ETSI/IQC Quantum Safe Cryptography Event

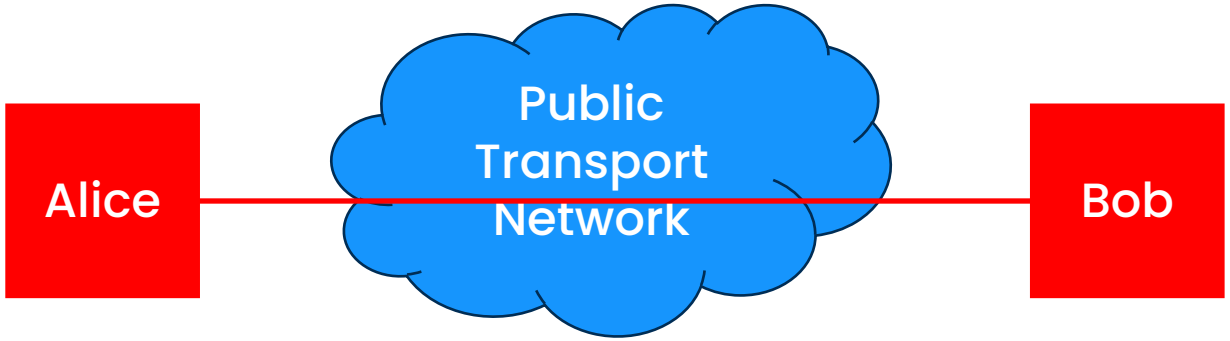
Trust in Secure Communication Networks

Felix Wissel, Deutsche Telekom

13/02/2023

Today's situation

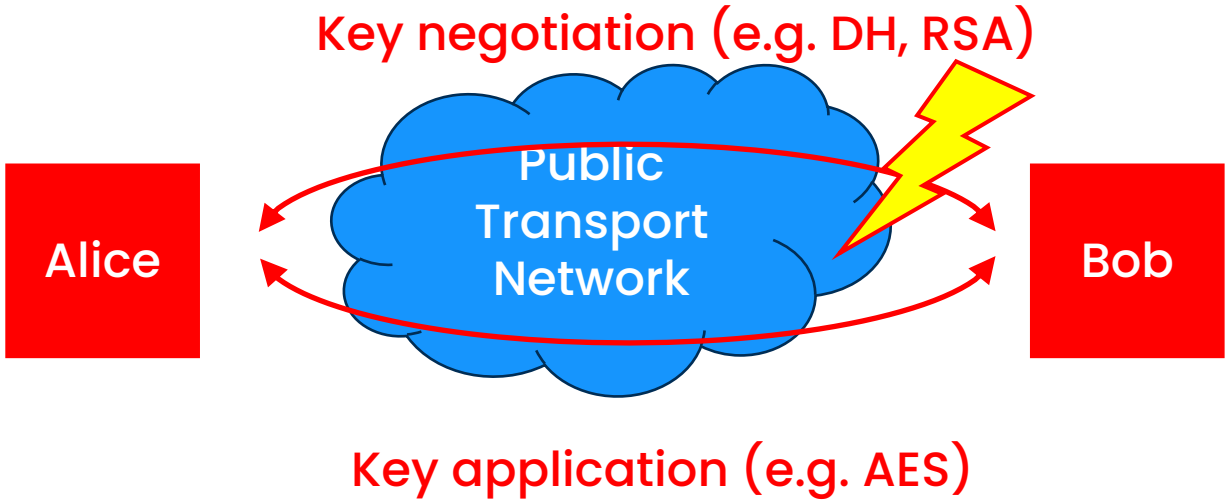
- End-to-end security is exclusively a matter of security at the end points.
- Protection measures are taken to counter specific threats:
  - Physical security
  - Access control
  - Accreditation processes
  - Cryptography



A closer look on cryptography

Cryptography is split in two phases

- asymmetric key exchange
- Symmetric en-/decryption



➢ Challenge: Well- established asymmetric algorithms can be broken by quantum computers

