양자정보통신 기술표준 개발

GISC 2021

엘타워

2021. 11. 12.

최태상

ETRI

Topics

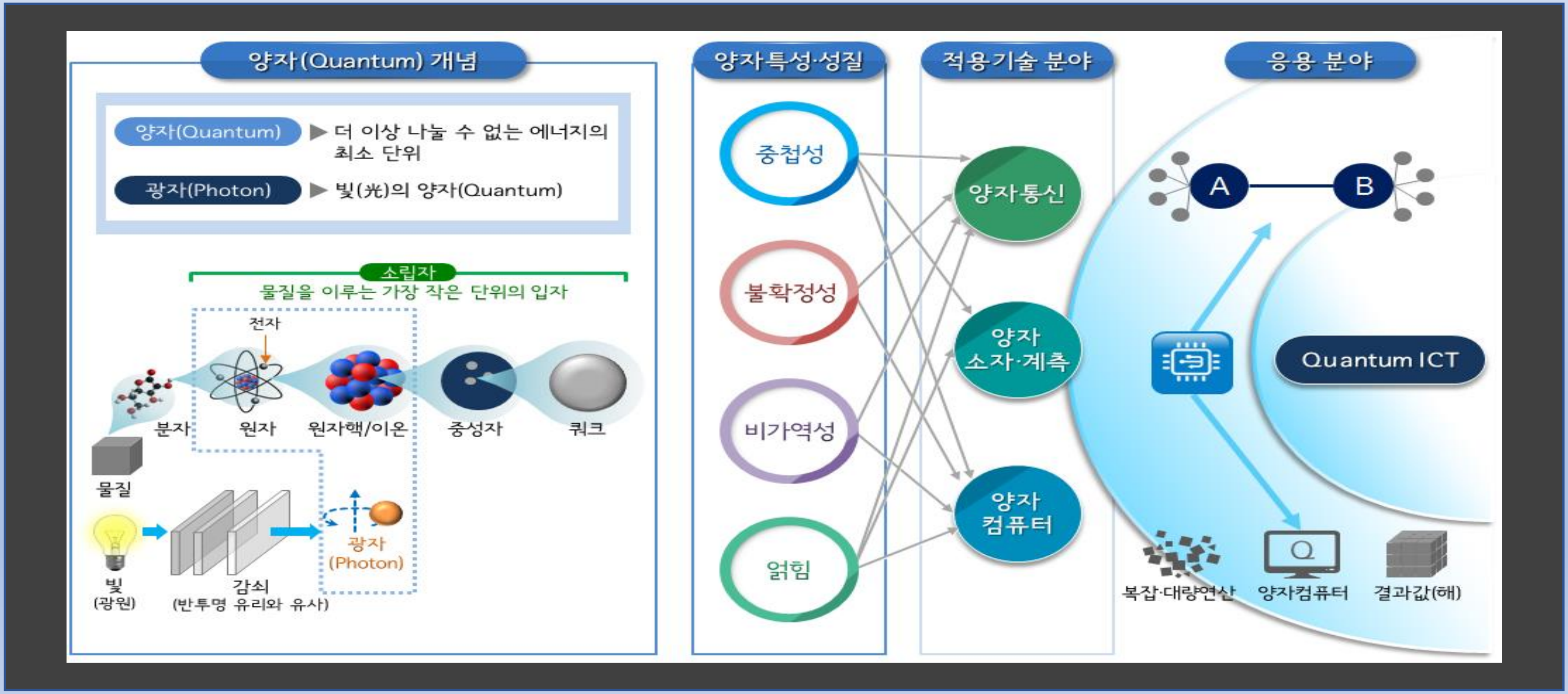
- Project Overview
- QKDN Standardization Status
- Main Contribution: Standards
- Main Contribution: Standard Patents
- Main Contribution: Market Deployment
- Future Challenges

Topics

- Project Overview
- QKDN Standardization Status
- Main Contribution: Standards
- Main Contribution: Standard Patents
- Main Contribution: Market Deployment
- Future Challenges

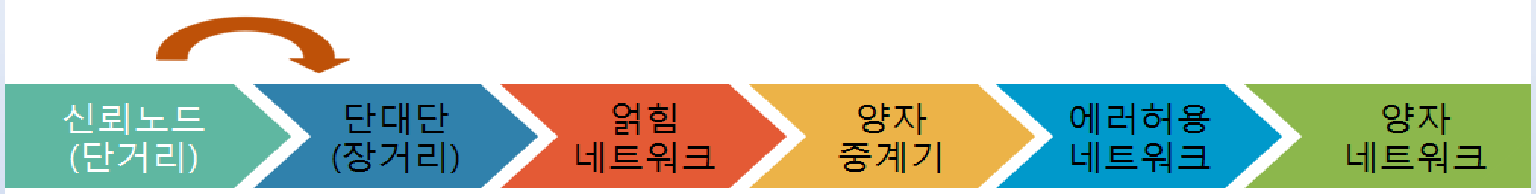
양자정보통신 기술 정의

- ◆ 양자의 물리학적 성질을 이용하여 정보를 생성, 전송, 저장, 가공하는 정보통신 기술로서, 크게 양자통신, 양자센서/이미징 및 양자컴퓨팅으로 분류
- ◆ 본 과제 범위: 양자암호 분배 네트워크 기술, 양자암호 제어 및 관리 기술, 양자전송 네트워크, 양자 저장 및 가공 기술을 포함하는 양자 정보통신 기술의 표준화
  - ➢ 양자암호통신 네트워크(QKDN): 암호화를 위한 비밀키는 안전한 양자채널로 전달하고 암호화된 데이터는 고전 채널로 전송
  - ➢ 양자 전송 네트워크(QITN): 양자 얽힘 특성을 이용하여 중첩 상태의 양자 정보 그대로를 전송



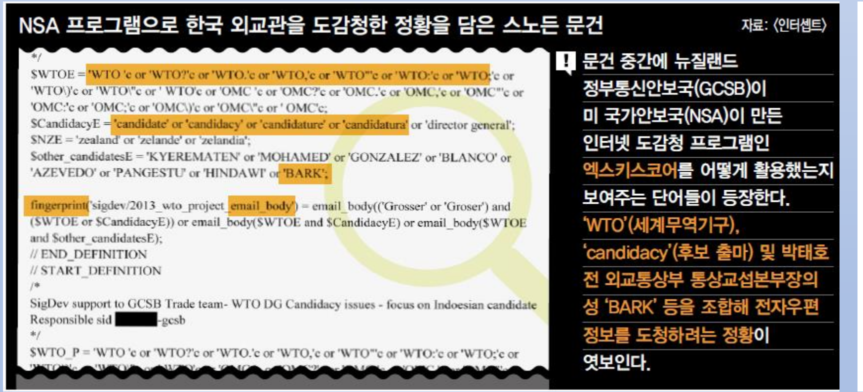
양자정보통신 기술 정의

◆ EU의 양자 인터넷 구성을 위한 6단계 모델에서 중·단거리 노드간 암호키를 교환하는 1~2 단계 수준



◆ 고전 통신의 유무선 채널은 전파·전기의 물리적 특성으로 도청 (광케이블을 살짝 구부리거나 광커플러, 광스플리터 등을 연결)에 매우 취약해 정보를 탈취해도 해독하지 못하게 하는 암호화 기술을 사용

◆ 반도체(연산속도), 병렬처리, 클라우드 등 정보통신 기술발전이 계산 복잡성에 의존하고 있는 암호화 기술을 위협



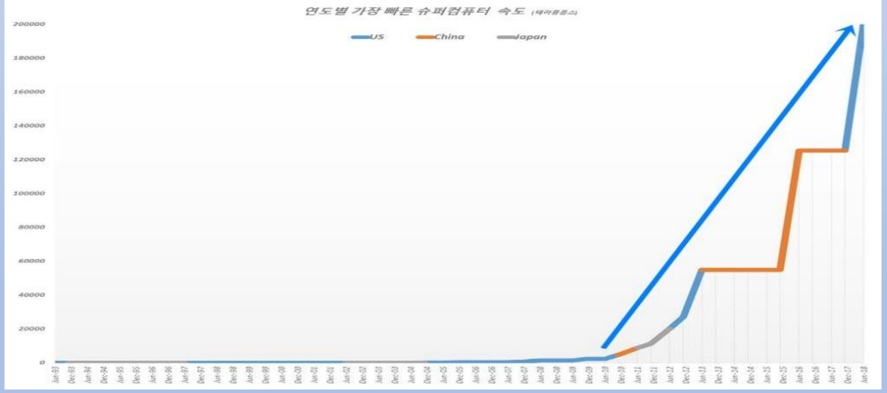
NSA 프로그램으로 한국 외교관을 도감청한 정황을 담은 스노든 문건

자료: 〈인터셉트〉

```
*/
$WTOE = 'WTO 'c or 'WTO?'c or 'WTO.'c or 'WTO,'c or 'WTO"'c or 'WTO:'c or 'WTO;'c or
'WTO\)'c or 'WTO\"c or ' WTO'c or 'OMC 'c or 'OMC?'c or 'OMC.'c or 'OMC,'c or 'OMC"'c or
'OMC:'c or 'OMC;'c or 'OMC\)'c or 'OMC\"c or ' OMC'c;
$CandidacyE = 'candidate' or 'candidacy' or 'candidature' or 'candidatura' or 'director general';
$NZE = 'zealand' or 'zelande' or 'zelandia';
$other_candidatesE = 'KYEREMATEN' or 'MOHAMED' or 'GONZALEZ' or 'BLANCO' or
'AZEVEDO' or 'PANGESTU' or 'HINDAWI' or 'BARK';

fingerprint('sigdev/2013_wto_project_email_body') = email_body(('Grosser' or 'Groser') and
($WTOE or $CandidacyE)) or email_body($WTOE and $CandidacyE) or email_body($WTOE
and $other_candidatesE);
// END_DEFINITION
// START_DEFINITION
/*
SigDev support to GCSB Trade team- WTO DG Candidacy issues - focus on Indoesian candidate
Responsible sid [redacted]-gcsb
*/
$WTO_P = 'WTO 'c or 'WTO?'c or 'WTO.'c or 'WTO,'c or 'WTO"'c or 'WTO:'c or 'WTO;'c or
```

문건 중간에 뉴질랜드 정부통신안보국(GCSB)이 미 국가안보국(NSA)이 만든 인터넷 도감청 프로그램인 엑스키스코어를 어떻게 활용했는지 보여주는 단어들이 등장한다. 'WTO'(세계무역기구), 'candidacy'(후보 출마) 및 박태호 전 외교통상부 통상교섭본부장의 성 'BARK' 등을 조합해 전자우편 정보를 도청하려는 정황이 엿보인다.

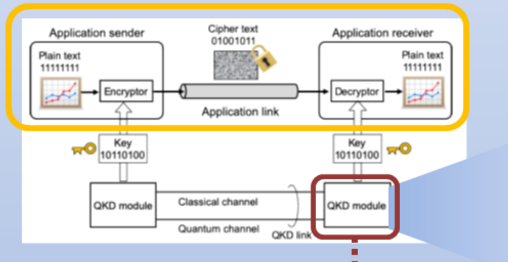

연도별 가장 빠른 슈퍼컴퓨터 속도 (테라플롭스)

◆ 양자암호통신은 이론적으로 무조건적 보안성을 제공하는 현존하는 유일한 기술

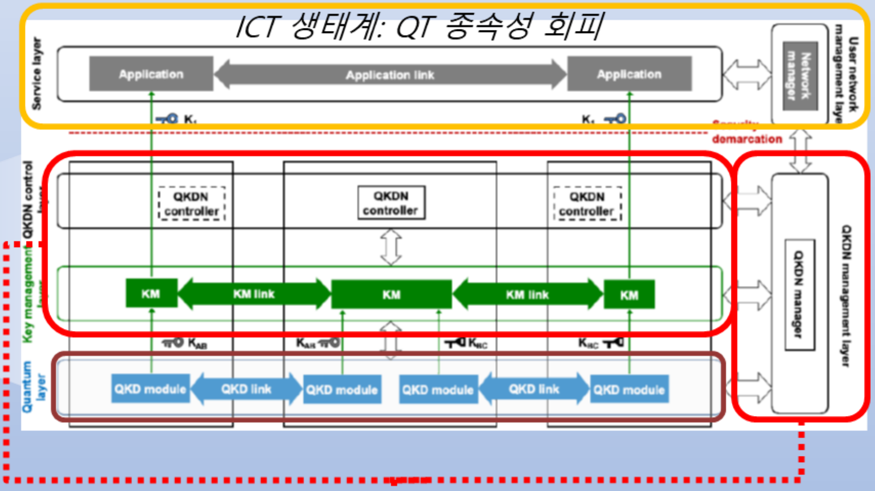
양자정보통신 기술 표준화 필요성

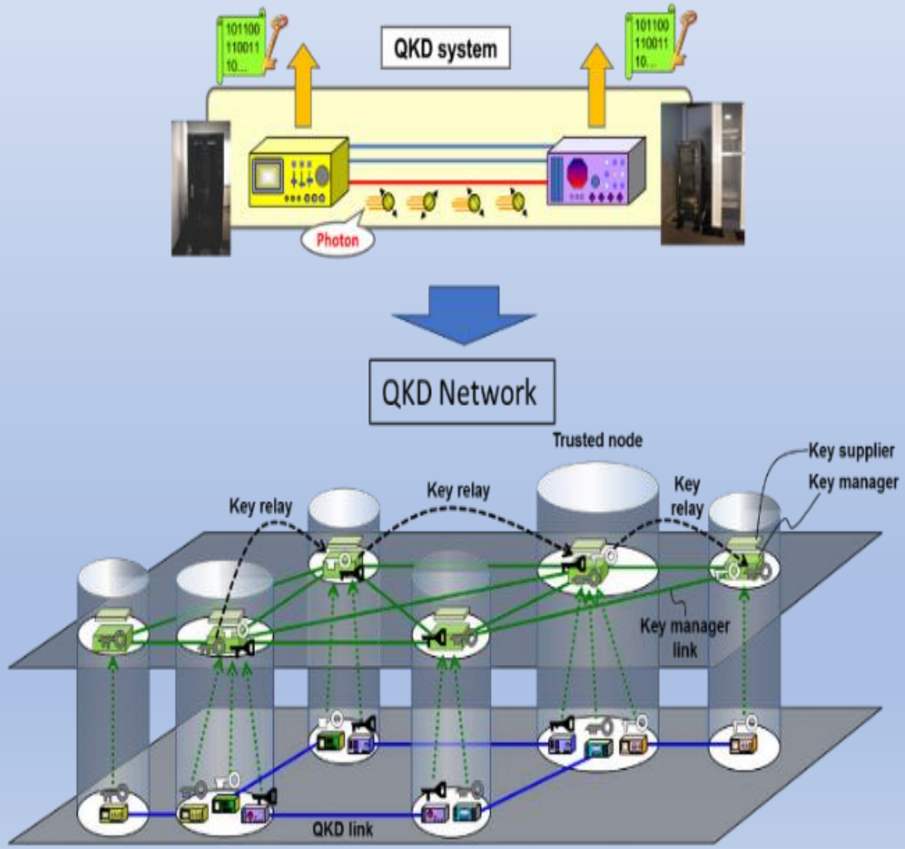
- ◆ETSI에서 최초로 양자암호통신 관련 7건의 표준규격 및 9건의 연구보고서/가이드 발행 하였으나, 장비 제조회사 관점에서의 기술 중심 표준임, **실제 양자암호통신망 구성을 위해서는 네트워크 관점에서의 표준**이 필요
- ◆KT를 포함한 국내 7개 기업의 ITU-T 표준 작업을 통해 **최초로 양자암호통신 네트워크 표준화 진행 중**, 계층별로 분리된 다양한 플레이어가 참여할 수 있는 환경 제공, 표준화 된 개방형 인터페이스 연결 및 다양한 벤더간 상호 호환성 제공
- ◆양자암호통신 표준화 경쟁을 장비 기술 개발에서 네트워크로 전환하여 **국내 기업의 기술 리더십 확보**

