Activities within ETSI Industry Specification Group ISG QKD

Presented by: **Martin Ward**
Secretary of ISG QKD

For: **ITU-T Workshop**

07.06.2019

About ETSI Industry Specification Group (ISG) QKD

Mission: To develop ETSI Group Specifications and Group Reports describing quantum cryptography for ICT networks

Membership includes QKD vendors, network equipment vendors, network operators, system integrators, NMIs and government labs, academia (>30 members/participants)

ETSI is an **international** member-led SDO

ISG QKD members from Japan, South Korea, China, US, Canada, Europe…
Open to new members and participants (without becoming members)

ETSI publications are free to download: **www.etsi.org/qkd**

Areas of activity

Security

- As for classical systems security is dependant upon the implementation
- Practical solutions to **implementation security** issues

Interoperability

- Currently of classical interfaces
- Considered too early to address quantum channel

Metrology of components and systems

- Measurements required at the single-photon level
- Few existing standards

Security

Security Proofs
ETSI GS QKD 005 V1.1.1 (2010-12)

Framework for Security Statements of QKD Implementations

- Security Definition and Requirements
- Modelling, Assumptions and Side Channels

Published in 2010

Last ISG meeting QKD#25 December 2018 decided to update this document

ETSI White Paper No. 27

Implementation Security of Quantum Cryptography: Introduction, challenges, solutions

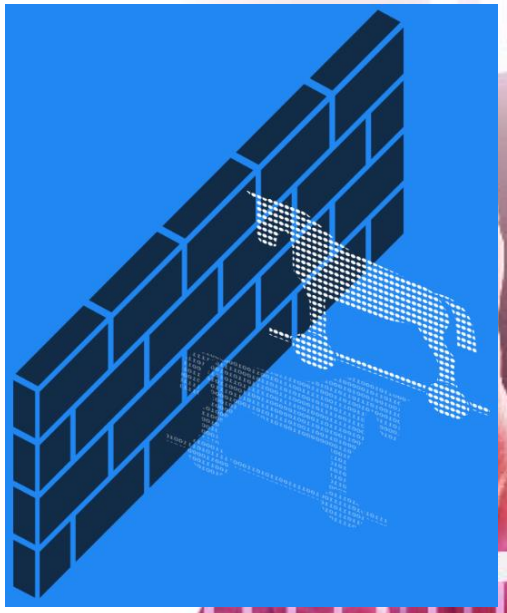
First edition – July 2018

ISBN No. 979-10-92620-21-4

Readable overview of implementation security issues and solutions

www.etsi.org/qkd

Implementation security: protection against Trojan horse attacks in one-way QKD systems DGS/QKD-0010_ISTrojan (GS QKD 010)



Attacker injects strong optical signals and seeks to measure the state of internal components from reflections

Specifies design guidance & passive countermeasures against attack

- Includes characterisation procedures

First of a series of specifications on implementation security

- Steep learning curve
- Considerable research has been required
- Highlighted requirements for other technical background documents

Publication expected in 2019

Common Criteria Protection Profile for QKD DGS/QKD-016

ISG will publish a Protection Profile (PP) written under the Common Criteria framework. This work will:

- Be performed in collaboration with a national cyber security authority
- Use the skills of a certification lab to ensure quality
- In parallel the ISG will create new work items to write additional technical background documents
  - This will involve the most work

Writing PP itself is expected to complete by September 2020

Networks and Interoperability

Protocol and data format of REST-based key delivery API
ETSI GS QKD 014 V1.1.1 (2019-02)

HTTPS REST-based API for key requests / delivery to an application

- Specifies implementation, protocol, data formats etc.
- How key is transferred over QKD network is out of scope
- Simple design to encourage adoption by application vendors

Published February 2019

Application Interface
ETSI GS QKD 004 V1.1.1 (2010-12)

Specifies an OMG IDL remote-function-call-based application interface to request streams of keys