Good news

Quantum computers cannot break

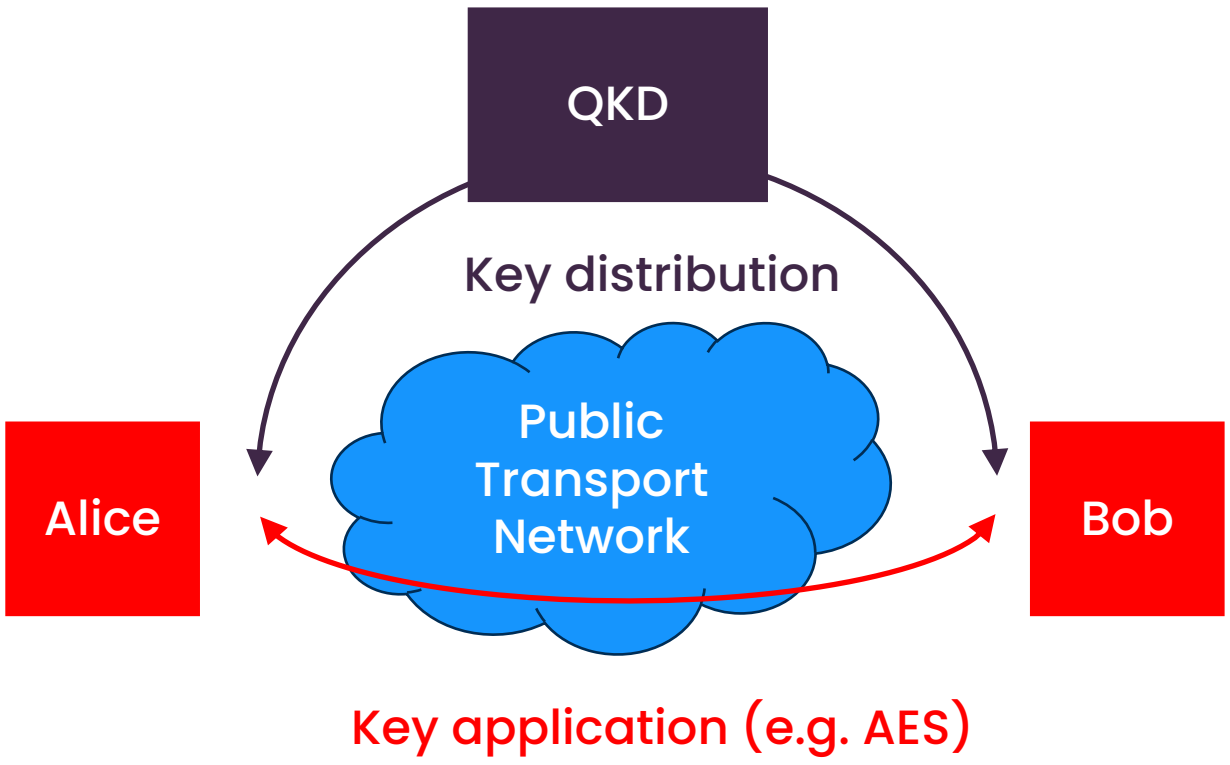
- Physical security
- Access control
- Accreditation processes

➢ From now on: we exclusively look at key exchange

QKD promises and non-promises

- QKD may replace vulnerable asymmetric algorithms
- QKD might guarantee quantum secure keys

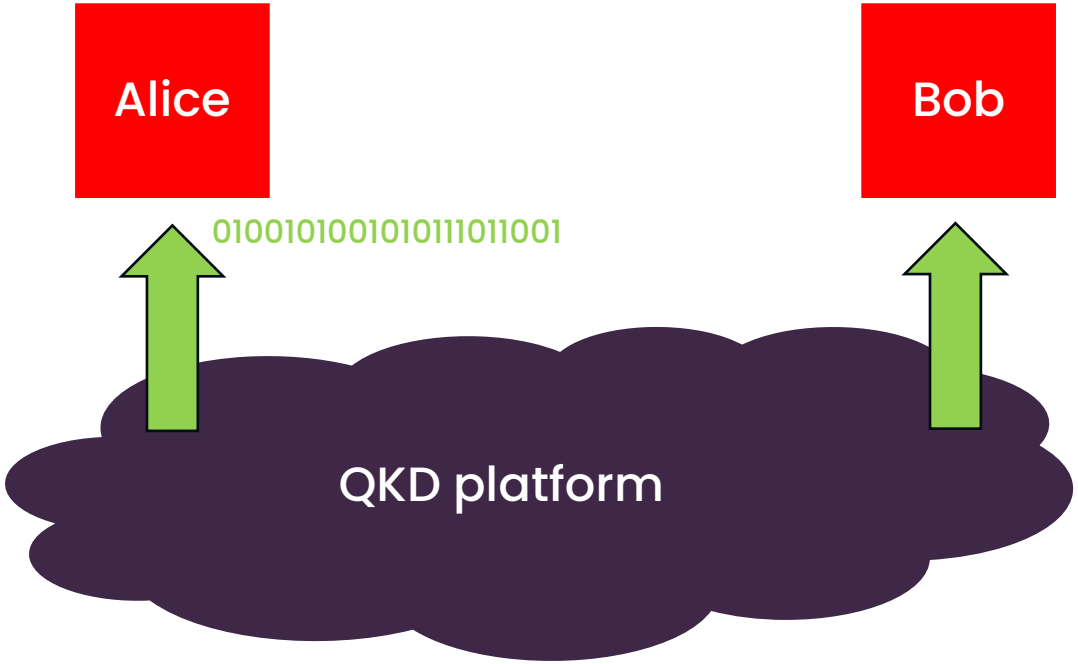
- QKD cannot offer end-to-end security
- QKD still requires trust between end points and QKD infrastructure



