ETSI ISG QKD

Industry Specification Group on QKD

Martin Ward (Toshiba Europe Limited) Chair of ISG QKD

28 September 2021

 ‘Standardisation and certification of QKD systems and QKD networks’ 1st Workshop, AIT (online)

Areas of activity of ETSI ISG QKD

Security

- Common Criteria Protection Profile for QKD
- Design of QKD interfaces with Authentication
- Structuring security models
- Implementation security

Interoperability

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

Optical characterisation

- Characterization of optical components
- Optical characterization of QKD modules

Vocabulary

- Improving and aligning terminology

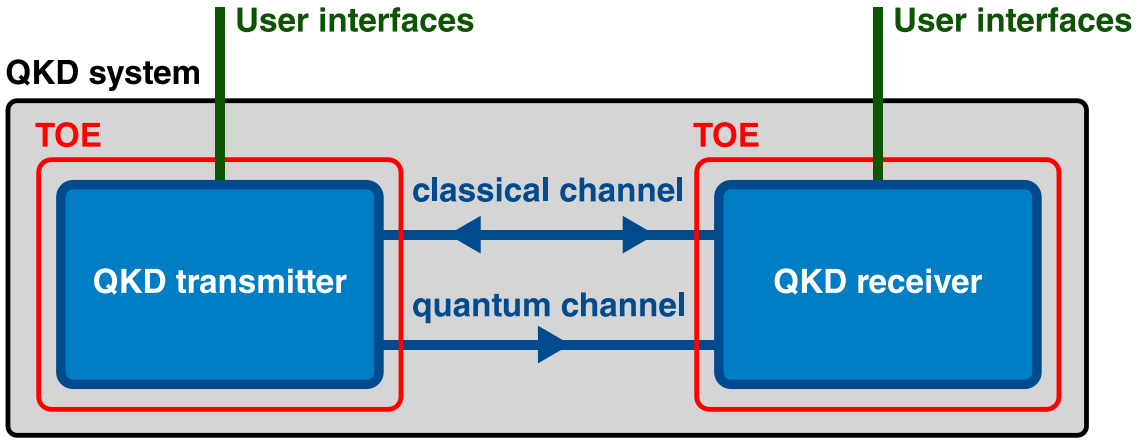
https://www.etsi.org/committee/qkd

Participation in an ETSI ISG

- ISG composed of ETSI Member and ISG Participants
  (ETSI membership is not a requirement to participate in an ISG)
- QKD specifications require a broad range of expertise
- ISG QKD benefits from the expertise of Members and Participants from:
  - QKD vendors
  - Telecom operators
  - Application vendors
  - National Bodies and Certification Labs
  - National Metrology Institutes
  - Academic experts
- International profile: Europe, Japan, South Korea, Canada, US, Russia etc.

DGS/QKD-016-PP
Common Criteria Protection Profile

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



- PP will frame future ISG security work to develop background documents
- Manfred Lochter (BSI) will explain in the next session

RGS/QKD-0005ed2_SecProofs
Security Proofs Revision

We are preparing an update to ETSI GS QKD 005

- 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
- Common assumptions on the environment, the adversary etc.
- Developments in post-processing techniques:
  - Data Partitioning, Sifting, Symbol Map, Refined Symbol Map, Error Correction, Error Verification, Parameter Estimation, Privacy Amplification
- Implementation security is not the main subject of this deliverable

DGS/QKD-0010_ISTrojan
Protection against Trojan horse attacks

First work item on implementation security

- Example of the analysis of implementation security issues
- Attempting to align with the Protection Profile at the moment

- Design guidance
- Time-resolved reflectivity measurements (e.g., OTDR)
- Bounding the probability of relevant reflected photon
- Advice on subsequent security analysis

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

Behaviour of components and modules is critical to evaluation activities for QKD systems

- Previously: ETSI GS QKD 011 V1.1.1
  Component characterization: characterizing optical components for QKD systems
  - many properties of components of transmitter and receiver module