ICT 생태계: QT 종속성



ICT 생태계: QT 종속성 회피





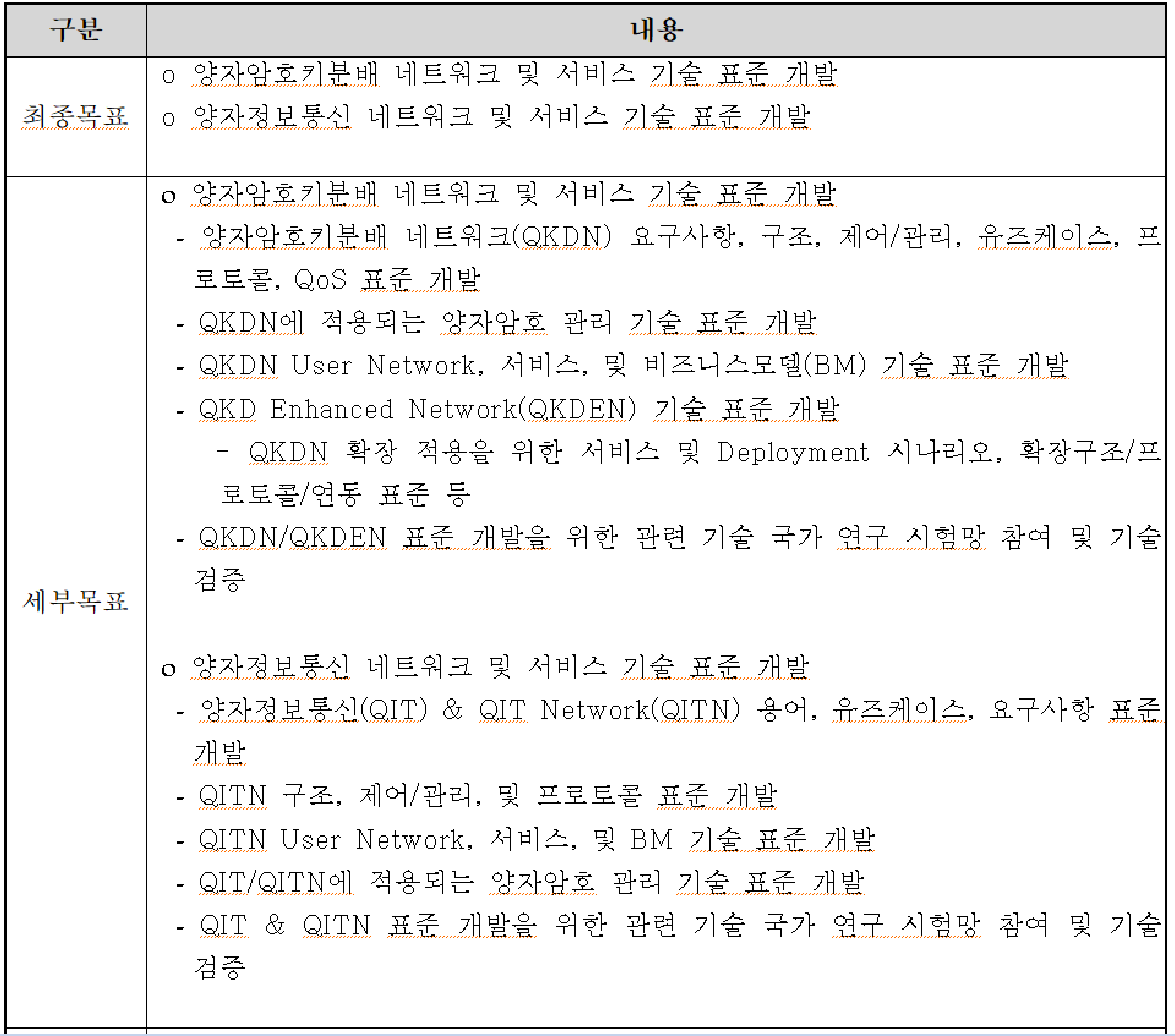
양자암호시스템
(All-in-one; Quantum Tech.가 핵심)
* 전세계 10개 이내 제조사: 한국 無

ICT Technologies
(Quantum Tech.는 Commodity化)
* 한국, Global Top ICT-tech.

사업 개요

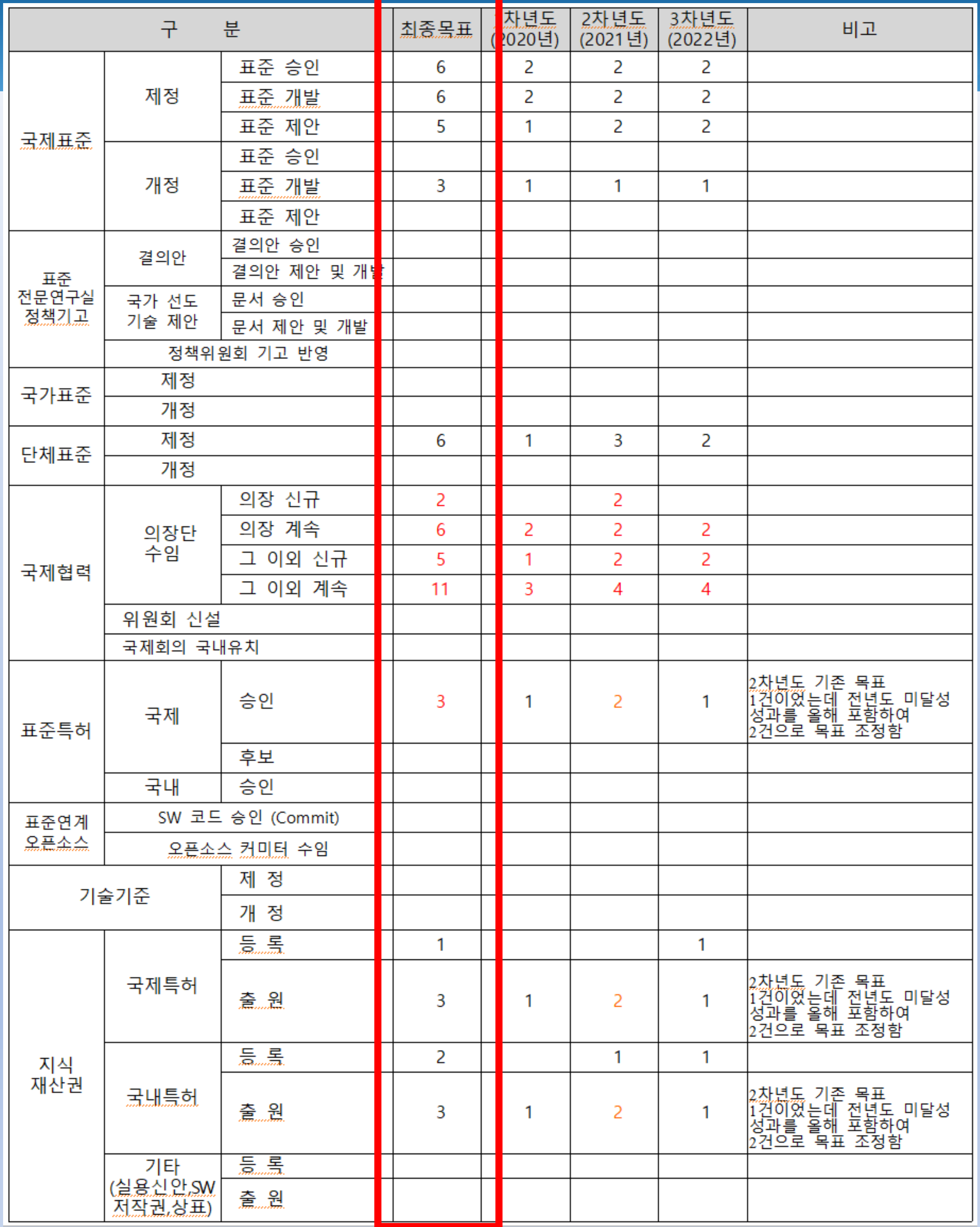
<table>
<tr><td colspan="2">사업 구분</td><td colspan="4">정보통신방송표준개발지원사업</td></tr>
<tr><td colspan="2">과제명</td><td colspan="4">양자정보통신 기술 표준 개발</td></tr>
<tr><td colspan="2">총 기간</td><td colspan="2">2020.4.1. ~ 2022.12.31. (33개월)</td><td>당해년도
기간</td><td>2020.4.1. ~ 2020.12.31. (9개월)</td></tr>
<tr><td rowspan="4">예산
(단위:천원)</td><td>년도</td><td>1차년도 ('20)</td><td>2차년도 ('21)</td><td>3차년도 ('22)</td><td>합계</td></tr>
<tr><td>정부</td><td>210,000</td><td>280,000</td><td>280,000</td><td>770,000</td></tr>
<tr><td>민간</td><td>17,100</td><td>22,700</td><td>22,700</td><td>62,500</td></tr>
<tr><td>합계</td><td>227,100</td><td>302,700</td><td>302,700</td><td>832,500</td></tr>
<tr><td colspan="2">주관기관</td><td colspan="4">● 한국전자통신연구원
● 사업책임자: 최태상 책임연구원</td></tr>
<tr><td colspan="2">공동
연구기관</td><td colspan="4">● (주)케이티
● 사업책임자: 김형수 팀장</td></tr>
</table>

연구 목표



구분	내용
최종목표	o 양자암호키분배 네트워크 및 서비스 기술 표준 개발 o 양자정보통신 네트워크 및 서비스 기술 표준 개발
세부목표	o 양자암호키분배 네트워크 및 서비스 기술 표준 개발 - 양자암호키분배 네트워크(QKDN) 요구사항, 구조, 제어/관리, 유즈케이스, 프로토콜, QoS 표준 개발 - QKDN에 적용되는 양자암호 관리 기술 표준 개발 - QKDN User Network, 서비스, 및 비즈니스모델(BM) 기술 표준 개발 - QKD Enhanced Network(QKDEN) 기술 표준 개발 – QKDN 확장 적용을 위한 서비스 및 Deployment 시나리오, 확장구조/프로토콜/연동 표준 등 - QKDN/QKDEN 표준 개발을 위한 관련 기술 국가 연구 시험망 참여 및 기술검증 o 양자정보통신 네트워크 및 서비스 기술 표준 개발 - 양자정보통신(QIT) & QIT Network(QITN) 용어, 유즈케이스, 요구사항 표준개발 - QITN 구조, 제어/관리, 및 프로토콜 표준 개발 - QITN User Network, 서비스, 및 BM 기술 표준 개발 - QIT/QITN에 적용되는 양자암호 관리 기술 표준 개발 - QIT & QITN 표준 개발을 위한 관련 기술 국가 연구 시험망 참여 및 기술검증

연구 목표

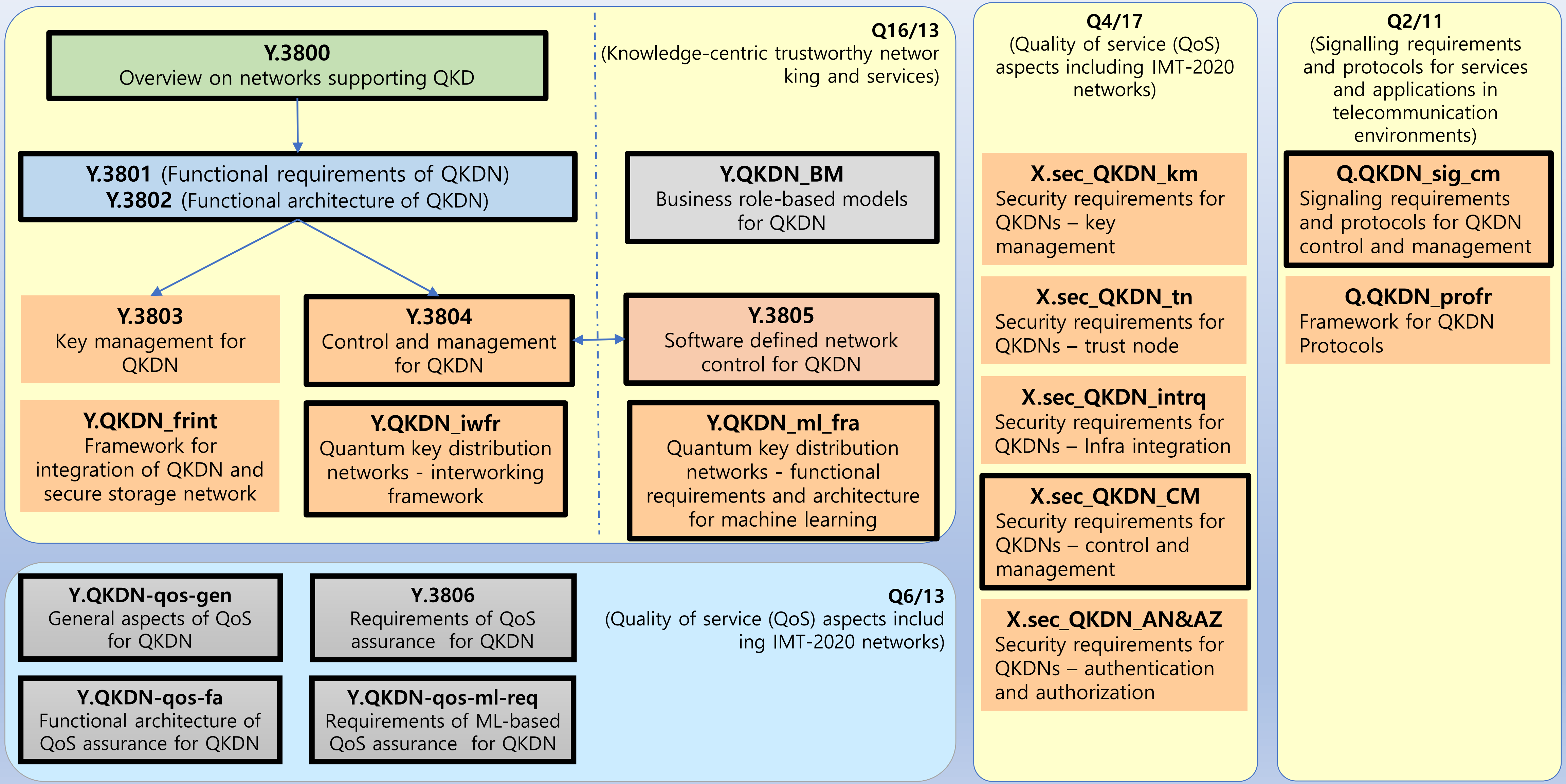


구 분			최종목표	1차년도 (2020년)	2차년도 (2021년)	3차년도 (2022년)	비고
국제표준	제정	표준 승인	6	2	2	2	
		표준 개발	6	2	2	2	
		표준 제안	5	1	2	2	
	개정	표준 승인					
		표준 개발	3	1	1	1	
		표준 제안					
표준 전문연구실 정책기고	결의안	결의안 승인					
		결의안 제안 및 개발					
	국가 선도 기술 제안	문서 승인					
		문서 제안 및 개발					
	정책위원회 기고 반영						
국가표준	제정						
	개정						
단체표준	제정		6	1	3	2	
	개정						
국제협력	의장단 수임	의장 신규	2		2		
		의장 계속	6	2	2	2	
		그 이외 신규	5	1	2	2	
		그 이외 계속	11	3	4	4	
	위원회 신설						
	국제회의 국내유치						
표준특허	국제	승인	3	1	2	1	2차년도 기존 목표 1건이었는데 전년도 미달성 성과를 올해 포함하여 2건으로 목표 조정함
		후보					
	국내	승인					
표준연계 오픈소스	SW 코드 승인 (Commit)						
	오픈소스 커미터 수임						
기술기준		제 정					
		개 정					
지식 재산권	국제특허	등 록	1			1	
		출 원	3	1	2	1	2차년도 기존 목표 1건이었는데 전년도 미달성 성과를 올해 포함하여 2건으로 목표 조정함
	국내특허	등 록	2		1	1	
		출 원	3	1	2	1	2차년도 기존 목표 1건이었는데 전년도 미달성 성과를 올해 포함하여 2건으로 목표 조정함
	기타 (실용신안,SW 저작권,상표)	등 록					
		출 원					

Topics

- Project Overview
- QKDN Standardization Status
- **Main Contribution: Standards**
- **Main Contribution: Standard Patents**
- Main Contribution: Market Deployment
- Future Challenges

QKDN related documents in ITU-T SG13/11/17



Q16/13
(Knowledge-centric trustworthy networking and services)

Y.3800
Overview on networks supporting QKD

Y.3801 (Functional requirements of QKDN)
Y.3802 (Functional architecture of QKDN)

Y.3803
Key management for QKDN

Y.3804
Control and management for QKDN

Y.QKDN_frint
Framework for integration of QKDN and secure storage network

Y.QKDN_iwfr
Quantum key distribution networks - interworking framework

Y.QKDN_BM
Business role-based models for QKDN

Y.3805
Software defined network control for QKDN

Y.QKDN_ml_fra
Quantum key distribution networks - functional requirements and architecture for machine learning

Q6/13
(Quality of service (QoS) aspects including IMT-2020 networks)

Y.QKDN-qos-gen
General aspects of QoS for QKDN

Y.3806
Requirements of QoS assurance for QKDN

Y.QKDN-qos-fa
Functional architecture of QoS assurance for QKDN

Y.QKDN-qos-ml-req
Requirements of ML-based QoS assurance for QKDN

Q4/17
(Quality of service (QoS) aspects including IMT-2020 networks)

X.sec_QKDN_km
Security requirements for QKDNs – key management

X.sec_QKDN_tn
Security requirements for QKDNs – trust node

X.sec_QKDN_intrq
Security requirements for QKDNs – Infra integration

X.sec_QKDN_CM
Security requirements for QKDNs – control and management

X.sec_QKDN_AN&AZ
Security requirements for QKDNs – authentication and authorization

