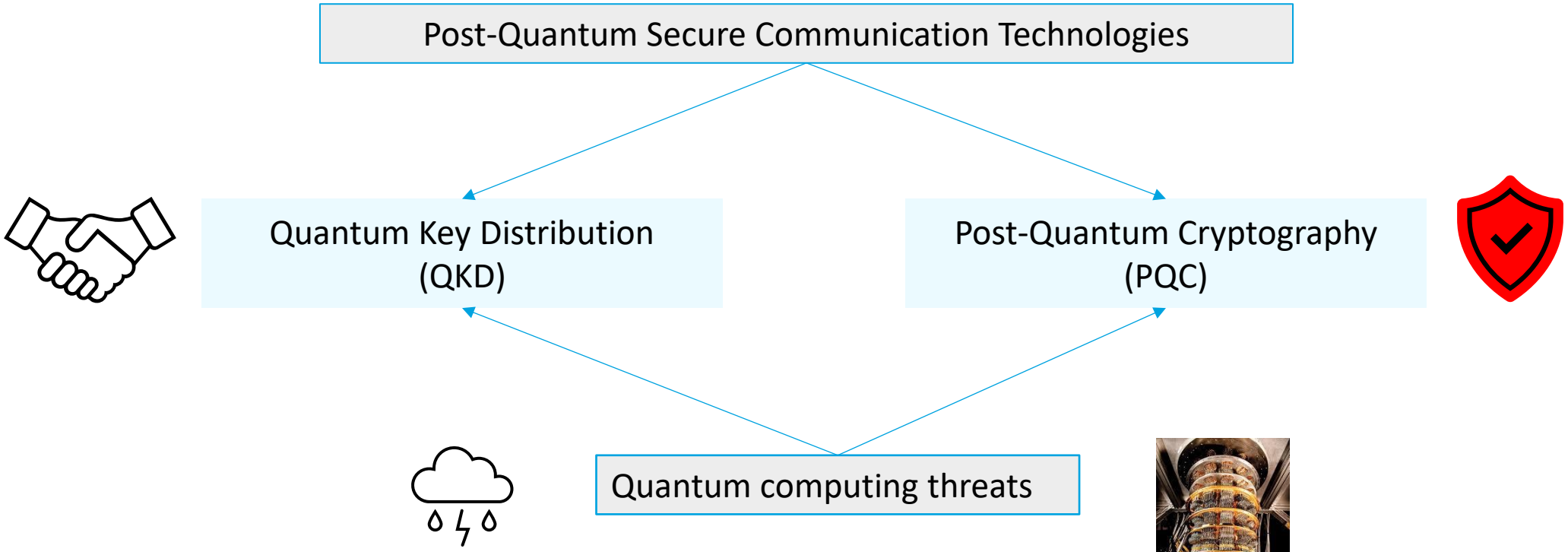
Threats from Quantum computers

Traditional cryptosystem is under attacks from a large-scale Quantum computer.



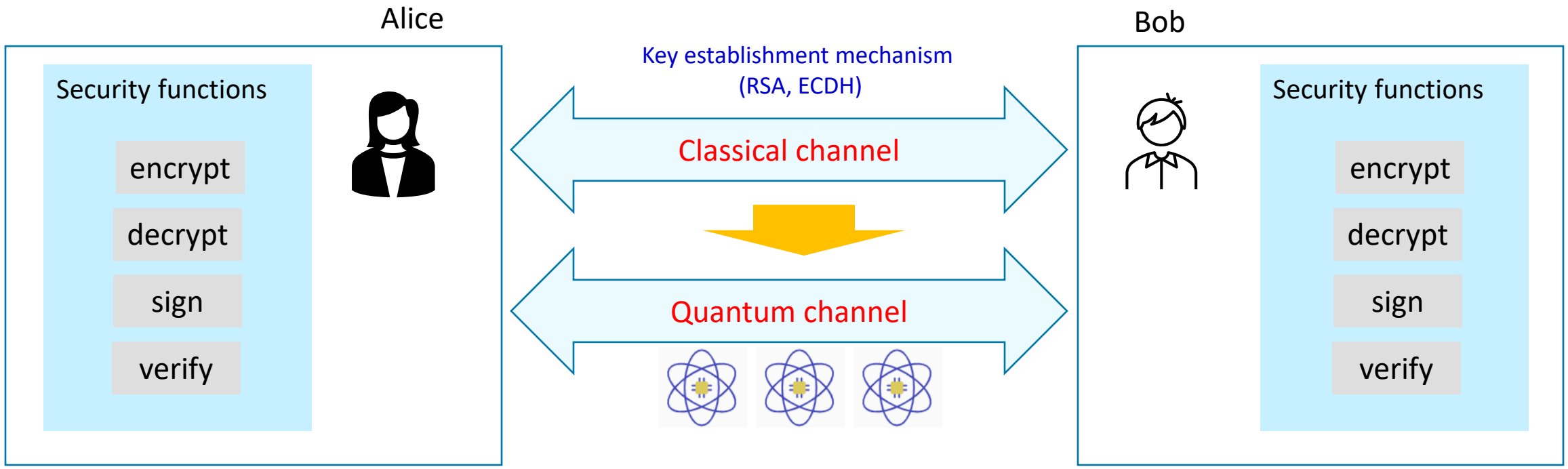
In the future, PQC and QKD are required to be used.

How to respond to threats of Quantum computers



- PQC and QKD are not competing.
- PQC and QKD can work together.
- Two security technologies with different properties.
- They can cover the security needs of a wide variety of applications.

QKD (Quantum Key Distribution) - fundamentals



- A method for securely distributing cryptographic keys between two parties using the principles of quantum mechanics.
- To establish a shared secret key between two parties in a way that is provably secure against eavesdropping or interception by an adversary.
- QKD can be applied in various sectors, including healthcare, finance, and government.

Impact on AES and RSA algorithms to Quantum computing threats

Type of attacks	Symmetric encryption	Key length	Bits of security	Public key encryption	Key length	Bits of security
Classical computers	AES-128	128	128	RSA-2048	2048	112
	AES-256	256	256	RSA-15360	15,360	256
Quantum computers	AES-128	128	64	RSA_2048	2048	25
	AES-256	256	128	RSA-15360	15,360	31

★ Bits of security should be grater than 128.

- RSA, ECC, DHKE, AES can be broken with Quantum computers.

A need for Post quantum cryptographies that are secure against a cryptanalytic attacks by a quantum computer.

ITU-T SG17 QKD standardization activities

SG17 Questions for the next study period (2025-2028)

SG17 proposed **12** Questions for the next study period (2025-2028).

