

글로벌 ICT 표준 컨퍼런스 2023

Global ICT Standards Conference 2023

(세션1) 양자기술: 디지털 세상의 새로운 패러다임

표준기반의 양자암호통신 신뢰노드 및 QSDN연동

박상길 책임연구원, 한국전자통신연구원(ETRI)
wideideal@etri.re.kr

주최



과학기술정보통신부
Ministry of Science and ICT



특허청
Korean Intellectual
Property Office

주관



국립전파연구원
National Radio Research Agency



IITP

KEA

kista

ETRI

Index

01 양자암호통신 테스트베드 in KOREN

02 QKDN and Standard

03 QSDN을 이용한 이종솔루션간 양자키 전달

00. 과제 일반사항

QKD 프로토콜간 상호 운용성 확보를 위한



신뢰노드 코어 및 인터페이스 개발

주관연구기관

한국전자통신연구원 양자기술연구본부/네트워크연구본부

수행기간

2020.4.1. ~ 2024.12.31. (57개월)

공동연구기관

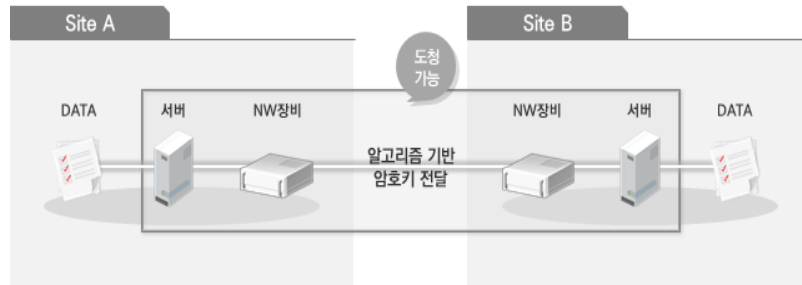
KIST, KT, SKT, NIA, TTA, IDQ (대기업, 외국기업 포함 5개 기관)

위탁 연구기관

KAIST

00. 양자암호통신과 신뢰노드 기술

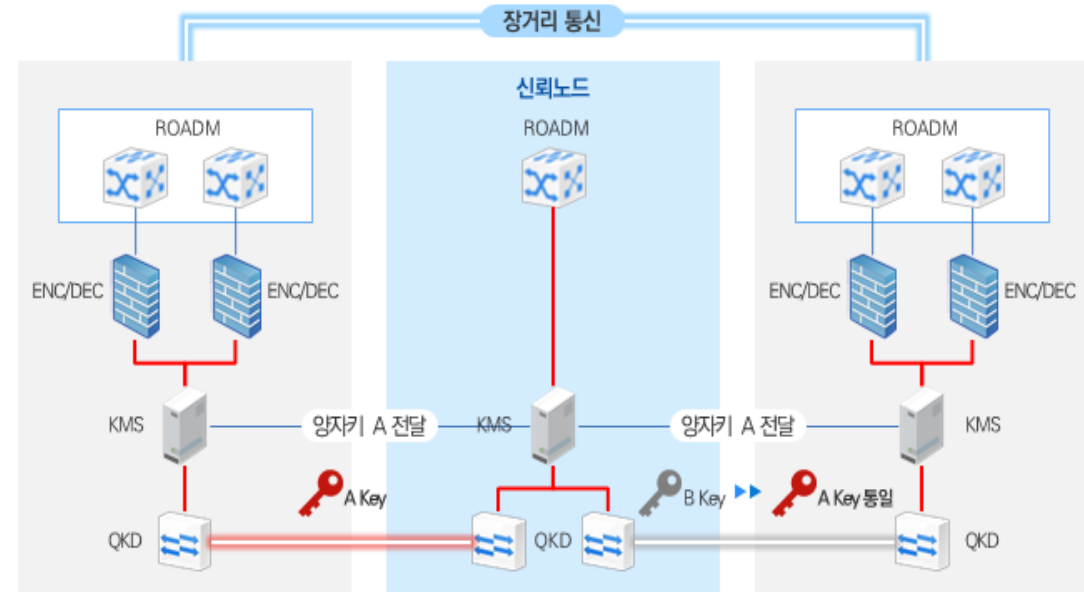
기존 통신(AS-IS)



양자암호통신 구조(TO-BE)



신뢰노드 기술 적용



양자암호통신 테스트베드

- **KT형 양자암호통신 장비 신뢰노드 실증**
- **SK형 양자암호통신 장비 신뢰노드 실증**



IDQ항 장비랙

대전
KOREN
POP

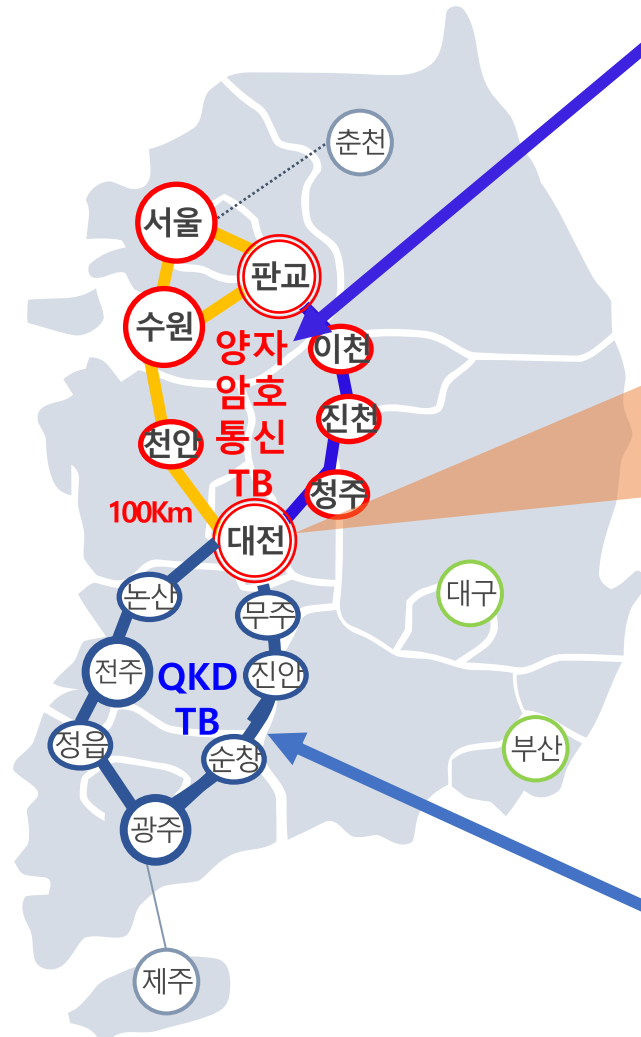
- LEA 암호알고리즘이 적용된 광전송장비 실장
 - 우리넷 OPN3000
 - LEA : Lightweight Encryption Algorithm