Q2/11
(Signalling requirements and protocols for services and applications in telecommunication environments)

Q.QKDN_sig_cm
Signaling requirements and protocols for QKDN control and management

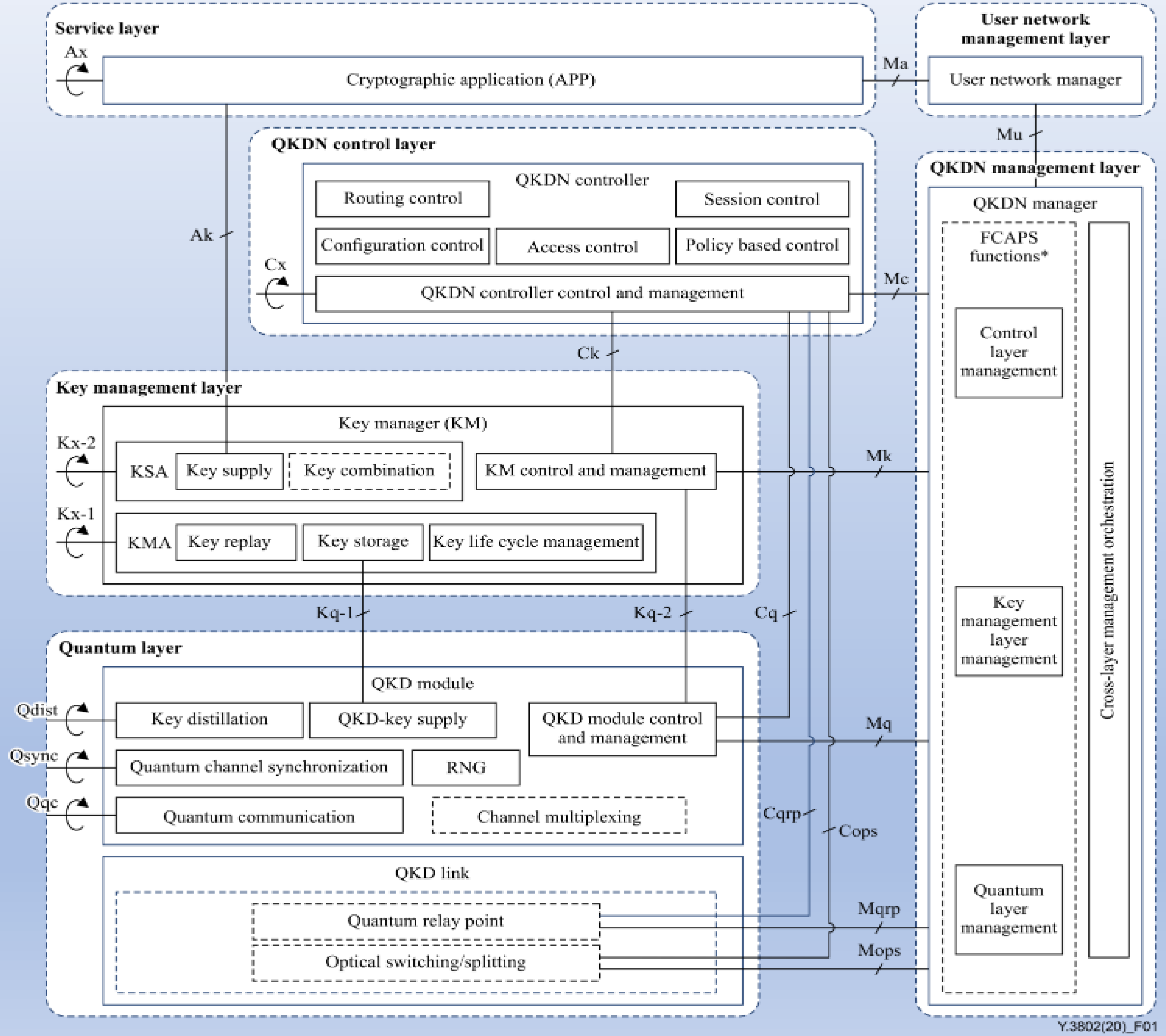
Q.QKDN_profr
Framework for QKDN Protocols

Functional Architecture of Quantum Key Distribution Networks

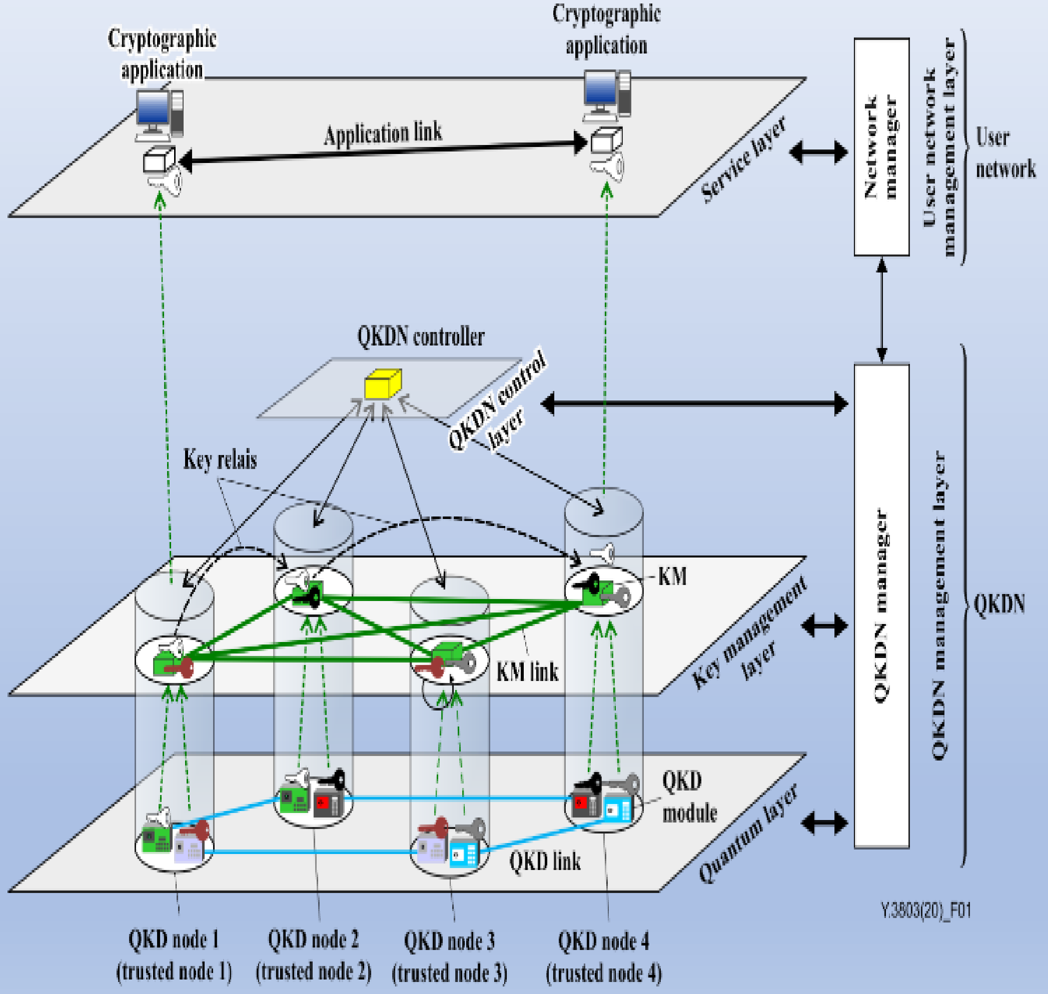
Specifies

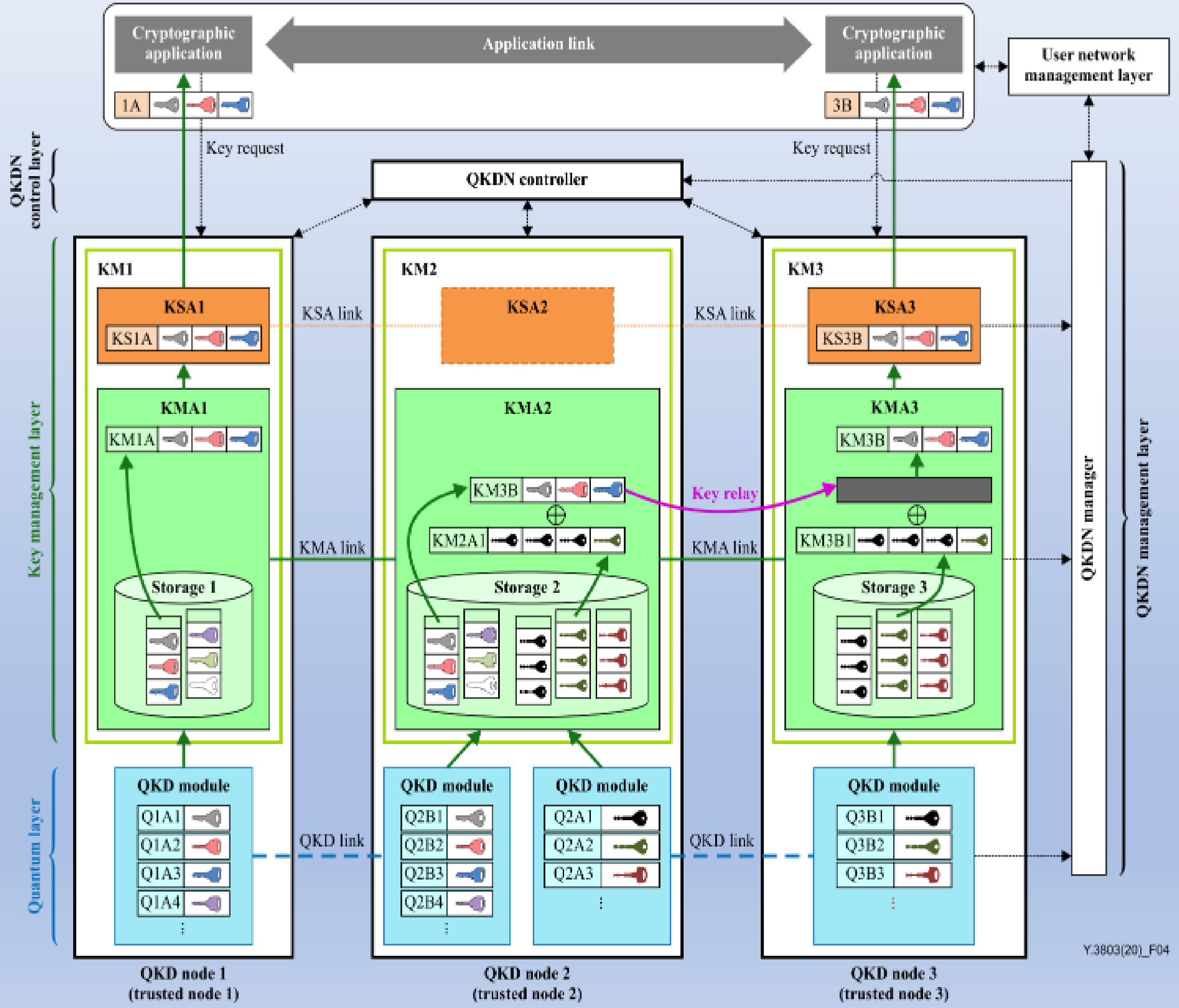
- Functional elements of QKD network (QKDN) control, management, and orchestration;
- Functions of QKDN control, management, and orchestration;
- Procedures of QKDN control, management, and orchestration.

Traditional fault, configuration, accounting, performance and security (FCAPS) functionality which is not specific to QKDN is out of scope of this Recommendation.



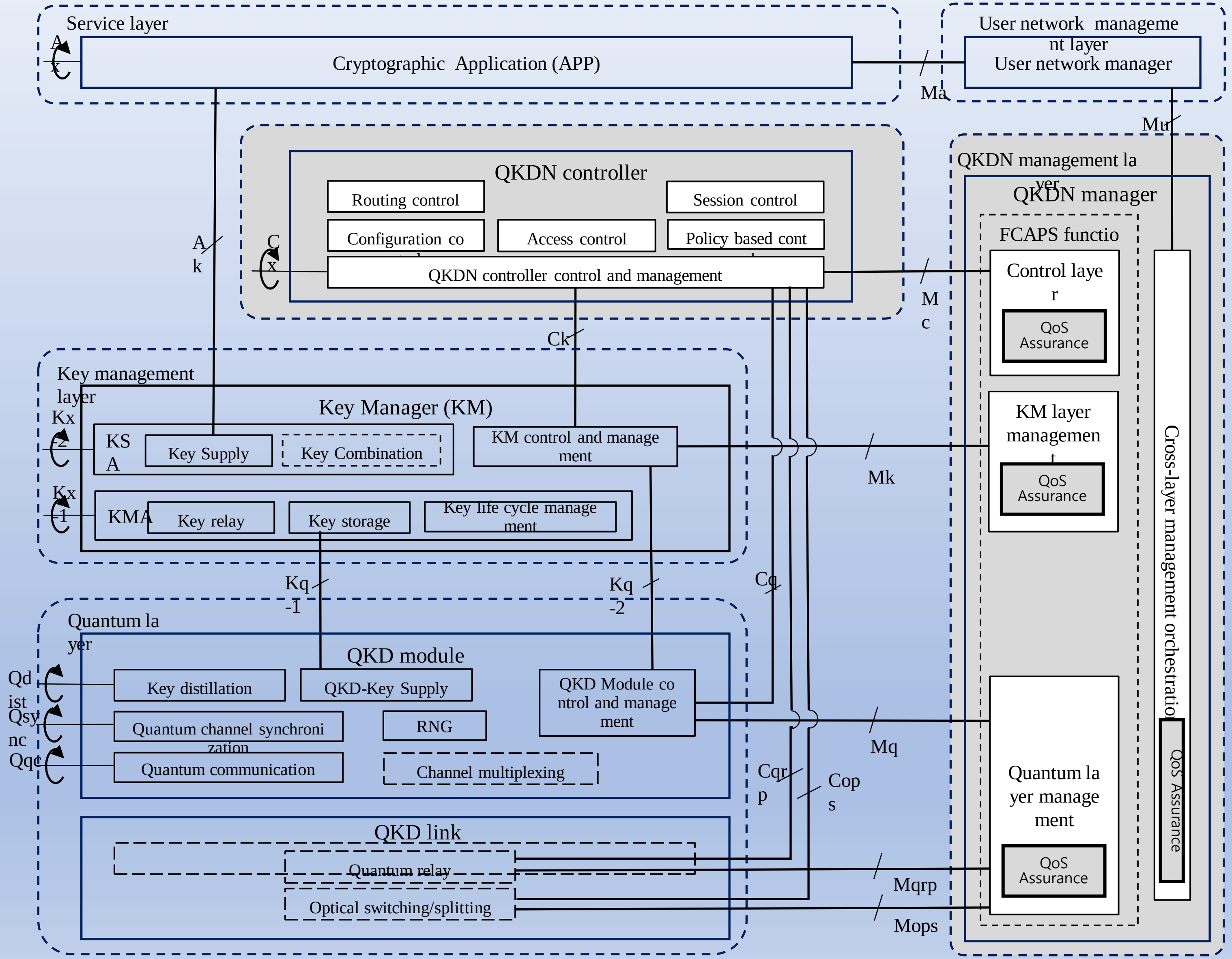
Key Management of Quantum Key Distribution Networks





Control and Management of Quantum Key Distribution Networks

- Functional elements of QKD network (QKDN) control, management, and orchestration;
- Functions of QKDN control, management, and orchestration;
- Procedures of QKDN control, management, and orchestration.
- Traditional fault, configuration, accounting, performance and security (FCAPS) functionality which is not specific to QKDN is out of scope of this Recommendation.