- Current work item: DGS/QKD-0013_TransModChar
  Characterisation of Optical Output of QKD transmitter modules
  - including photon number statistical properties, spectral properties, polarization states
- A similar work item on receiver modules is expected to follow
- Focus is on measurements of complete QKD modules

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

Authentication is a critical element of QKD protocols

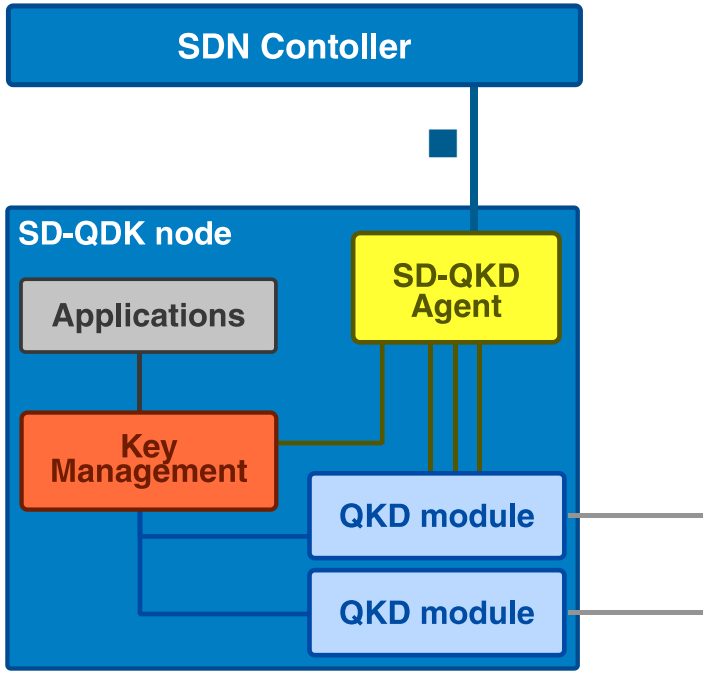
- The ISG is studying uses of authentication in QKD systems
- Protocols used in the classical channel of a quantum link
- Assumptions on long-term or physical security
- Information-theoretic secure (e.g., Wegman Carter) authentication protocols
- Currently a lack of existing standards

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 via dedicated interfaces

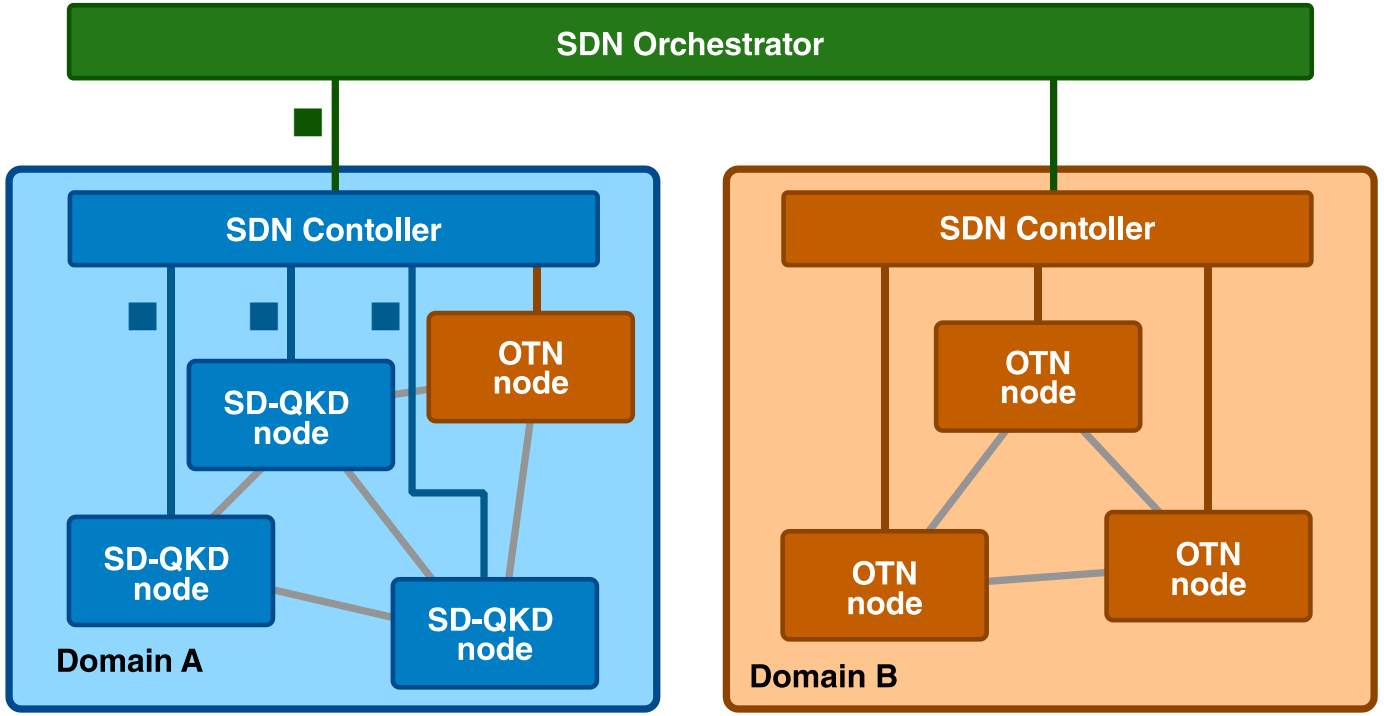
- ETSI GS QKD 015 V1.1.1 (2021-03)
- Abstraction models and workflows between a SD-QKD node and the SDN Controller:
  - Resource discovery; Capabilities; Dissemination; System configuration operations