QKD/QKMS의 개발단계 검증·실증 환경 제공
- 이미 구축된 광전송장비와 연동을 통한 양자암호통신 실증

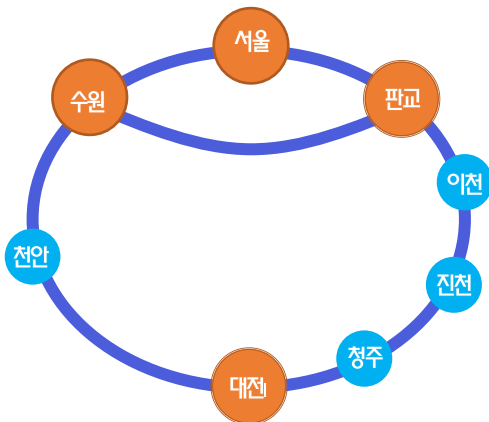
QKD 테스트베드

대전-전주-광주 등 총 445Km 구간의 QDK, 양자통신 관련개발·실증 제공



01. 양자암호통신 테스트베드 in KOREN

양자암호통신 장비구축 현황



- SK형 QKD : Clavis 300(IDQ)
- KT형 QKD : WQN-100(우리넷)
UTRANS-0810(코위버)

양자암호통신 장비별 구성

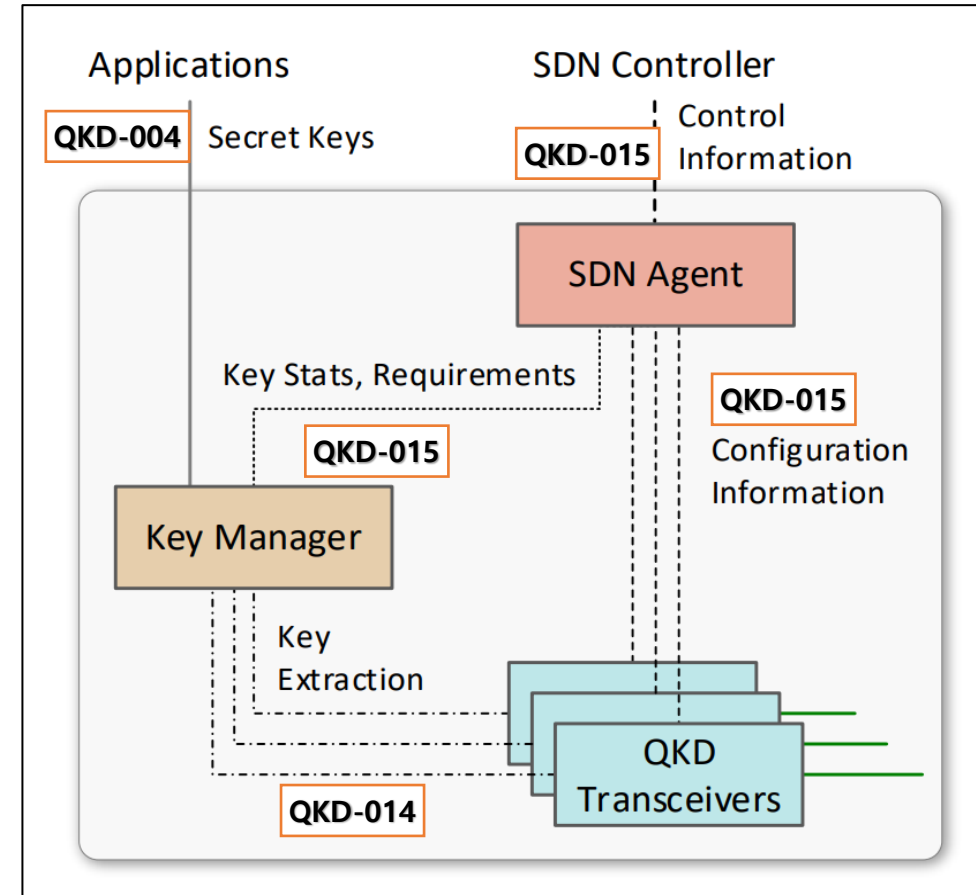
구분	QKD	KMS	ENC	전송장비
A Type	Clavis 300	Clavis 300 QMC	OPN SYSTEM	
B Type	WQN-100	다임즈	UTRANS-6300p	Any OTN
C Type	UTRANS-0810			Any OTN
D Type	QKD+			Any OTN

구분	서울	수원	천안	판교	대전	청주	진천	인천
QKD	Clavis 300	Clavis 300	Clavis 300	Clavis 300	Clavis 300	WQN-100	WQN-100	UTRANS-0810
				QKD+	UTRANS-0810	UTRANS-0810	QKD+	QKD+
KMS	Clavis 300 QMC	Clavis 300 QMC	Clavis 300 QMC	Clavis 300 QMC	Clavis 300 QMC	다임즈	QKD+	QKD+
				다임즈	다임즈			
ENC	O208CLU	O208CLU	O208CLU	O208CLU	O208CLU	UTRANS-6300p	UTRANS-6300p	UTRANS-6300p
				UTRANS-6300p	UTRANS-6300p			
전송장비	OPN-3100	OPN-1000	OPN-3000	OPN-3000	OPN-3000	OPN-3000	OPN-3000	OPN-3000