Example Management Procedures

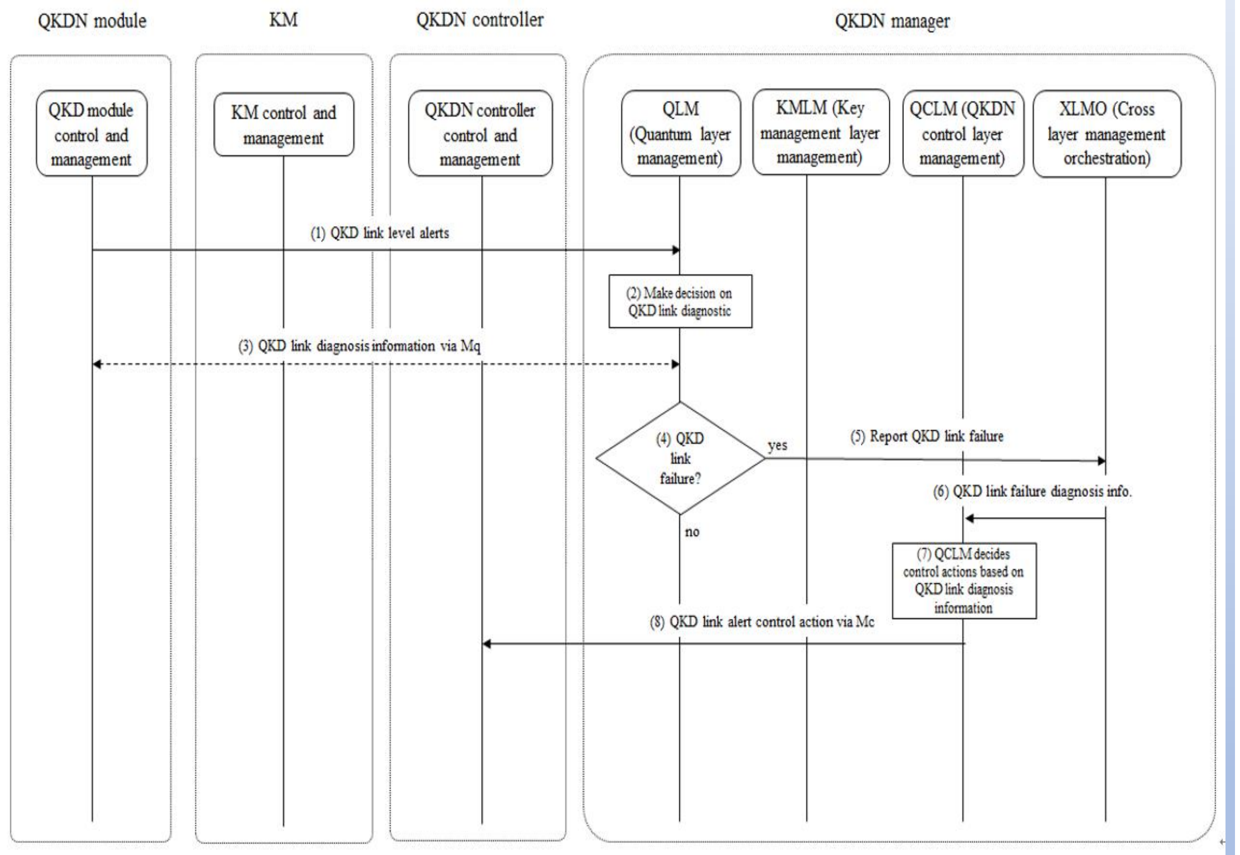

QKDN module
KM
QKDN controller
QKDN manager
QKD module control and management
KM control and management
QKDN controller control and management
QLM (Quantum layer management)
KMLM (Key management layer management)
QCLM (QKDN control layer management)
XLMO (Cross layer management orchestration)
(1) QKD link level alerts
(2) Make decision on QKD link diagnostic
(3) QKD link diagnosis information via Mq
(4) QKD link failure?
yes
no
(5) Report QKD link failure
(6) QKD link failure diagnosis info.
(7) QCLM decides control actions based on QKD link diagnosis information
(8) QKD link alert control action via Mc

Figure 2. An example of fault management procedures: QKD link failure

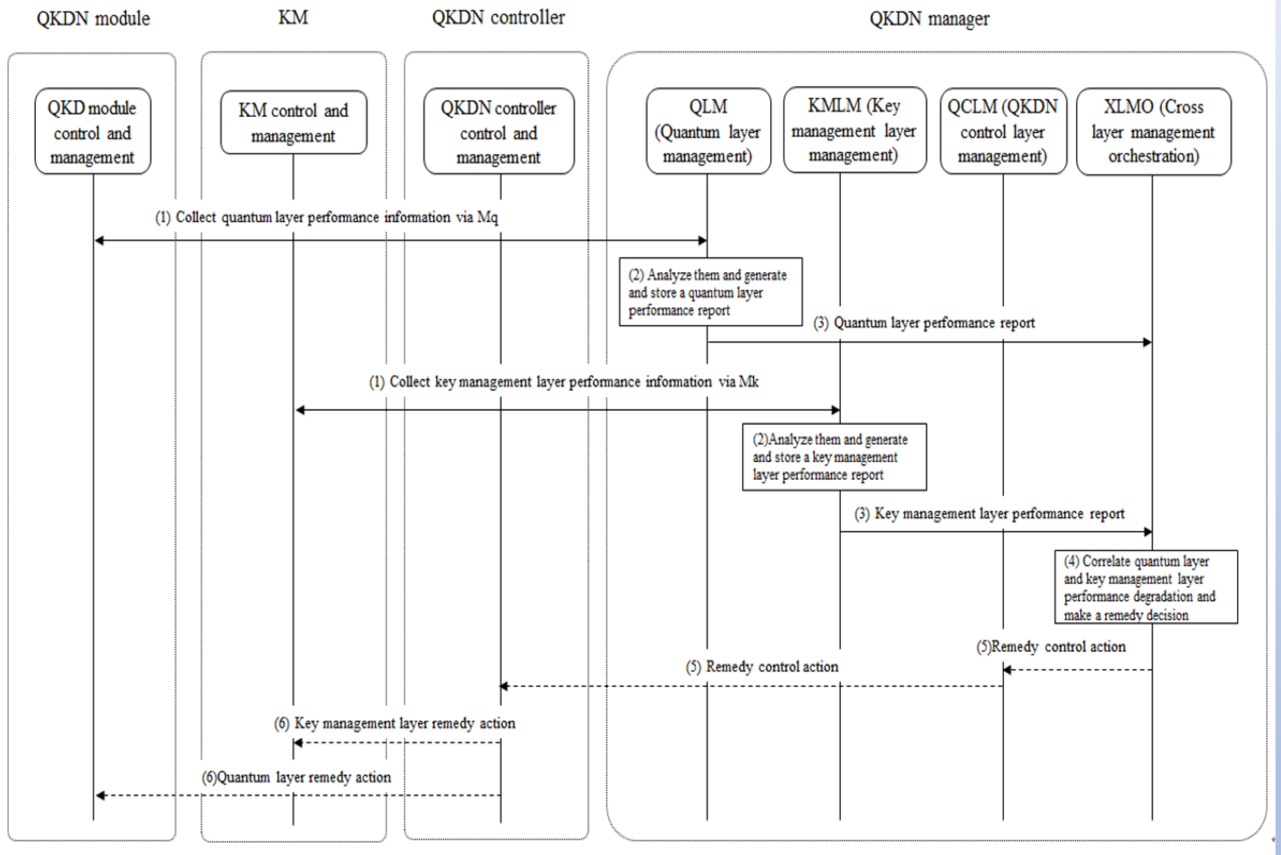
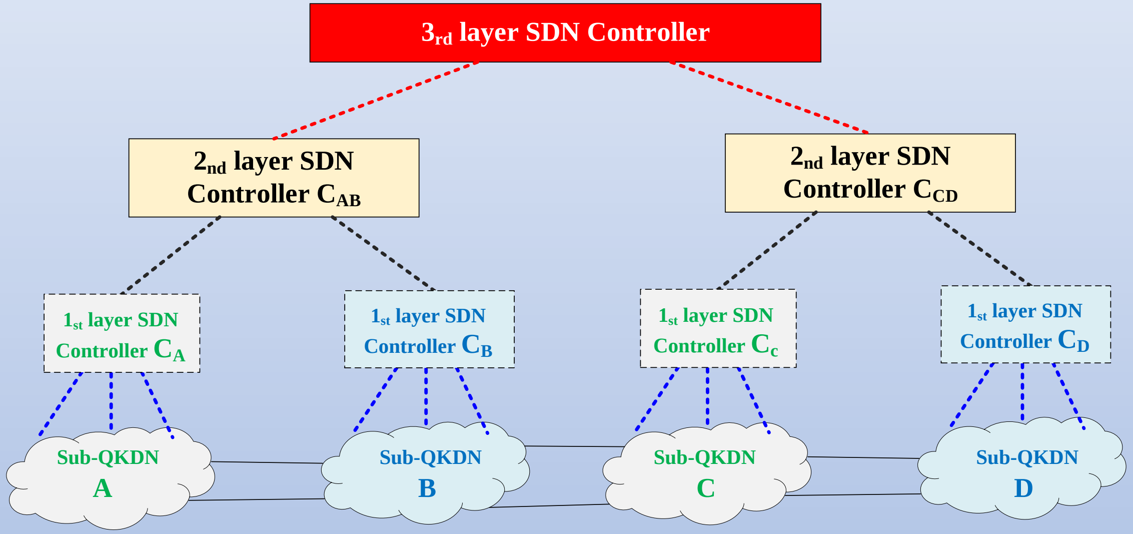

QKDN module
KM
QKDN controller
QKDN manager
QKD module control and management
KM control and management
QKDN controller control and management
QLM (Quantum layer management)
KMLM (Key management layer management)
QCLM (QKDN control layer management)
XLMO (Cross layer management orchestration)
(1) Collect quantum layer performance information via Mq
(2) Analyze them and generate and store a quantum layer performance report
(3) Quantum layer performance report
(1) Collect key management layer performance information via Mk
(2)Analyze them and generate and store a key management layer performance report
(3) Key management layer performance report
(4) Correlate quantum layer and key management layer performance degradation and make a remedy decision
(5)Remedy control action
(5) Remedy control action
(6) Key management layer remedy action
(6)Quantum layer remedy action

Figure 6. An example of performance management procedures

SDN Control of Quantum Key Distribution Networks



3_{rd} layer SDN Controller

2_{nd} layer SDN Controller C_{AB}

2_{nd} layer SDN Controller C_{CD}

1_{st} layer SDN Controller C_A

1_{st} layer SDN Controller C_B

1_{st} layer SDN Controller C_c

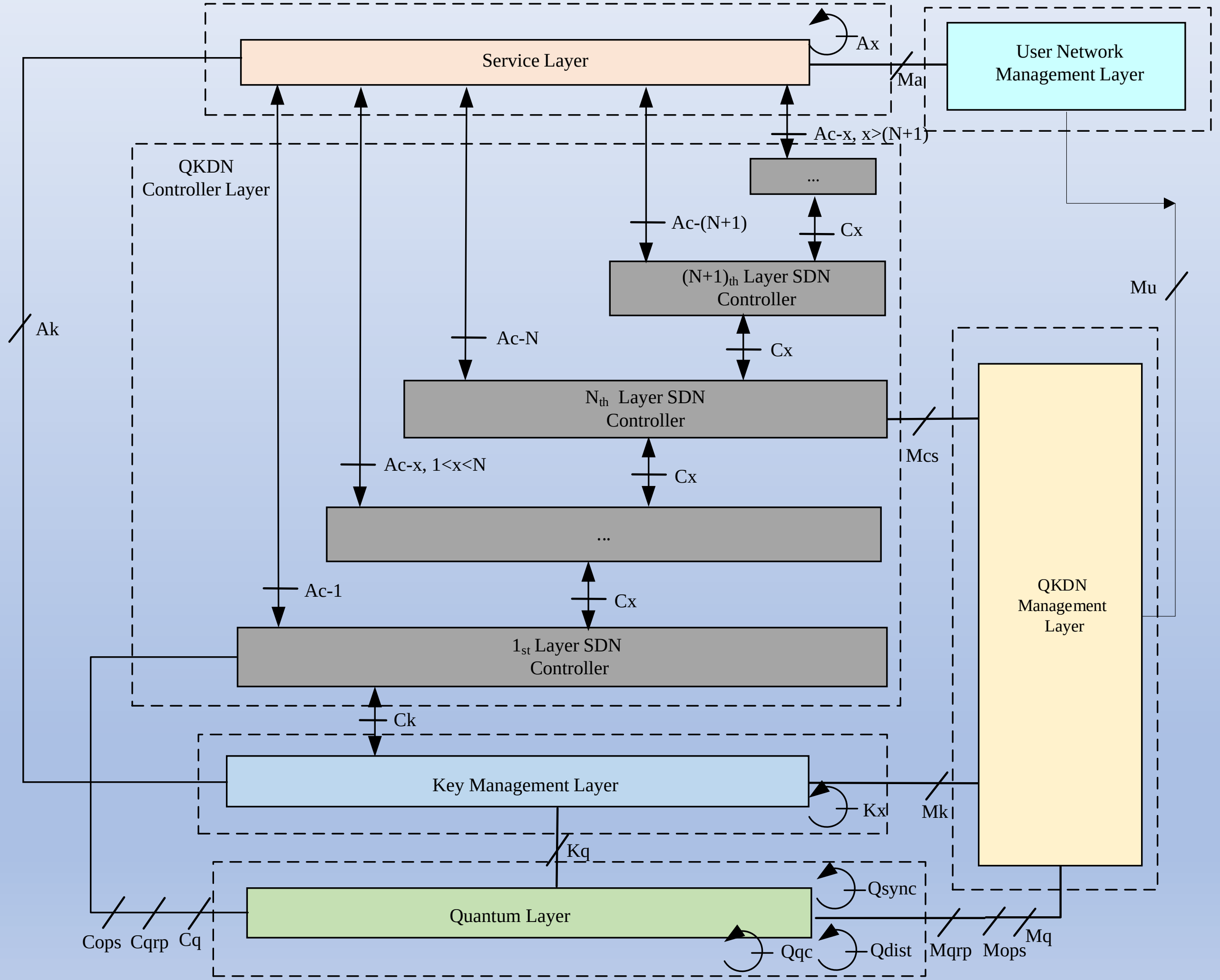
1_{st} layer SDN Controller C_D

Sub-QKDN A

Sub-QKDN B

Sub-QKDN C

Sub-QKDN D



Service Layer

User Network Management Layer

QKDN Controller Layer

...

$(N+1)_{th}$ Layer SDN Controller

N_{th} Layer SDN Controller

...

