ETSI/IQC Quantum Safe Cryptography Conference 2026

ETSI ISG QKD update

Presented by: Martin Ward

TOSHIBA

17/06/2026

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

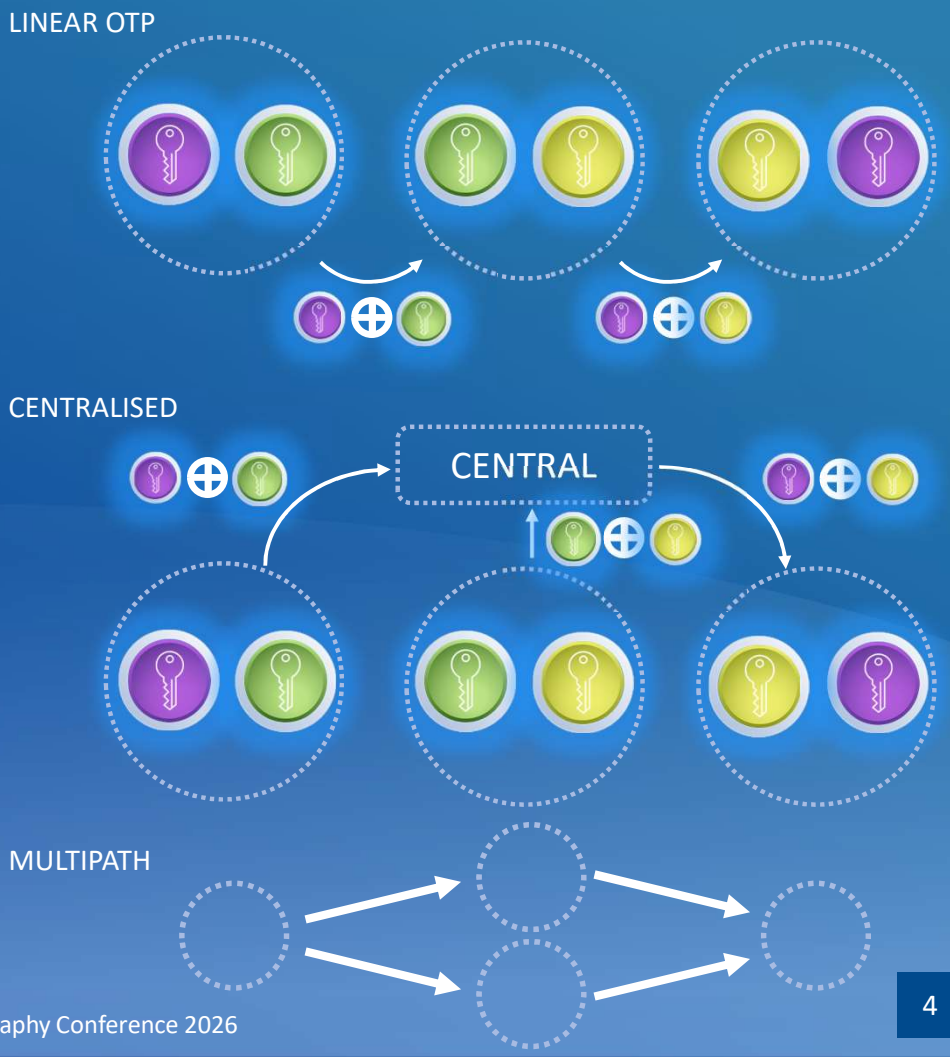
Key establishment including relay (e.g. with range of epsilon-secure composable protocols) across a network (potentially via multi-path protocols etc.)

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

Hybridisation, privacy amplification etc.