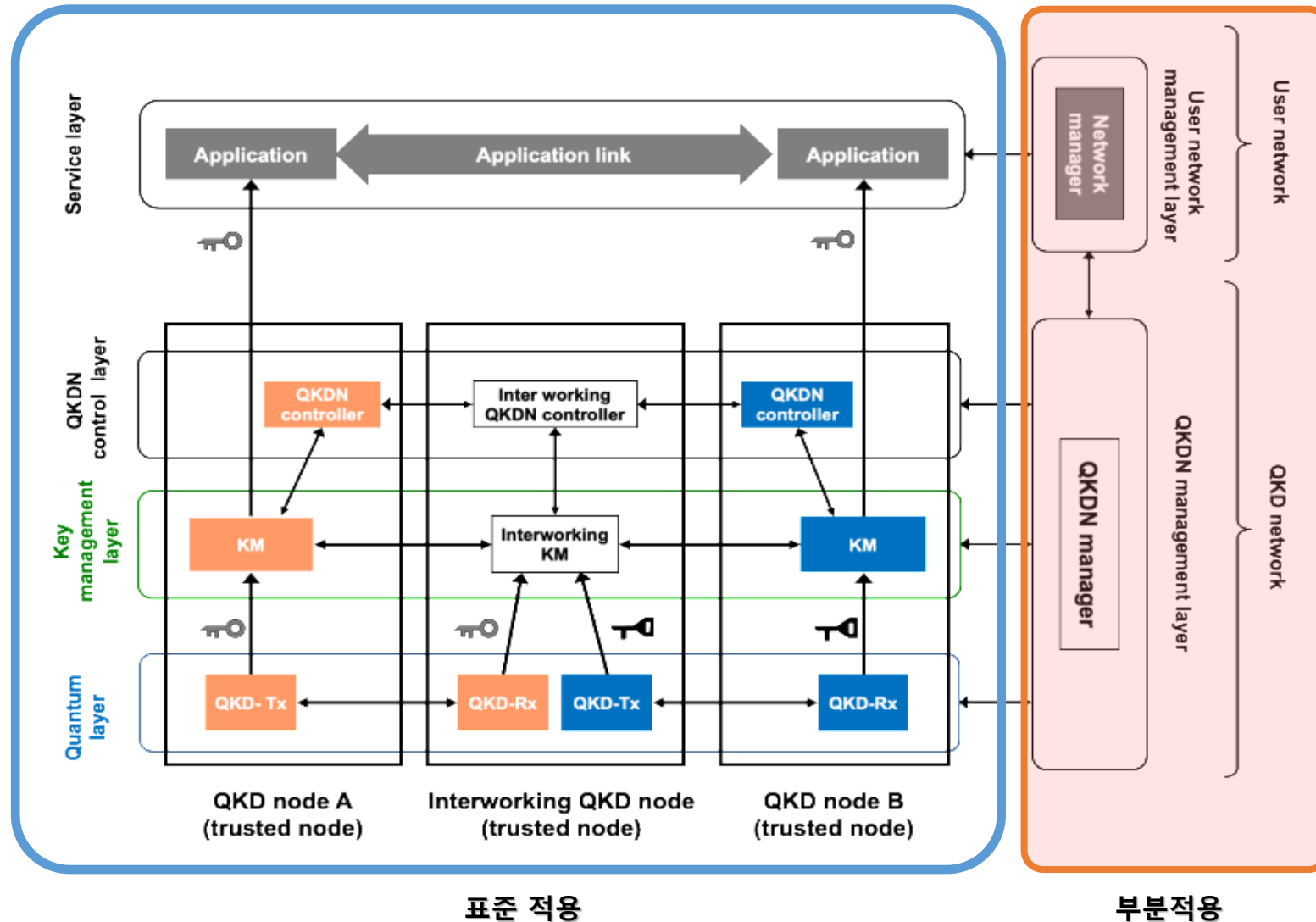
02. QKDN and Standard

<표 1> ETSI 양자암호키 분배 표준문서

표준번호	표준명	내용
ETSI GS QKD 002 V1.1.1 (2010-06)	Use Cases	양자암호키분배의 사용사례
ETSI GR QKD 003 V2.1.1 (2018-03)	Components and Internal Interfaces	양자암호키분배의 구성요소와 내부 인터페이스
ETSI GS QKD 004 V2.1.1 (2020-08)	Application Interface : 1	양자암호키분배 애플리케이션의 인터페이스
ETSI GS QKD 005 V1.1.1 (2010-12)	Security Proofs	양자암호키분배의 보안 증명
ETSI GR QKD 007 V1.1.1 (2018-12)	Vocabulary	양자암호키분배 용어정의
ETSI GS QKD 008 V1.1.1 (2010-12)	QKD Module Security Specification	양자암호키분배 모듈의 보안 규격
ETSI GS QKD 011 V1.1.1 (2016-05)	Component characterization: characterizing optical components for QKD systems	부품 특성: 양자암호키 분배시스템용 광학 부품 특성
ETSI GS QKD 012 V1.1.1 (2019-02)	Device and Communication Channel Parameters for QKD Deployment	양자암호키분배 배포를 위한 장치와 통신채널 파라미터
DGS/QKD-0013 (GS QKD 013)	Transmitter module characterisation	양자암호키분배 전송 모듈의 특성
ETSI GS QKD 014 V1.1.1 (2019-02)	Protocol and data format of REST-based key delivery API : 3	REST 기반 암호 전달 응용프로그램 인터페이스의 프로토콜과 데이터 포맷
ETSI GS QKD 015 V2.1.1 (2022-04)	Control Interface for Software Defined Networks : 2 4 5	소프트웨어 정의 통신망의 제어 인터페이스
DGR/QKD-017 (GR QKD 017)	Network architectures	양자암호키 분배망 구조
ETSI GS QKD 018 V1.1.1 (2022-04)	Orchestration Interface for Software Defined Networks	소프트웨어 정의 통신망의 오케스트레이션 인터페이스
DGR/QKD-019 (GR QKD 019)	Design of QKD interfaces with Authentication	인증을 통한 양자암호키분배 인터페이스의 설계
DGS/QKD-020 (GS QKD 020)	Interoperable KMS API	상호운용이 가능한 암호키관리시스템의 응용프로그램 인터페이스