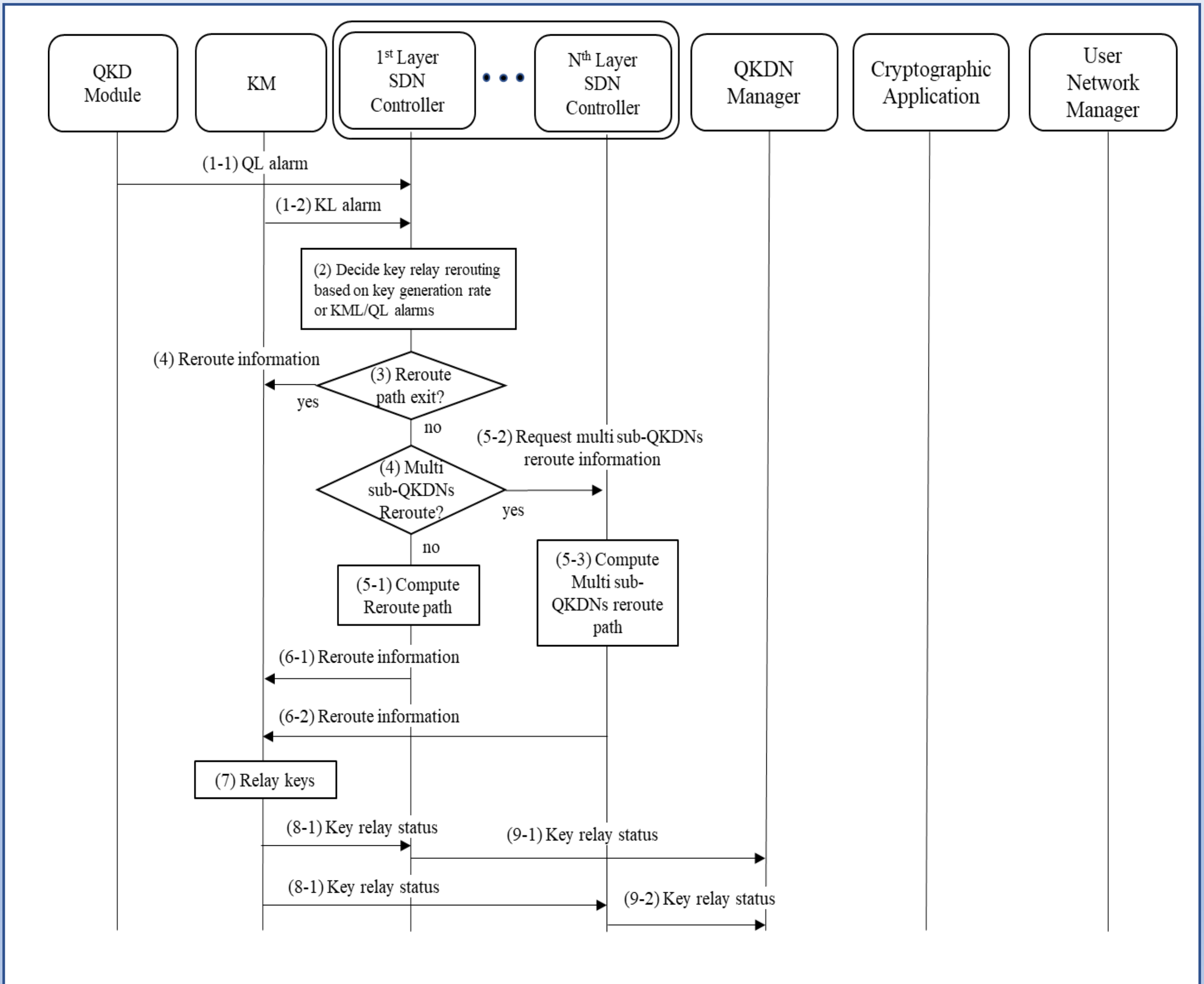
1_{st} Layer SDN Controller

Key Management Layer

Quantum Layer

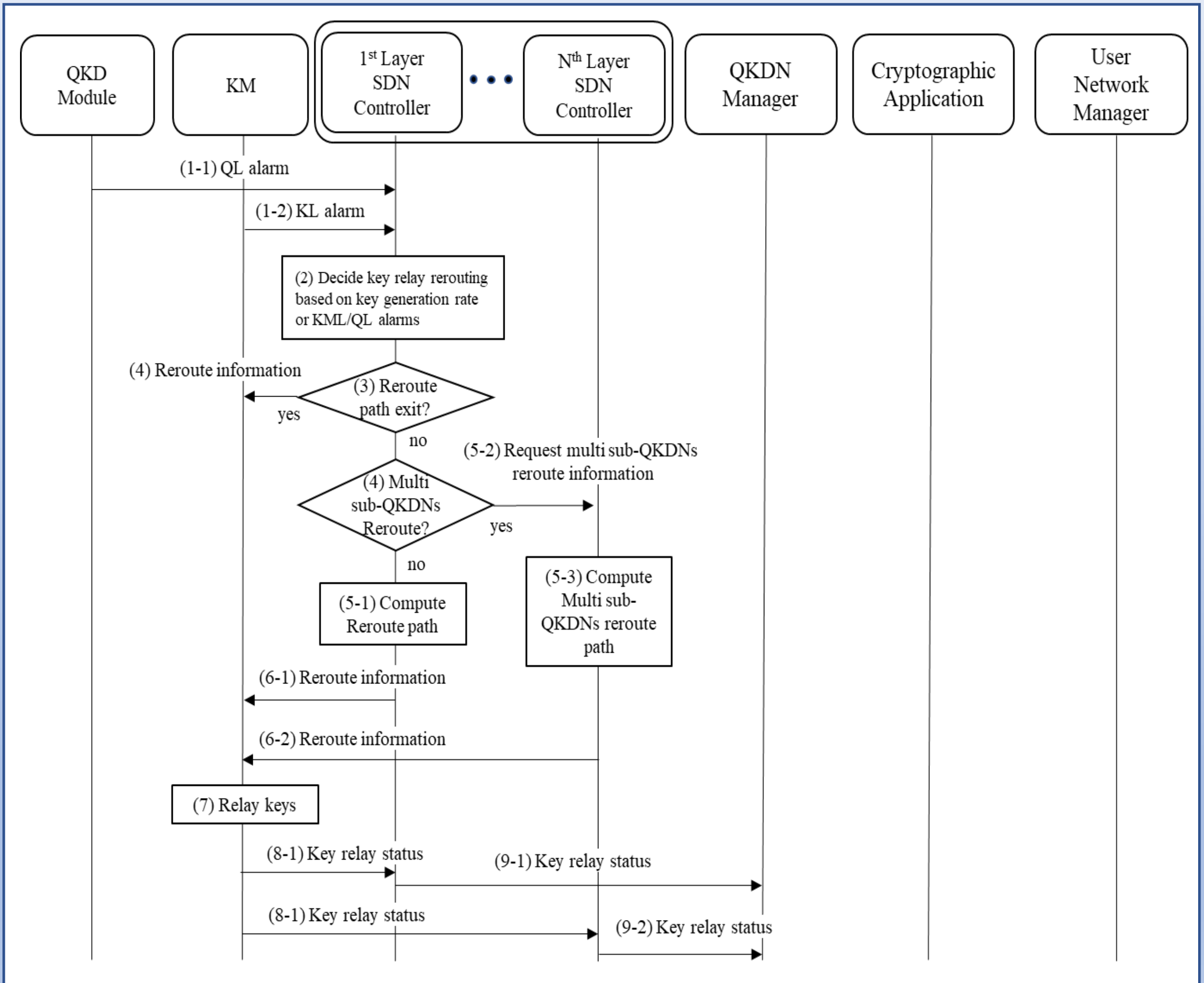
QKDN Management Layer

Example SDN Control Procedures



QKD Module
KM
1st Layer SDN Controller
• • •
Nth Layer SDN Controller
QKDN Manager
Cryptographic Application
User Network Manager
(1-1) QL alarm
(1-2) KL alarm
(2) Decide key relay rerouting based on key generation rate or KML/QL alarms
(4) Reroute information
(3) Reroute path exit?
yes
no
(5-2) Request multi sub-QKDNs reroute information
(4) Multi sub-QKDNs Reroute?
yes
no
(5-1) Compute Reroute path
(5-3) Compute Multi sub-QKDNs reroute path
(6-1) Reroute information
(6-2) Reroute information
(7) Relay keys
(8-1) Key relay status
(9-1) Key relay status
(8-1) Key relay status
(9-2) Key relay status

Hierarchical Key Rerouting Procedure



QKD Module
KM
1st Layer SDN Controller
• • •
Nth Layer SDN Controller
QKDN Manager
Cryptographic Application
User Network Manager
(1-1) QL alarm
(1-2) KL alarm
(2) Decide key relay rerouting based on key generation rate or KML/QL alarms
(4) Reroute information
(3) Reroute path exit?
yes
no
(5-2) Request multi sub-QKDNs reroute information
(4) Multi sub-QKDNs Reroute?
yes
no
(5-1) Compute Reroute path
(5-3) Compute Multi sub-QKDNs reroute path
(6-1) Reroute information
(6-2) Reroute information
(7) Relay keys
(8-1) Key relay status
(9-1) Key relay status
(8-1) Key relay status
(9-2) Key relay status

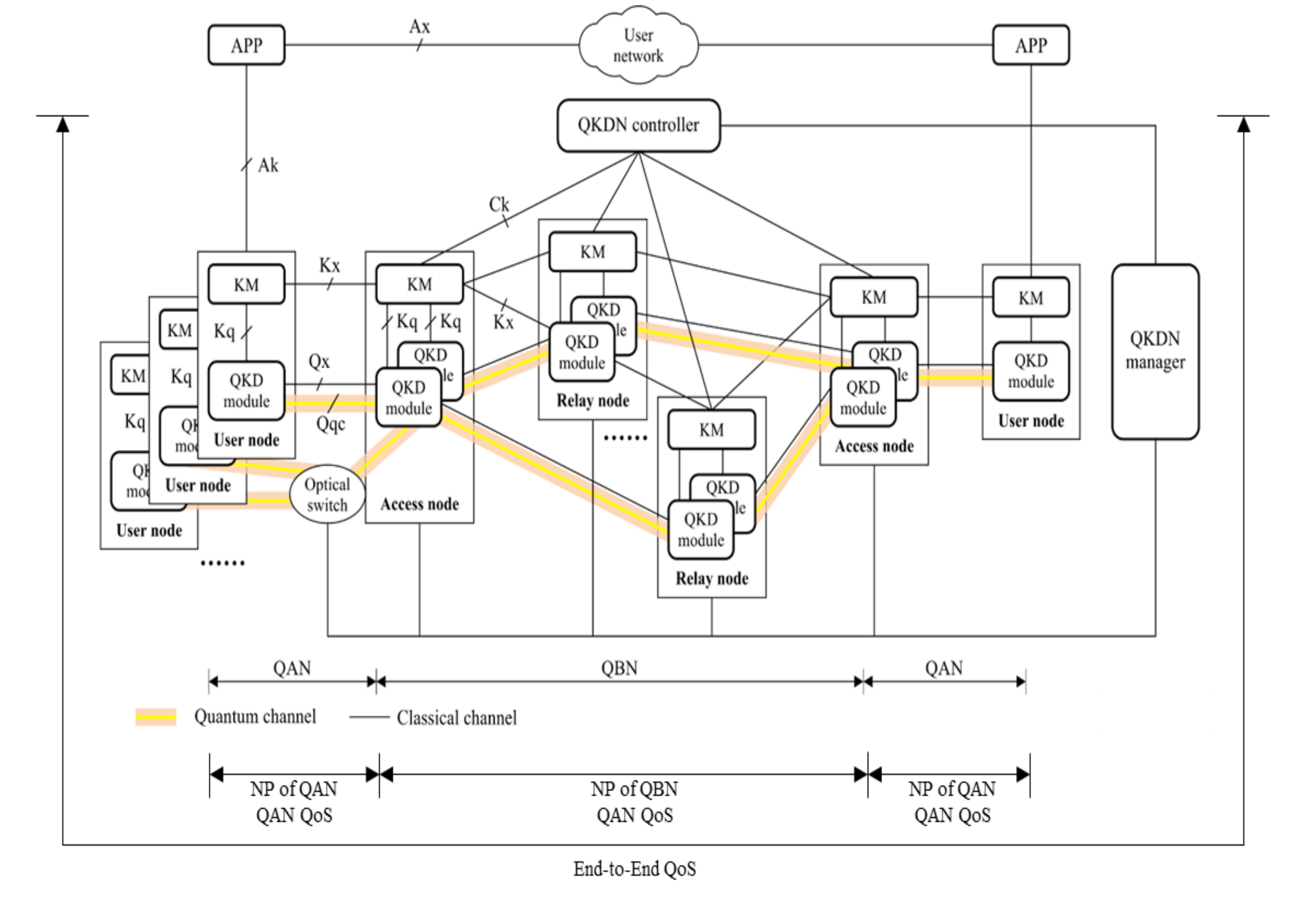
Hierarchical Key Rerouting Procedure

Requirements for QKDN QoS assurance

Functional requirements of

- QoS planning,
- QoS monitoring,
- QoS optimization,
- QoS provisioning, and
- QoS protection and recovery.

Requirements in this Recommendation is limited to a single QKDN



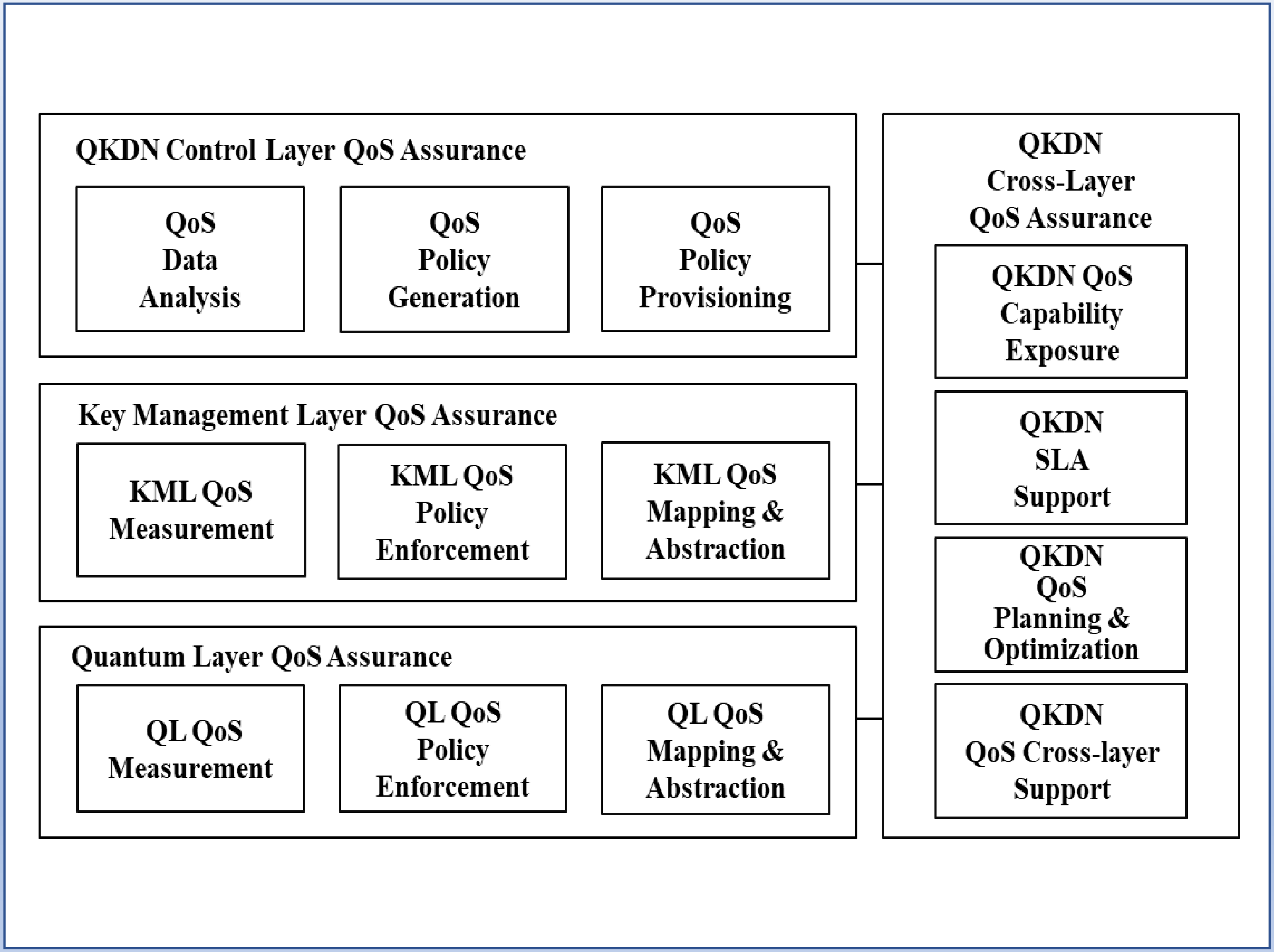
Scope of the QKDN QoS and relationship with Network Performance

On-going Work Items of QKDN in SG13

SG/Q	Work item
Q16/13	**Y.QKDN_BM: Quantum key distribution networks - Business role-based models (12/21 Consent Planned)**
	Y.QKDN_frint: Framework for integration of QKDN and secure storage network
	Y.QKDN-iwfr: Quantum key distribution networks - interworking framework
	Y.QKDN-ml-fra: Quantum key distribution networks - Functional requirements and architecture to enable machine learning
	Y.QKDN-rsfr: Quantum key distribution networks - resilience framework
	Y.supp.QKDN-roadmap: Standardization roadmap on Quantum Key Distribution Networks
Q6/13	**Y.QKDN-QoS-pa: Quantum key distribution networks – QoS parameters (12/21 Consent Planned)**
	Y.QKDN-QoS-fa: Functional architecture of QoS assurance for quantum key distribution networks
	Y.QKDN-QoS-ml-req: Requirements of machine learning based QoS assurance for quantum key distribution networks

