Standardization Activities: ETSI

Presented by: **Martin Ward**
Toshiba Europe Limited, Cambridge, UK
Chairman of ETSI ISG QKD

QCrypt 2020 Industry Session (12 August)

ETSI ISG QKD areas of activity

Security

- Practical solutions for secure **implementations**
- Security evaluation and certification

Metrology of components and systems

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

Networks and Interoperability

- Integration into conventional network infrastructures
- Common interfaces to promote adoption and development

Security

Security

QKD has a rather unique security proposition

It is different from things has been certified before

Specifications reviewed by a wide range of experts are helpful for certification processes

Security analysis of systems consider all aspects of security

Experts with a range of established security skills in addition to QKD experts are required

Common Criteria Protection Profile for QKD
DGS/QKD-016

Written under the Common Criteria framework

This work will:

- be performed in collaboration with BSI, Germany
- employ an experienced certification lab
- consider prepare and measure protocols only
- the TOE will consist of a pair of QKD modules

Additional Group Specification will be prepared as background documents

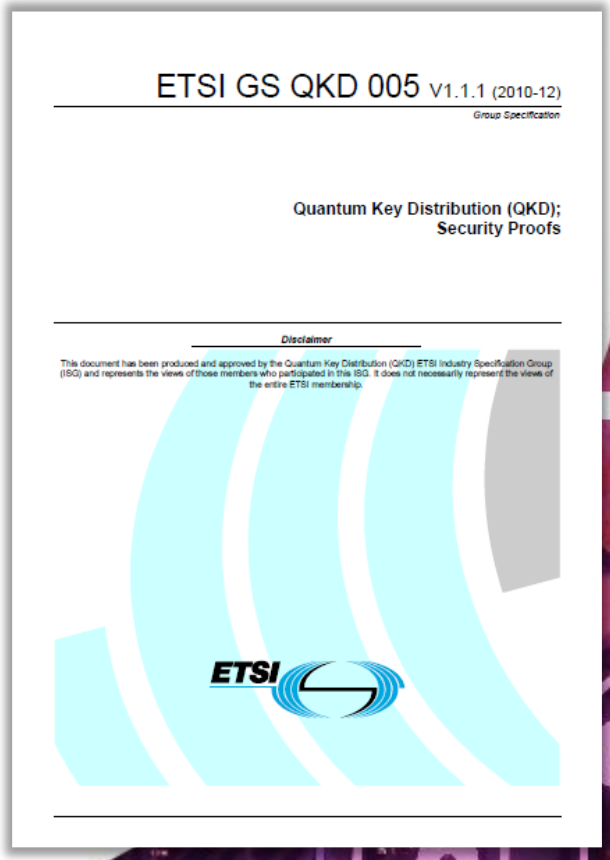
Writing the PP itself is expected to take until summer 2021

Security Proofs
ETSI GS QKD 005 V1.1.1

Framework for Security Statements of QKD Implementations

- Security definition and requirements
- Relationship between security proof and QKD protocol
- Modelling, assumptions and side channels
- Substantially revised definitions

Revised version to be finalised by September 2020

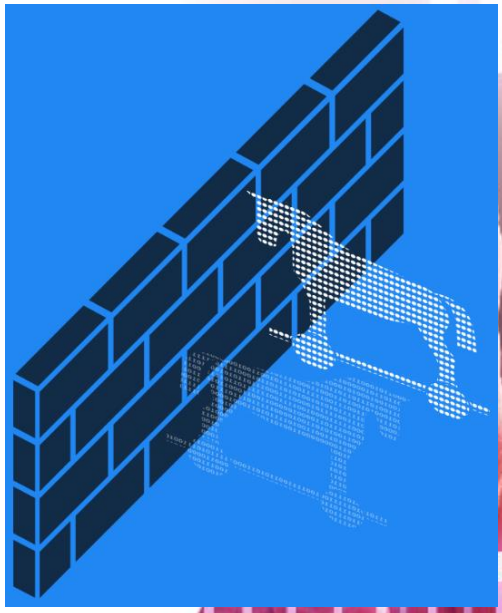

ETSI GS QKD 005 V1.1.1 (2010-12)
Group Specification

Quantum Key Distribution (QKD);
Security Proofs

Disclaimer

This document has been produced and approved by the Quantum Key Distribution (QKD) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG. It does not necessarily represent the views of the entire ETSI membership.