02. QKDN and Standard

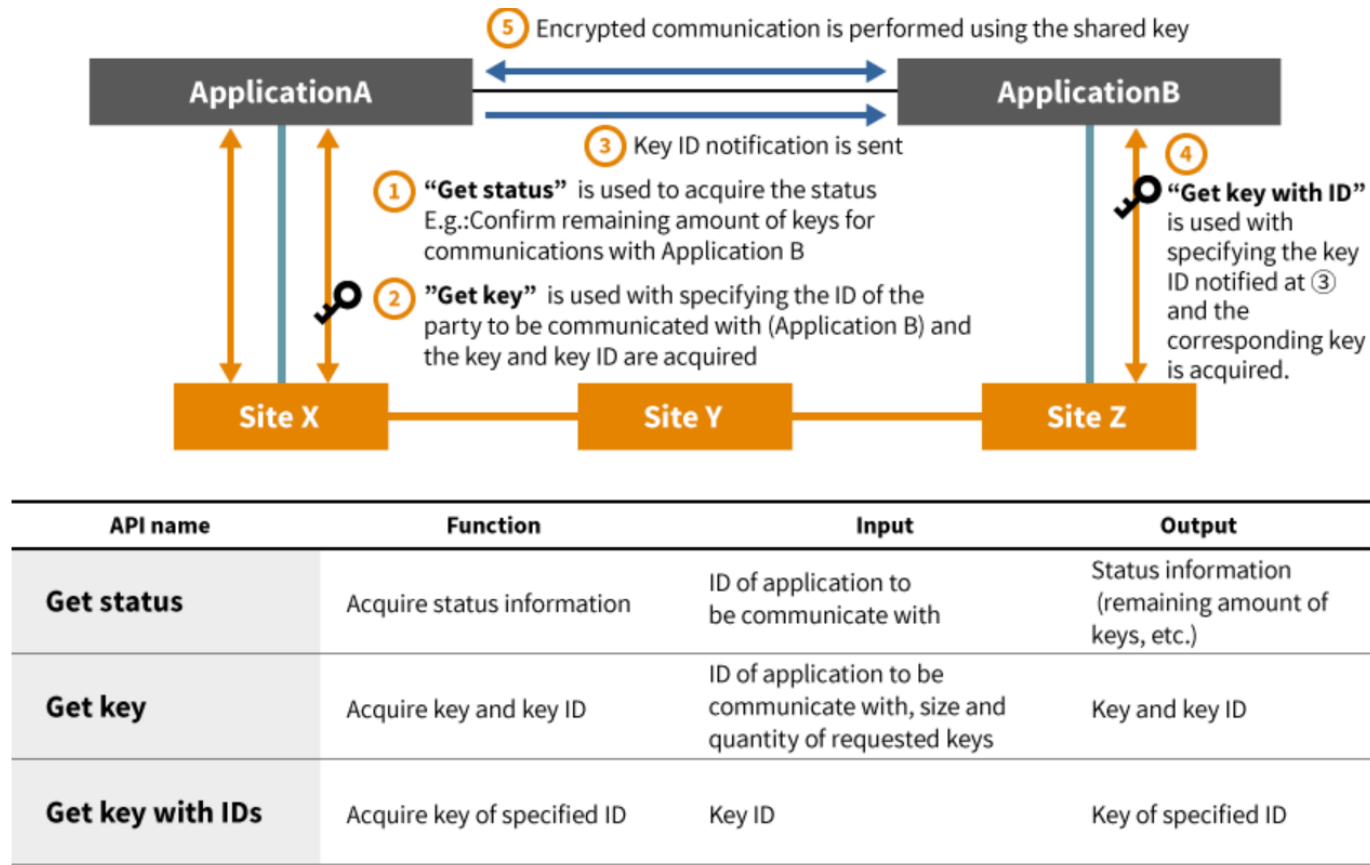


1. Key relay encryption methods
2. Key relay schemes
3. Key relay alternatives(XORs ..)
4. QKDN Controller 구성

QKDN 상호연동 기술의
개념적 모델(ITU-T)