Problem Statement

- There is no way to prevent that a key provider knows the key.
- This is not a problem of trusted nodes but a fundamental fact.

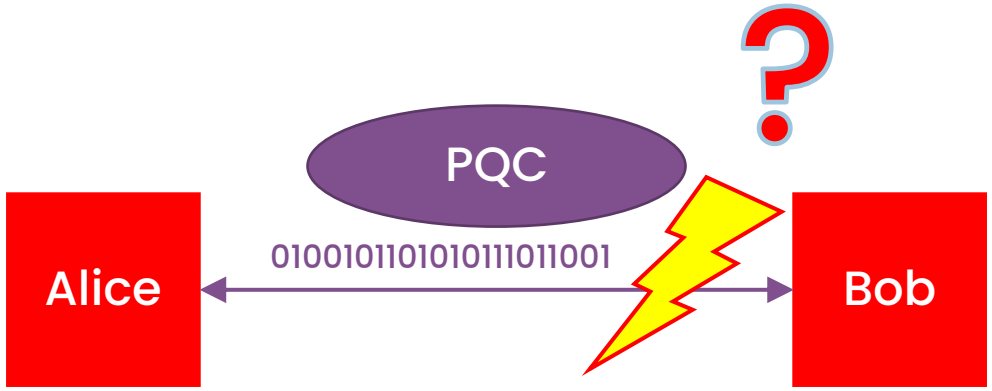
➢ End-to-end security provided by QKD is a misconception.



Problem Statement II

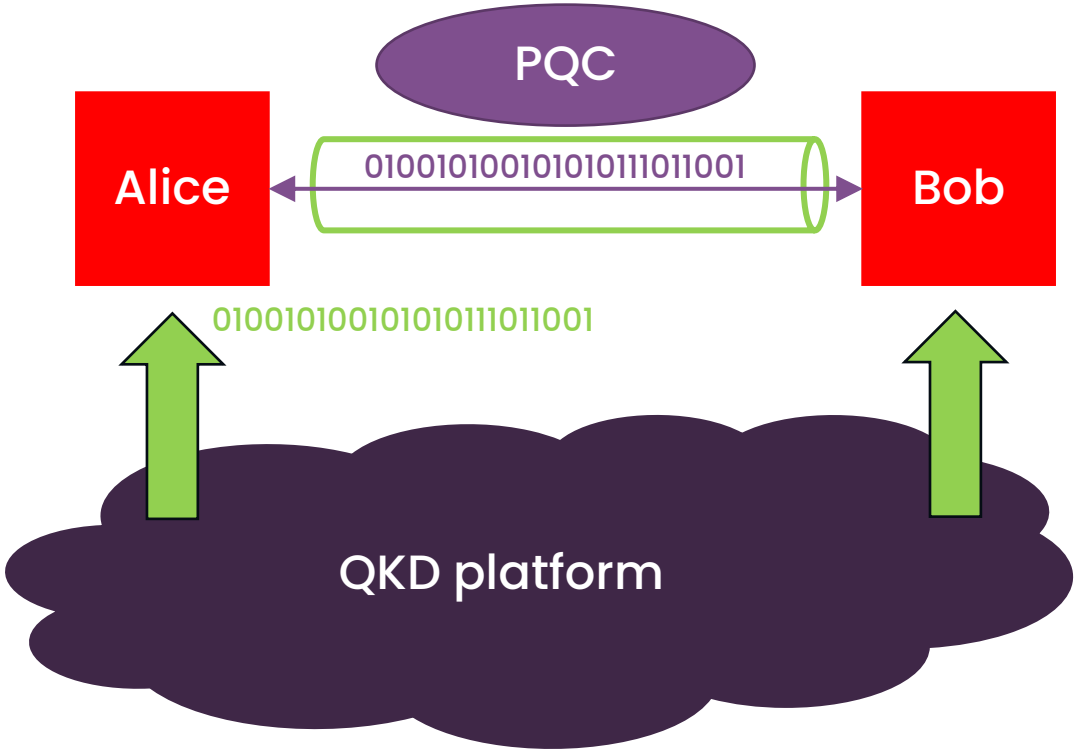
- Today's asymmetric algorithms are well proven since the 70's.
- Zillions of PhD students worked on them.

