ETSI/IQC Quantum Safe Cryptography Event

ETSI ISG QKD Activities

Martin Ward (Chair)

TOSHIBA

14/02/2023

Areas of activity of ETSI ISG QKD

Security

- Implementation security
- Evaluation activities
- Protocol security proofs
- Authentication

Optical characterisation

- Optical components
- Complete QKD modules
- Penetration testing

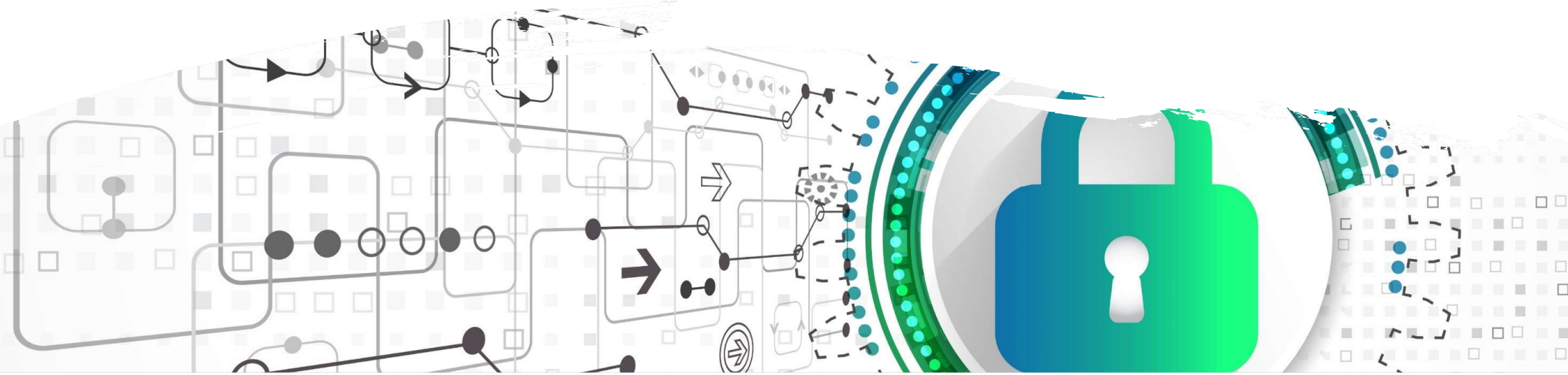
Interoperability

- Application / key delivery interfaces
- Interoperable KMS interface
- QKD in SDN networks
- Network architectures

Vocabulary

- Improving and aligning use of terminology

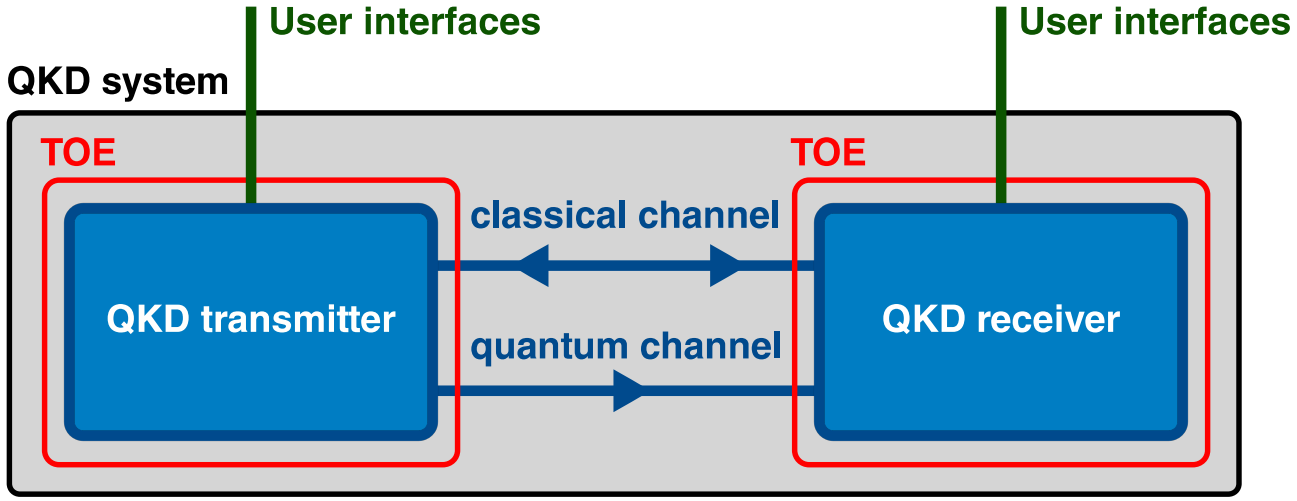
Security



DGS/QKD-016-PP
Common Criteria Protection Profile

Certification of QKD systems is an important objective for QKD vendors and users

- Target of Evaluation (TOE): Pair of Prepare and Measure Quantum Key Distribution Modules (transmitter + receiver)



