ETSI/IQC Quantum Safe Cryptography Conference 2026

On developing quantum-safe hybrid cryptographic standards

Presented by: Christoph Striecks

with

Joint work by AIT Austrian Institute of Technology with Telefónica ID (TID) for ETSI STF 684 “Quantum-Safe Cryptographic Solutions”: Augustine Bugler (AIT), David Gomez (TID), Josemi Hernandez (TID), Stephan Laschet (AIT), Luca Torresetti (AIT)

17/06/26

Co-funded by the European Union

Co-funded by EFTA

ETSI/IQC Quantum Safe Cryptography Conference 2026

On developing quantum-safe defense-in-depth cryptographic standards

Presented by: Christoph Striecks

with

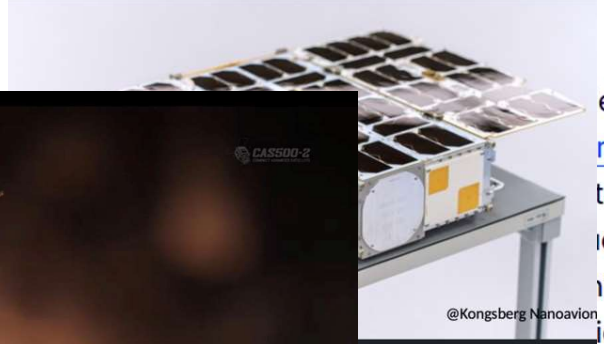
Joint work by AIT Austrian Institute of Technology with Telefónica ID (TID) for ETSI STF 684 “Quantum-Safe Cryptographic Solutions”: Augustine Bugler (AIT), David Gomez (TID), Josemi Hernandez (TID), Stephan Laschet (AIT), Luca Torresetti (AIT)

17/06/26

Co-funded by the European Union

Co-funded by EFTA

Launch of quantum satellite QUBEII tomorrow



We are very happy to announce the launch of the quantum satellite QUBE-II on 3 May 2026.

The QUBE-II satellite is set to demonstrate the exchange of quantum cryptographic keys between a microsatellite (CubeSat) and a ground station – a crucial step towards secure quantum communication.

The project sponsored by BMFTR is a joint research initiative led by OHB System AG in collaboration with DLR, ZfT Würzburg, LMU Munich and FAU Erlangen-Nuremberg.

Launch Event in Erlangen at #FAU

Shapi

Home

Home >

DIGIBYTE

The
netw

At the Dig es
(Belgium, ration
agreeing tum
communi icture would
enable int nication
assets all ional
communi making use
of existin der level,
and a spa ts.

The QCI v st cyber
threats, protecting smart energy grids, air traff nore from
hacking. It will also enable data centres to stor preserve
the long-term privacy of government data. The e to become
the backbone for Europe's Quantum Internet, c and
sensors via quantum networks to distribute inf urope.

The first service to make use of this new infras QKD). QKD

https://digital-strat

MAIN CHALLENGE: AUTHENTICATION

- "Authentication provides **guarantees** on the **identities** of the parties involved in the protocol execution." [GFW19]
- Problem: quantum networks (e.g., based on QKD) do not solve **source authenticity**
- Solutions:
  - **Pre-placed keys:** e.g., via trusted couriers or key-distribution centers (but difficult to scale to multiple domains)
  - **Asymmetric Cryptography:** using PQC via public key infrastructures (PKIs)

<u>"Everlasting" security vision</u>:
PQC required to bootstrap, but the key may inherit the strong security guarantees from quantum-based cryptography

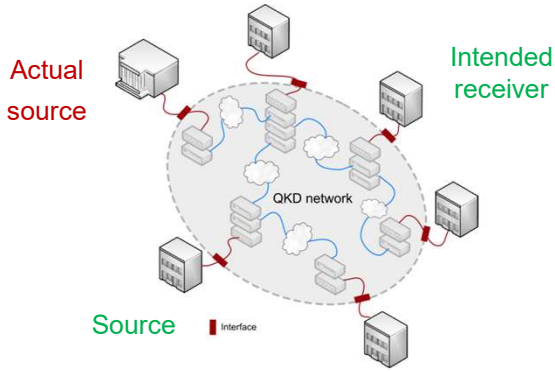
Technical limitations

1. **Quantum key distribution is only a partial solution.** QKD generates keying material

Reliance on classical cryptography for peer authentication

Establishment of cryptographic keys between communicating parties in a network is only one of a number of necessary steps needed to ensure secure communications. A critical additional mechanism is **authentication**; that is, establishing the identity of those parties. QKD does not provide authentication, nor do any other quantum techniques. Therefore, in practice, QKD must be combined with other cryptographic services to provide security against the threat from quantum computing, and therefore should not be relied on as a mechanism that provides substantial security value.

https://www.ncsc.gov.uk/paper/quantum-networking-technologies



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

DEFENSE-IN-DEPTH (HYBRID) MECHANISMS

AUSTRIAN INSTITUTE OF TECHNOLOGY

Combination of **conventional** (asymmetric and symmetric), **post-quantum**, and **quantum-based cryptography** with certain *security requirements*.