12 Questions	
Security standardization strategy, incubation and coordination	Cloud computing and big data infrastructure security
Security architecture and network security	Identity management and telebiometrics architecture and mechanisms
Telecommunication information security management and security services	Generic technologies to support secure applications
Cybersecurity and countering spam	Intelligent transport system (ITS) and Connected Autonomous Vehicle (CAV) security
Security for telecommunication services, Internet of Things (IoTs), digital twin, and metaverse	Distributed Ledger Technology (DLT) security
Secure application services	Quantum-based security

Use of PQC **for general**

QKD and use of PQC **for network infrastructure**

Q15/17 QKD work (approved)

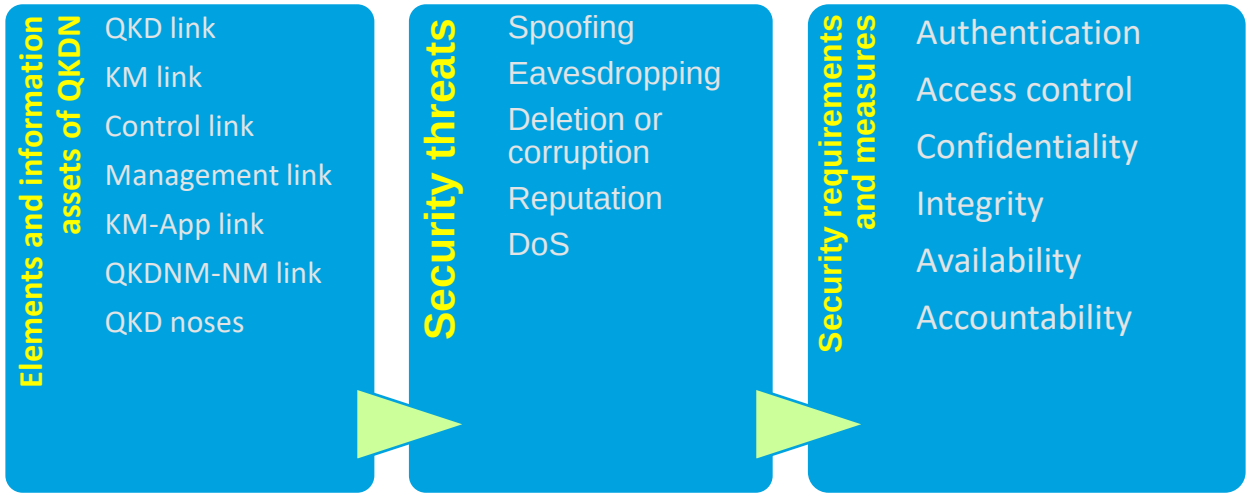
- X.1710:2022, Security framework for quantum key distribution networks
- X.1712:2021, Security requirements and measures for quantum key distribution networks – key management
- X.1713:2024, Security requirements for the protection of quantum key distribution nodes
- X.1714:2020, Key combination and confidential key supply for quantum key distribution networks
- X.1715:2022, Security requirements and measures for integration of quantum key distribution network and secure storage network

Q15/17 QKD work : X.1710:2022, Framework of QKDN security

Scope

This Recommendation is the first in a series on the security of quantum key distribution (QKD) and provides a security framework for other related Recommendations. In particular, this Recommendation addresses the following items:

– security aspects for quantum key distribution networks (QKDNs);
– security threats to QKDNs;
– security requirements (SReqs) for QKDNs;
– security measures for QKDNs.



Typical structure of a QKDN and user network

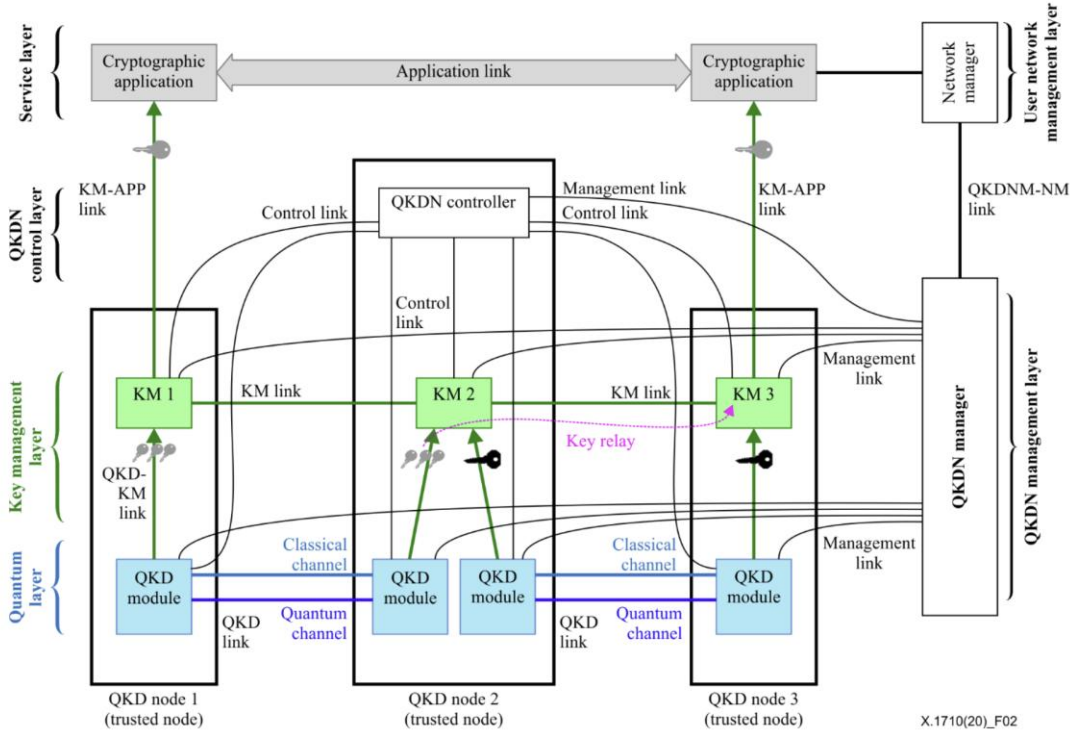


Figure 2 – Typical structure of a QKDN and user network

ITU-T X.509 migration to Post Quantum Cryptography

Key elements for migration to post-quantum cryptography

- Security for PQC (KEM, Digital signature)
- Performance for PQC, such as length of signature and key, speed of PQC
- Certificate trust chain for PKI
- Various kinds of migration scenarios
  - All in one migration from scratch
  - Step by step migration
- Harmonized approach for the security protocols that are based on Cryptographic algorithms
- Complexity of public infrastructure

NIST major PQC standardization milestones

April 2016, NISTIR8105, Report on PQC

July 2019, second-round, candidates were announced

July 2022, third-round candidates were announced

2016	2017	2018	2019	2020	2021	2022	2023-24

December 2016, call for submission

December 2017, first-round candidates were announced

In 2024, three PQCs have been selected.