DGS/QKD-016-PP
Common Criteria Protection Profile

Assurance level: EAL4 augmented with AVA_VAN.5 and ALC_DVS.2

AVA_VAN.5	ALC_DVS.2
Advanced methodical vulnerability analysis Whether potential vulnerabilities identified could allow attackers to violate the SFRs Considers attackers possessing High attack potential	**Developer environment security: Sufficiency of security controls** Whether security controls on the development environment are adequate to provide the necessary confidentiality and integrity to ensure secure operation

DGS/QKD-016-PP
Common Criteria Protection Profile

Definition of custom components for QKD

FCS_QKD

Prepare and Measure Quantum Key Distribution

The main SFRs for QKD

Extend Class FCS: Cryptographic Support

Require QKD protocol with a **security parameter threshold**

Requirements within protocol:

quantum states

post processing algorithms

parameter estimation

tracking deliberately disclosed information

privacy amplification ratio

DGS/QKD-016-PP
Common Criteria Protection Profile

Base PP and four optional packages

Trusted user interfaces with authentication

Base PP assumes TOE is operated in a secure environment so only authorized users access user interfaces

Package defines trusted paths for the user interfaces as an alternative

Self protection

Base PP assumes secure environment so attacker cannot approach the device

Package set out how TOE may be equipped with sufficient self protection

Provisioning after delivery

Base Protection Profile assumes TOE delivered with full trust provisioning

Package for case where all pre-operational tasks are performed after delivery

Local authentication of users

- are mutually exclusive

Package allows users to authenticate their identity while physically interacting with TOE

DGS/QKD-016-PP
Common Criteria Protection Profile

ISG QKD has approved for publication the first version of its Protection Profile for a Pair of QKD

- The PP will frame future work to develop background documents
  - Protocol descriptions (quantum and classical)
  - Attacks
  - Evaluation methodology
  - etc.
- PPs for other protocols / use cases might be developed later

RGS/QKD-0005ed2_SecProofs
Protocol Structure & Security Proofs

An update to ETSI GS QKD 005 is being developed

- Structuring security proofs of QKD protocols and security models

V1.1.1 was published in 2010 → **Fundamentals remain unchanged** | **General updates to terminology and examples** | **Alignment with Protection Profile**

- Developments in post-processing techniques:
  - Data Partitioning, Sifting, Symbol Map, Refined Symbol Map, Error Correction, Error Verification, Parameter Estimation, Privacy Amplification
- Assumptions on the environment, the adversary etc.

While discussed, implementation security is not the main subject of this deliverable

ESTI GS QKD 011 Component characterization: characterizing optical components for QKD systems

Behaviour of components is critical to the evaluation of QKD systems

- Detailed measurement methods for properties of components found in transmitter and receiver modules
- Normative specifications for new devices or those used in unusual operating range(s)

Also help build ecosystem for component supply chains

Photon Sources
photon number statistics
temporal profile
stability
spectral properties

Single photon detectors
detection efficiency
dark counts
after-pulse probability

DGS/QKD-0013_TransModChar Optical Characterisation of QKD transmitter modules

Evaluation activities for QKD systems deal with complete devices

- Follows on from ETSI GS QKD 011 V1.1.1
- Focus is on measurements of complete QKD modules
- Includes photon number statistical properties, spectral properties, polarization states

Complicating factors when performing measurements on complete modules

Ideally measurements should be on the module running in (or close to) operating mode

Want representative results

Not modified by additional probes etc.