02. QKDN and Standard

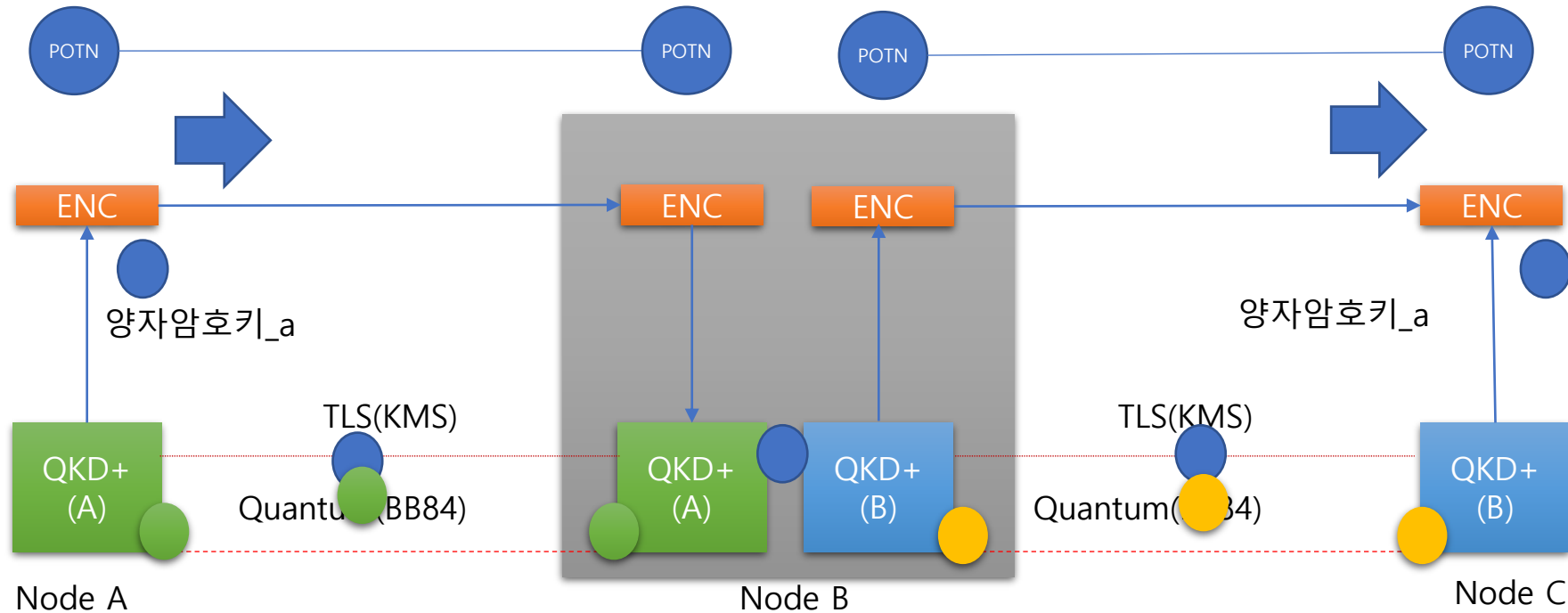
신뢰노드 기반 양자암호키 전달



Procedure using the ETSI GS QKD 014 Key supply interface standard - Toshiba

02. QKDN and Standard

신뢰노드 기반 양자암호키 전달

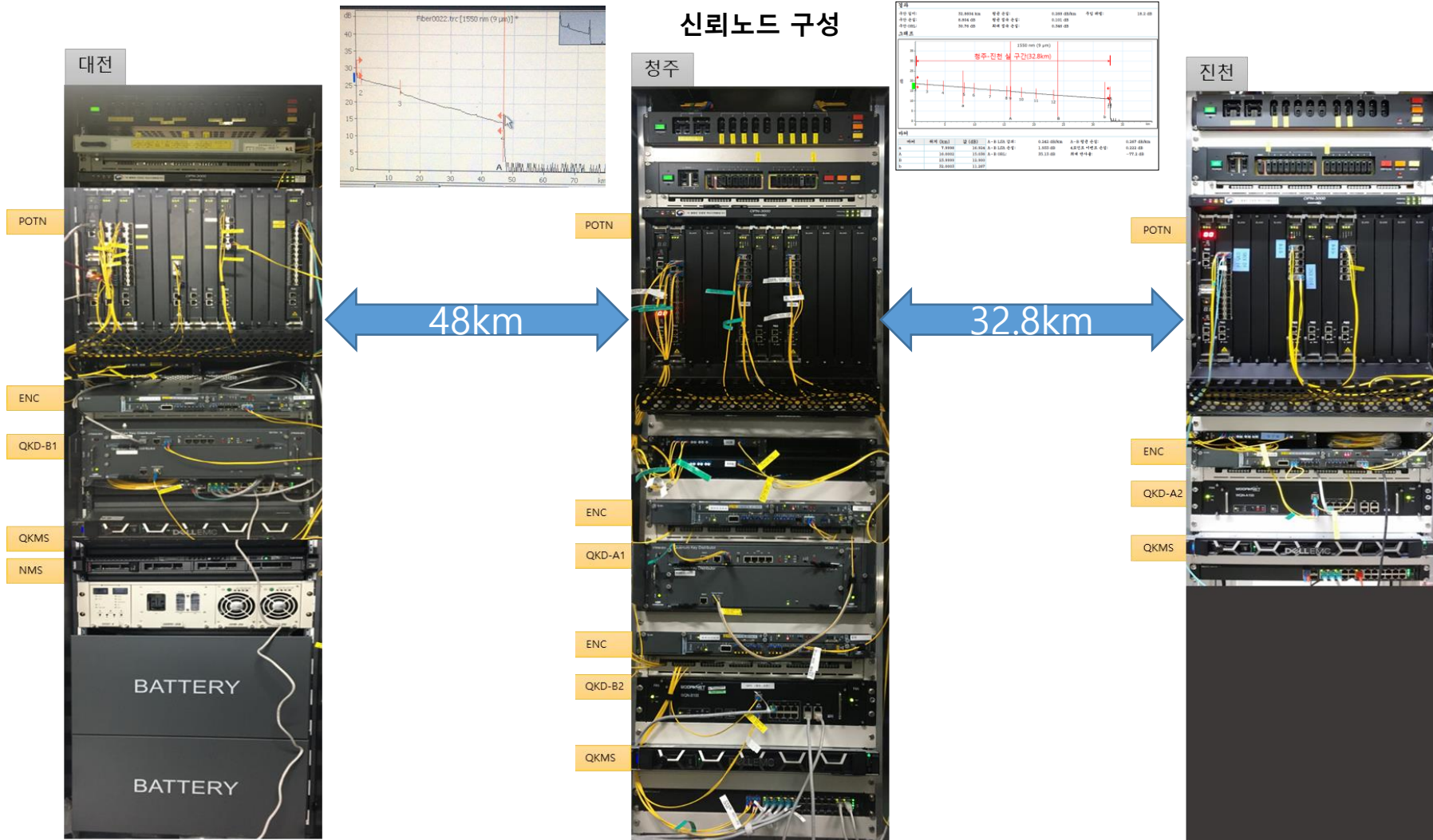
QKD+간
KEY Relay발생

※ 전제조건

- 키 도난을 방지하기 위한 대책을 구현한 신뢰노드는 QKD네트워크에 연결된것을 전제
- 사이트 내에서 수행되는 처리를 위한 적절한 암호화기술의 사용
- QKD 자체 및 QKMS와 연결된 배선 및 회선의 물리적 보호가 포함
- 장비가 위치한 건물, 랙등의 물리적 보안

02. QKDN and Standard

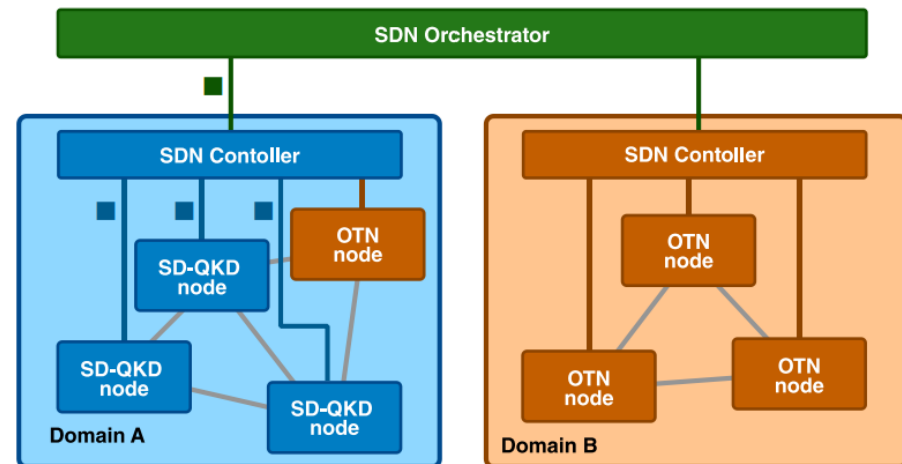
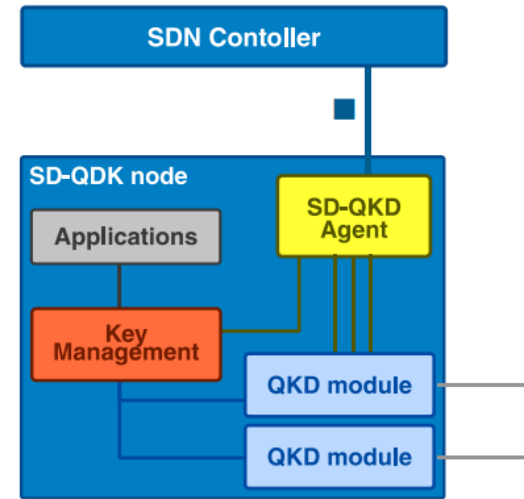
KOREN 기반 양자암호통신 솔루션 시험검증



03. QSDN을 이용한 이중솔루션간 양자키 전달

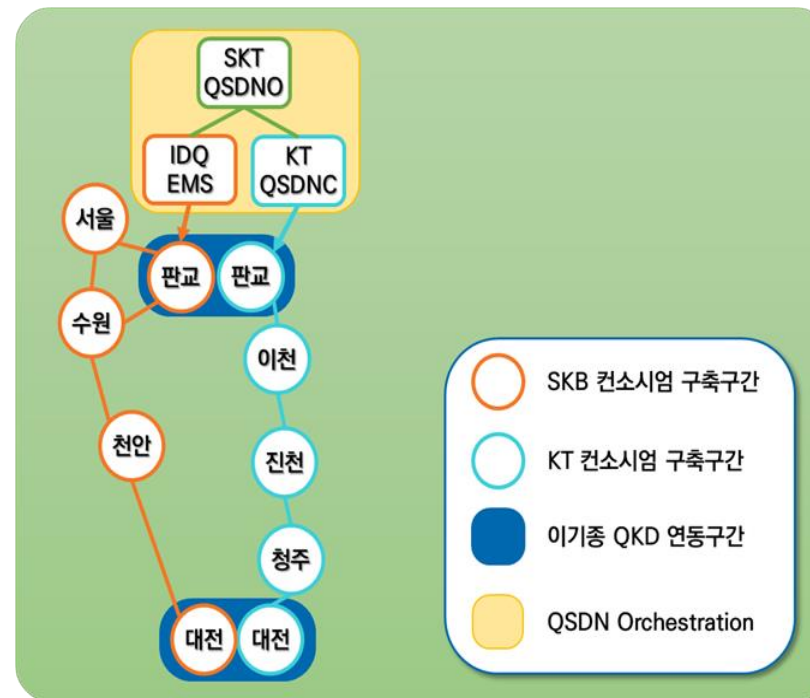
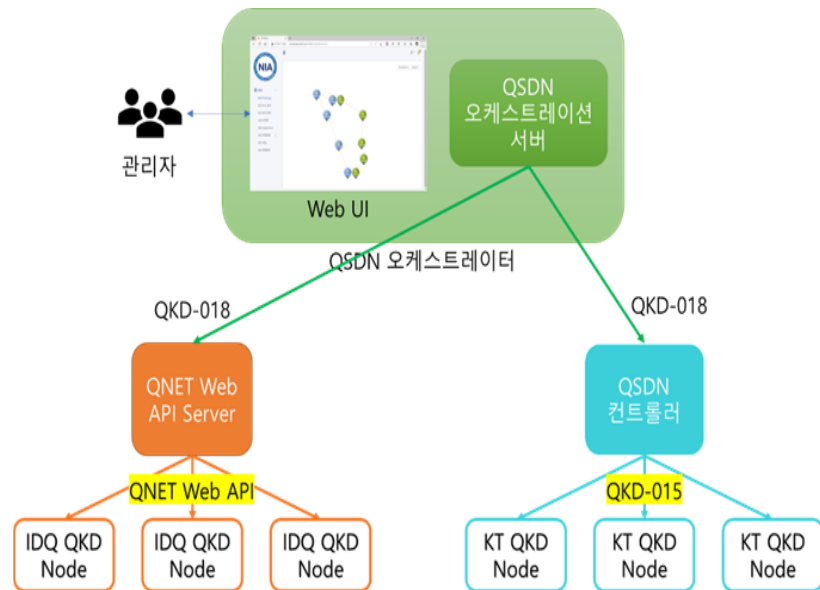
● SDN과 QKD 연동 기술의 통합(1)