- Only recently, new PQC approaches have been investigated.
- There is no long-term guarantee for them yet.



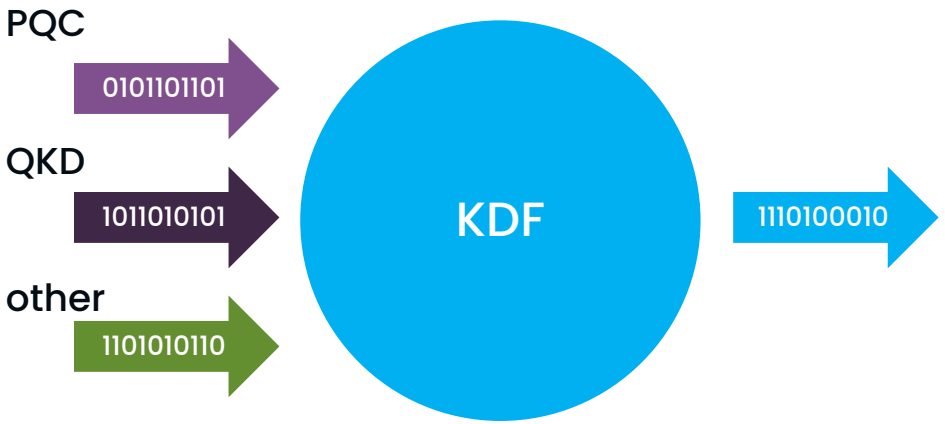
How to restore end-to-end security

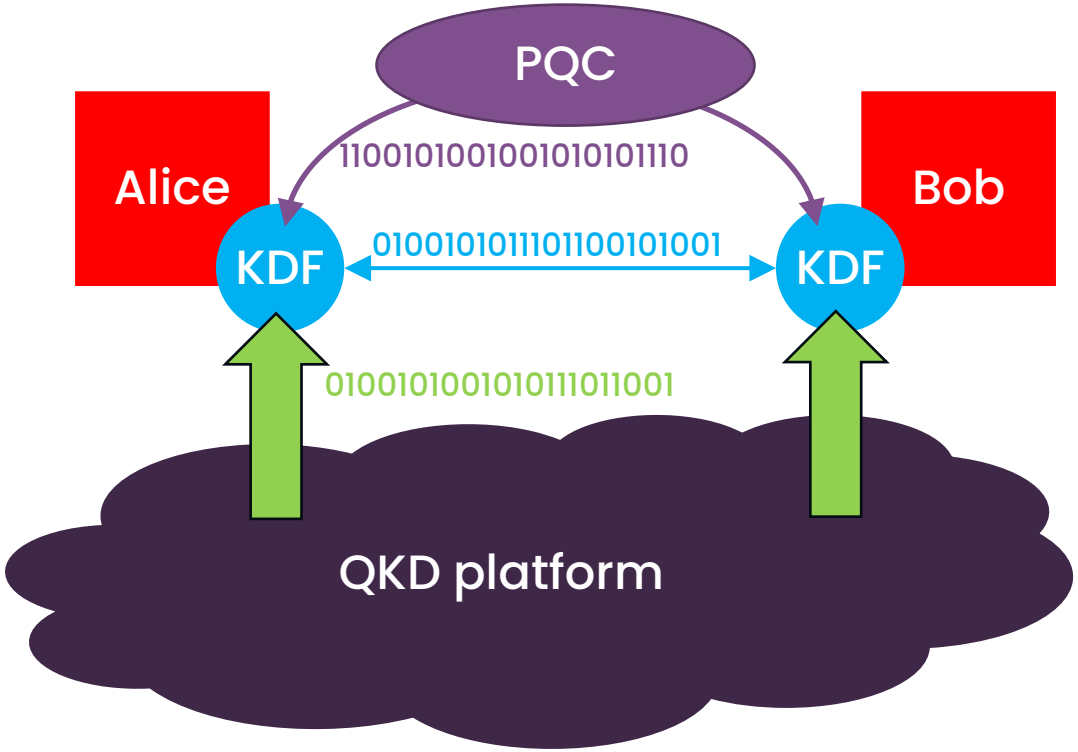
- Use QKD key to establish a quantum secure channel and negotiate classic key inside the symmetric encrypted channel.