DGR/QKD-019_AUTH
Design of QKD interfaces with Authentication

Authentication is a critical element of QKD protocols

- Studying uses of authentication in QKD systems

QKD protocols assume an authenticated classical channel

Composable authentication schemes e.g. Wegman Carter

- Assumptions on long-term or physical security
- Authentication on the key delivery and management interfaces
- Currently a lack of existing standards

Interoperability

Application / Key delivery APIs

To enable vendors to develop applications to use QKD the ISG has defined two application / key delivery APIs:

```
{ "keys": [{ "key_ID": "bc490419-
             "key": "wHHVxRwDJs3
```

ETSI GS QKD 014 V1.1.1 (2019-02)

- REST-based key delivery API defined over HTTPS
- Ease of adoption by application vendors, e.g. encryptors

ETSI GS QKD 004 V2.1.1 (2020-08)

- Session based application interface
- Use cases include restricted power / performance

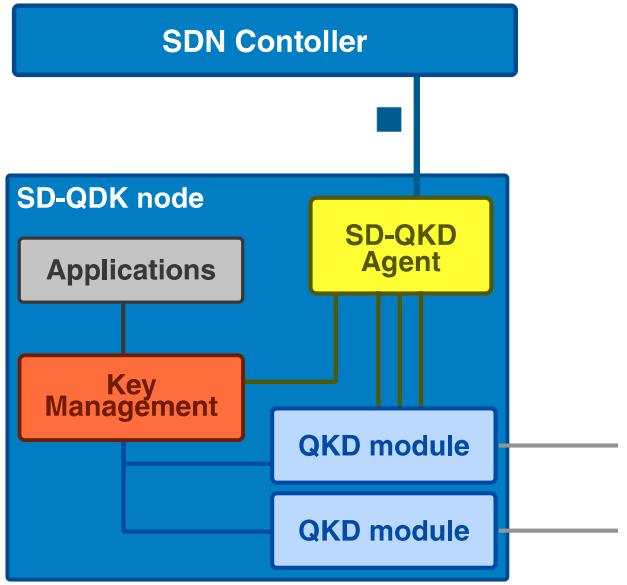
- A mapping is possible between the APIs

```
Interface QKD {
   OPEN_CONNECT (in source, in destination, inout QOS, inout Key_stream_ID, out status);
   GET_KEY (in Key_stream_ID, inout index, out Key_buffer, inout Metadata, out status);
   CLOSE (in Key_stream_ID, out status); }
```

Introducing QKD into Software Defined Networks

SDN is of growing importance to many telecom operators

- Need integration of QKD services into SDN
- Define management interfaces
  - Delivery of QKD keys remains via dedicated interfaces



ETSI GS QKD 015 V2.1.1 (2022-04)

Abstraction models and workflows between a SD-QKD node and the SDN Controller:

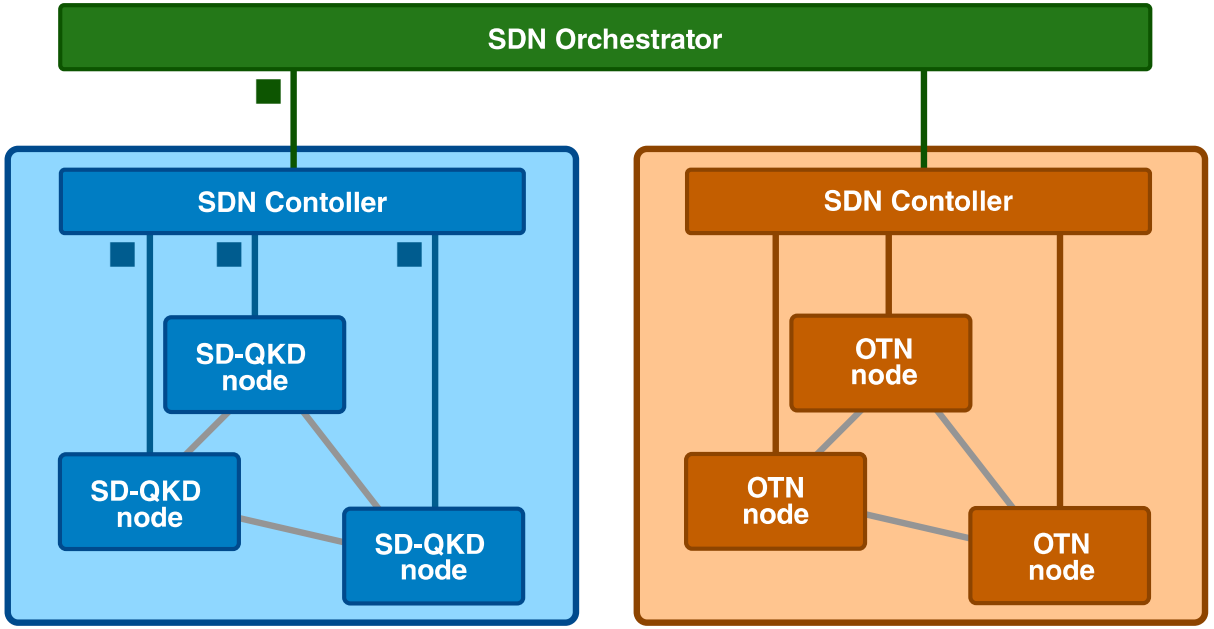
Resource discovery; Capabilities; Dissemination; System configuration operations