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 suitable to be referenced by a Security Target

Expected to be finalized in September 2020

ETSI White Paper No. 27

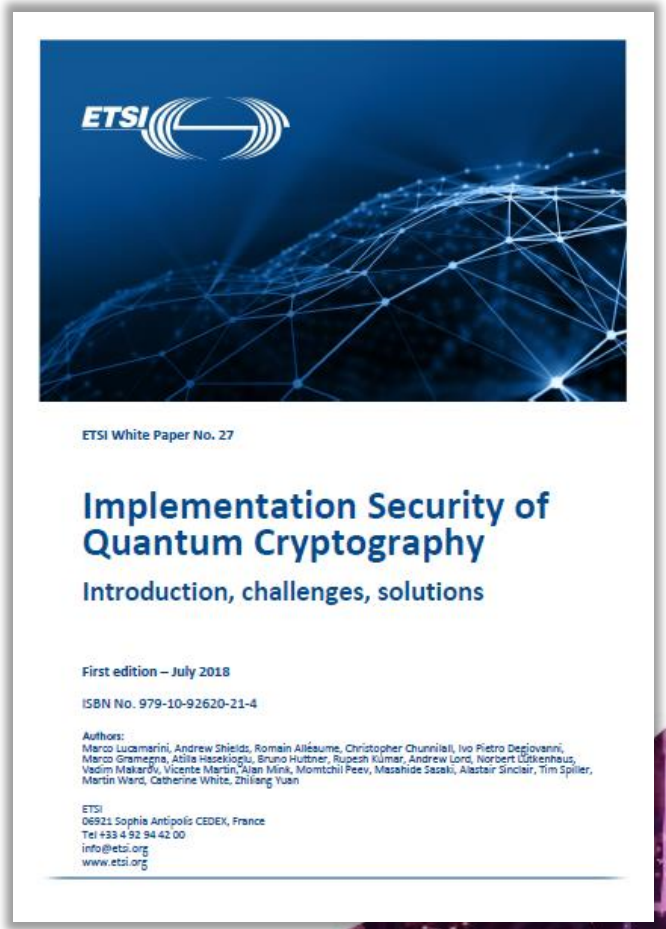
Implementation Security of Quantum Cryptography: Introduction, challenges, solutions

First edition – July 2018

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

Readable overview of implementation security issues and solutions

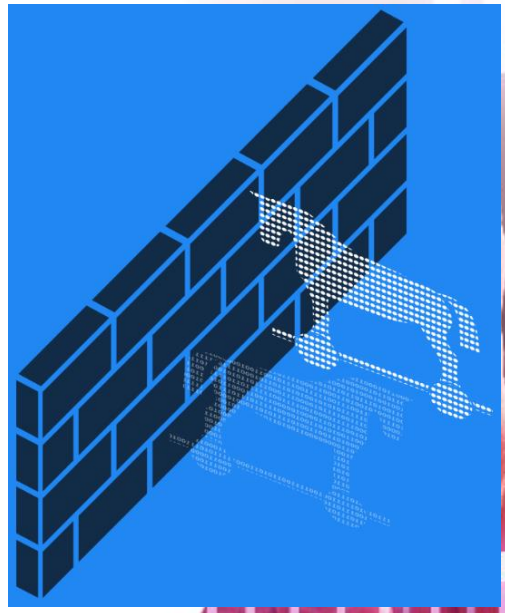
www.etsi.org/qkd



New work item on Authentication under consideration

Design of classical interfaces for QKD systems that include authentication

- Protocols used in discussion channels and auxiliary channels
- Management interfaces and key delivery interfaces
- Wegman Carter etc. authentication
- Appropriate use of public key algorithms