Functional Architecture for QKDN QoS Assurance

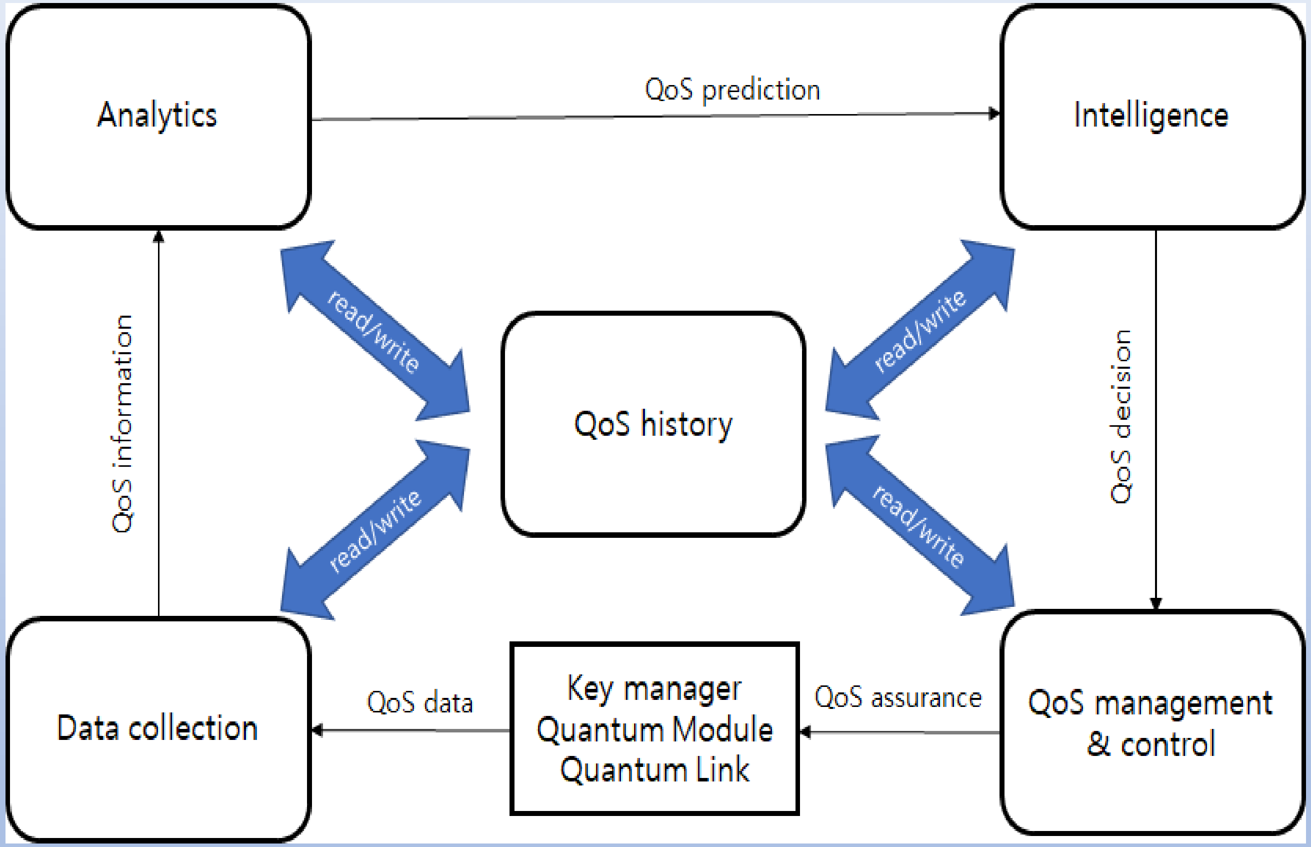
- Functional entities for QKDN QoS assurance
  - ✓ Functional entities & reference point specification is almost complete
  - ✓ Procedures are to be defined
  - ✓ Target to consent in 1st half of 2022


QKDN Control Layer QoS Assurance
QoS Data Analysis
QoS Policy Generation
QoS Policy Provisioning
Key Management Layer QoS Assurance
KML QoS Measurement
KML QoS Policy Enforcement
KML QoS Mapping & Abstraction
Quantum Layer QoS Assurance
QL QoS Measurement
QL QoS Policy Enforcement
QL QoS Mapping & Abstraction
QKDN Cross-Layer QoS Assurance
QKDN QoS Capability Exposure
QKDN SLA Support
QKDN QoS Planning & Optimization
QKDN QoS Cross-layer Support

Requirements for ML-based QKDN QoS Assurance

- First QKDN ML draft Recommendation
  - ✓ Specify functional model for QKDN QoS assurance based on ML
  - ✓ Specify high-level & functional requirements for QKDN QoS assurance based on ML
  - ✓ Use cases of ML-based QKDN QoS assurance defined in Appendix
  - ✓ Target to consent in 1st half of 2022

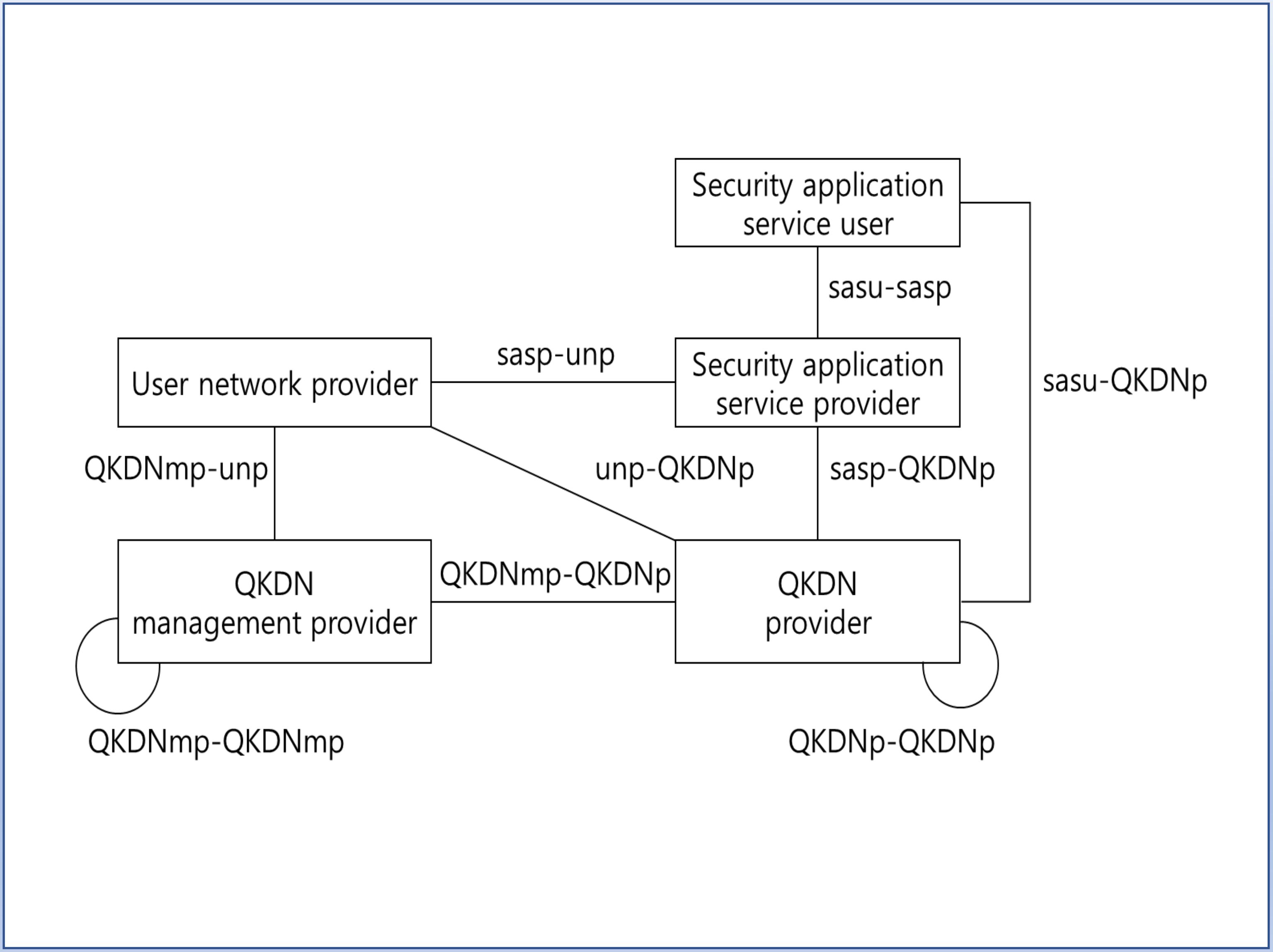
- Defined Use Cases:
  - ✓ Quantum channel performance
  - ✓ QoS Fault diagnosis and prediction
  - ✓ Optimized key resource utilization relate d service provisioning for QKDN



Business Models for QKDN

Y.QKDN_BM defines,

- Business roles
- Business role-based models
- Service scenarios in QKDN from different deployment and operation perspectives
- Identifies various business models that require security application services with QKDN and exiting user networks.



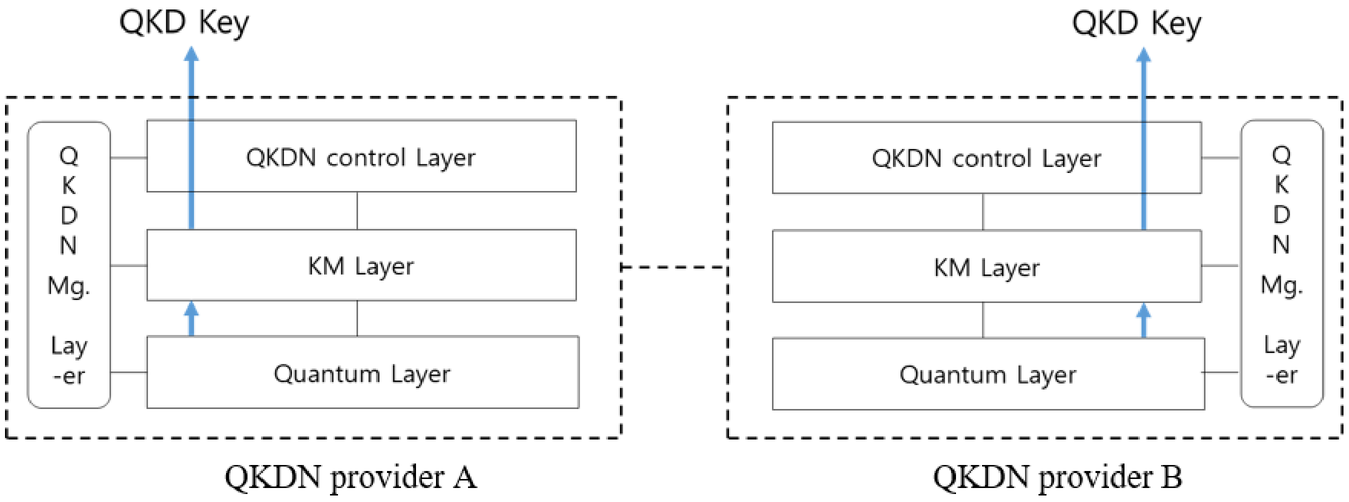
Interworking Framework for QKDN

Constructing a large scale QKDN which covers wide area, it may consist of multiple QKDNs and they are interworking each other

Y.QKDN-iwfr mainly focuses on the interworking between QKDNs supported by multiple QKDN providers.

There are several issues to be standardized for interworking between QKDNs with different technologies.

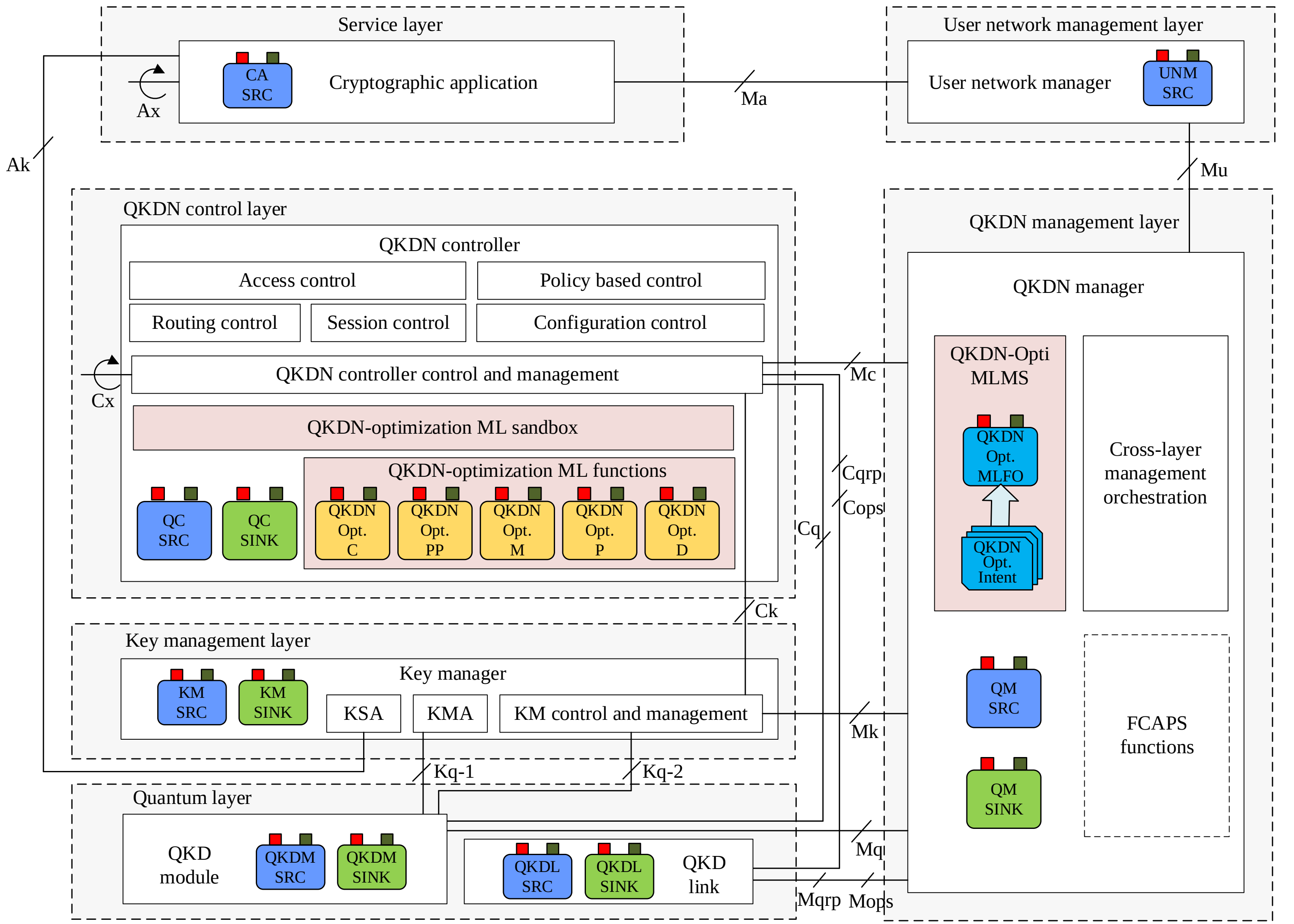
Different technologies can be used in QKDNs: key relay encryption methods, key relay schemes, key relay alternatives, configurations of QKDN controller, and protocols in the key management layer, the QKDN control layer and the QKDN management layer.



Functional Architecture for ML-enabled QKDN

Specifies

- Role of ML in QKDN
- Functional requirements and architecture for ML-enabled QKDN
- Roles and functional requirements and
- Functional architecture model of ML-enabled QKDN



🟥 Service for egress (producer)
🟩 Service for ingress (consumer)

C: collector; PP: preprocessor; M: model; P: policy; D: Distributor; SRC: source of data; SINK: target of ML output; MLFO: ML function orchestrator; FCAPS: fault, configuration, accounting, performance and security;

Security Requirements for QKDN CM

- Security requirements for quantum key distribution networks – control and management
  - Initiated at April 2021 SG17 & first contribution in August 2021
  - Target to consent in 2nd half of 2022