How to restore end-to-end security II

- Use QKD key, classic key, PQC key and appropriate key derivation function (KDF)

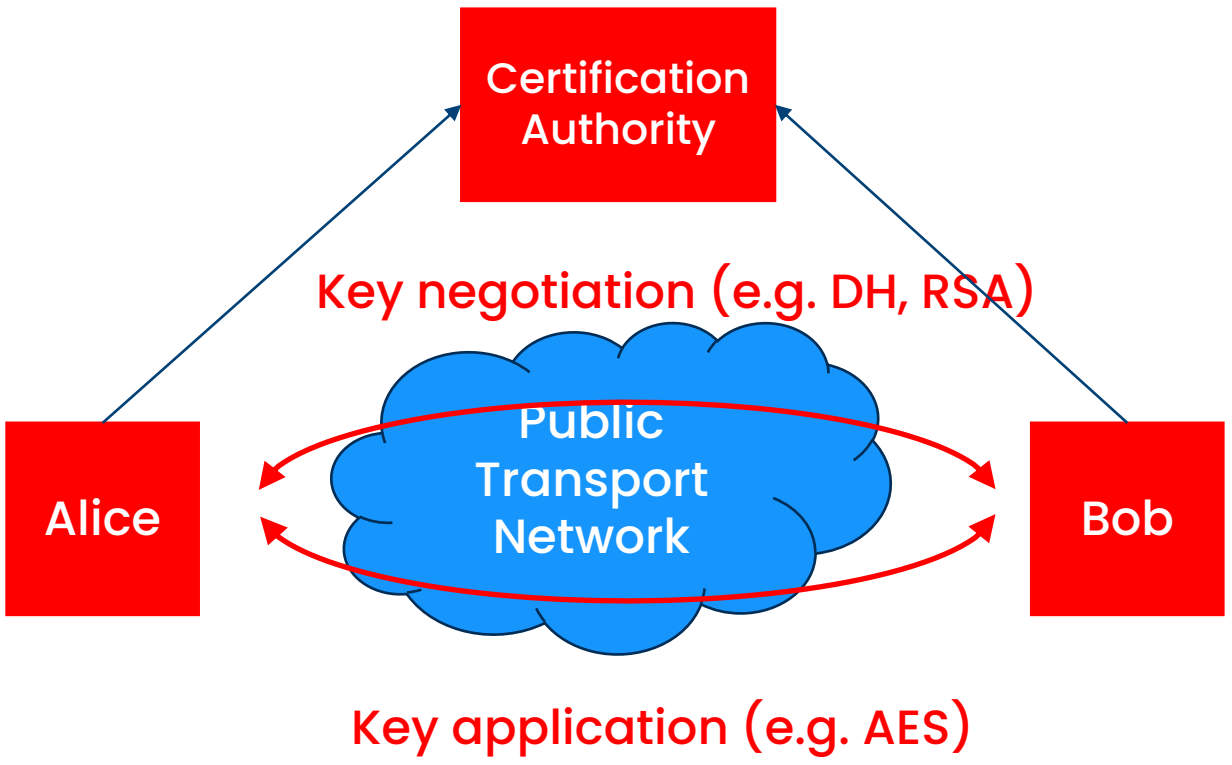




A closer look on cryptography – part II

- Symmetric encryption relies on the existence of a shared secret.
- Key exchange relies on authenticated end points.
- Authentication relies on a public key infrastructure.