- SDN은 많은 Telco 운영자에게 중요한 요소로 부상
 - QKD 서비스의 SDN기술을 통한 통합이 필요
 - QKD key를 전달하기 위한 MGMT Interface 정의
- ETSI GS QKD 015 : SDN을 위한 제어 인터페이스
 - SD-QKD node와 SDN Controller간의 추상화 모델과 업무흐름을 정의
 - Resource Discovery, Capabilities, Dissemination, System configuration operations 등
- ETSI GS QKD 018 : SDN을 위한 Orchestration 인터페이스



03. QSDN을 이용한 이중솔루션간 양자키 전달

● SDN과 QKD 연동 기술의 통합(2)

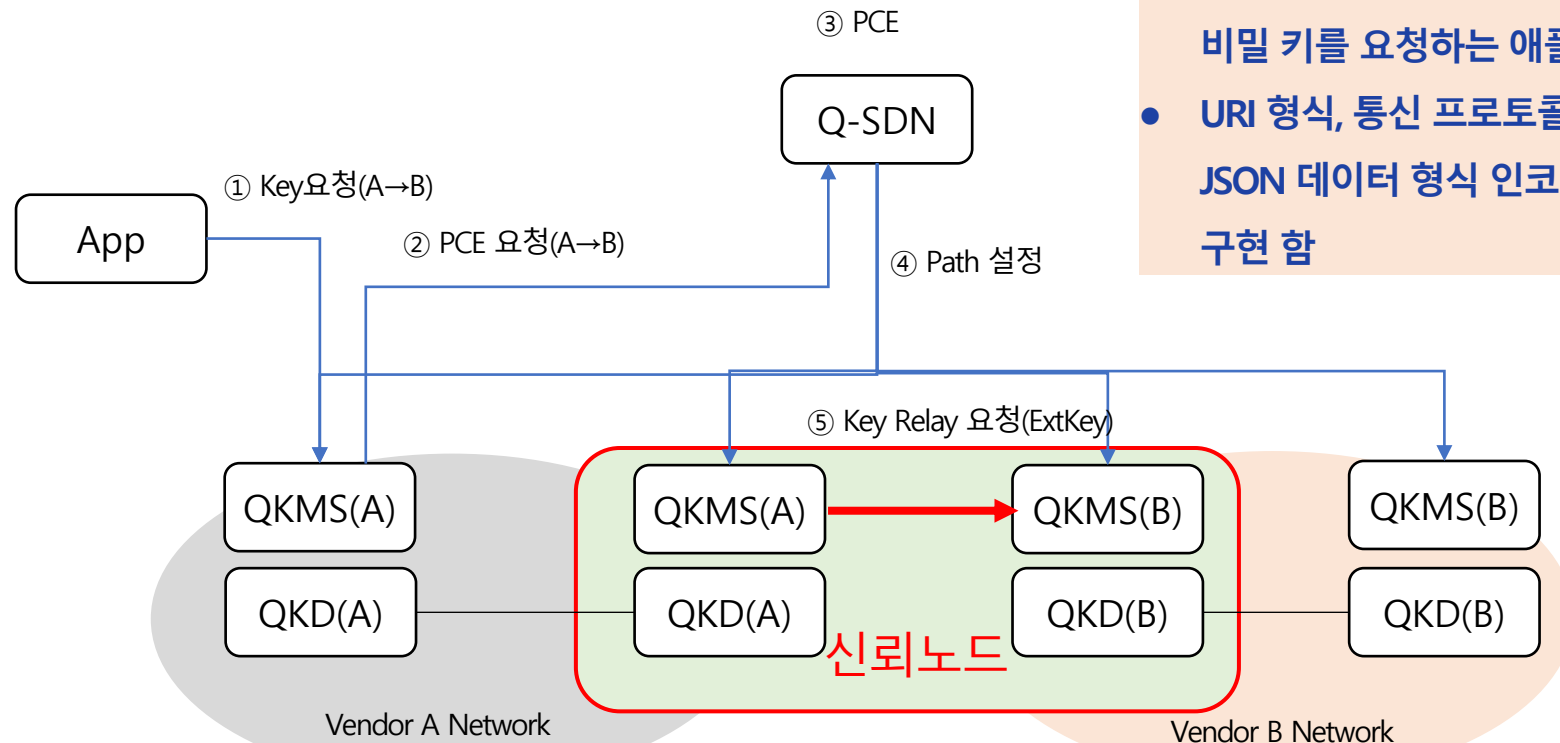


- 이기종 솔루션간 통합 관리를 위하여 QSDNO와 QSDNC 간에는 ETSI QKD-018 표준 을 준용하고, QSDNC는 신뢰노드(QKMS)와 ETSI QKD-015 표준을 준용
- KOREN 양자암호통신망에서 판교PoP과 대전PoP은 이중 솔루션간 신뢰노드(QKMS) 키 공유구간 존재.
- 이중솔루션간 키를 교환하는 메커니즘은 EU OpenQKD에서도 적용하였고, ETSI의 새로운 Work Item으로 제안된 QKD-020_InteropKMS(Protocol and data format of REST-based Interoperable Key Management System API) 문서에서 제시하는 키교환 방법을 준용