v1.1.1 Published in December 2010

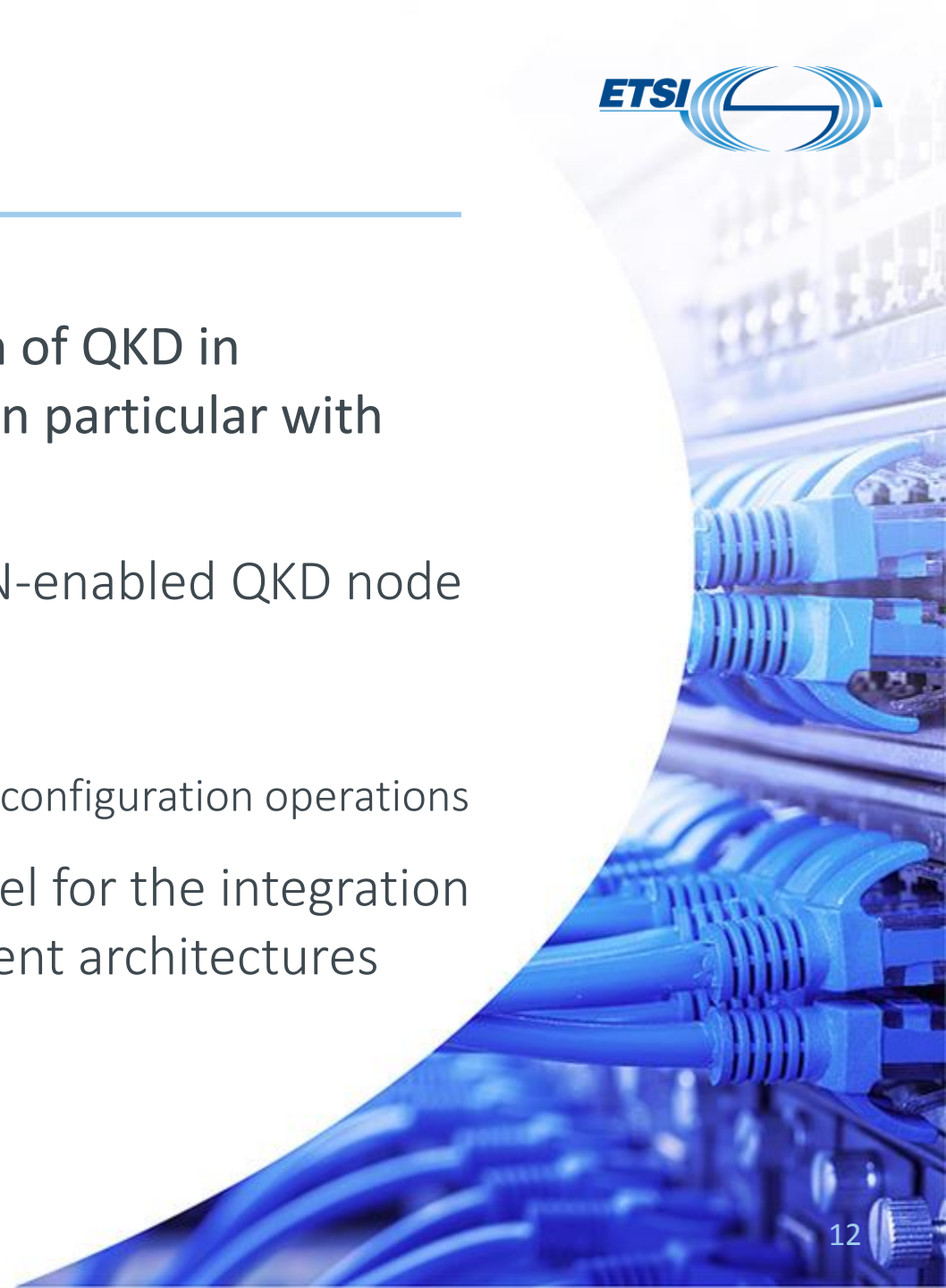
An update is underway and is expected to be approved in August 2019
RGS/QKD-004ed2_AppIntf (GS QKD 004)

Control Interface for SDN
DGS/QKD-015_ContIntSDN (GS QKD 015)

Specifies **management interfaces** for the integration of QKD in disaggregated network control plane architectures, in particular with Software Defined Networks (SDN)

- Abstraction models and workflows between a SDN-enabled QKD node and the
  SDN Controller, including:
  - Resource discovery; Capabilities; Dissemination; System configuration operations
- YANG model is designed to be a base or core model for the integration of QKD technologies into an operator's management architectures

Publication due 2019



Device and Communication Channel Parameters for QKD
ETSI GS QKD 012 V1.1.1 (2019-02)

- Facilitate effective communication between potential customers and suppliers
- Sets out the parameters that are likely to be important to plan a deployment