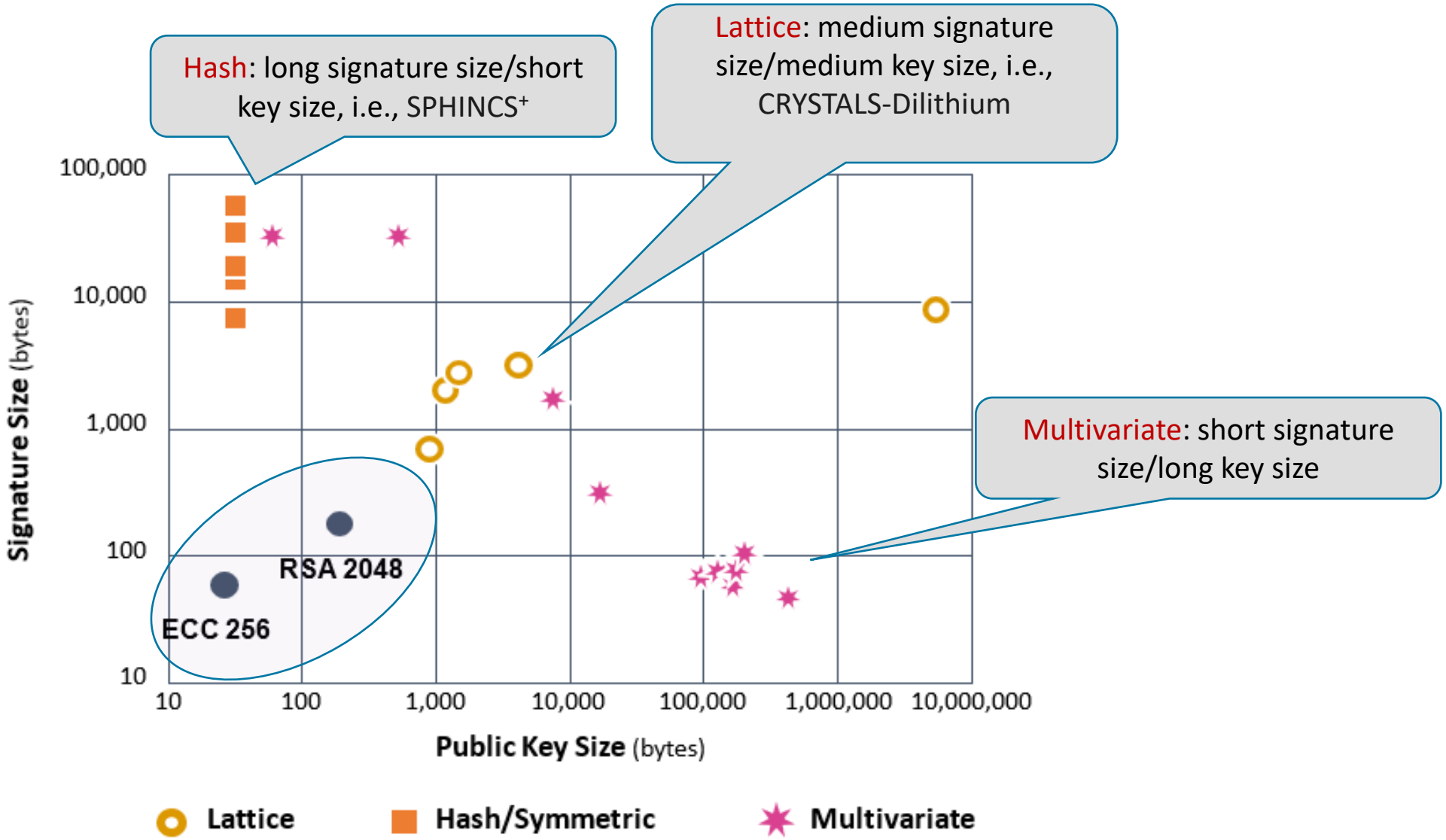
NIST approved three FIPS for Post Quantum Cryptography in 2024

(August 13, 2024)

Type	Algorithms	Family	Derived from	standard
Key Encapsulation Mechanism	Module-Lattice-Based Key-Encapsulation Mechanism Standard	Lattice	CRYSTALS-KYBER	FIPS 203
Digital Signature	Module-Lattice-Based Digital Signature Standard	Lattice	CRYSTALS-Dilithium	FIPS 204
	Stateless Hash-Based Digital Signature Standard	Stateless, hash-based	SPHINCS$^+$	FIPS 205

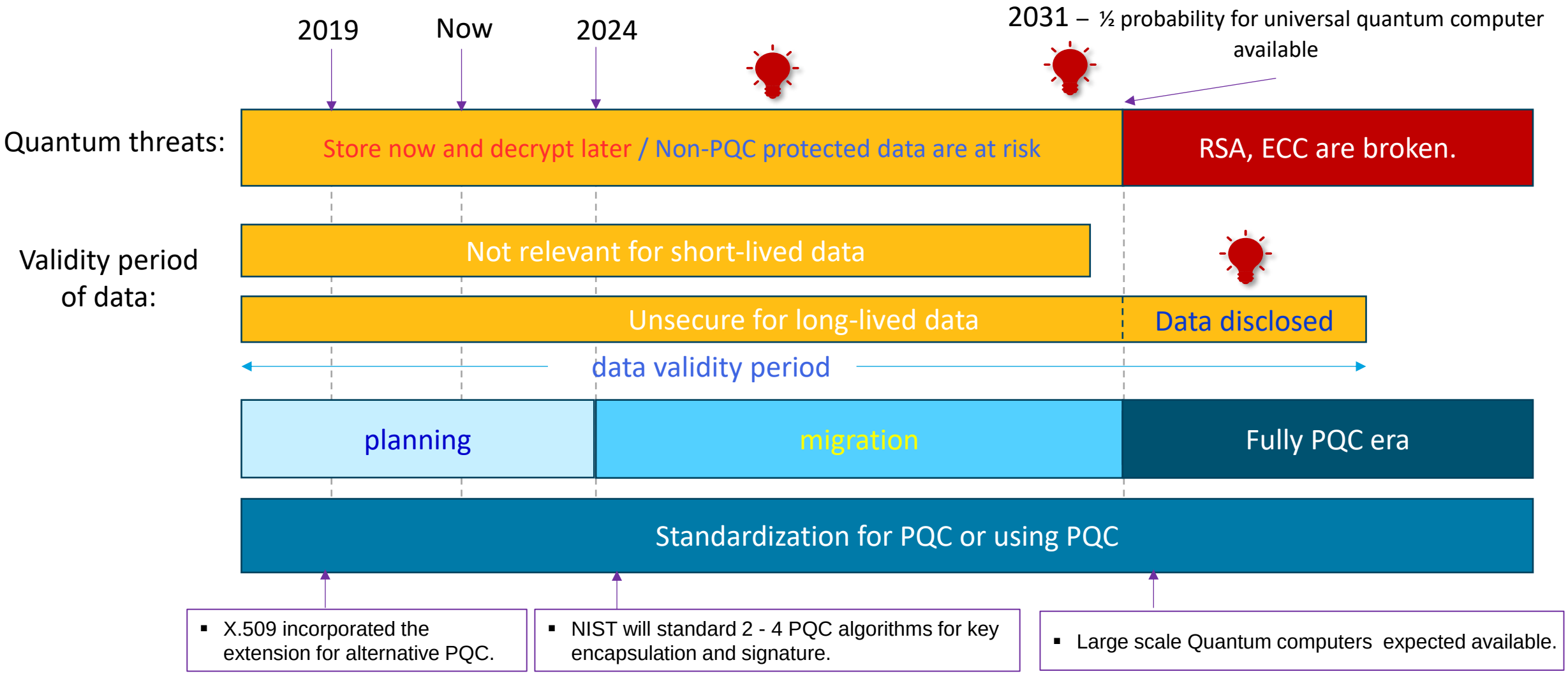
(Source: NIST)

Signature size vs public key size of PQC by NIST



(Source: NIST's Standardization of PQC at https://www.creaplus.com/index.php?option=com_content&view=article&id=1001:nist-pqc-en&catid=310:blog&lang=en-GB)