03. QSDN을 이용한 이중솔루션간 양자키 전달

● 이중 QKD 연동 신뢰노드 구현

- KT형 /IDQ형 동종 신뢰노드~QKD간 연동 인터페이스 보완
- 이중 QKD와 신뢰노드 간 연동 인터페이스 개발

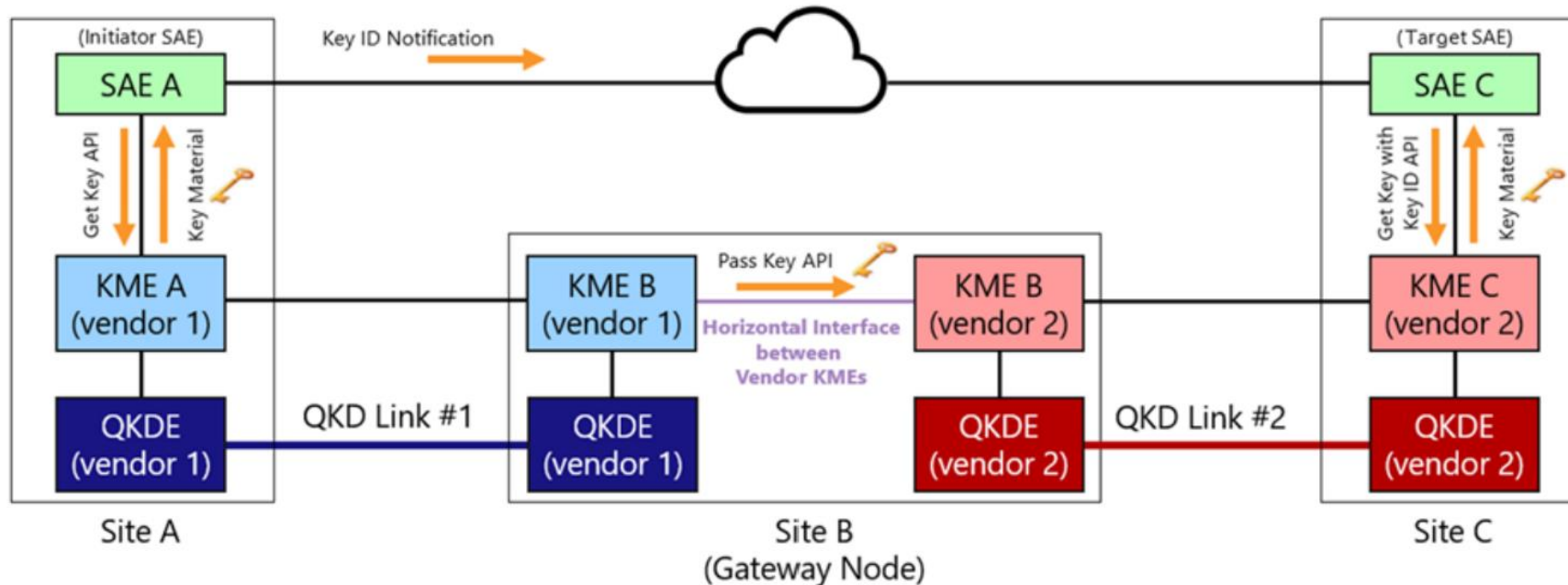


- 공통의 신뢰할 수 있는 노드에 위치한 두 시스템 간에 키를 수평으로 키를 전달하기 위해 키 관리시스템(QKMS)이 상호 운용할 수 있는 REST API를 지정
- API를 사용하면 QKD 네트워크가 동일한 공급업체의 연속적인 시스템 체인에 의해 연결되지 않은 키 관리시스템(QKMS)에서 공유 비밀 키를 요청하는 애플리케이션에게 서비스를 제공할 수 있음
- URI 형식, 통신 프로토콜(HTTPS), 파라미터 및 응답(키 자료 포함)의 JSON 데이터 형식 인코딩에 대해서는 SK, KT가 협의하여 결정 후 구현 함

03. QSDN을 이용한 이중솔루션간 양자키 전달

- 상호운용가능한 Key Management System API

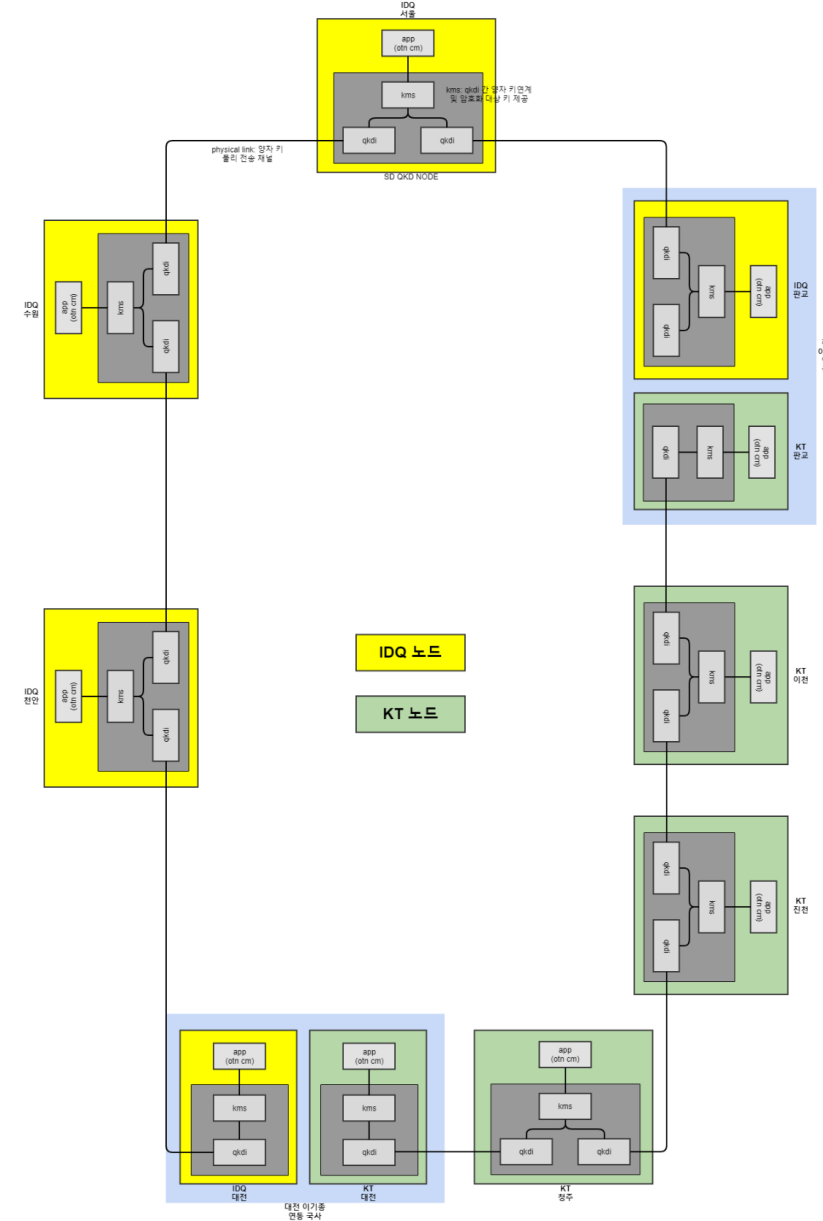
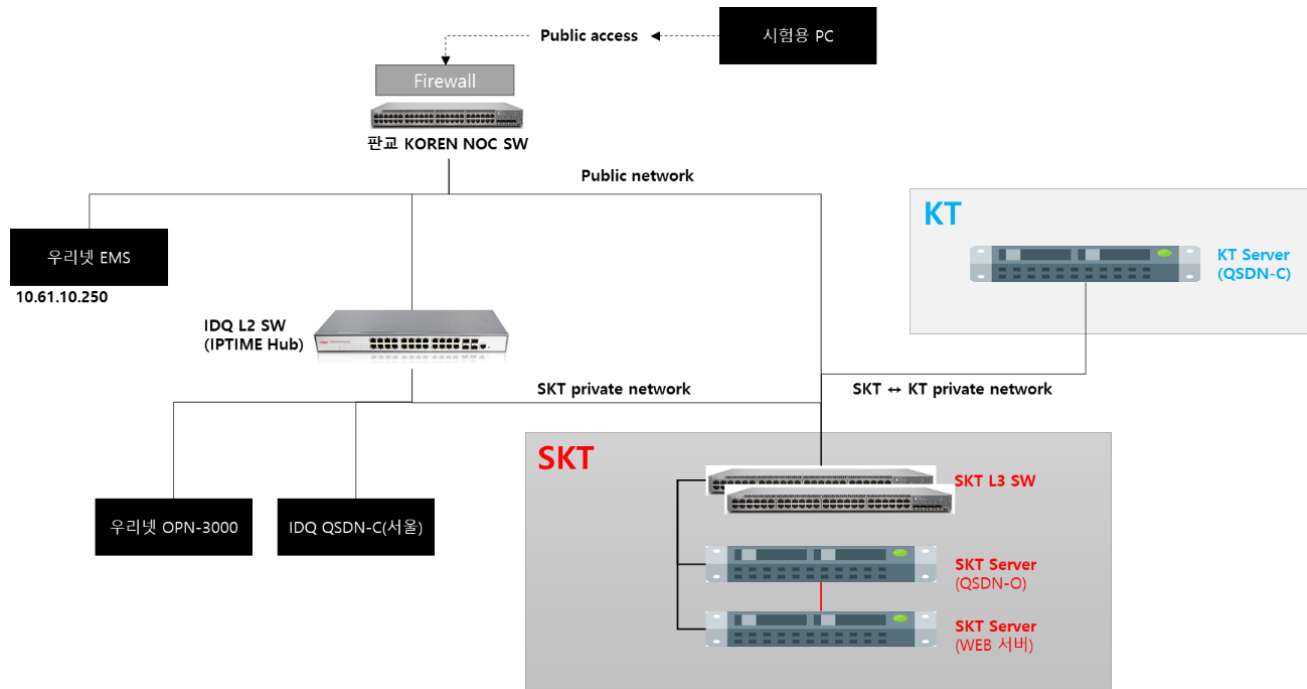
- 신뢰노드로서 동작하는 QKMS간 키를 전달하는 수평적인 인터페이스 필요
 - 이중 QKD 연동을 위한 ETSI 020 ExtKey(Pass Key) Interface 기반 구현 및 실제망에 적용



