Quantum Security Standardization Activities - Prerequisite for Building up Ecosystem

Dong-Hi SIM, Head of Global Standards, SK Telecom

ITU Workshop on Quantum Information Technology

June 5 -7, 2019

Quantum Security 2.0

Quantum Security being used in real life

Quantum Security 1.0

Technology Development

Labs and PoC

Quantum Security 2.0

Being used in Real Life

Real use case development for telecom Network, Finance etc

Prerequisite for building up Ecosystem of Quantum Security

Scalable, Service Oriented
& Cost Effective
Quantum Safe Communication?

Interoperable QKD device for various types of Application?

Lack of Standards (especially for telecom operators) for Quantum Security

Standards to support Quantum Key Distribution Network

Application of QKD

Until Now…

Point to Point

- Secure Communication for QKD itself
- Distance limit

Recently…

Multi-user QKD Network

- Overcome the distance limit with Trusted Node
- Key Distribution and Management
- Interface to the Application (Consumer)

Recommendations for QKD & QRNG in SG17

SG17	QKD

- Security Framework for QKD (TR)
- Security Requirements for QKD networks – Overview
- Security Requirements for QKD networks – Key Management
- Use of cryptographic functions on key generated in QKD networks

SG17	QRNG

- QRNG Architecture

Security Framework for QKD

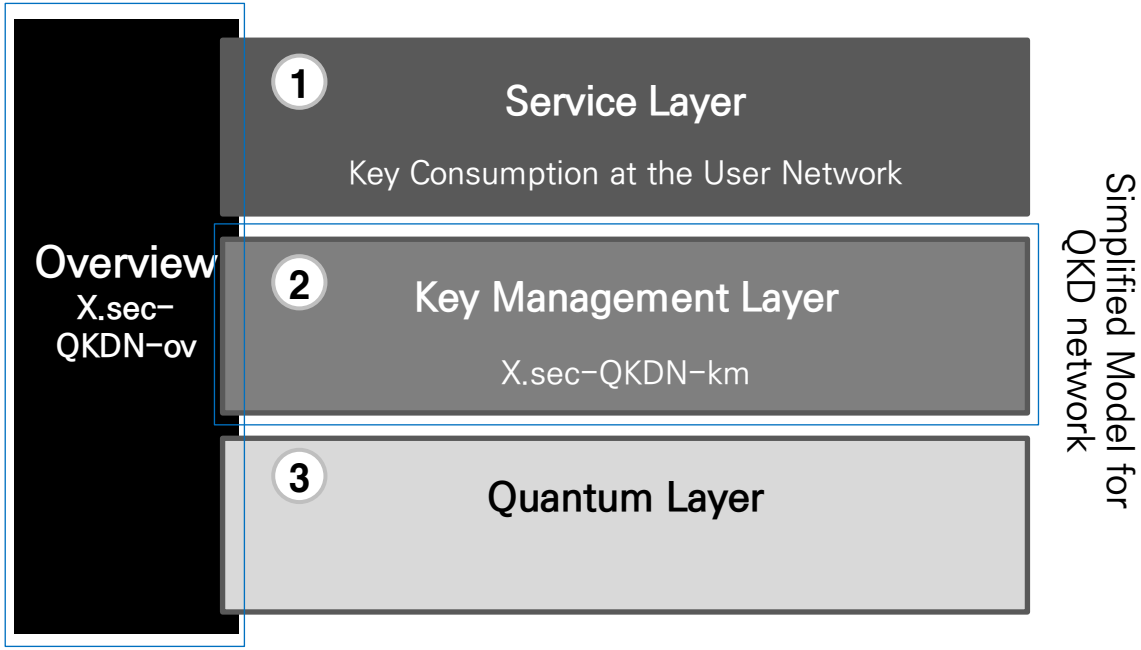
QKD in General

- Security aspects for QKD
  - Trusted Relay
- Gap analysis between ETSI & ISO/IEC and ITU-T