DGS/QKD-018OrchIntSDN
Introducing QKD into SDN networks

Orchestration between QKD and OTN networks

- ETSI GS QKD 018 V1.1.1 (2022-04)

Orchestration Interface of SDN



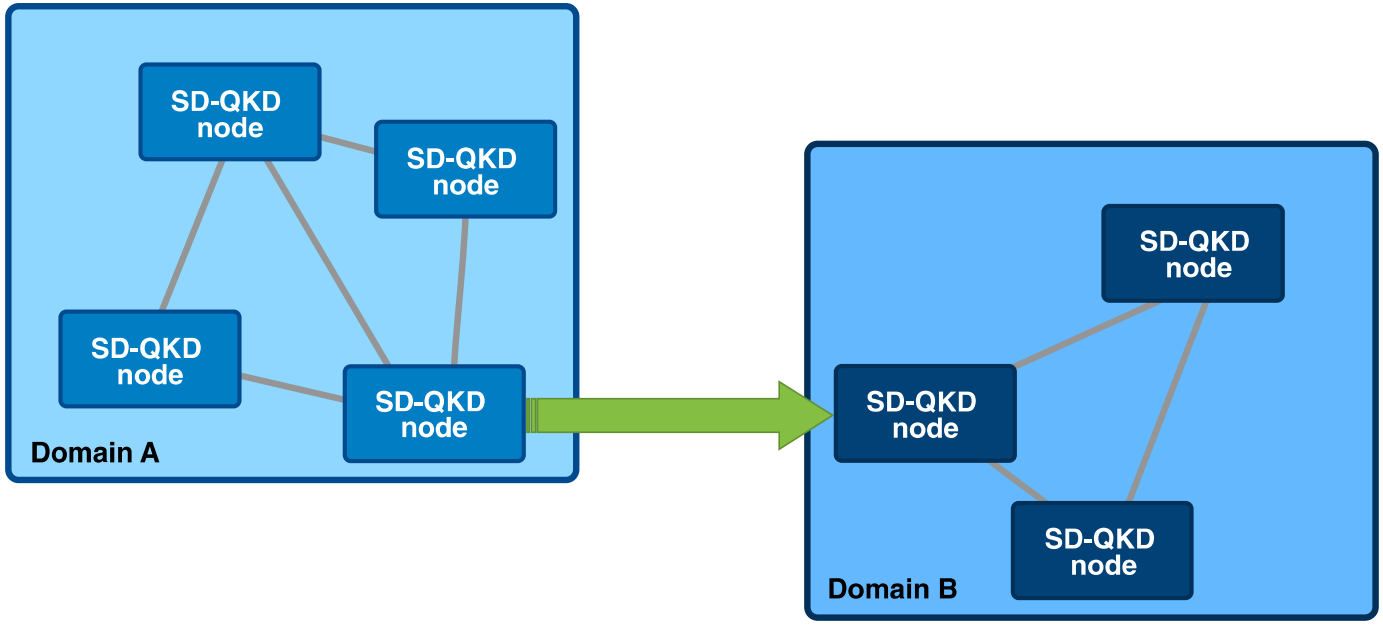
YANG models are available on ETSI Forge:
https://forge.etsi.org/rep/qkd