Possible migration stages for Post-quantum cryptography

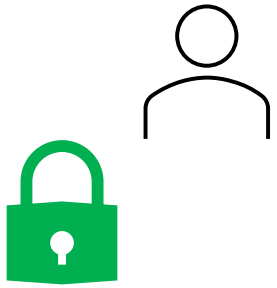


Hybrid approaches for migration

- Use of traditional algorithms and PQC algorithms together:
  - use hybrid cipher suites incorporating one traditional public-key algorithm and one PQC algorithm
  - reduce risks from uncertainty if either one of them is broken
  - maintain compliance with old standards and use of validation
- For example, adopt hybrid ciphersuites involving one traditional public-key algorithm and one PQC algorithm
  - For key encapsulation, both parties may establish two shared secrets – using one traditional key encapsulation mechanism and one PQC based key encapsulation mechanism

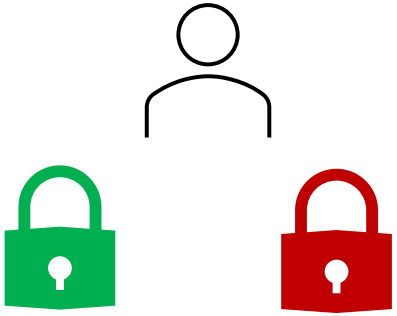
Comparison between traditional, hybrid, and quantum-safe PKI certificate

Traditional PKI certificate



- Subject Public key: *Traditional_PublicKey*
- Issuer signature: *Traditional_Signature*

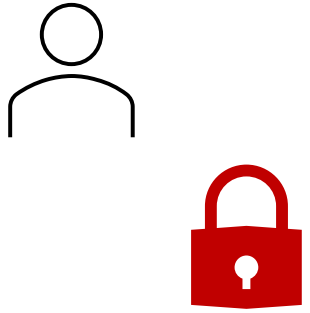
Hybrid PKI certificate



- Subject Public key: *Traditional_PublicKey*
- Issuer signature: *Traditional_Signature*

- Subject Public key: *QuantumSafe_PublicKey*
- Issuer signature: *QuantumSafe_Signature*

Quantum-safe PKI certificate



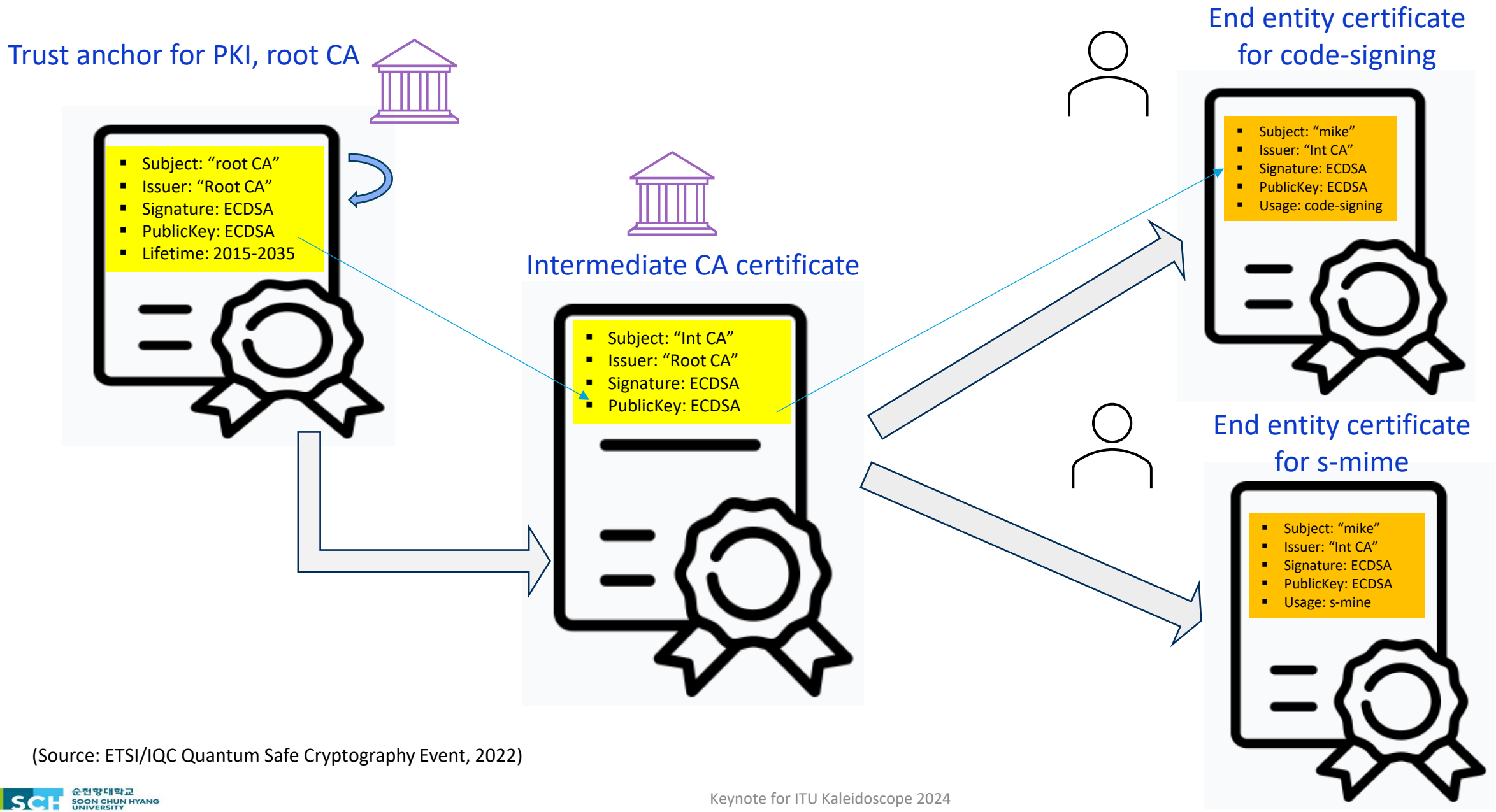
- Subject Public key: *QuantumSafe_PublicKey*
- Issuer signature: *QuantumSafe_Signature*

Four types of PKI certificates for PQC migration

Certificate Type		Cryptographic algorithm	Description	Purpose
Traditional PKI certificates		RSA or ECC	Traditional non-quantum-safe PKI certificates	▪ Used for current PKI system
Hybrid /composite PKI certificate	Hybrid PKI certificates [in X.509]	Traditional digital signature algorithm and quantum-safe signature algorithm	Contains both traditional and quantum-safe digital signature keys and values	▪ Used for migration to quantum-safe algorithms. ▪ System can use wither the traditional or quantum-safe keys
	Composite PKI certificates [in IETF]	Multiple traditional (ECC of RSA) and/or Quantum safe cryptographic algorithm	Contains multiple traditional and/or quantum-safe keys.	▪ Used for systems requiring the highest level of security and protection while recognizing the provenance of some encryption algorithms is still unknown.
Quantum-safe PKI certificates		New Quantum-safe cryptographic algorithms	Quantum-safe PKI certificate	▪ Used for Quantum-safe PKI

(Source: https://www.sectigo.com/resource-library/all-about-quantum-safe-certificates-for-next-generation-cybersecurity)

Trust chain for traditional PKI – trust chain



(Source: ETSI/IQC Quantum Safe Cryptography Event, 2022)

Terms and definitions related to Post-Quantum Traditional (PQ/T) Hybrid Schemes

- Defined by IETF draft on “Terminology for Post-Quantum Traditional Hybrid Schemes”, Published 7 March 2023.

- Post-Quantum Traditional (PQ/T) Hybrid Scheme
  - A multi-algorithm scheme where at least one component algorithm is a post-quantum algorithm and at least one is a traditional algorithm.

