



ETSI/IQC Quantum Safe Cryptography Conference 2026

ETSI ISG QKD update

Presented by: Martin Ward

TOSHIBA

17/06/2026

© ETSI 2026. All rights reserved.

Quantum Key Distribution

QKD

Agrees shared secret bit strings between remote parties

Involves the transport of quantum states

Security is based on quantum mechanics

QKD protocols: composable epsilon-secure security proof

Sustained secure key expansion

CRYPTOGRAPHIC AGILITY

Consider appropriate use-cases for modernized symmetric key infrastructure (SKI)

Systems that can use symmetric keys from a key manager



About ISG QKD



PLENARY MEETINGS

2 per year often at Member sites (hybrid access)

Next: QKD#41 Warsaw, Poland 30 November–2 December 2026

ONLINE MEETINGS

Typically 1st and 3rd Tuesday of month

CHAIR

Martin Ward

VICE CHAIRS

Norbert Lütkenhaus

Vicente Martin Ayuso

Momtchil Peev

Atilla Hasekioğlu

TECHNICAL OFFICER

Carmine (Lino) Rizzo

EXPERTS WITH BROAD SKILLS AND EXPERIENCE

QKD vendors; application vendors; network operators; government bodies; certification labs; National Metrology Institutes; academic experts



Protection Profile Key Processing Module



DGS/QKD-024_PP-KPM

Ease the certification of QKD network products

Key establishment including relay (e.g. with range of epsilon-secure composable protocols) across a network (potentially via multi-path protocols etc.)

Preparation of keys for applications (allocation, splitting, combination etc.)

Hybridisation, privacy amplification etc.

Ensure delivery only to assigned recipients

Enforce policies / request requirements

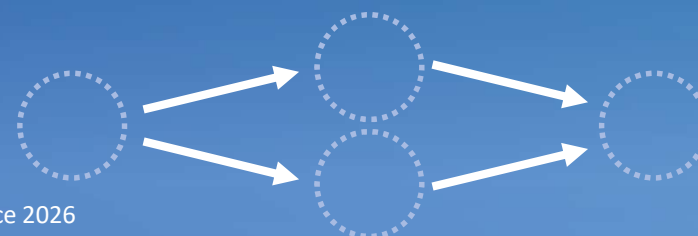
LINEAR OTP



CENTRALISED



MULTIPATH



Protection Profile Key Processing Module



DGS/QKD-024_PP-KPM

Preparatory milestones completed; **formal CC drafting underway**

ETSI STF 684 from EISMEA call to develop PP for Key Processing Modules for trusted node networks and authenticated hybrid key exchange protocol



Existing certified PP for QKD Modules:

ETSI GS QKD 016 V2.1.1

https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/02.01.01_60/gs_QKD016v020101p.pdf

BSI Certification Report

https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0120.html

Protocol Structure and Security Proofs



RGS/QKD-0005ed2_SecProofs

Complete stand-alone Protocol Security Proof documents starting to be published in academic literature

Looking towards standardisation of practical QKD protocols

- block-wise (iterative) sifting
- more realistic physical models etc.

Updating to match Protection Profile for QKD modules GS QKD 016

Title added “Protocol Structure” to better reflect contents



REASONS FOR CREATING

Security model

Trust model

Specific hardware considerations

- QKD modules
- QKD links (optical)

Place interface specifications in context

MULTI-OPERATOR NETWORKS

Global architecture needs to be adaptable

Different approaches to network / infrastructure management and orchestration

Range of trust: domains of same operator to desire to minimize shared of network information