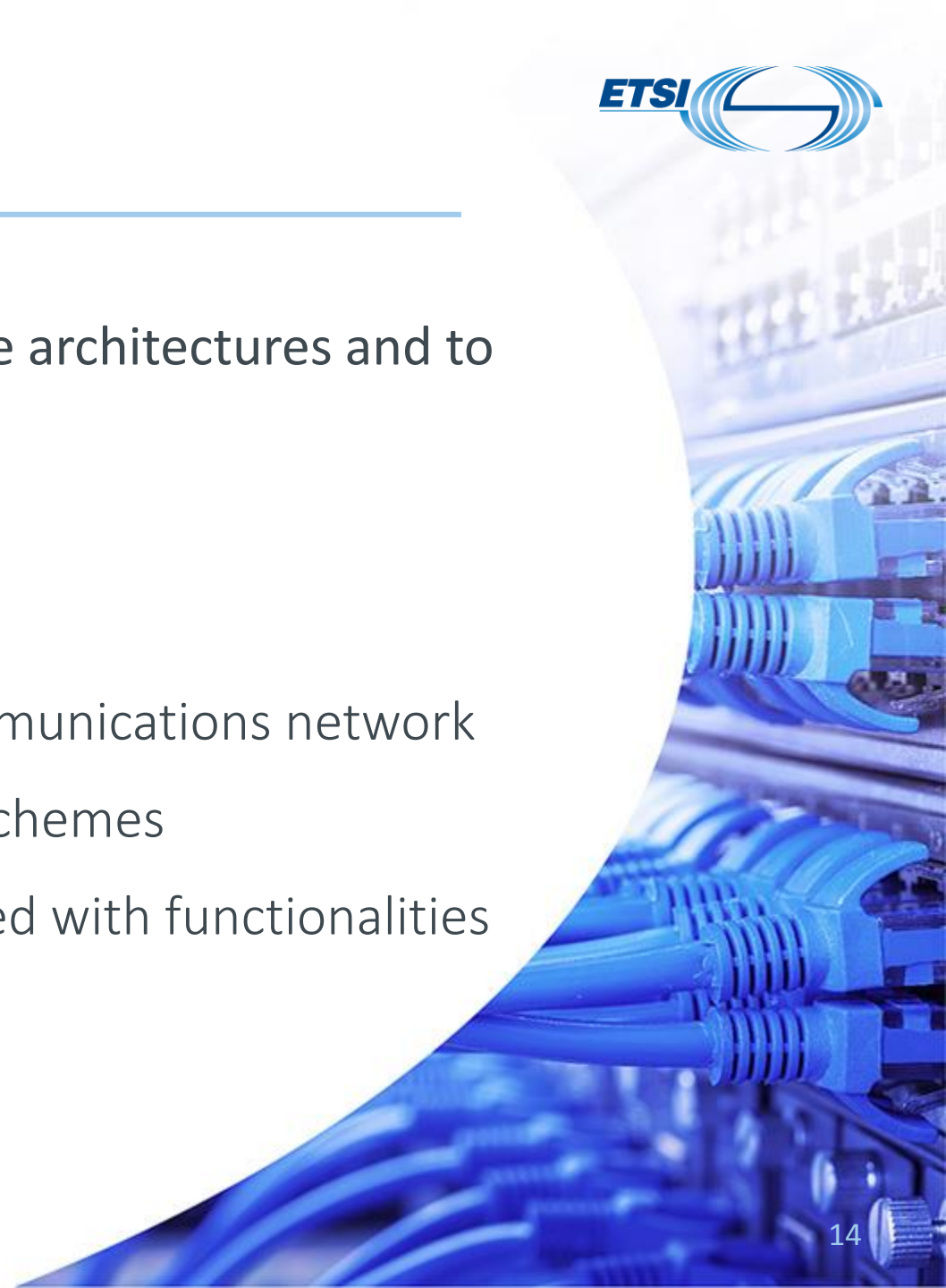
Published February 2019

Network architectures
DGR/QKD-017NwkArch

ISG QKD has undertaken preliminary work to analyse architectures and to identify underlying similarities at an abstract level

Scope includes:

- Several architectures for QKD networks
- Stand-alone and integration models with telecommunications network
- Traditional (layered model) and novel (e.g. SDN) schemes
- Main components in each scheme will be identified with functionalities and interfaces



Metrology of Components and Systems

Component characterization: characterizing optical components for QKD systems ETSI GS QKD 011 V1.1.1 (2016-05)

Important base document for many future work items

- Critical for security analysis
- Supply chain for components

- Specified characterization procedures required for security specifications
- Centralises procedures that can be referenced in multiple specifications
- No existing specifications for many components in the quantum regime
- Drafting was driven by member NMIs

Published in 2016

Characterisation of Optical Output of QKD transmitter modules DGS/QKD-0013_TransModChar (GS QKD 013)

Characterisation of complete QKD transmitter modules

- Unlike ETSI GS QKD 011 that addresses individual components
- Some measurements specified that treat a module as a black-box
- Other measurements specified where additional information is available

Publication expected in 2019

A work item on QKD receiver modules will follow

Summary

Vocabulary ETSI GR QKD 007 V1.1.1 (2018-12)

Attempt to improve consistency between ISG QKD documents

- Available for wider use
- This document will be updated regularly as other documents are published
- Internal procedure to review definitions in new documents and updates

Overview

- ETSI was first SDO to introduce work on QKD in 2008
- Scientists had to learn about SDOs
- ISG QKD has stimulated relevant research activities
- Activities are accelerating as members commit more resources
- 8 publications expected 2018–2019

Closing thoughts

- ISG QKD has experts with a range of backgrounds from QKD manufacturers, application vendors, telecom operators, academics and National Metrology Institutes
- The work remaining to be done on QKD is extensive
- Resources are finite: duplication adds cost for all
- Time consuming for members to follow activities across all SDOs
- Working to improve liaison and coordination:
  - **ITU-T SG17** QKD Network Security
  - **ITU-T SG13** QKD Network framework, architecture, key management
  - **ISO/IEC JTC 1/SC 27/WG 3** Security requirements, test and evaluation methods