- PQ/T Hybrid Digital Signature
  - A multi-algorithm digital signature scheme made up of two or more component digital signature algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm.

- PQ/T Hybrid Key Encapsulation Mechanism (KEM)
  - A multi-algorithm KEM made up of two or more component KEM algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm.

- PQ/T hybrid KEMs, PQ/T hybrid PKE, and PQ/T hybrid digital signatures are all examples of PQ/T hybrid schemes

Migration stages - Use of PQ/T hybrid system

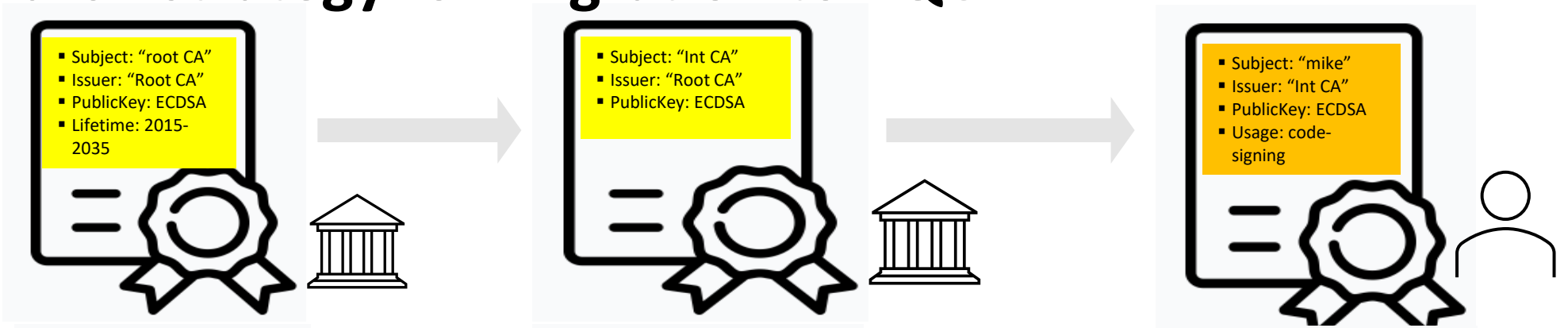
- The migration to PQ symmetric key encryption, PQ KEM and PQ PKI certificates need to implemented.

Migration stages:	planning	migration	Fully PQC era
PKI certificate:	Conventional PKI certificate (using RSA-2048 with SHA-2)	PQ/T PKI certificate	PQ PKI certificate
Key Encapsulation Mechanism:	Conventional KEM (RSA, ECDH)	PQ/T Key Encapsulation Mechanism (one using RSA-2048, other using Crystal-Kyber, …)	PQ KEM (Crystal-Kyber, …)
Digital Signature:	Conventional digital signature (RSA-2048)	PQ/T digital signature (one using RSA-2048, other using Crystal Dilithium)	PQ digital signature (Crystal Dilithium, …)
Symmetric key encryption:	Conventional symmetric cryptography (AES-128)	Migration (AES-256, …)	PQ symmetric cryptography (AES-256, ChaCha20, …)
Hash algorithm:	Hash algorithm(SHA-2)	Migration (SHA-2, SHA-3)	PQ hash algorithm (SHA-3, …)

Need to establish strategy for migration to PQC

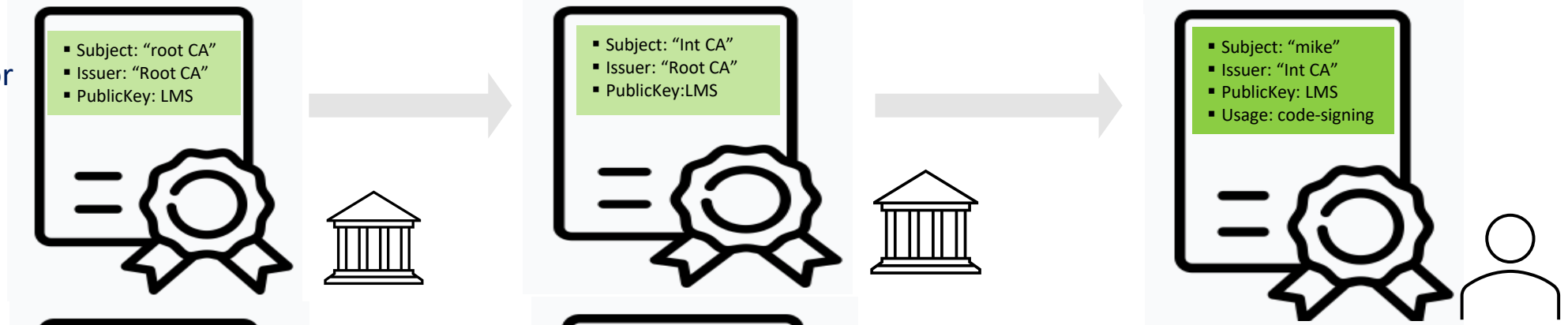
Current ECDSA PKI

- Backwards compatibility
- Root CA certificate already distributed



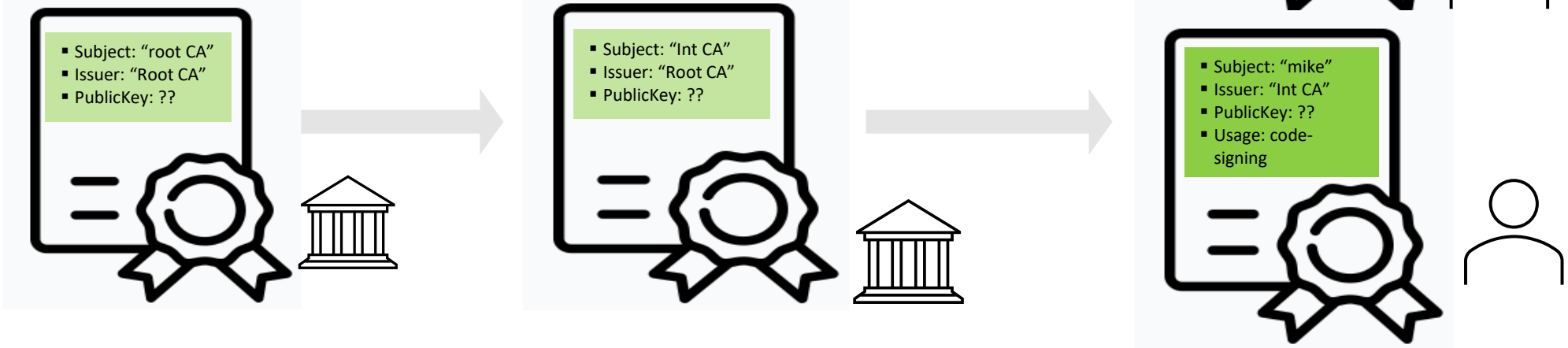
QS LMS (Leighton-Micali Signatures) based PKI cert. for code-signing