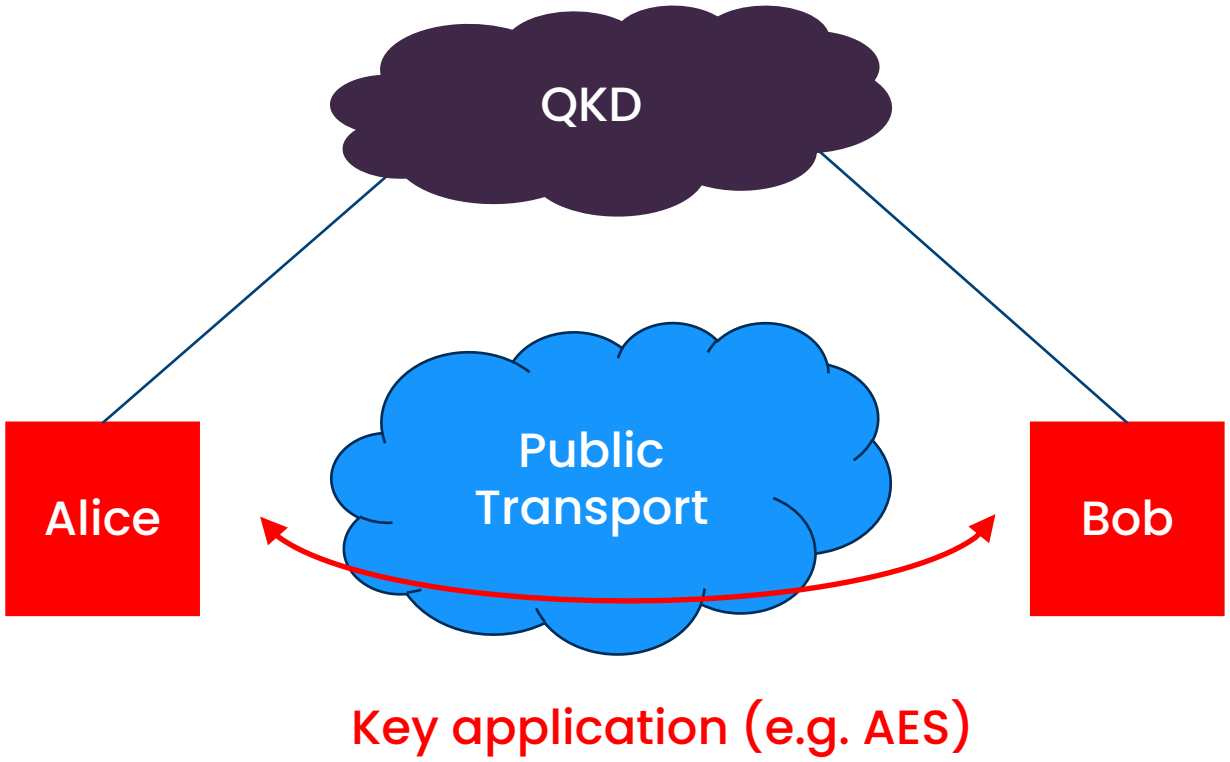
➢ Trust in a third party is already part of the concept.



QKD opportunities

- Quantum secure keys
- Authentication

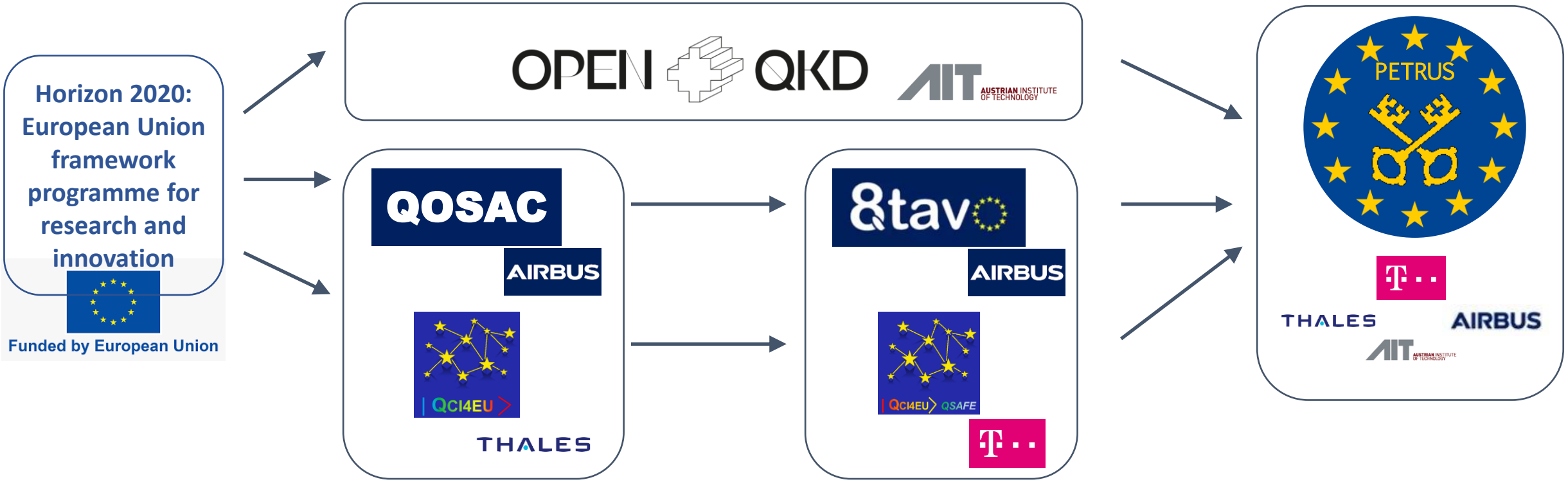
➢ Think of QKD platform as an extended PKI