Ensure delivery only to assigned recipients

Enforce policies / request requirements



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

Co-funded by the European Union

Co-funded by EFTA

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

Network Architecture

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

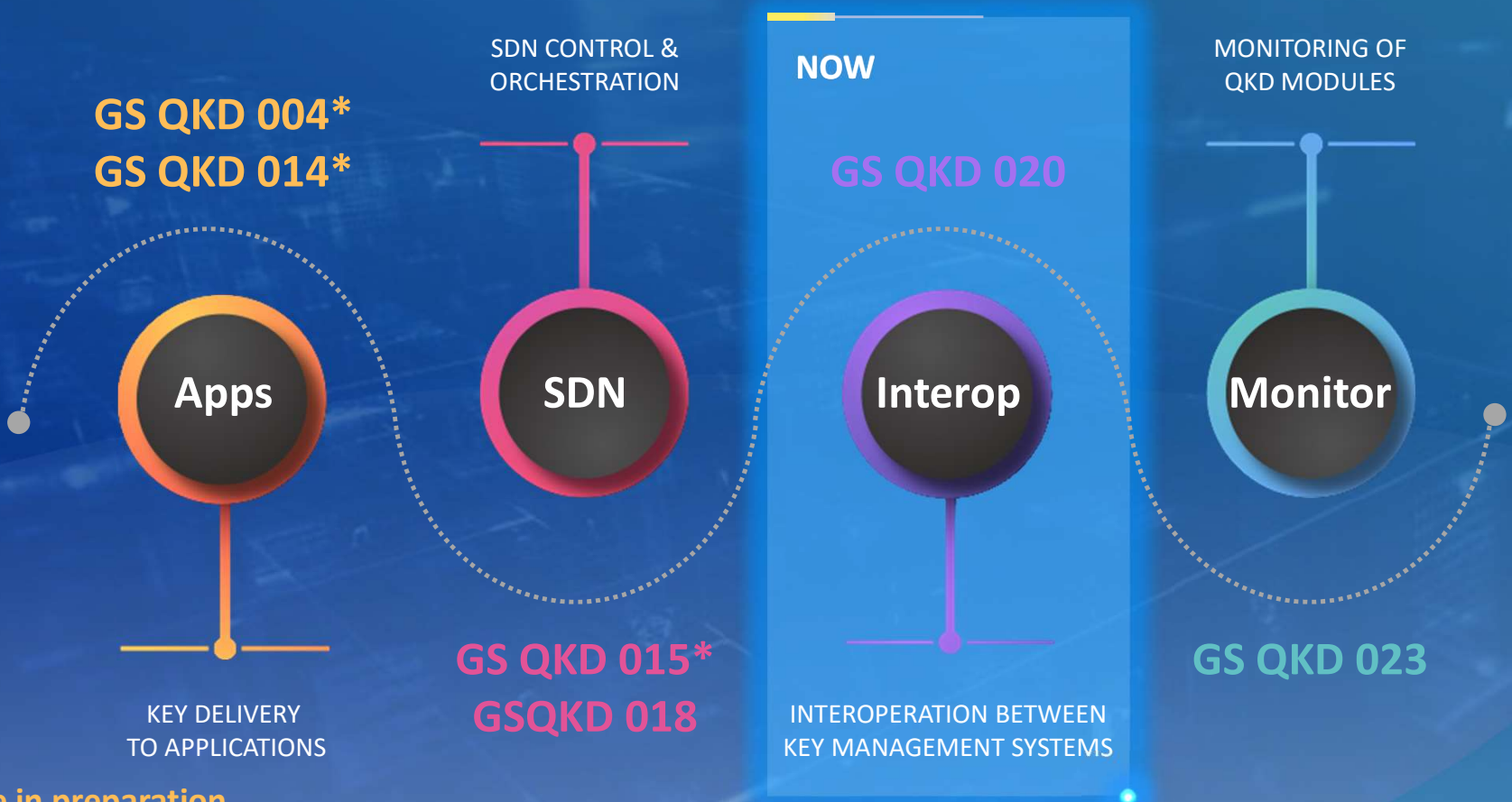
Expect different groupings

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