Metrology of Components and Systems

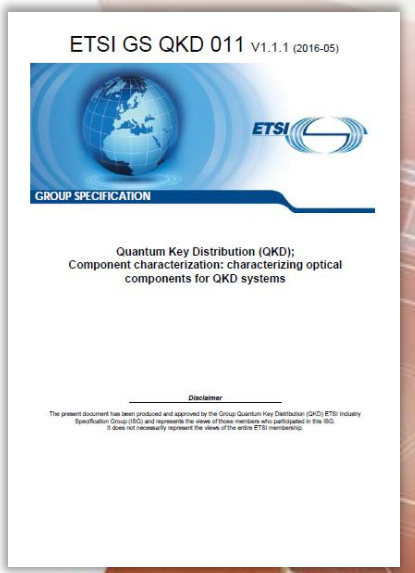
Metrology

Reliable characterisation of components is critical for security analysis

Fortunate to have several NMIs involved

While many common telecom components are used they can be operated under different conditions and additional parameters can be significant

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
- Stimulate a 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

- GS011 addresses individual components; GS013 whole module
- Ideally treat QKD module as a black-box
- Some measurements require additional tagging information

Approval expected by end of 2020

New work item on QKD receiver modules is planned

Networks and Interoperability

Main requirements

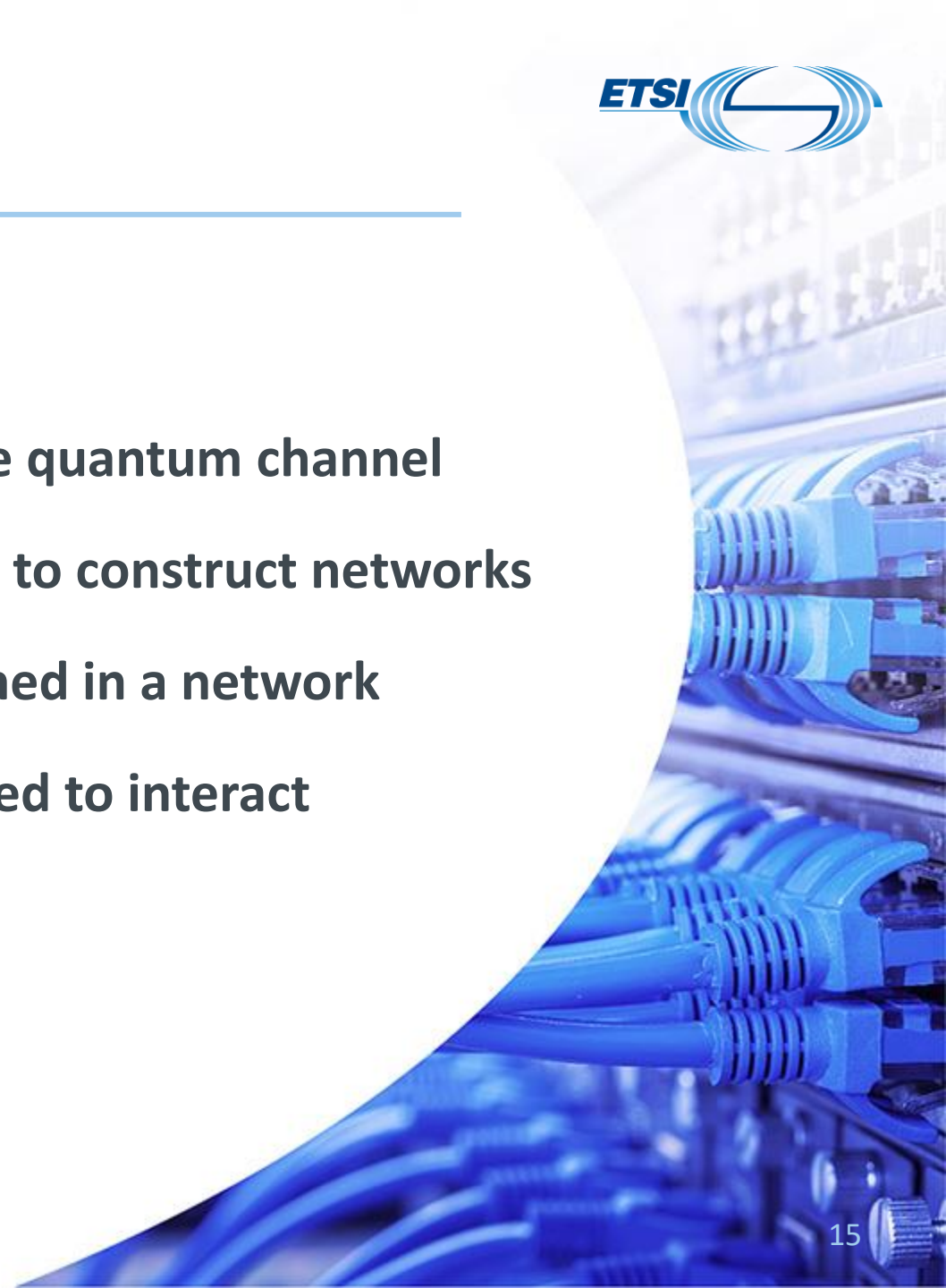
Isolated QKD links serve limited use cases