DGS/QKD-018OrchIntSDN
Introducing QKD into SDN networks

Considering multi-domain SDN networks

- ETSI GS QKD 015 V1.1.1
  - Control Interface for SDN
- ETSI DGS/QKD-018OrchIntSDN
  - Orchestration Interface of SDN
  - Final draft stage



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

Application / Key delivery APIs

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

- 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

```
{ "keys": [{ "key_ID": "bc490419-7d60-487f-adc1-4ddcc17
  "key": "wHHVxRwDJs3/bXd38GHP3oe4svTuRpZS0
```

- ETSI GS QKD 004 V2.1.1 (2020-08)
  - Session based application interface
  - Use cases include restricted power / performance

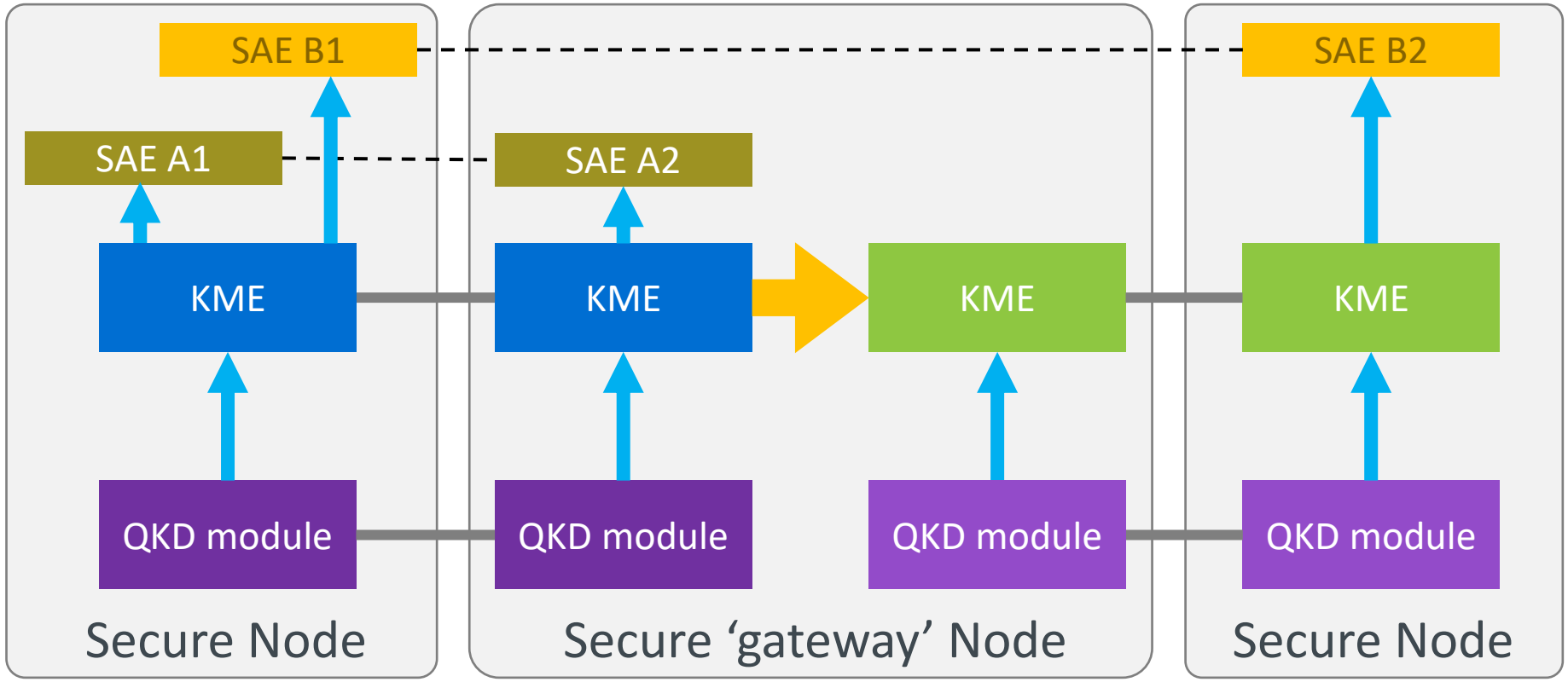
```
Interface QKD {
  OPEN_CONNECT (in source, in destination, inout QOS, inou
  GET_KEY (in Key_stream_ID, inout index, out Key_buffer,
  CLOSE (in Key_stream_ID, out status); }
```

- A mapping is possible between the APIs

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



DGR/QKD-017NwkArch
Network architectures

Group Report analysing aspects of QKD network architectures

- Survey of some existing QKD network architectures
- Architectural components: purposes and conceptual interfaces
- Commonalities between architectures and potential interoperability

GR/QKD-007ed2_Vocab
Vocabulary

The ISG is reviewing its use of terms

- GR QKD 007 V1.1.1 (2018-12) pulled together definitions from existing ISG deliverables