- 서로 다른 벤더의 호환되지 않는 시스템을 사용하여 두 부분으로 구성된 3개의 노드 네트워크의 게이트웨이 노드에서 QKMS(KME) 간에 키를 수평적으로 전달하는 ext_keys 메서드를 사용하는 사용 사례를 보여줍니다.

03. QSDN을 이용한 이중솔루션간 양자키 전달

KOREN 양자암호통신망 내 QSDN 장비구축 현황

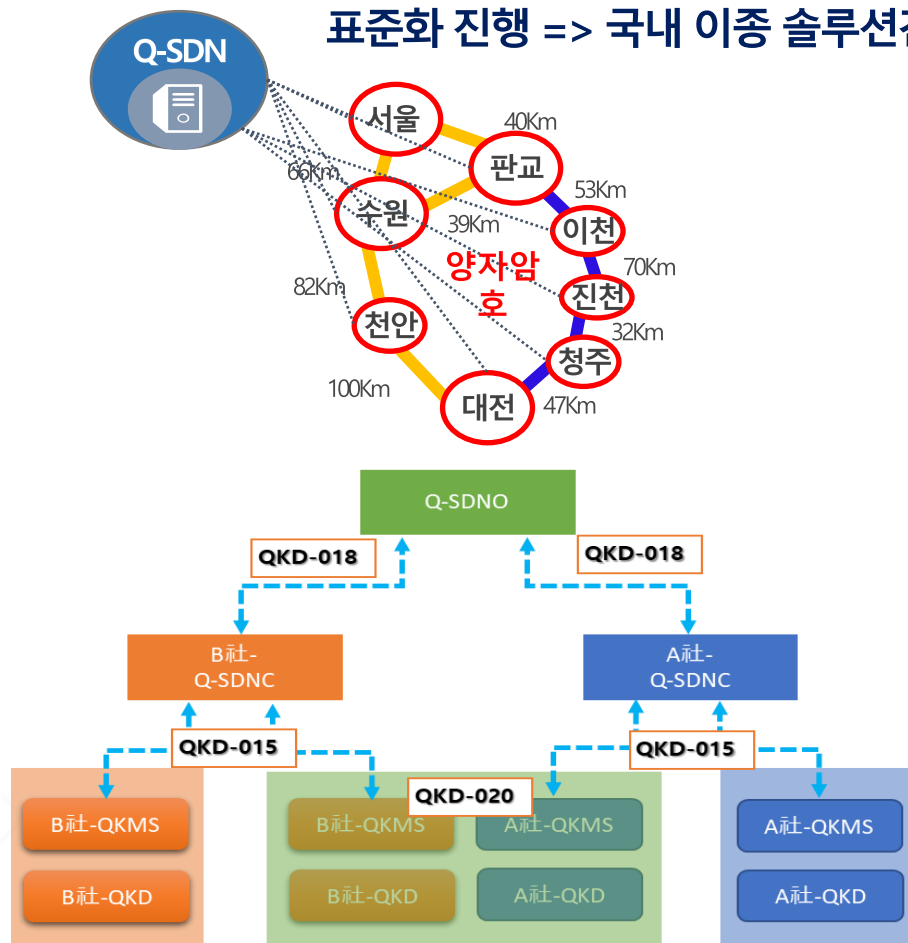


03. QSDN을 이용한 이종솔루션간 양자키 전달

QSDN Orchestrator와 QSDN Controller를 통한 멀티 벤더 상호운용성

- IDQ와 도시바가 제안한 이기종 QKD 간 양자키 관리시스템을 이용한 연동방안이 ETSI-GS-QKD-020으로

표준화 진행 => 국내 이종 솔루션간 상호운용성 검증



이종 솔루션 접점구간 – KOREN 테스트베드 內 대전, 판교 지점

❖ SKT-KT-SKT 키 공유(수원->천안, 천안->수원)

수원(SKT)	판교(접점)	이천(KT)	진천(KT)	청주(KT)	대전(접점)	천안(SKT)
키 송신	External Key	key-relay	key-relay	key-relay	External key	키 수신
키 수신	External Key	key-relay	key-relay	key-relay	External key	키 송신

❖ KT-SKT-KT 키 공유

이천(KT)	판교(접점)	수원(SKT)	천안(SKT)	대전(접점)	청주(KT)	진천(KT)
키 송신	External Key	key-relay	key-relay	External key	key-relay	키 수신
키 수신	External Key	key-relay	key-relay	External key	key-relay	키 송신

❖ SKT->KT, KT->SKT 키 공유

수원(SKT)	판교(접점)	이천(KT)	진천(KT)	청주(KT)
키 송신	External Key	key-relay	key-relay	키 수신
키 수신	External Key	key-relay	key-relay	키 송신



감사합니다.

박상길 책임연구원, 한국전자통신연구원(ETRI)
wideideal@etri.re.kr