Currently too early to look at interoperability of the quantum channel

Systems still need to communicate with each other to construct networks

Matched pairs of QKD modules can then be combined in a network

External applications and management systems need to interact with QKD devices in many use cases



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

Specifies an low level function-call-based application interface to request streams of keys

v1.1.1 Published in December 2010

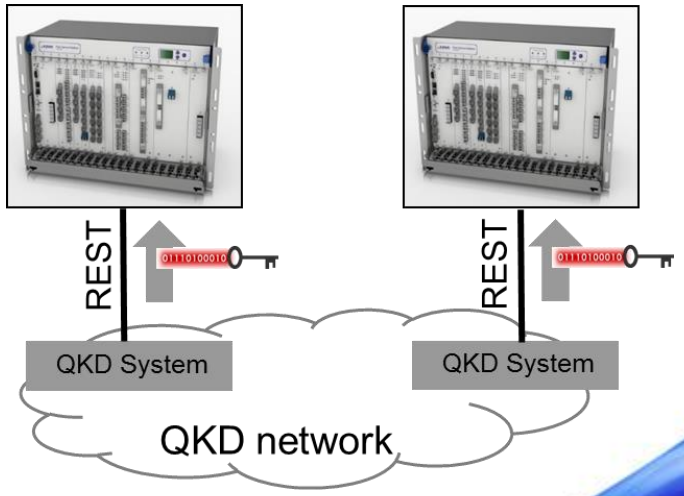
An update has recently been approved
RGS/QKD-004ed2_AppIntf (GS QKD 004)

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.
- Simple design to encourage adoption by application vendors
- Already implemented by several QKD and encryption vendors