- RGR/QKD-007ed2_Vocab will update this vocabulary
- Significant review of some fundamental terminology undertaken
- Consistency with terminology from other areas of cryptography
- Additional text and figures to explain intended usage of key terms
- Terms in other deliverables will be aligned as updates are published

Current Work Items

RGS/QKD-0005ed2_SecProofs	Security Proofs
RGS/QKD-007ed2_Vocab	Update to Vocabulary
DGS/QKD-0010_ISTrojan	Implementation security against Trojan horse
DGS/QKD 0013_TransModChar	Characterisation of Optical Output of QKD Transmitter Module
DGS/QKD-016-PP	Protection Profile
DGR/QKD-017NwkArch	Network architectures
DGS/QKD-018OrchIntSDN	Orchestration Interface of SDN
DGR/QKD-019_AUTH	Design of QKD interfaces with Authentication
DGS/QKD-020_InteropKMS	Interoperable KMS API

https://portal.etsi.org/tb.aspx?tbid=723

Published Deliverables

- GS QKD 015 Control Interface for Software Defined Networks
- GS QKD 014 Protocol and data format of REST-based key delivery API
- GS QKD 012 Device and Communication Channel Parameters for QKD Deployment
- GS QKD 011 Component characterization: characterizing optical components for QKD systems
- GS QKD 008 QKD Module Security Specification
- GR QKD 007 Vocabulary
- GS QKD 005 Security Proofs
- GS QKD 004 Application Interface
- GR QKD 003 Components and Internal Interfaces
- GS QKD 002 Use Cases

https://www.etsi.org/committee/qkd

The Standards People