- **Confidentiality**: only intended parties know the key; may be based *on symmetric keys, classical KEMs, PQ KEMs & quantum-based cryptography* (e.g., QKD via ETSI 014 interface)
- **Authentication & Integrity**: parties are certain of each other's identity, untampered data; based on *symmetric keys, PQ signatures, MACs*
- **Security Proof**: combining technologies maintains overall security, *"core claim of the security analysis"*

Particularly: suitable mechanism for securing quantum (communication) networks.

Confidentiality alone is insufficient for nearly all use cases!

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]

https://eprint.iacr.org/2020/099.pdf

The security proof is the toughest challenge, as it must encompass all requirements.

DEF-IN-DEP WORKS WITH SECURITY PROOFS

AUSTRIAN INSTITUTE OF TECHNOLOGY

HAKE Protocols	Connection Types	Confidentiality	Authentication
Muckle [DBP20]	Point-to-Point (P2P)	Computational (KDF)	Pre-Shared Key (PSK)
Muckle+ [BRS23]	End-to-End (E2E)	Computational (KDF)	PQ Signatures
Muckle++ [GPH+24]	P2P	Computational (KDF)	PSK *or* PQ Signatures
Muckle# [BSP+24]	E2E	Computational (KDF)	KEMs
VMuckle [BBB+25]	E2E	Computational (KDF)	PSK/PQ Signature
ITS AKE [HPSV26]	P2P	“Long-term” (XOR, in their model)	KEMs
Non-BB Hybrid [Fer26]	P2P	Computational (KDF, in their model)	PQ Signatures
VMuckle-ES [ETSI26]	E2E/P2P	Computational/”long-term” (KDF/XOR)	PQ Signatures (PSK fallback)

[DBP20] Dowling, Brandt Hansen, Paterson: Many a Mickle Makes a Muckle: A Framework for Provably Quantum-Secure Hybrid Key Exchange. PQCrypto 2020: 483-502

[BRS23] Bruckner, Ramacher, Striecks: Muckle+: End-to-End Hybrid Authenticated Key Exchanges. PQCrypto 2023: 601-633

[GPH+24] Garms, Paraïso, Hanley, Khalid, Rafferty, Grant, Newman, Shields, Cid, O'Neill: Experimental Integration of Quantum Key Distribution and Post-Quantum Cryptography in a Hybrid Quantum-Safe Cryptosystem. Wiley 2024

[BSP+24] Battarbee, Striecks, Perret, Ramacher, Verhaeghe: Quantum-Safe Hybrid Key Exchanges with KEM-Based Authentication. CoRR abs/2411.04030 (2024)

[BBB+25] Buruaga, Bugler, Brito, Martin, Striecks: Versatile Quantum-Safe Hybrid Key Exchange. EPJ Quantum Journal 2025

[HPSV26] Hövelmanns, Planken, Schaffner, R. Verschoor: QKD Oracles for Authenticated Key Exchange. https://arxiv.org/abs/2509.12478

[Fer26] Ferreira: AKE Protocol Combining PQC and QKD. IACR Communications in Cryptology 2026.

[ETSI26] https://docbox.etsi.org/CYBER/qsc/open/ETSI%20TS%20104%20146%20for%20public%20consultation.pdf

TS 104 146 IN STF 684 “QUANTUM-SAFE CRYPTOGRAPHIC SOLUTIONS” WP3

- **WP3 goal:** combine *Quantum and Post-Quantum Cryptography Components in defense-in-depth (hybrid) approach* with **authentication** and **security proofs**

- **Status TS 104 146 (V0.0.4, 4/2026):**
  - Protocol description stable, document available in *stable draft* for comments, based on TS 103 744
    - https://docbox.etsi.org/CYBER/qsc/open/ETSI%20TS%20104%20146%20for%20public%20consultation.pdf
  - Generic approach: but at least PQC components required
  - *Final draft* expected

- **Reference implementation** by Telefónica ID and AIT started

Co-funded by the European Union

Co-funded by EFTA

TAKE-AWAYS AND RECOMMENDATIONS

- **Emerging: TS 104 146 in STF 684 "Quantum-Safe Cryptographic Solutions"**
  - **Vision: particularly useful** in large-scale secure **quantum communication networks**
  - **Now: def-in-dep quantum-classical** key exchange protocol with **long-term security**
  - **Final draft** to be expected soon; reference implementation ongoing

- **Open Points Remain**
  - **Standardisation efforts** should be intensified for **quantum-based networks** (e.g., PQ PKI)
  - **Further harmonisation** of integrating **quantum technologies** into classical infrastructures

- **Strengthen Collaboration**
  - Community effort of **quantum** and **non-quantum** experts required

THANK YOU!

Co-funded by the European Union and EFTA.

Christoph.Striecks@ait.ac.at

„LONG-TERM“ DEF-IN-DEP CONCEPT

- **Until the end of the (initial) key-exchange run**, the adversary must be computationally bounded
  - Consequence: no PSKs for authentication in multi-domain networks required

- **After the protocol run**, the shared key is protected at least by post-quantumm *and* quantum-based cryptography
  - Consequence: attacker must break at least both layers

Particularly: key inherits the strong security properties from quantum-based cryptography