- ETSI GS QKD 015 V2.1.1
Control Interface for SDN

DGS/QKD-020_InteropKMS
Interoperable Key Management System API

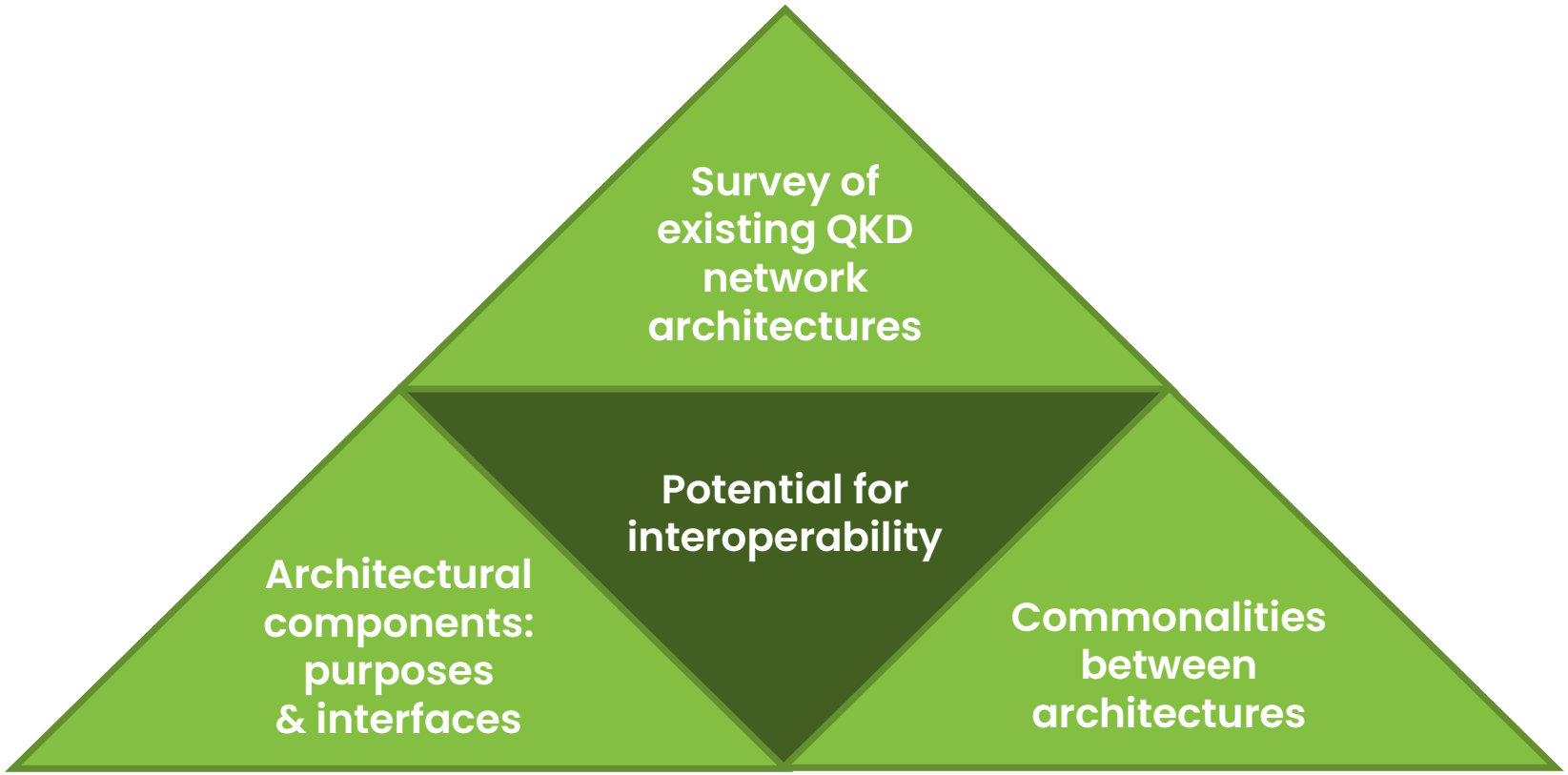
Horizontal interface for key transfer between KMEs within a trusted node

- Enable key requests to be handled between different parts of a QKD network
- Multiple QKD networks / domains