- Standardized in 2020 (NIST SP 800-208)
- For long lifetime deployments



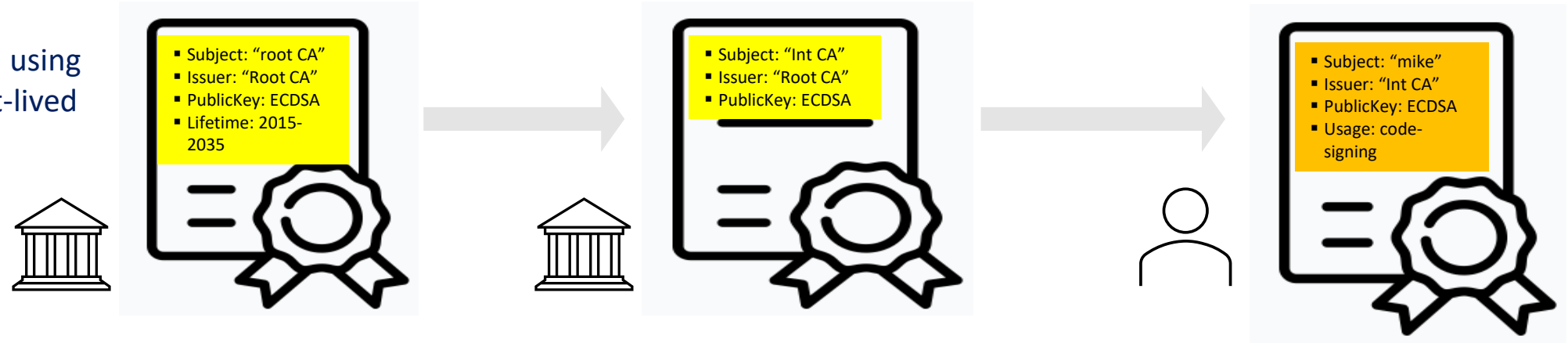
What PQ resistant PKI do we use here during migration period?

- ❑ Possibility #1: Multiple PKIs
- ❑ Possibility #2: Mixed PQ PKI
- ❑ Possibility #3: Composite/hybrid PKI

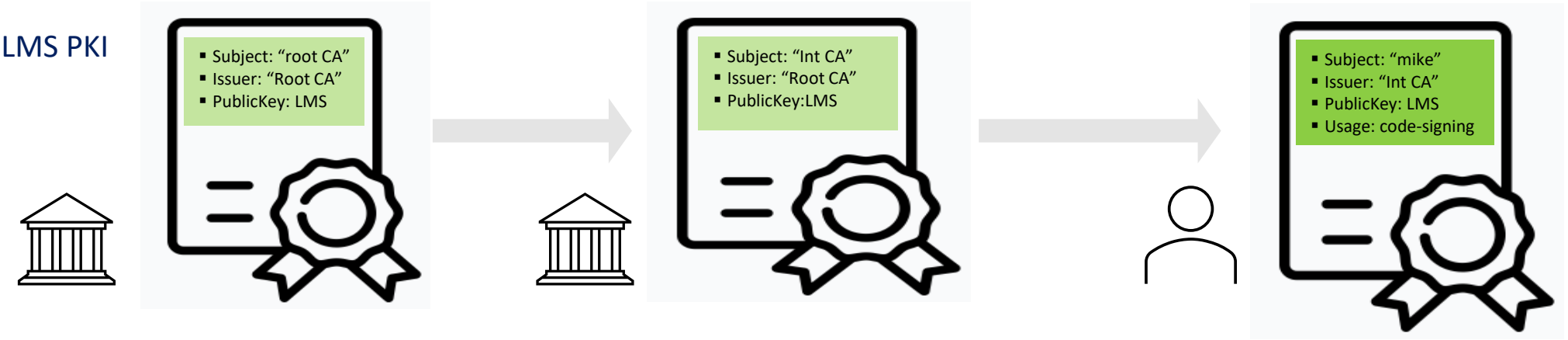


Possibility #1: Multiple PKIs (depending on lifecycle of data)

Traditional PKI cert. using ECDSA PKI for short-lived data



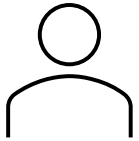
PQC PKI cert. using LMS PKI for long-lived data



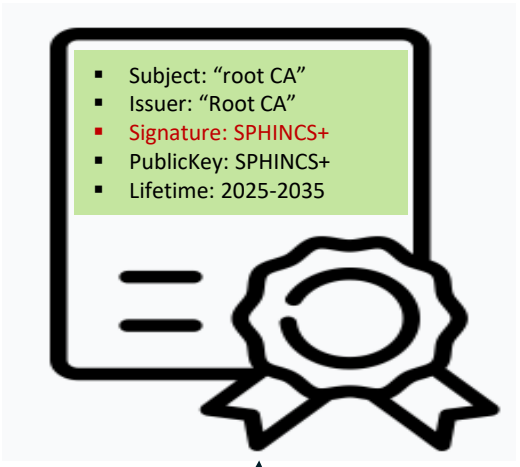
Possibility #2: Mixed PQ PKI – use of different PQ cryptographies