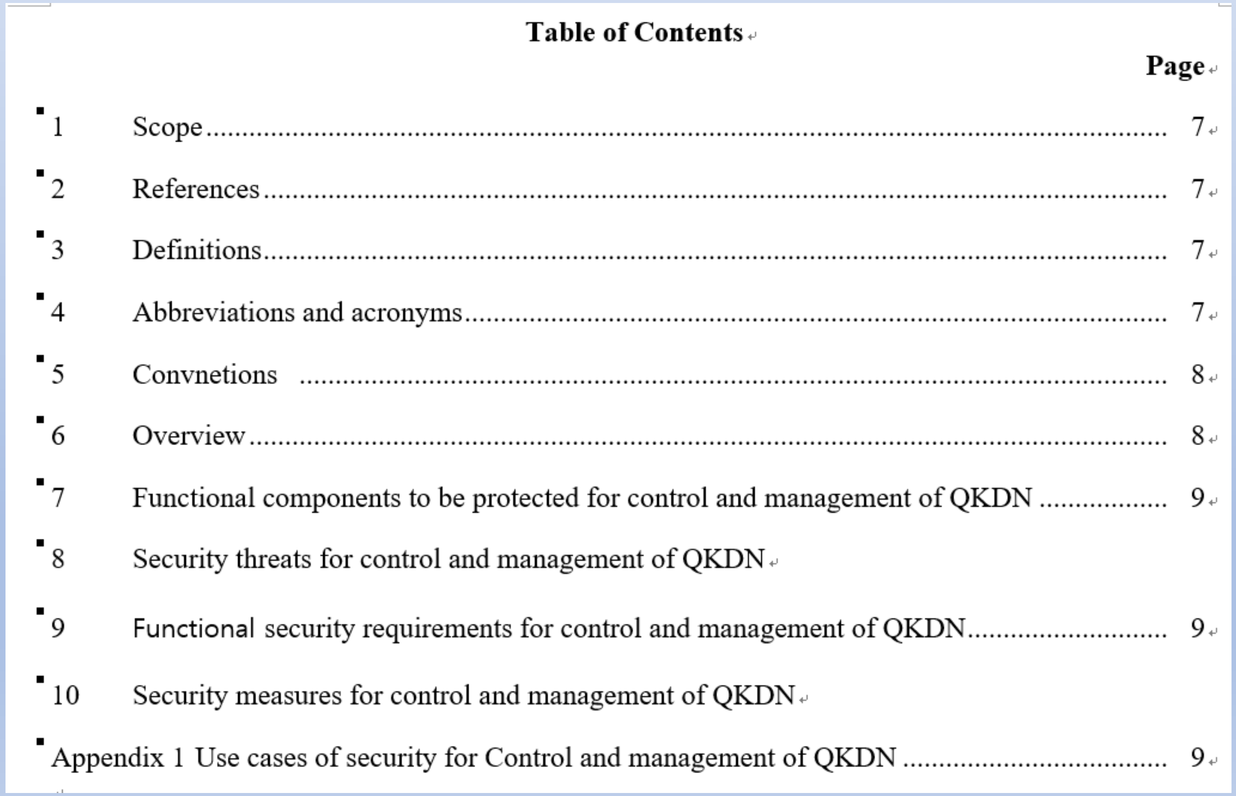
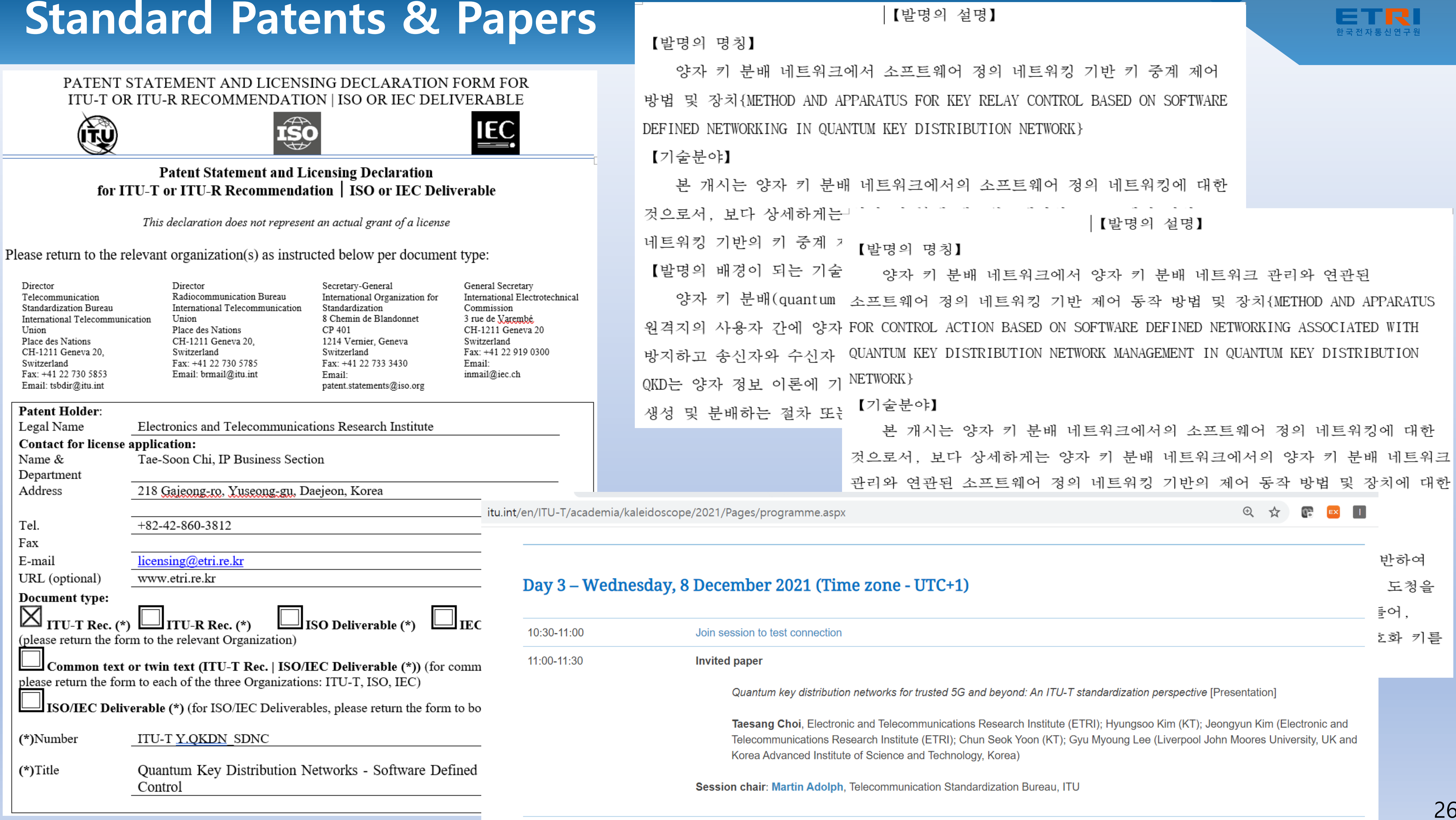


Table of Contents

Page

Standard Patents & Papers



PATENT STATEMENT AND LICENSING DECLARATION FORM FOR
ITU-T OR ITU-R RECOMMENDATION | ISO OR IEC DELIVERABLE

Patent Statement and Licensing Declaration
for ITU-T or ITU-R Recommendation | ISO or IEC Deliverable

This declaration does not represent an actual grant of a license

Please return to the relevant organization(s) as instructed below per document type:

Director
Telecommunication
Standardization Bureau
International Telecommunication
Union
Place des Nations
CH-1211 Geneva 20,
Switzerland
Fax: +41 22 730 5853
Email: tsbdir@itu.int

Director
Radiocommunication Bureau
International Telecommunication
Union
Place des Nations
CH-1211 Geneva 20,
Switzerland
Fax: +41 22 730 5785
Email: brmail@itu.int

Secretary-General
International Organization for
Standardization
8 Chemin de Blandonnet
CP 401
1214 Vernier, Geneva
Switzerland
Fax: +41 22 733 3430
Email:
patent.statements@iso.org

General Secretary
International Electrotechnical
Commission
3 rue de Varembé
CH-1211 Geneva 20
Switzerland
Fax: +41 22 919 0300
Email:
inmail@iec.ch

Patent Holder:
Legal Name Electronics and Telecommunications Research Institute

Contact for license application:
Name & Department Tae-Soon Chi, IP Business Section
Address 218 Gajeong-ro, Yuseong-gu, Daejeon, Korea
Tel. +82-42-860-3812
Fax
E-mail licensing@etri.re.kr
URL (optional) www.etri.re.kr

Document type:
☒ **ITU-T Rec. (*)** ☐ **ITU-R Rec. (*)** ☐ **ISO Deliverable (*)** ☐ **IEC**
(please return the form to the relevant Organization)
☐ **Common text or twin text (ITU-T Rec. | ISO/IEC Deliverable (*))** (for comm
please return the form to each of the three Organizations: ITU-T, ISO, IEC)
☐ **ISO/IEC Deliverable (*)** (for ISO/IEC Deliverables, please return the form to bo

(*)Number ITU-T Y.QKDN_SDNC
(*)Title Quantum Key Distribution Networks - Software Defined Control

【발명의 설명】

【발명의 명칭】

양자 키 분배 네트워크에서 소프트웨어 정의 네트워킹 기반 키 중계 제어 방법 및 장치{METHOD AND APPARATUS FOR KEY RELAY CONTROL BASED ON SOFTWARE DEFINED NETWORKING IN QUANTUM KEY DISTRIBUTION NETWORK}

【기술분야】

본 개시는 양자 키 분배 네트워크에서의 소프트웨어 정의 네트워킹에 대한 것으로서, 보다 상세하게는
네트워킹 기반의 키 중계
【발명의 배경이 되는 기술
양자 키 분배(quantum
원격지의 사용자 간에 양자
방지하고 송신자와 수신자
QKD는 양자 정보 이론에 기
생성 및 분배하는 절차 또는

【발명의 설명】

【발명의 명칭】

양자 키 분배 네트워크에서 양자 키 분배 네트워크 관리와 연관된 소프트웨어 정의 네트워킹 기반 제어 동작 방법 및 장치{METHOD AND APPARATUS FOR CONTROL ACTION BASED ON SOFTWARE DEFINED NETWORKING ASSOCIATED WITH QUANTUM KEY DISTRIBUTION NETWORK MANAGEMENT IN QUANTUM KEY DISTRIBUTION NETWORK}

【기술분야】

본 개시는 양자 키 분배 네트워크에서의 소프트웨어 정의 네트워킹에 대한 것으로서, 보다 상세하게는 양자 키 분배 네트워크에서의 양자 키 분배 네트워크 관리와 연관된 소프트웨어 정의 네트워킹 기반의 제어 동작 방법 및 장치에 대한
반하여
도청을
들어,
도화 키를

itu.int/en/ITU-T/academia/kaleidoscope/2021/Pages/programme.aspx

Day 3 – Wednesday, 8 December 2021 (Time zone - UTC+1)

10:30-11:00	Join session to test connection
11:00-11:30	**Invited paper**

Quantum key distribution networks for trusted 5G and beyond: An ITU-T standardization perspective [Presentation]

Taesang Choi, Electronic and Telecommunications Research Institute (ETRI); Hyungsoo Kim (KT); Jeongyun Kim (Electronic and Telecommunications Research Institute (ETRI); Chun Seok Yoon (KT); Gyu Myoung Lee (Liverpool John Moores University, UK and Korea Advanced Institute of Science and Technology, Korea)

Session chair: Martin Adolph, Telecommunication Standardization Bureau, ITU

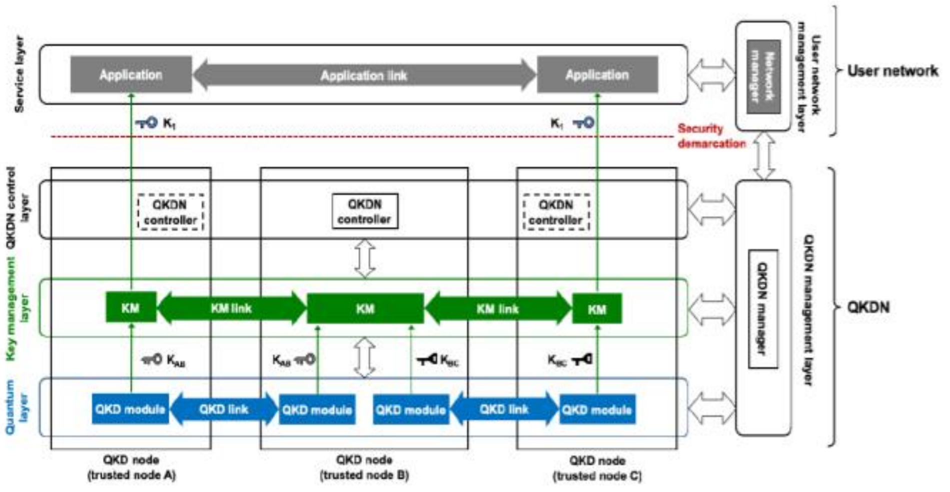
Topics

- Project Overview
- QKDN Standardization Status
- Main Contribution: Standards
- Main Contribution: Standard Patents
- **Main Contribution: Market Deployment**
- Future Challenges

Deployment of QKDN: Field Trial for Government Sector

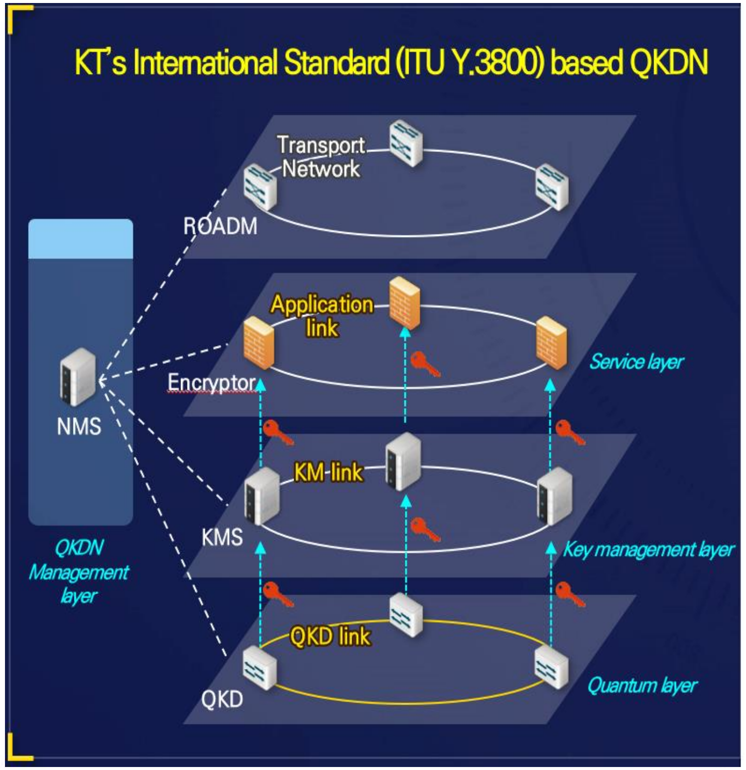
KT developed and deployed World-first QKDN system based on Y.3800

Based on ITU-T Recommendation Y.3800; layered model - Quantum, KM, Service and Network Management layers



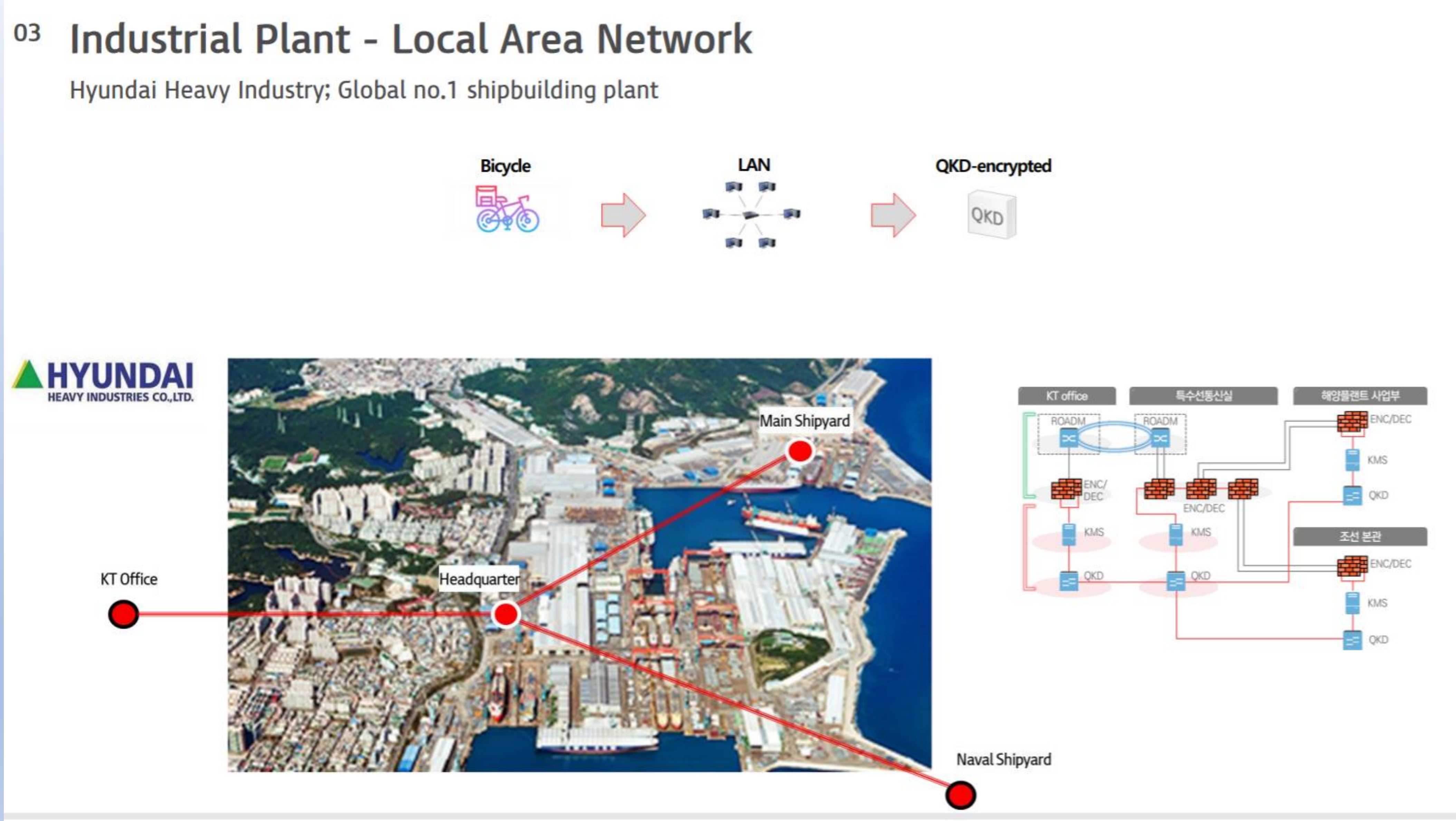
<Conceptual structure of QKDN in Rec. Y.3800>