SECURITY ANALYSIS

Identify fundamental local functionalities

How these interact

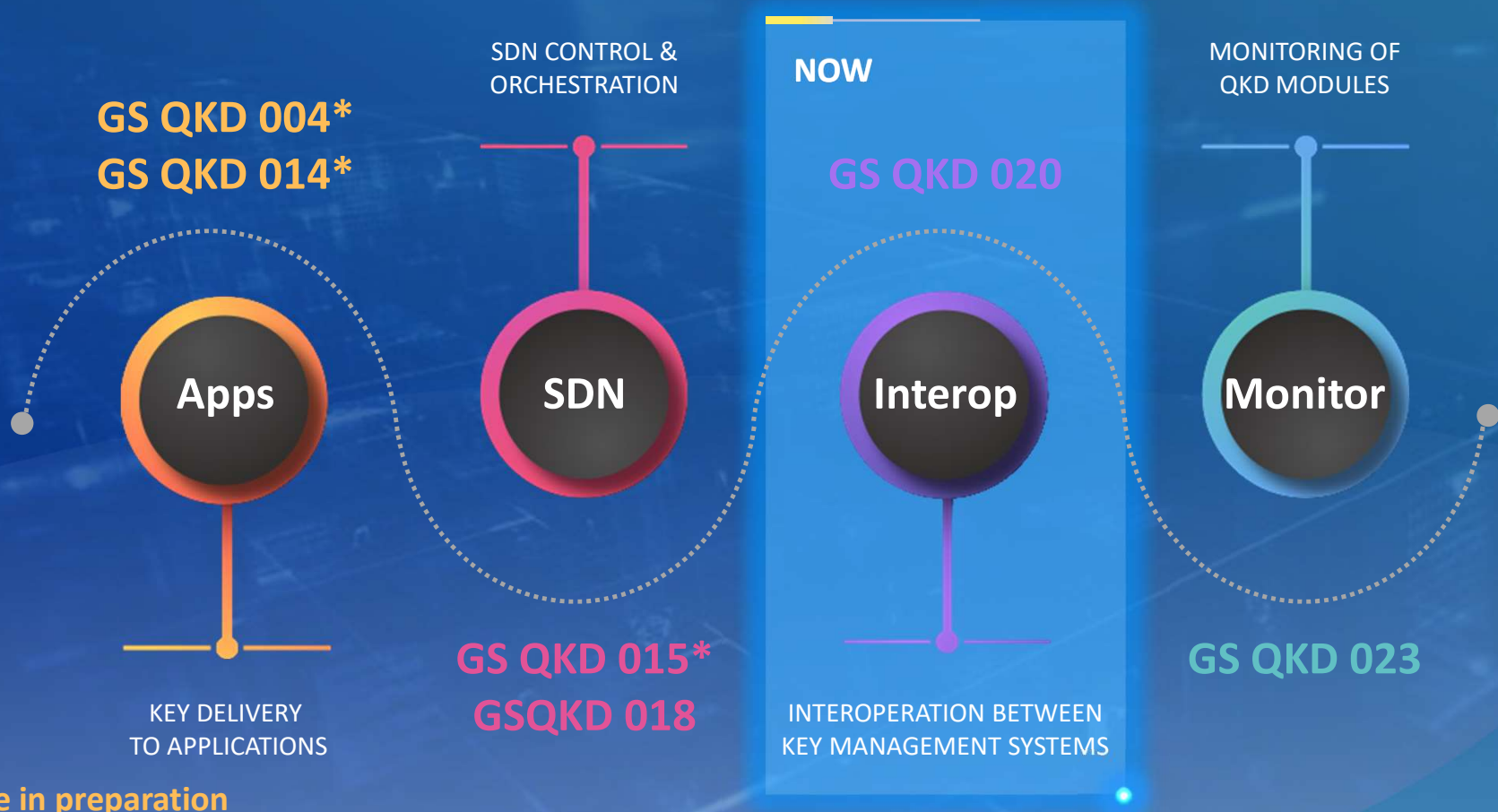
Expect different groupings

Architecture aids users analyse security arguments

- traversing operator boundaries etc.

Timeline overview of interfaces

ETSI IS MEMBER-DRIVEN SDO
Specify interfaces when commercial need based on Member contributions



*** Update in preparation**

Interoperable KMS API (GS QKD 020)



DGS/QKD-020_InteropKMS

REST API for horizontal transfer of keys between key management from different domains / network operators etc.

Multi-operator networks increasingly common

OpenAPI-first (v3.1) with ETSI specification largely derived from this

Recently approved; publication expected by July





GR QKD 007 V1.2.1 “Quantum Key Distribution (QKD); Vocabulary”

Update published January 2026

Many updated definitions including for QKD

From this version we intend the document to form the base definitions of terms for new ISG QKD publications

quantum key distribution: procedure involving the transport of quantum states to agree shared secret bit strings between remote parties using a protocol with security based on quantum entanglement or the impossibility of perfectly cloning or measuring the unknown transported quantum states

independent ancilla: quantum state that is uncorrelated with the signal information relating to an

QKD link: set of active and/or passive components that connect QKD modules to enable them to perform QKD

prepare and measure QKD: a QKD system to establish a QKD system to establish a QKD module prepares quantum state and other measures quantum state



Join us

Help the community develop specifications for QKD

Published deliverables available as free downloads

ETSI MEMBERS

Use the portal to view drafts or register for meetings

Join the QKD ISG mailing list

OTHERS...

The screenshot displays the ETSI portal interface. At the top, there is a search bar and a 'Member Portal' link. Below the search bar, a message indicates 'There are 17 results'. The main content area is divided into two columns. The left column contains a 'Filter search results' section with the following options:

- SEARCH TERM:** A search input field.
- SEARCH IN:** Checkboxes for 'Title', 'ETSI number', and 'Content'. 'Title' and 'ETSI number' are checked.
- VERSION / STATUS:** Radio buttons for 'All versions' (selected) and 'Major versions only'.
- Checkboxes:** 'ENs, EGs or ESs on Approval' (checked), 'Published' (checked), 'Withdrawn' (checked), and 'Historical' (checked).
- FILTER BY Markers:** Checkboxes for 'Current' (checked) and 'Superseded' (checked).

The right column displays a list of search results. Each result includes a checkbox, the specification title, the status (Published), and a 'CURRENT' or 'SUPERSEDED' label. The results shown are:

- ☐ ETSI GS QKD 018 V1.1.1 (2022-04) **Published** **CURRENT**
Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks
- ☐ ETSI GS QKD 016 V2.1.1 (2024-01) **Published** **CURRENT**
Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules
- ☐ ETSI GS QKD 016 V1.1.1 (2023-04) **Published** **SUPERSEDED**
Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules

A group of diverse people in business casual attire are gathered outside a modern building with large glass windows. They are engaged in conversation, and some are holding white disposable cups. The scene is brightly lit, suggesting daytime. The text 'Meet ETSI' is overlaid on the right side of the image in a large, white, sans-serif font.

Meet ETSI

at the info Stand