Published February 2019

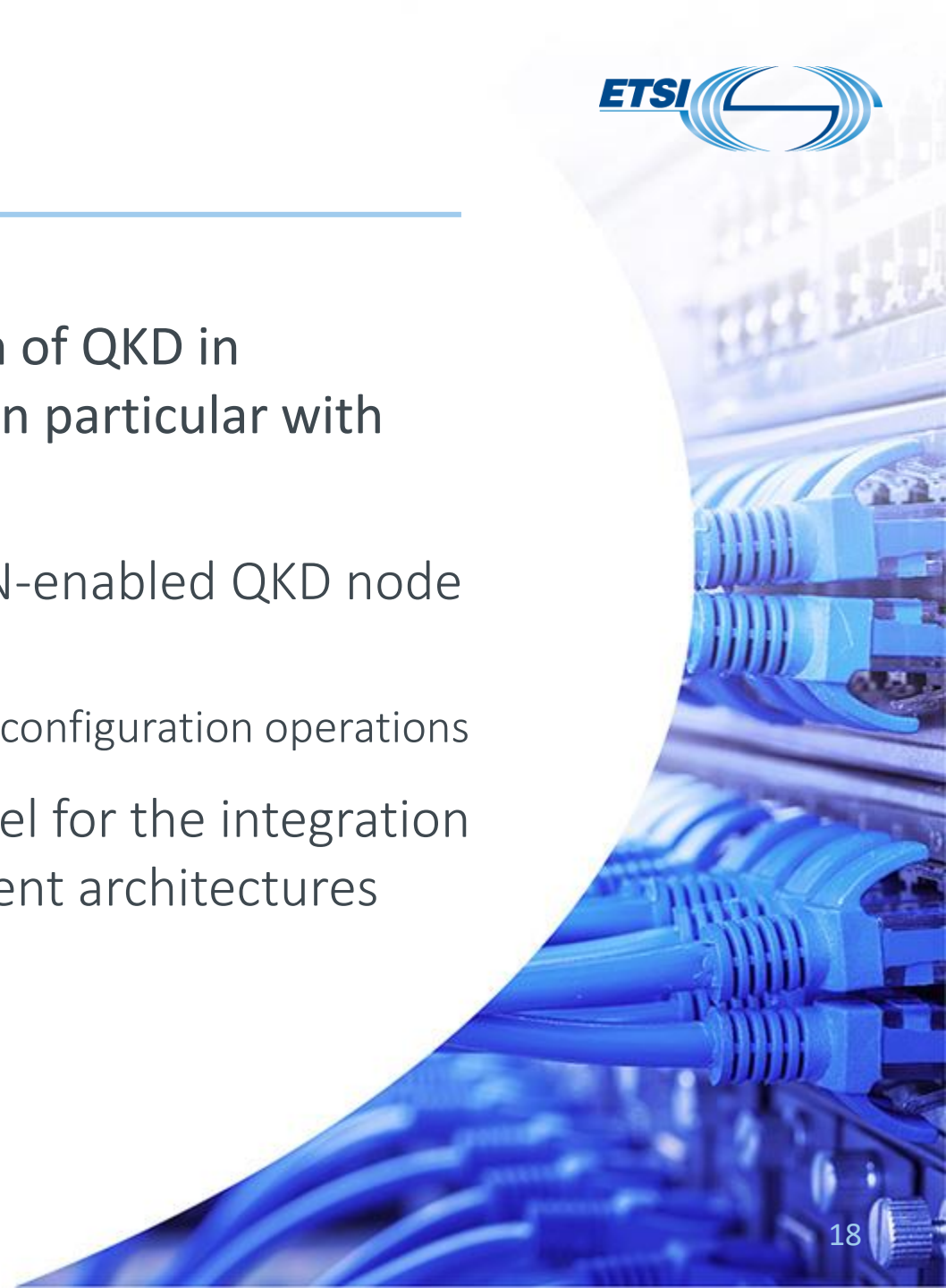


Control Interface for SDN
DGS/QKD-015_ContIntSDN (GS QKD 015)

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

Approval expected September 2020



Orchestration Interface of Software Defined Networks DGS/QKD-018OrchIntSDN (GS QKD 018)

Specifies **orchestration interfaces** between SDN Orchestrator(s) and SDN Controller(s) of QKD networks

- abstraction models
- workflows between SDN Orchestrator(s) and SDN Controller(s) of QKD networks
  - resource and system configuration management
  - performance management and alarm
  - service provisioning
  - management of multi-domain QKD networks.