Conclusion & Wrap up

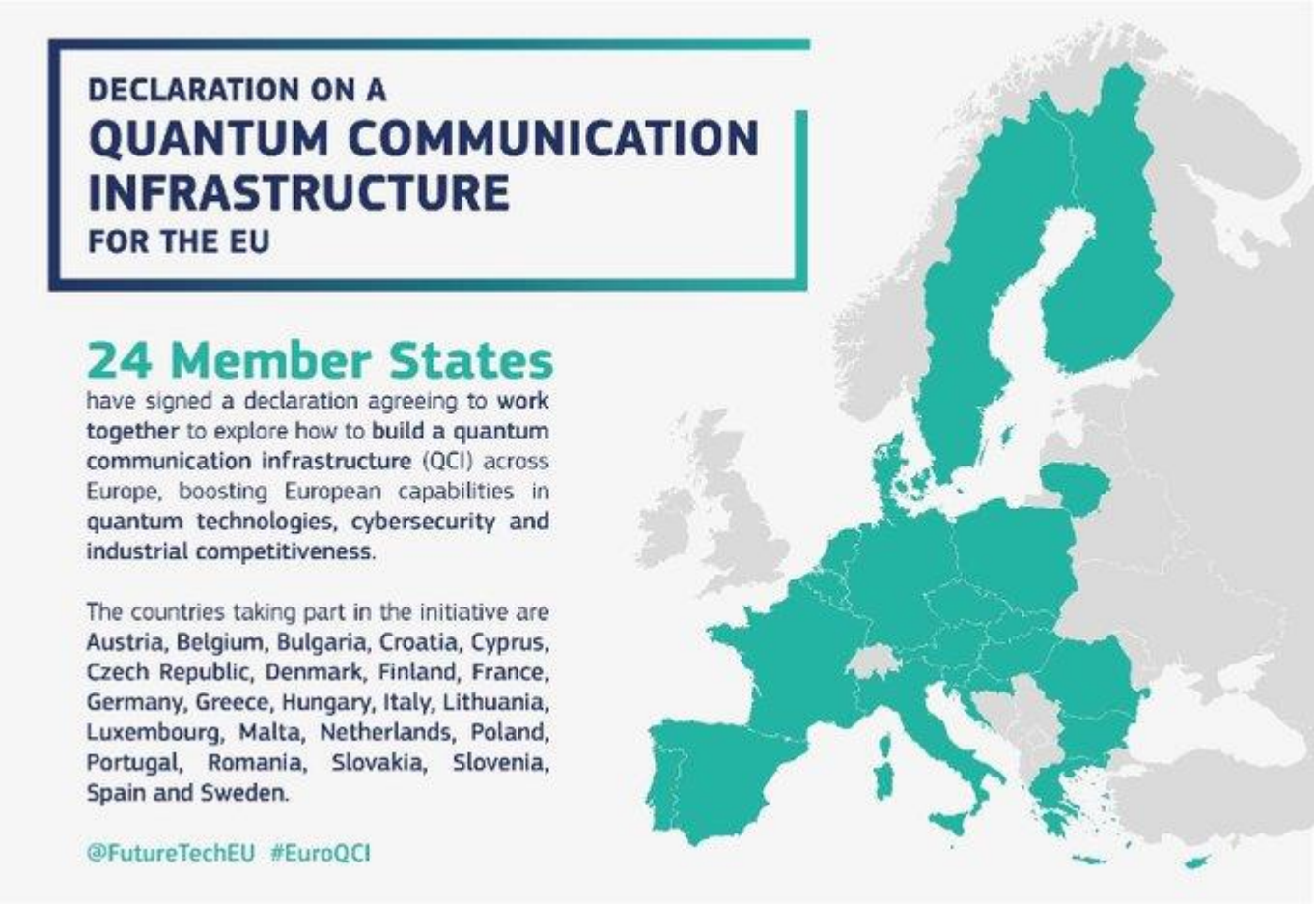
- Trust in a third party infrastructure is already a necessary ingredient by today.
- Exception:
  - Special networks with strongest security requirements for which special countermeasures and solutions are taken anyway
- Best of both worlds:
  - Combine advantages of QKD and PQC
  - Enable end-to-end security

PETRUS


Horizon 2020: European Union framework programme for research and innovation
Funded by European Union
OPEN QKD
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
QOSAC
AIRBUS
QCI4EU
THALES
8tavo
AIRBUS
QCI4EU QSAFE
PETRUS
THALES
AIRBUS
AIT

EuroQCI

The first operational system in the world providing Quantum Key Distribution (QKD) for the protection of government data & communications, telecommunications networks, data centres, critical infrastructure (energy, finance, etc.)