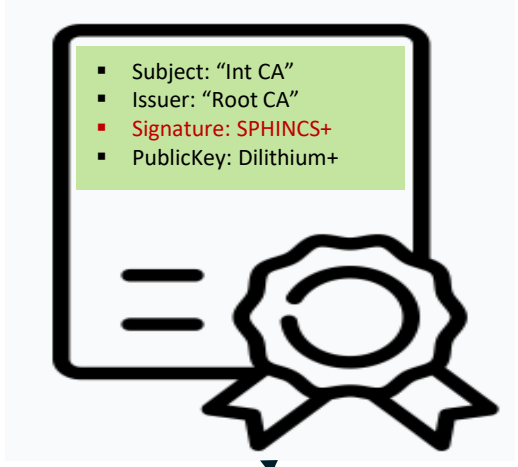
Self-signed root CA using SPHINCS+

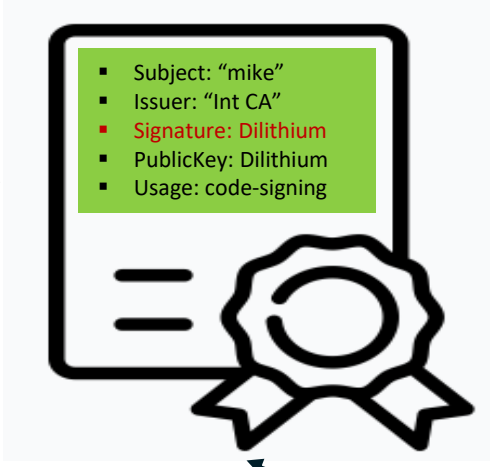
Intermediate CA using SPHINCS+



End entity certificate using Dilithium







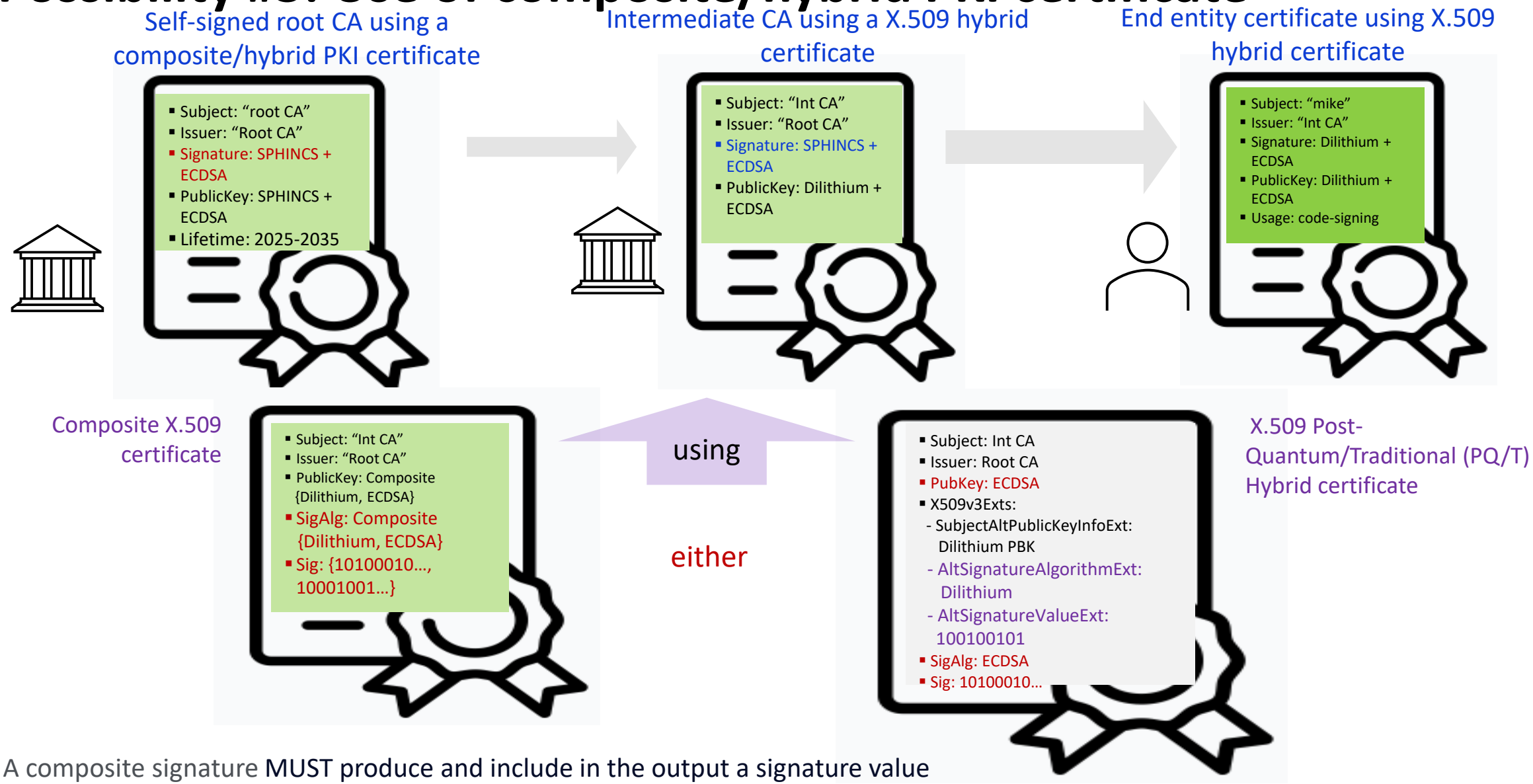
- A long-lived Root CA, it use SPHINCS+, a hash-based signature.
- SPHINCS+ is easier to manage: short to verify and long to generate.

- Root and Int CAs certs will be large because of SPHINCS+ signature.
- Root and Int CAs can be cached by the client and not sent over the network.

- End Entity certs are short and fast.

(Source: ETSI/IQC Quantum Safe Cryptography Event, 2022)

Possibility #3: Use of composite/hybrid PKI certificate



- A composite signature MUST produce and include in the output a signature value for every component key in the corresponding CompositePrivateKey.

TLS overview – existing cypher suite

- Privacy
  - Symmetric key encryption for application data.
  - Typically, Advanced Encryption Standard (AES).
- Integrity
  - Authenticated Encryption with Additional Data (AEAD)
  - Usually AES-GCM (Galois/Counter Mode) cipher mode.
- Authentication
  - X509 certificates signed by a mutually trusted third party
  - Typically, server authenticated only.

- Agree on a master secret
  - Using Key exchange algorithm

Example of migration to quantum safe TLS protocol

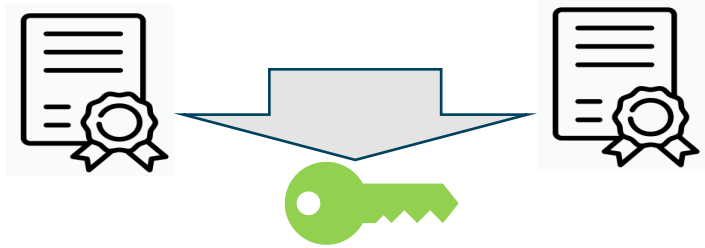
Current TLS

Client

Server

Handshake protocol

- Agree a cipher suite
- Agree a master secret
- Authentication using PKI certificate(s)



Record protocol

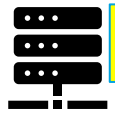
Provide confidentiality and integrity of the application data

Migration period

- Use of X.509 hybrid PKI certificate
  - PQ/T digital signature
  - PQ/T KEM
- Use of AES-256, SHA-3

Quantum safe TLS

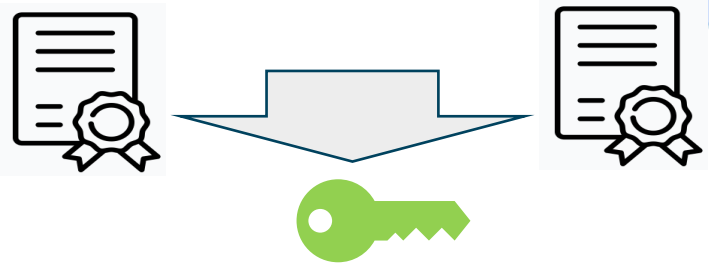
Client



Server

Handshake protocol

- Quantum safe PKI certificate (mixed PQ PKI) for authentication
- Quantum safe KEM for the master secret using Quantum safe digital signature



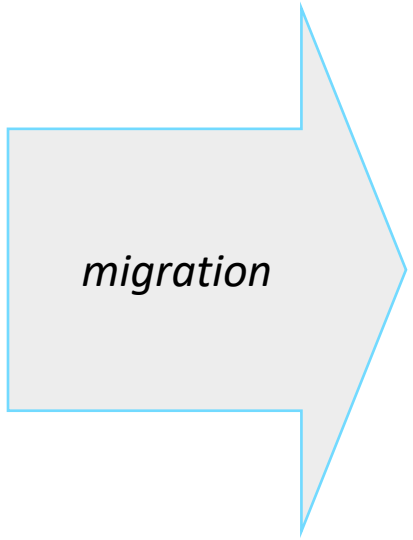
Record protocol

Provide confidentiality and integrity of the application data using Quantum safe symmetric encryption (AES-256, SHA-3)

Examples of Quantum safe TLS1.3 cipher suites

Current cipher suite

- Key Exchange
  - RSA
- Encryption algorithms
  - AES-128, Cha-cha20-poly1305
- Cryptographic Hash algorithms
  - SHA-2, SHA-3.
- DSA Signatures
  - ECDSA ≥ 224 bit



Quantum safe cipher suite

- Key Exchange
  - Lattice based Crystal-Kyber
- Encryption algorithms
  - AES-256, Cha-cha20-poly1305
- Cryptographic Hash algorithms
  - SHA-2, SHA-3
- DSA Signatures
  - Lattice-based Crystal-Dilithium