DGR/QKD-017NwkArch
Network architectures

Group Report analysing aspects of QKD network architectures



Vocabulary

RGR/QKD-007ed2_Vocab Vocabulary

The ISG is reviewing its use of terms and their definitions

- GR QKD 007 V1.1.1 (2018-12) pulled together definitions from existing ISG deliverables
- Significant review of some fundamental terminology undertaken
- Terms in other deliverables will be aligned as updates are published

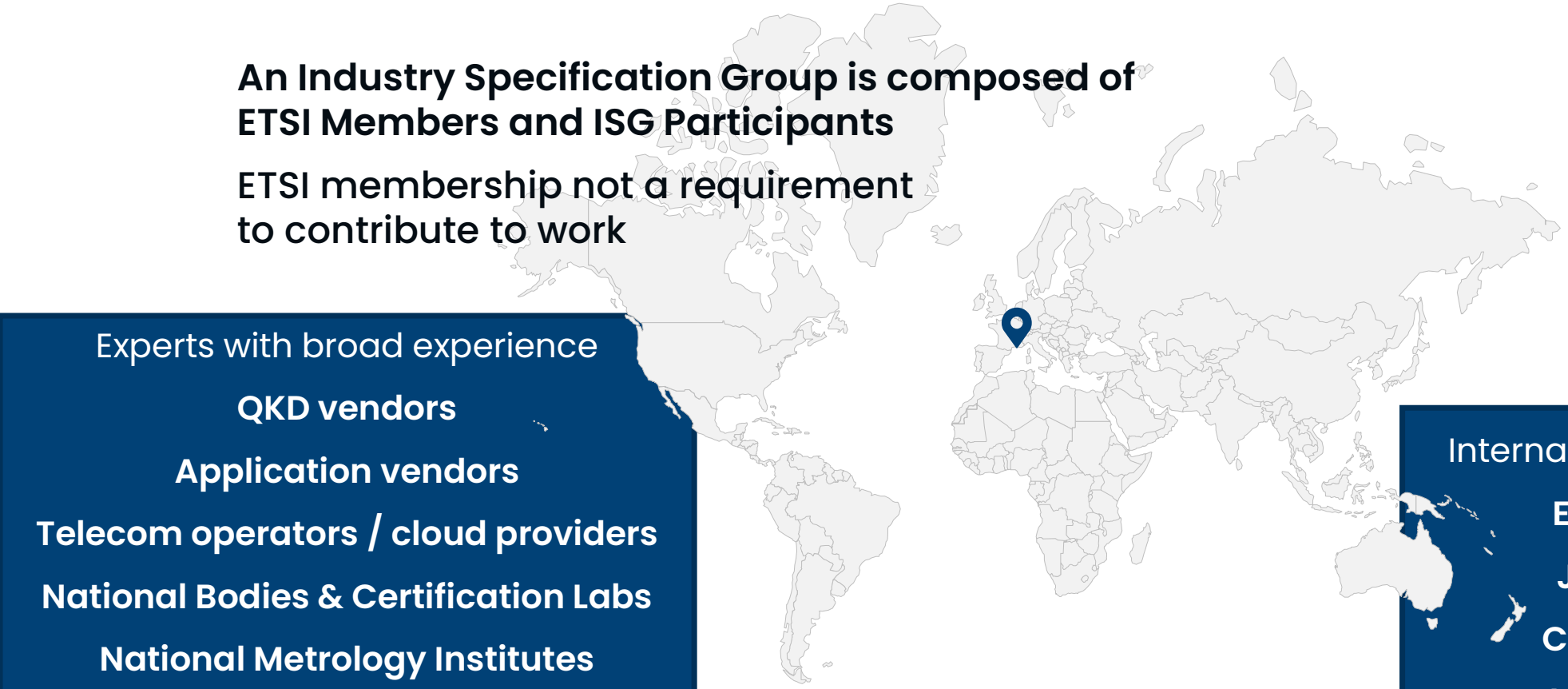
Consistency with terminology from other areas such as cryptography, metrology etc.

Additional text and figures to explain intended usage of key terms

About ETSI ISG QKD

An Industry Specification Group is composed of ETSI Members and ISG Participants

ETSI membership not a requirement to contribute to work



Experts with broad experience

QKD vendors

Application vendors

Telecom operators / cloud providers

National Bodies & Certification Labs

National Metrology Institutes

Academic experts

International profile

Europe

Japan

Canada

Republic of Korea

US

etc.

Thank you for your attention

Follow us on: