ETSI/IQC Quantum Safe Cryptography Event

HYBRID AUTHENTICATED KEY EXCHANGES

STATUS-QUO, NOVEL CONSTRUCTIONS, AND APPLICATIONS TO LONG-RANGE QUANTUM-SAFE NETWORKS

Christoph Striecks

AUSTRIAN INSTITUTE OF TECHNOLOGY

SORBONNE UNIVERSITÉ

14/02/2023

Joint work with S. Ramacher, L. Perret, S. Bruckner

CENTRAL TOPICS TO BE COVERED

Limitations of QKD in long-range quantum-safe networks

Hybridization for secure long-range quantum-safe networks (combines QKD with PQC)

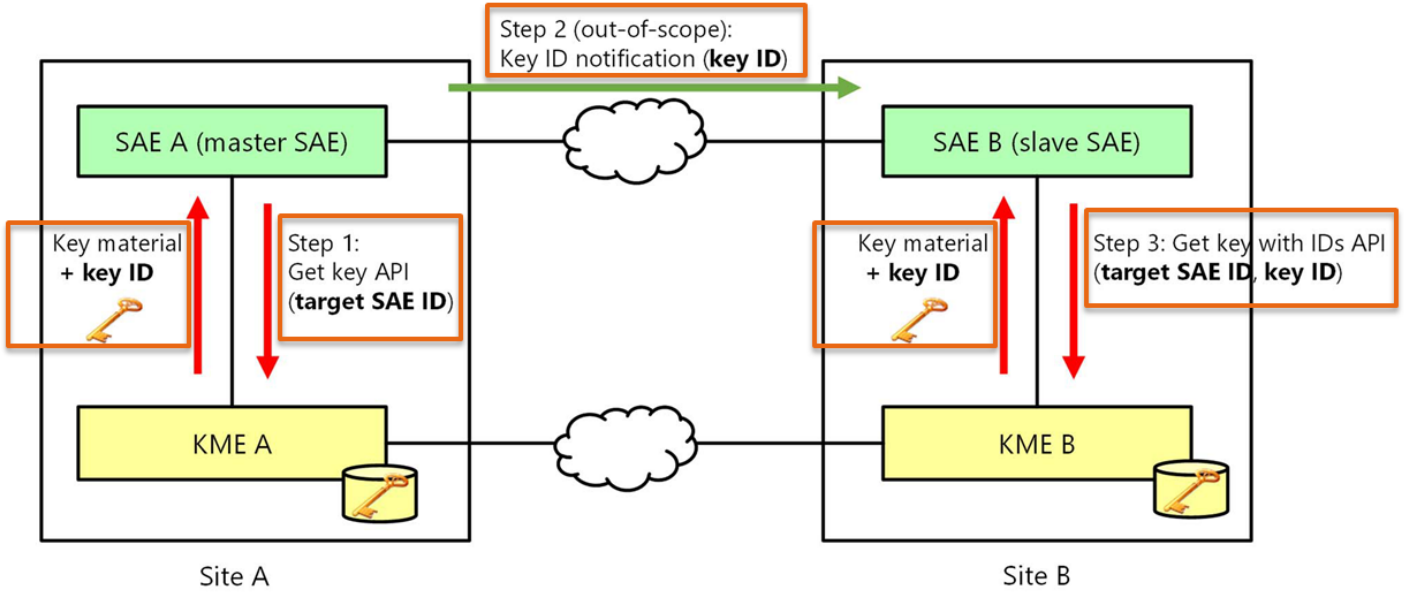
AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

QUANTUM KEY DISTRIBUTION

Establishing Shared Keys with Perfect Secrecy

QUANTUM KEY DISTRIBUTION (QKD)

- Main features:
  - **Perfectly** secret key distribution
  - Between any **two end-points**
  - **Terrestrially** or via **space**

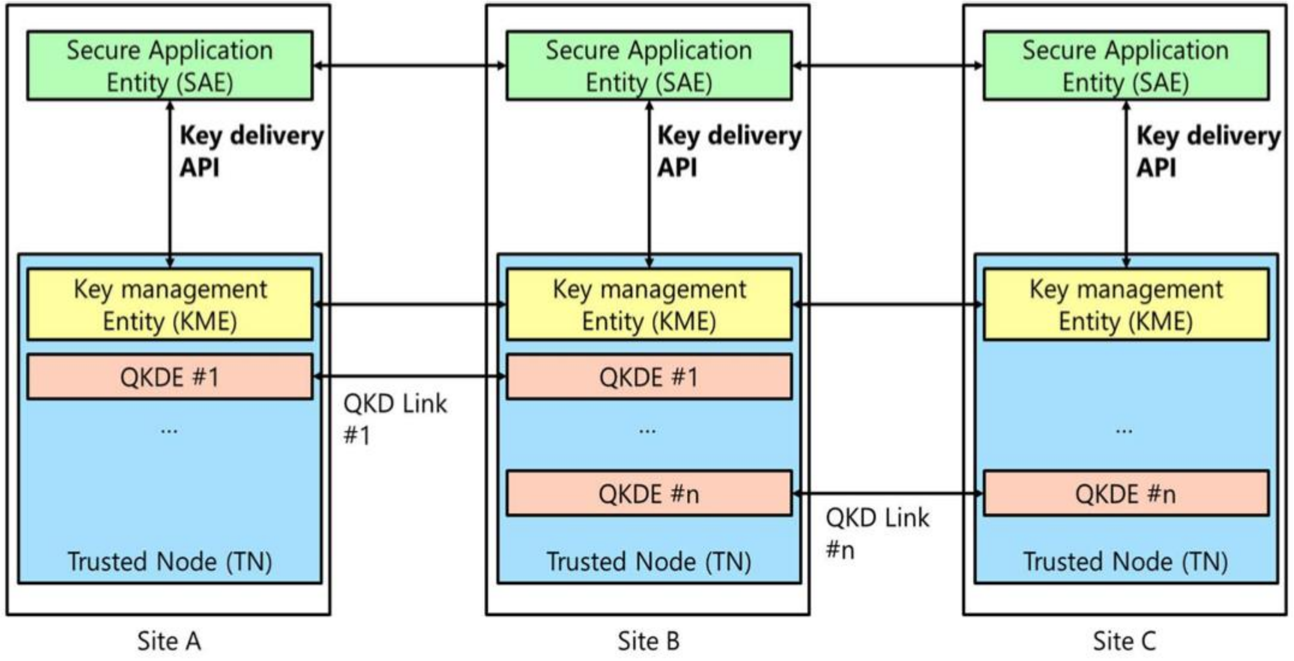


Key Establishment Scheme. Source: ETSI QKD GS 014 v1.1.1

QKD NETWORKS

- Gaps to solve:
  - QKD links have a **limited range** (depending on technology and desired key bit-rates)

- Needs:
  - **Trusted nodes** to bridge longer distances
  - **Pre-shared keys** to authen-ticate link-to-link nodes



QKD Network connecting different sites. Source: ETSI GS QKD 014 V1.1.1

LIMITATIONS FOR LONG-RANGE QKD NETWORKS

1. "QKD is [...] a solution for transforming a non-confidential **authenticated** channel into a confidential **authenticated** one." (Huttner et al.)

2. **Trusted nodes** are needed for long-range QKD

Long-Range QKD without Trusted Nodes is Not Possible with Current Technology

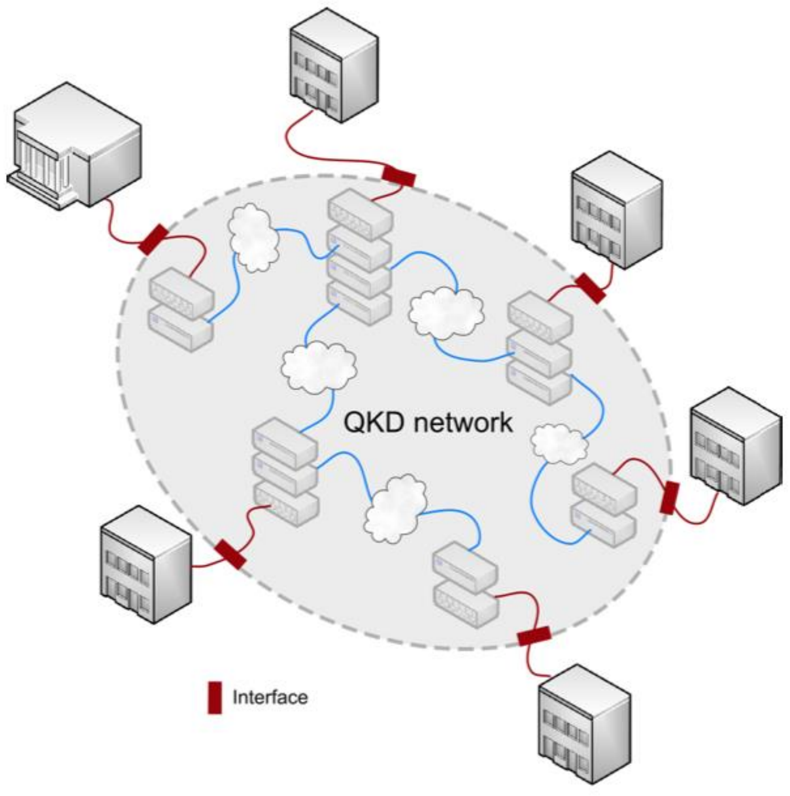
Authors:
Bruno Huttner, ID Quantique, Switzerland†;
Romain Alléaume, Telecom Paris - Institut Polytechnique de Paris, France;
Eleni Diamanti, Sorbonne University, CNRS - LIP6, France;
Florian Fröwis, ID Quantique Europe, Austria;
Philippe Grangier, Université Paris-Saclay, IOGS, CNRS, France;
Hannes Hübel, Austrian Institute of Technology, Austria;
Vicente Martin, Center for Computational Simulation / ETSIInf. Universidad Politécnica de Madrid, Spain;
Andreas Poppe, Austrian Institute of Technology, Austria;
Joshua A. Slater, QuTech - Delft University of Technology, The Netherlands ;
Tim Spiller, University of York, UK;
Wolfgang Tittel,
QuTech and Kavli Institute of Nanoscience, Delft Technical University, The Netherlands;
Department of Applied Physics, University of Geneva, Switzerland; Schaffhausen Institute of Technology in Geneva, Switzerland;
Benoit Tranier, ThalesAleniaSpace, France;
Adrian Wonfor, University of Cambridge, UK;
Hugo Zbinden, Department of Applied Physics, University of Geneva, Switzerland.

Source: https://arxiv.org/pdf/2210.01636.pdf

LIMIT 1: END-TO-END AUTHENTICITY

- Problem:
  - End-point (and node-to-node) authentication via pre-shared keys (PSKs) is **only link-to-link**
  - Authentication is **not transitive**

- One solution:
  - **Unique PSKs** for each entity that requires authentication (results in N^2 PSKs for N entities)
  - Requires **offline key exchanges** (e.g., via a “trusted courier”)
  - **Manageable** on a QKD device basis (but **inefficient** when the network gets larger)

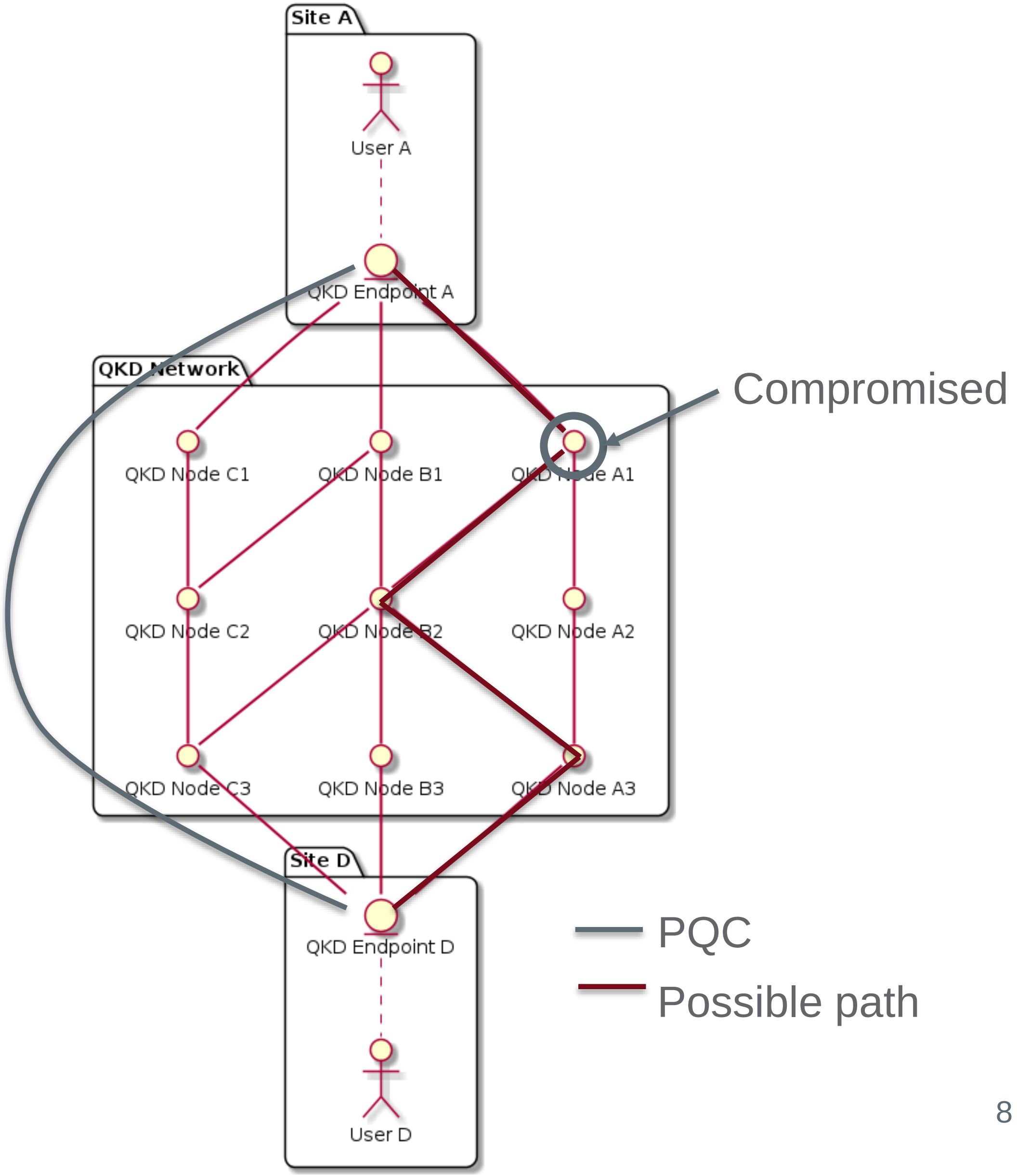


QKD network. Source: ETSI GS QKD 002 V1.1.1

LIMIT 2: TRUSTED NODES

- Problem:
  - Nodes on the QKD path **learn secret keys** (need to be trusted)
  - What happens if one node is **compromised**?

- One solution:
  - **Hybridization**, i.e., combine with post-quantum secure (PQC) mechanisms
  - Establishes **end-to-end confidentiality** (but cannot guarantee ITS as trade-off)



AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

HYBRID AUTHENTICATED KEY EXCHANGES

Resilient Key Exchanges with End-to-End Security

PRIMITIVE: HYBRID AUTHENTICATED KEY EXCHANGE (HAKE)

- Main features:
  - Protocol between **two entities**
  - Establishes **authenticated shared key**

- Goals:
  - **Authenticity** of both entities
  - **Confidentiality** of exchanged messages
  - Even more: **resilient keys** (forward secrecy and healing of channels)

- Authentication via:
  - PSKs, certificates, or passwords

- (Ephemeral) keys via:
  - Key encapsulation mechanisms and QKD keys

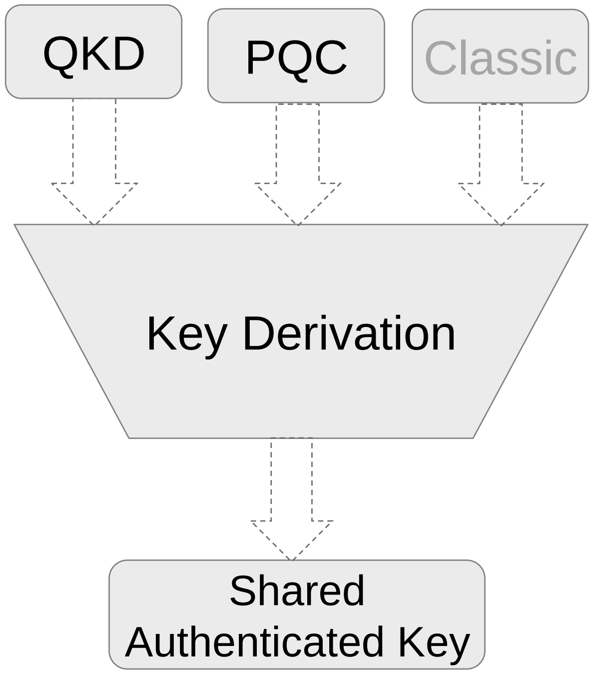
HAKE IMPLEMENTATION: MUCKLE

- Combining:
  - Keys from **QKD** layer
  - **PQC** key encapsulation mechanism
  - Optional: keys from **classical** cryptography (helps for migration to quantum-safe systems)
  - **PSK** for authentication

- Benefits:
  - **End-to-end authentication** and **confidentiality** (relying on PSKs)
  - **Resilience** (e.g., if PQC fails, guarantees for QKD still hold)
  - **"Backwards-compatibility"** (i.e., add a PQC/QKD layer to existing classical one)

Many a Mickle Makes a Muckle:
A Framework for Provably Quantum-Secure Hybrid Key Exchange

Benjamin Dowling[1], Torben Brandt Hansen[2], Kenneth G. Paterson[1]

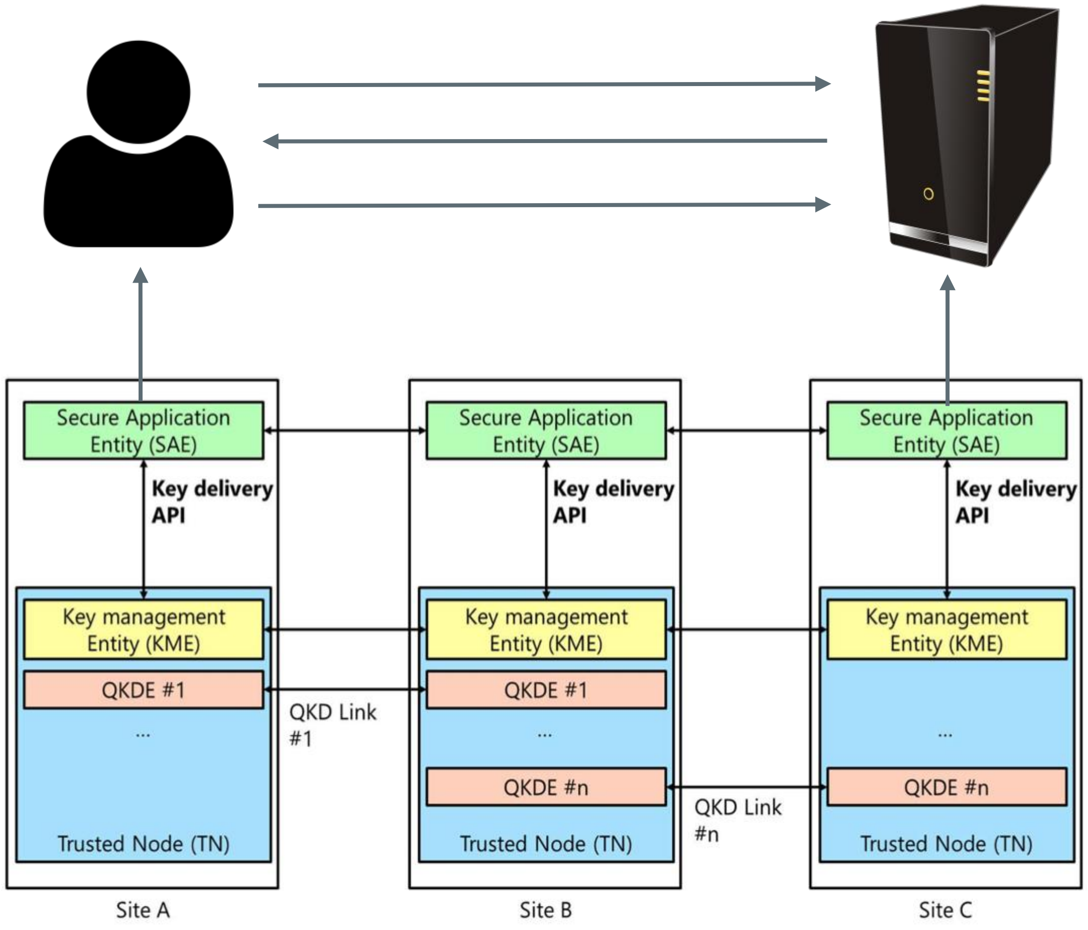


OUR PROPOSAL: MUCKLE+

- Features:
  - "**Muckle with PQC end-to-end authentication**" instead of PSKs
  - Requires only **hash functions** and **ciphers**:
    - XMSS: NIST SP 800-208
    - SPHINCS+ (selected for standardization), Picnic (3rd round candidate of NIST PQC)

- Trade-offs:
  - Enables (end-to-end) **services** with certificates
  - **Computational** security
  - Optimized for **long-range quantum-safe networks** such as the EuroQCI (without PSKs)

- PoC implementation:
  - **Available** (with **experimental results**), contact us if interested



QKD Network connecting different sites. Source: ETSI GS QKD 014 V1.1.1

ON POTENTIAL QDK/PQC END-TO-END HYBRIDIZATION OPTIONS (UPDATED: 15/2/2023)

	Confidentiality	Authenticity
QKD	• Perfect (trusted nodes) • No resilience	• Perfect (N^2 unique PSKs) • No resilience
QKD + PQC Signatures	• Computational (from ciphers, trusted nodes) • No resilience	• Computational (from hash function or ciphers) • No resilience
QKD + PQC Encryption	• Computational • Resilient - if PQC fails, perfect (trusted nodes) - if QKD fails, computational	• Perfect (N^2 unique PSKs) • No resilience
QKD + PQC (Encryption/Signatures)	• Computational • Resilient - if PQC fails, computational (from ciphers if PQC signatures are from hash functions or ciphers) - if QKD fails, computational	• Computational (from hash function or ciphers possible) • No resilience
PQC (Encryption/Signatures)	• Computational • No resilience	• Computational (from hash function or ciphers possible) • No resilience

MIGRATION TO QKD/PQC HYBRID SYSTEMS (CRYPTOGRAPHICALLY)

New system

- Build **agile** cryptographic systems; use **hybrid** approach (QKD/PQC)

Running system

- Add QKD/PQC to your classically secured cryptosystem if possible as an **extra layer** (via hybrid approach), then **switch off classical** layer

Source:
https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

THANK YOU!

Supported by EU DIGITAL project QCI-CAT (PID 101091642)
and Austrian national KIRAS project QKD4GOV

Christoph Striecks

Scientist
Security & Communication Technologies
Center for Digital Safety & Security

AIT Austrian Institute of Technology GmbH
Giefinggasse 4 | 1210 Vienna | Austria
T +43 50550-4113 | M +43 664 8251141
christoph.striecks@ait.ac.at | www.ait.ac.at