Concluding remark

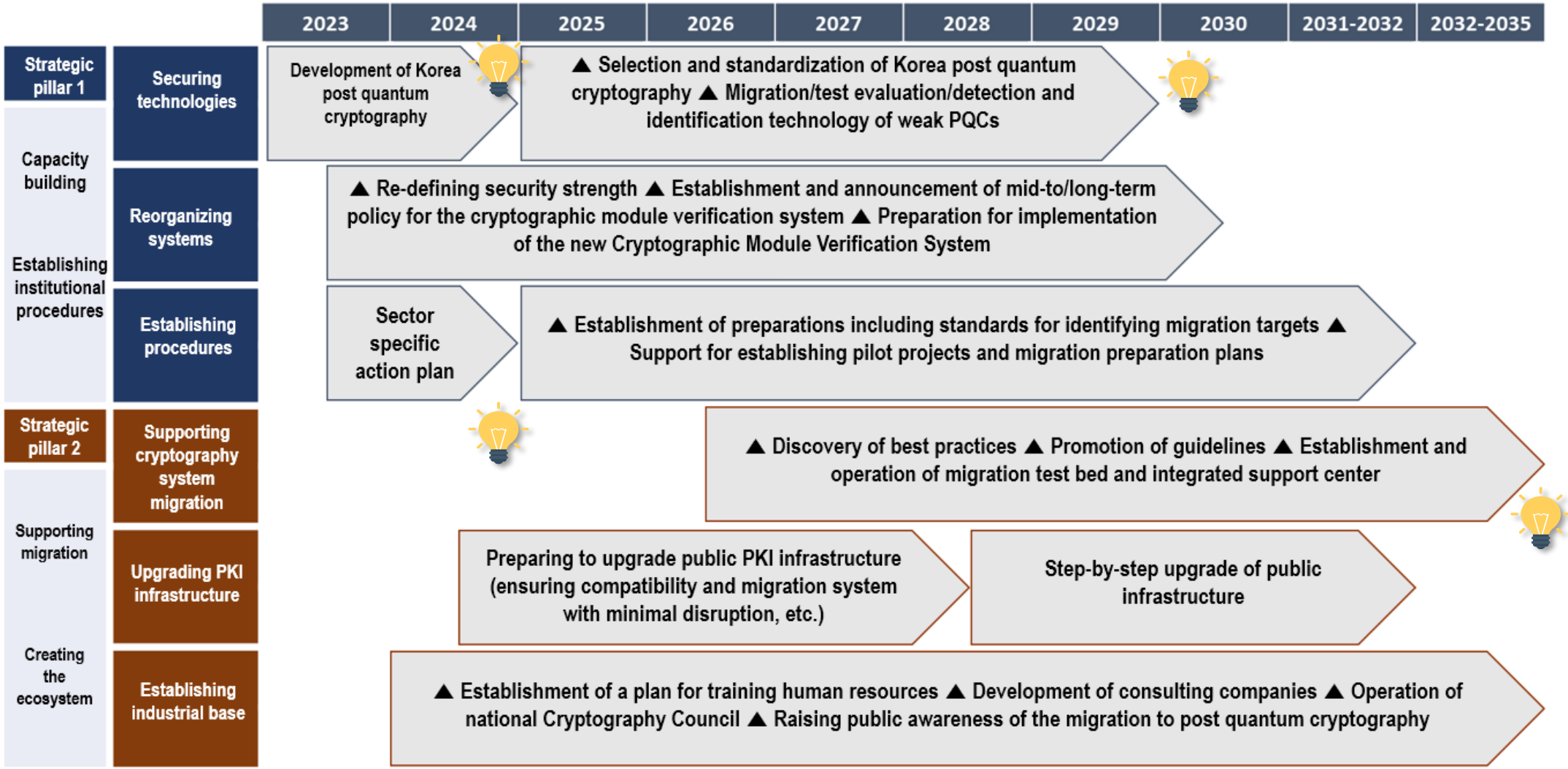
Republic of Korea's master plan for migration to post-quantum cryptography (1/2)

- Announced by both National Intelligence Service and the Ministry of Science and ICT announced on July 12, 2023
- Comprehensive measures to migrate domestic cryptographic system to post quantum cryptographic system.
  - By 2029,Korea post quantum cryptographies will be selected and standardized.
  - From 2028 to 2032, a step-by-step approach will be used to migrate to the public infrastructure with post quantum cryptographies.
  - By 2024, sector specific action plan for migration will be established.
  - From 2026 to 2035, the "integrated migration support center" will be established and operated.

Ministry of Science and ICT

NIS

Republic of Korea's master plan – roadmap for PQC migration(2/2)



(source: [11])

Way forwards

- It is recommended for organizations to migrate to post-quantum cryptography as soon as possible.
  - For flexibility and backward compatibility, use of composite/hybrid PKI certificates is preferred.
  - Three type of migration strategies could be considered: Mixed PQ PKI, X.509 composite/hybrid PKI and multiple PKIs.
- ITU-T SG17 and related SDOs need to consider:
  - assigning an OID (object Identifier) for all PQC algorithms selected by NIST in 2024
  - mapping the existing algorithms with new PQC algorithm
  - studying impacts on the performance, speed, complexity, and cost of PQC algorithm
  - developing best practices and strategical plans for migrating to PQC for the telecommunication networks, such as 6G.
  - assisting telecom organizations in migrating of telecom infrastructures to those based on PQC algorithms.

Bibliography

- [1] Mike Ounsworth, Juan Carlos Fernández, The hybrid bridge for migrating X.509 ecosystems to PQ, ETSI/IQC Quantum Safe Cryptography Event, February, 2023.
- [2] Alan Grau, All About Quantum-Safe Certificates for Next-Generation Cybersecurity, July 2020.
- [3] NIST SP 800-208, Recommendation for Stateful Hash-Based Signature Schemes, October 2020.
- [4] David Joseph, Rafael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables & Royal Hansen, Transitioning organizations to post-quantum cryptography, 11 May 2022
- [5] NIST IR 8105, Report on Post-Quantum Cryptography, April 2016
- [6] IETF internet-draft, Terminology for Post-Quantum Traditional Hybrid Schemes, 7 March 2023
- [7] Khondokar Fida Hasan, Leonie Simpson, Mir Ali Rezazadeh Baee, Chadni Islam, Ziaur Rahman, Warren Armstrong, Praveen Gauravaram, and Matthew McKague, Migrating to Post-Quantum Cryptography: a Framework Using Security Dependency Analysis, IEEE access
- [8] Karen Martin, Waiting for quantum computing: Why encryption has nothing to worry about, at https://techbeacon.com/security/waiting-quantum-computing-why-encryption-has-nothing-worry-about
- [9] SSH, Quantum-Safe Cryptography And the Quantum Threat, at https://www.ssh.com/academy/cryptography/what-is-quantum-safe-cryptography
- [10] ANSSI views on the Post-Quantum Cryptography transition, March 30, 2022
- [11] South Korea announces master plan for post-quantum cryptography, July 12, 2023, at https://thereadable.co/south-korea-announces-master-plan-for-post-quantum-cryptography/
- [12] ITU-T X.509, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
- [13] Jean-Paul Lemaire, Question 11/17 Rapporteur | ISO/IEC JTC1/SC 6/WG 10 Convenor: "History of X.509", First ITU-T X.509 Day, 2021
- [14] NIST, Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography, August 13, 2024

Thank you!