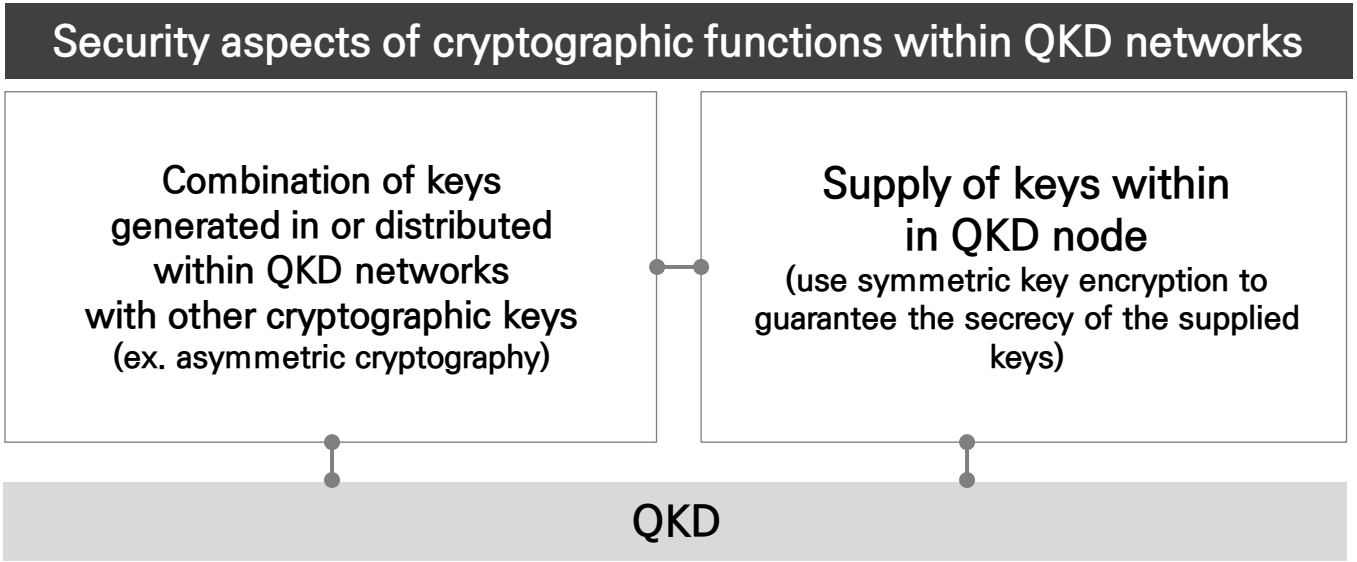
Standardization issues & suggestions

- QKD Network interoperability

Security Requirements for QKD



Use of cryptographic functions on a key generated or distributed within QKD networks



Standards to support Quantum Random Number Generator

QRNG standard

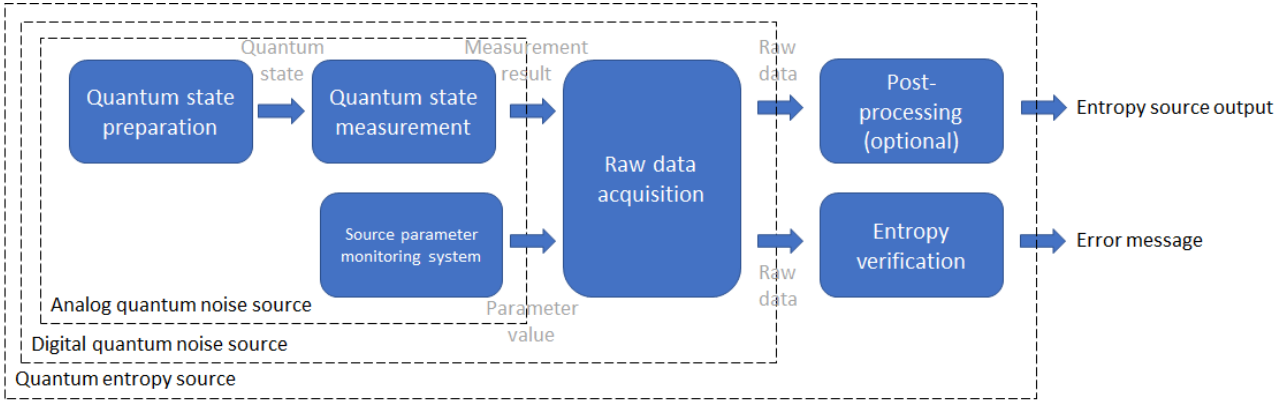
Past: TRNG

Now: QRNG

Unpredictability of physical entropy source is not well defined or known

Unpredictability of quantum entropy source comes from a complete definition of this source

Important to define this difference is important



Prerequisite for building up Ecosystem of Quantum Security


SK telecom
5GX


SK telecom