- EuroQCI Declaration signed by all the 27 Member States
- Joint Action Plan supporting the national terrestrial and space implementations

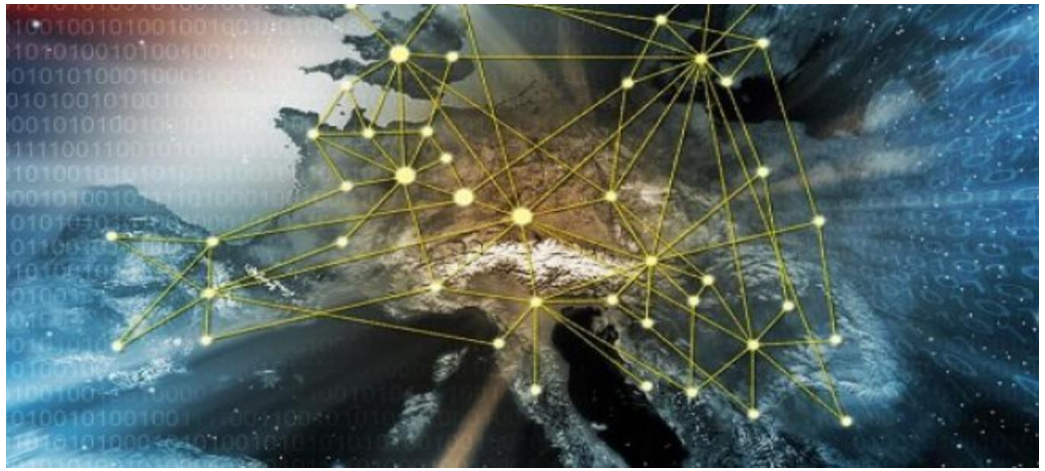
Source: European Commission

EuroQCI Overview

- **An integrated satellite and terrestrial system spanning the whole EU for ultra-secure exchange of cryptographic keys (Quantum Key Distribution)**
- Quantum communication infrastructure (QCI) is part of the European Cybersecurity Strategy and is **to be integrated in the new Secure Space Connectivity initiative 'IRIS²'**

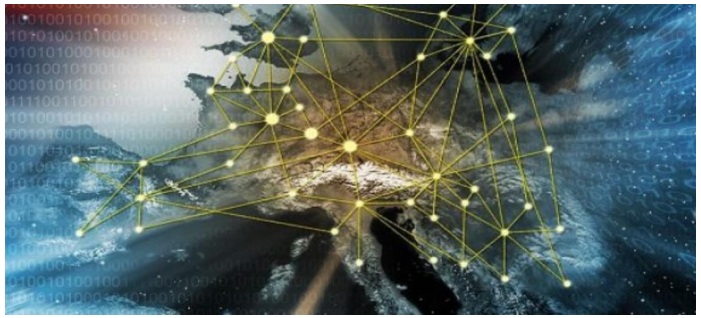
EuroQCI space segment
Distribution of quantum-secured encryption keys on a global scale

EuroQCI terrestrial segment
Federation of national terrestrial QCI networks with cross borders connections



Source: European Commission

EuroQCI Terrestrial Segment



2020 21 22 23 24 25 26 27 28

Studies: Design & Architecture

Preparatory and first deployment phase
- Establishing first national networks to experiment with QKD technology

Operational deployment phase
- Operational deployment, testing, validation and operationalisation

Key activities supported with EC funding from DEP and CEF in 2021-22

- Maturing EU quantum communication technologies (DEP QCI topic 1)
- Building the national QCI networks (DEP QCI topic 2)
- Coordination of national activities (DEP QCI topic 3)
- Cross-border links between national networks (CEF)
- Optical ground stations (CEF)
- Deployment of a European certification infrastructure (DEP QCI topic 4)

Source: European Commission

EuroQCI Space Segment

DIGITAL Europe
Industrial ecosystems
& national deployment

CEF - Connecting Europe Facility
Cross-border connections

21	22	23	24	25	26	27	28	29	30

Eagle 1

Preparation

Eagle 1 operation

EuroQCI – 1st generation

ESA / EU development
EuroQCI 1st Generation

1st generation
EuroQCI operation

Accredited QKD provision
integrated in secure connectivity

2nd Generation
EuroQCI operation

1st Generation

2nd Generation

Source: European Commission