Realization



<Conceptual structure of KT QKDN>

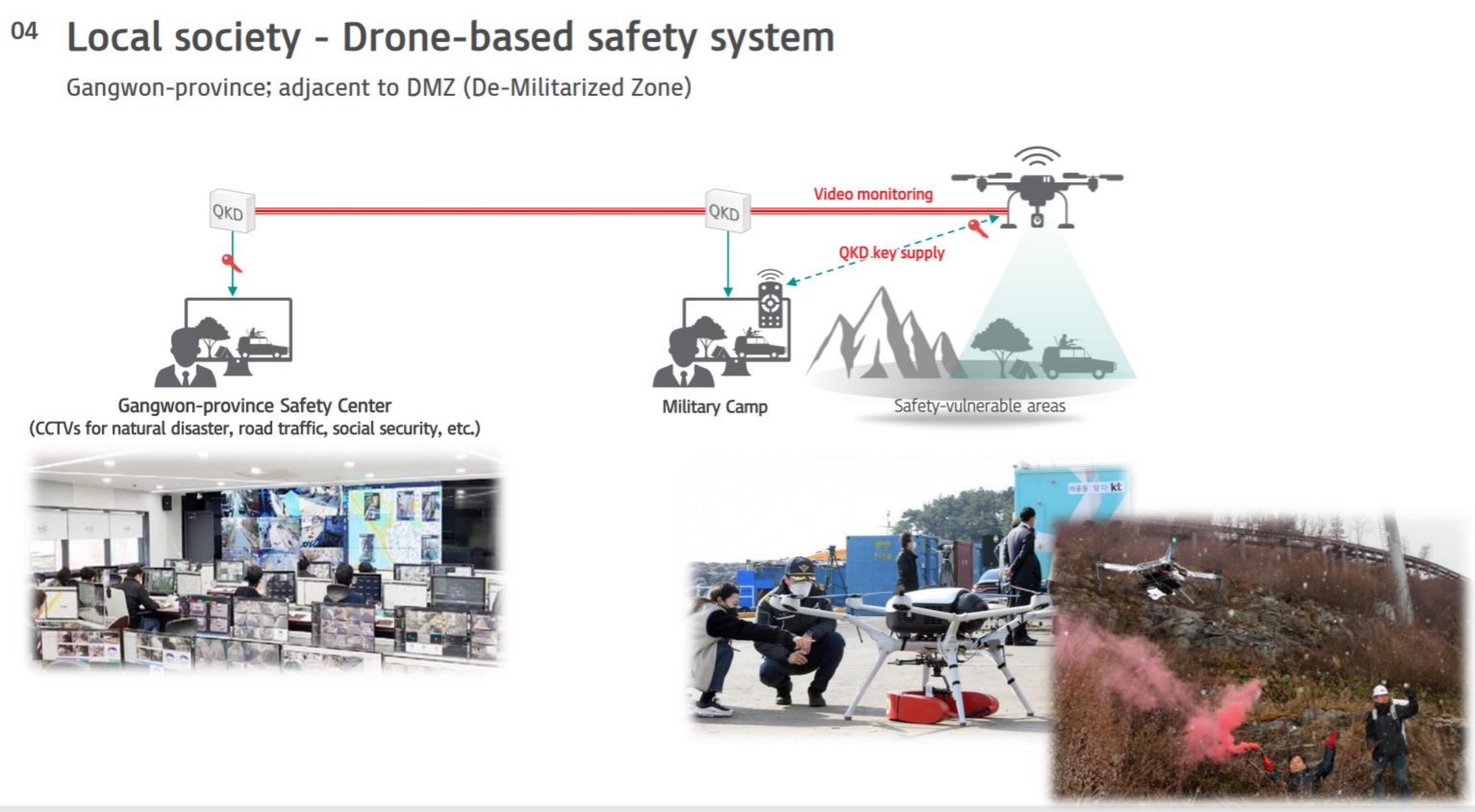
Deployment of QKDN: Field Trial for Industry Sector



03 Industrial Plant - Local Area Network

Hyundai Heavy Industry; Global no.1 shipbuilding plant

Deployment of QKDN: Field Trial for Military Sector

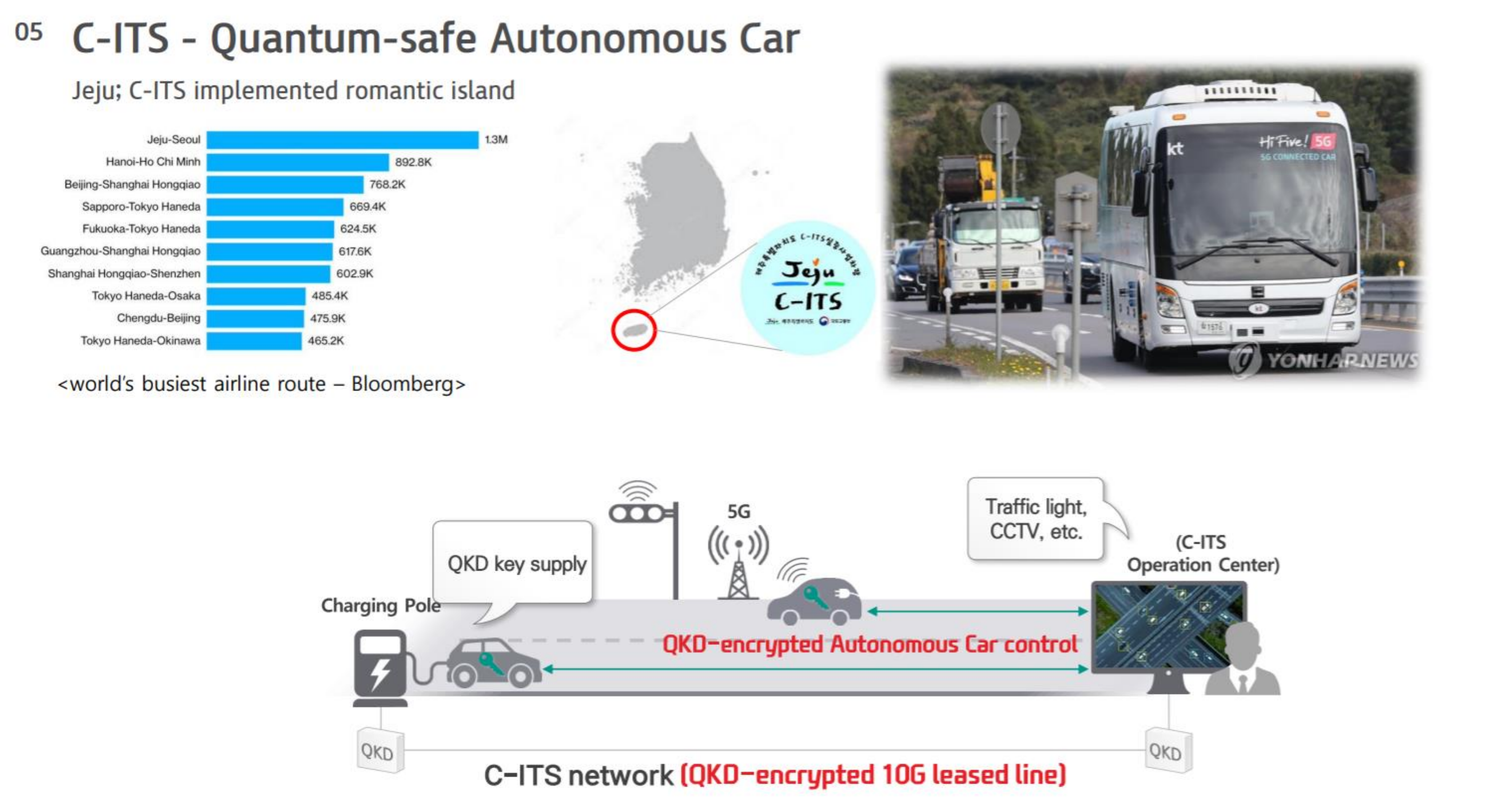


04 Local society - Drone-based safety system

Gangwon-province; adjacent to DMZ (De-Militarized Zone)

QKD
QKD
Video monitoring
QKD key supply
Gangwon-province Safety Center
(CCTVs for natural disaster, road traffic, social security, etc.)
Military Camp
Safety-vulnerable areas

QKDN Service Use Cases: Quantum Safe Autonomous Car



05 C-ITS - Quantum-safe Autonomous Car

Jeju; C-ITS implemented romantic island

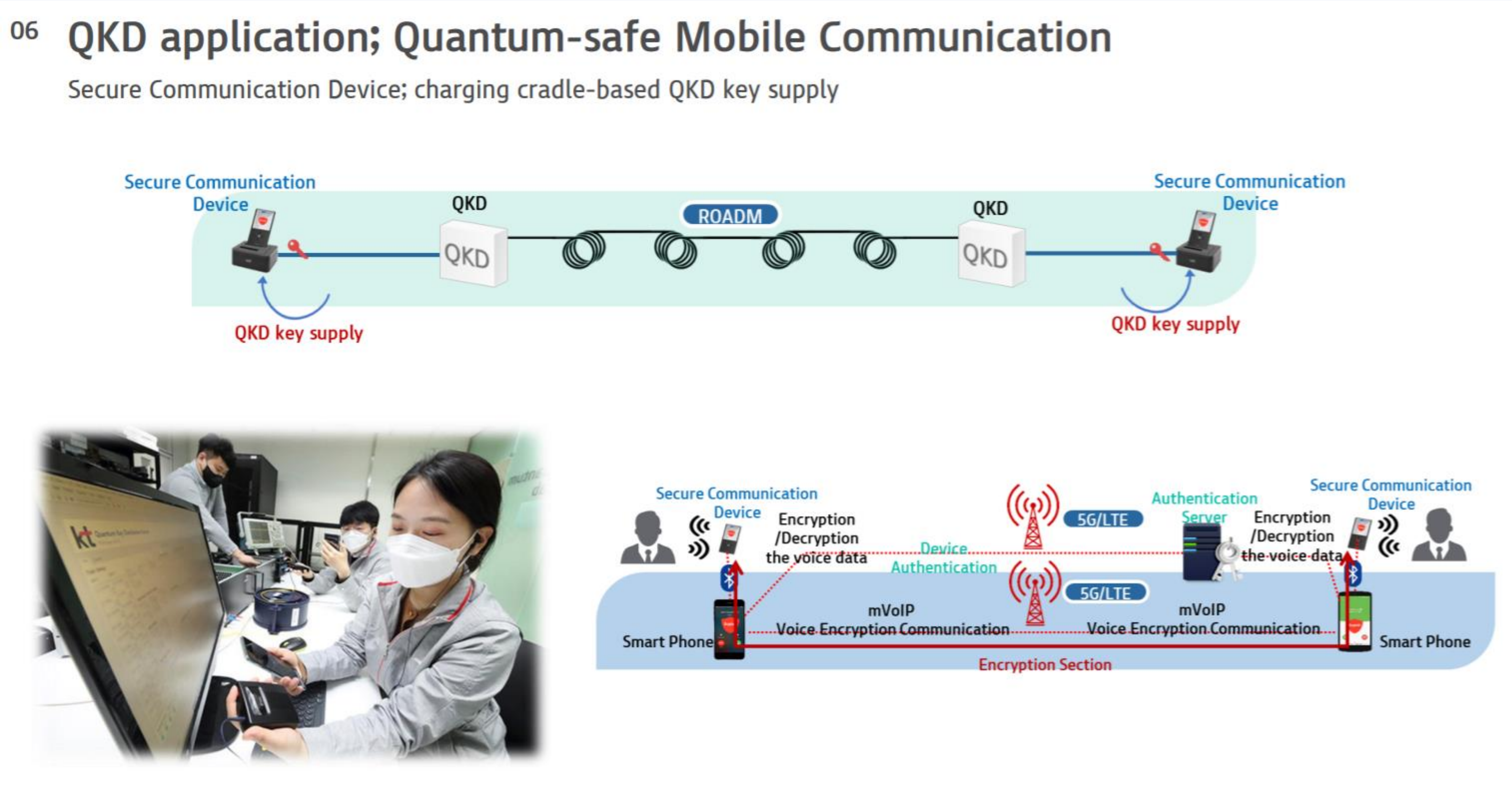
Jeju-Seoul 1.3M
Hanoi-Ho Chi Minh 892.8K
Beijing-Shanghai Hongqiao 768.2K
Sapporo-Tokyo Haneda 669.4K
Fukuoka-Tokyo Haneda 624.5K
Guangzhou-Shanghai Hongqiao 617.6K
Shanghai Hongqiao-Shenzhen 602.9K
Tokyo Haneda-Osaka 485.4K
Chengdu-Beijing 475.9K
Tokyo Haneda-Okinawa 465.2K

<world's busiest airline route – Bloomberg>

Jeju C-ITS
kt
Hi Five! 5G
5G CONNECTED CAR
YONHAPNEWS
QKD key supply
Charging Pole
5G
Traffic light, CCTV, etc.
(C-ITS Operation Center)
QKD-encrypted Autonomous Car control
QKD
QKD

C-ITS network (QKD-encrypted 10G leased line)

QKDN Service Use Cases: Quantum Video Conferencing



06 QKD application; Quantum-safe Mobile Communication

Secure Communication Device; charging cradle-based QKD key supply

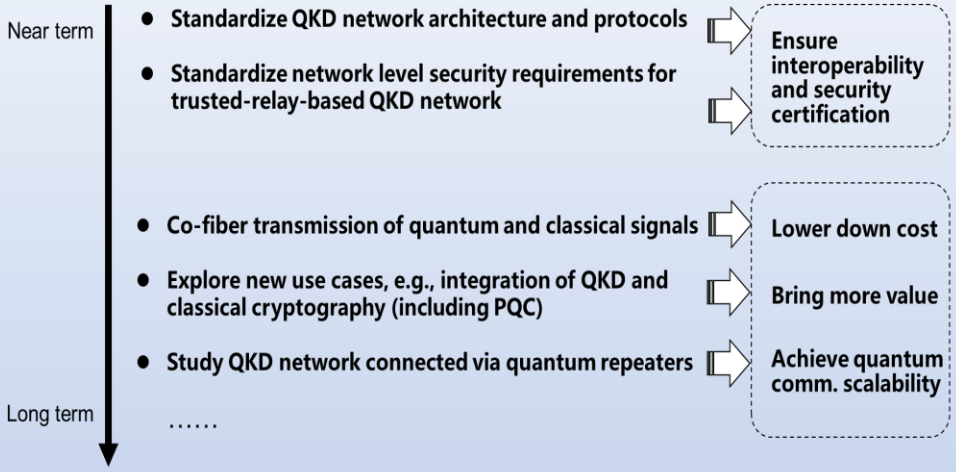
Secure Communication Device
QKD
ROADM
QKD
Secure Communication Device
QKD
QKD
QKD key supply
QKD key supply
Secure Communication Device
Encryption /Decryption the voice data
Device Authentication
5G/LTE
Authentication Server
Encryption /Decryption the voice data
Secure Communication Device
5G/LTE
mVoIP Voice Encryption Communication
mVoIP Voice Encryption Communication
Smart Phone
Smart Phone
Encryption Section

Topics

- Project Overview
- QKDN Standardization Status
- Main Contribution: Standards
- Main Contribution: Standard Patents
- Main Contribution: Market Deployment
- Future Challenges

Challenges and Future Plan

- **Support of QKDN interoperability**: it's necessary to develop interoperable solutions among multiple providers and different technologies.
- **Specifications of QKDN protocols**: From a QKD system perspective, most of protocols have been developed. For a QKDN perspective, these protocols should be extended to support a network with many nodes and new protocols.
- **Synchronization**: Frequency and time synchronization plays a fundamental supporting role in networks. Therefore, specific requirements and related protocols for synchronization should be standardized.
- **Multi-protocol connectivity**: There is a lack of detailed schemes to effectively coordinate different QKD devices of manufacturers and regions under multi-protocol.
- **The adoption of AI/ML to QKDN**: It is very important to use AI/ML for improving network performance while supporting QoS.
- **Integration of user networks** (e.g., 5G and beyond) with QKDN
- **Trusted-relay-based QKDN**: Trustworthy networking is fundamentally important to ensure security and privacy with legal compliance. The efforts for related security solutions on QKDN should be continued in align with architectural frameworks to be developed.
- **Scale up QKDN**: Feasible approaches for building up a large-scale QKDN and its cost-effective deployment for user networks should be investigated with candidate technical solutions (e.g., with quantum relay).
- **Towards QENS from QKDN**: Technical solutions for QKDN are necessary to be expanded for supporting QENS with QITs. QENS basically needs QIN and its services with advanced features from quantum computing and communication as well as quantum sensing and metrology.



Near term

- Standardize QKD network architecture and protocols
- Standardize network level security requirements for trusted-relay-based QKD network

Ensure interoperability and security certification

- Co-fiber transmission of quantum and classical signals
- Explore new use cases, e.g., integration of QKD and classical cryptography (including PQC)
- Study QKD network connected via quantum repeaters

……

Lower down cost

Bring more value

Achieve quantum comm. scalability

Long term

감사합니다

choits@etri.re.kr