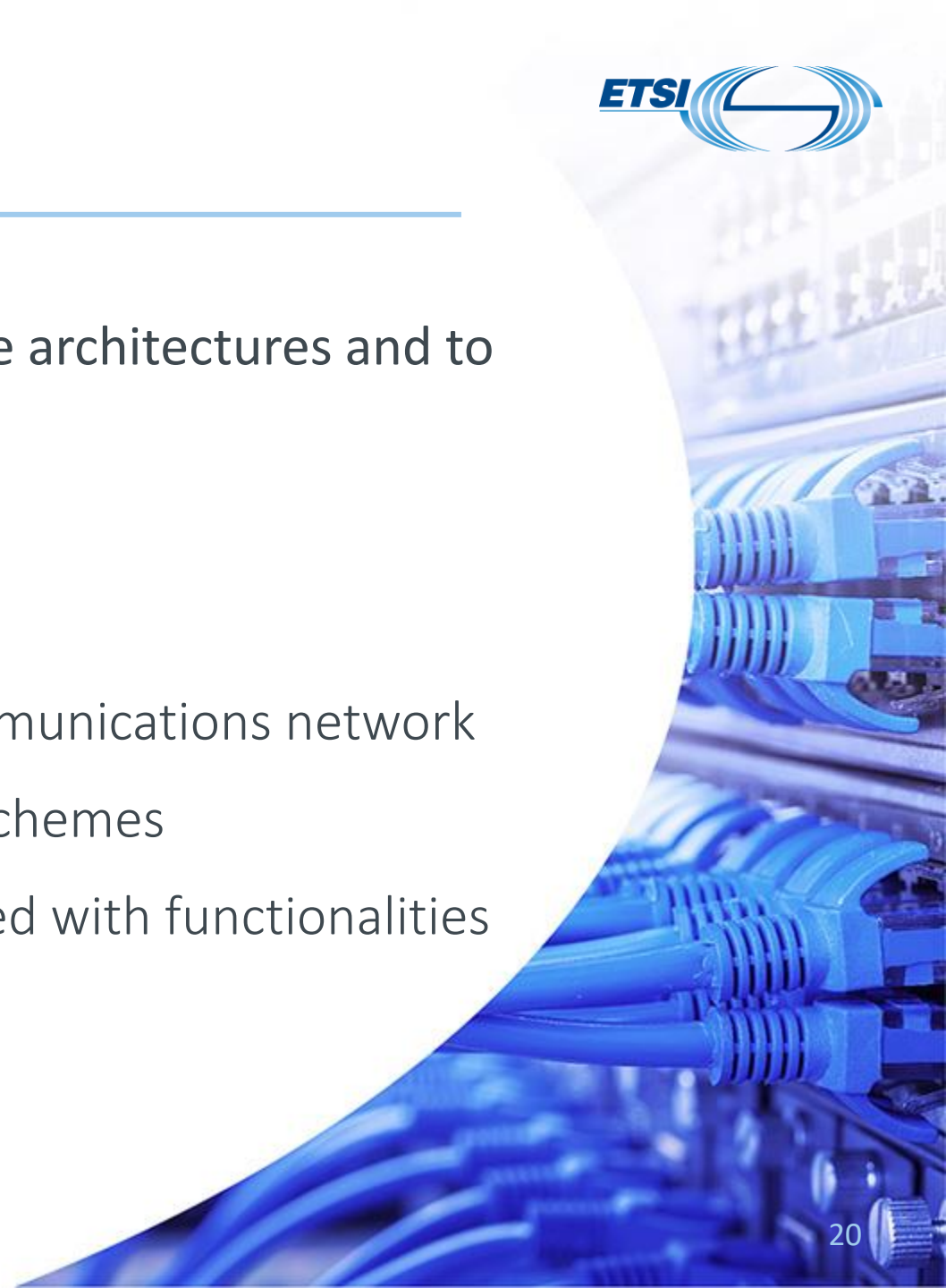
Target publication date September 2021

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



ETSI ISG QKD

- ETSI is an international member-led SDO
- Published documents are available to download (free)
- ISG QKD has experts from QKD manufacturers, application vendors, telecom operators, academics and National Metrology Institutes
- Active members from Canada, China, Europe, Russia, South Korea, US, Turkey, etc.
- Open to new members and participants (without ETSI membership)

For more information:
www.etsi.org/qkd
martin.ward@crl.toshiba.co.uk


ETSI
The Standards People