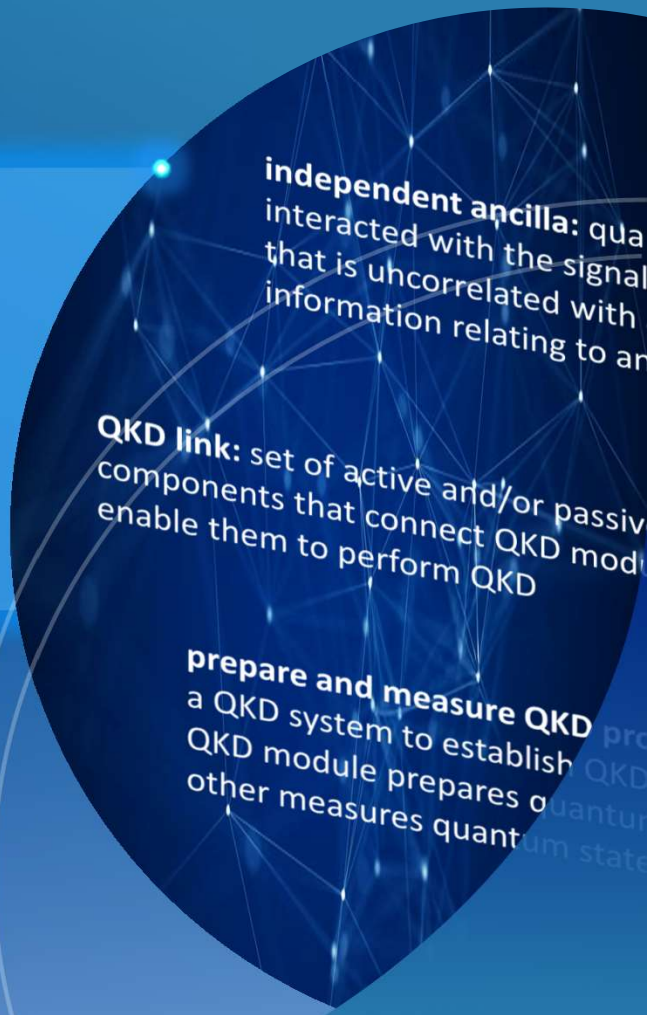
Vocabulary

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

Join us

Help the community develop specifications for QKD

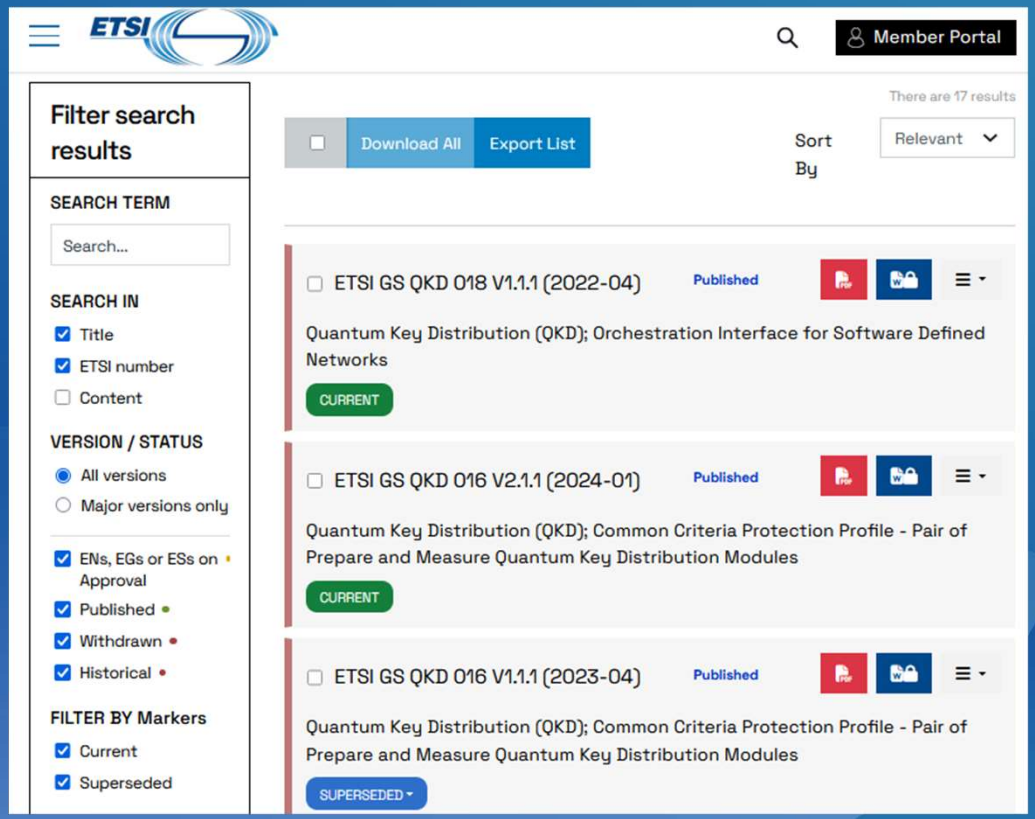
Published deliverables available as free downloads

ETSI MEMBERS

Use the portal to view drafts or register for meetings

Join the QKD_ISG mailing list

OTHERS…




Meet
ETSI
at the info Stand