Post-Quantum

Cryptography Conference

NQSN Singapore: Quantum-Safe Network Testbed with Versatile Reference Applications

Jing Yan Haw
Senior Research Fellow at Centre for Quantum Technologies, National University of Singapore

Hao Qin
Senior Research Fellow at Centre for Quantum Technologies, National University of Singapore

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

NQSN Singapore: Quantum-Safe Network Testbed with Versatile Reference Applications

Dr. Jing Yan (Joshua) HAW,[*] *Dr. Hao QIN*[*]
Centre for Quantum Technologies, National University of Singapore
**contributed equally*
jy.haw@nus.edu.sg; *hao.qin@nus.edu.sg*

PKI Consortium

Post-Quantum Cryptography Conference 2025
30 Oct 2025

Centre for Quantum Technologies
Fraunhofer SINGAPORE
NUS National University of Singapore
NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

QUANTUM-SAFE COMMUNICATIONS

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

Software	Hardware	
		
Post-quantum cryptography Development and implementation of quantum-safe algorithms that are secure against quantum computer-supported attacks.	**Quantum key distribution** Deployment of cryptographic protocols for distribution of symmetric keys, in order to avoid vulnerable key exchange mechanisms.	**Random number generation** Generating true random numbers based on the laws of quantum mechanics, as opposed to the pseudo-random numbers generated by traditional techniques.

Transitioning to a Quantum-Secure Economy, World Economic Forum, Sept 2022
https://www.weforum.org/whitepapers/transitioning-to-a-quantum-secure-economy/

QUANTUM-SAFE COMMUNICATIONS INITIATIVES IN SINGAPORE

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

2006 — Free space QKD across 1.5 km with entangled photon pairs

2007 — Centre for Quantum Technologies (CQT)

2016 — NUS-SingTel Cyber Security R&D to support QKD trials

2017 — SPEQTRAL

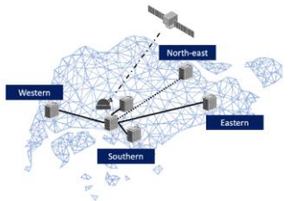
2019 — Quantum nanosatellite SpooQy-1 deployed from ISS

2020 — Entanglement over Fiber Network & Nano-sat.

SQUAREROOT8

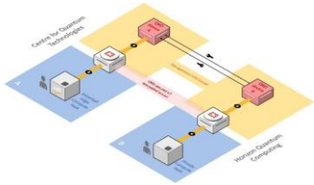
Entanglement-based QKD System

2022 — NATIONAL QUANTUM-SAFE NETWORK SINGAPORE



NQSN Phase I

QKD over Data Centre & Edge Cloud



2023 — INFOCOMM MEDIA DEVELOPMENT AUTHORITY

Digital blueprint: vision of a quantum-safe nation in 10 years & **NQSN+**, Southeast Asia's first quantum-safe network infra.

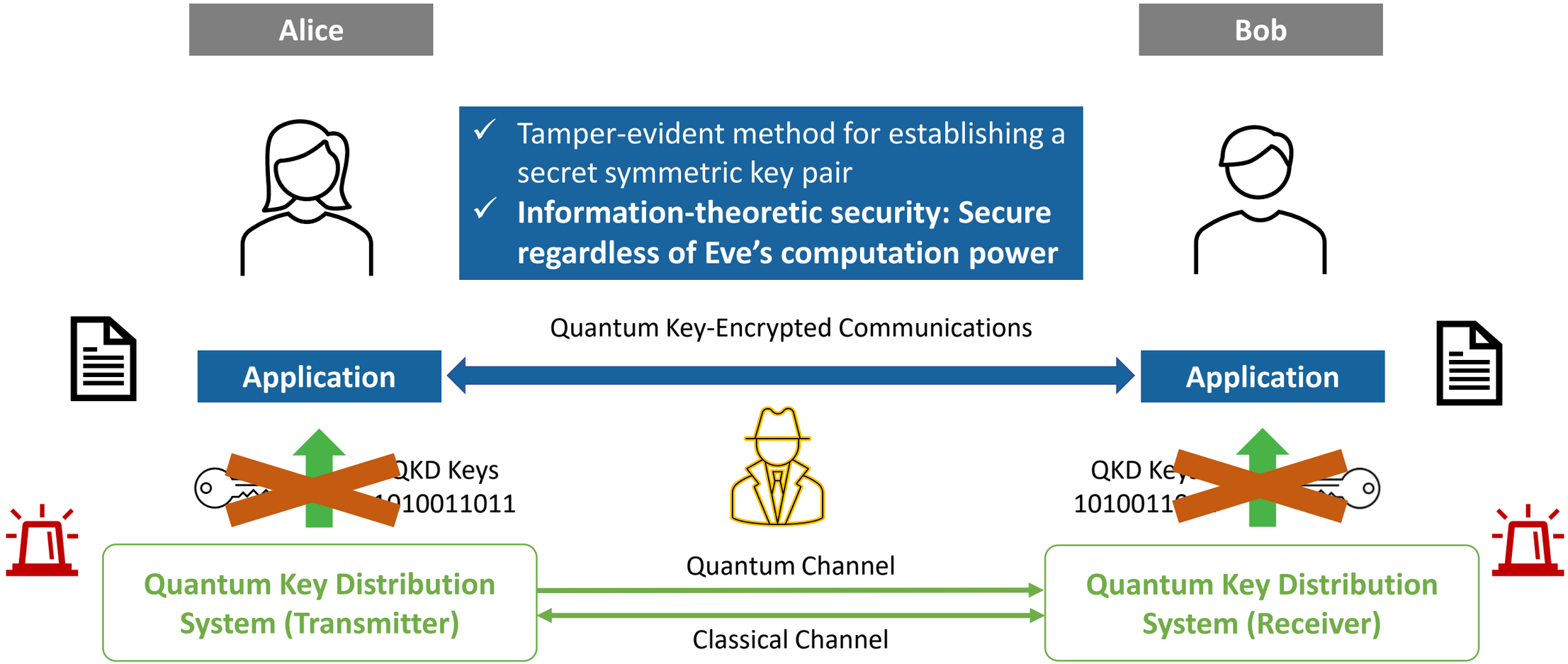
2025 — Led ITU-T work item on QKD protocol framework

Published Singapore's 1st standard on QKD Networks

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

NQSN Testbed Phase II

QUANTUM KEY DISTRIBUTION



QKD & PQC SIDE-BY-SIDE

Table 4. Comparison between PQC and QKD

	PQC	QKD
Implementation	Software and hardware	Hardware
Protocol security	Computational complexity	ITS
Implementation loopholes	Exist	Exist
Application and usage	Public-key encryption and key establishment, Digital signature	Key establishment
Migration	Software and hardware upgrade	Infrastructure and hardware upgrade
Standardisation and certification	Required	Required

PQC: Post quantum cryptography; QKD: quantum key distribution; ITS: information-theoretic security.

Qiu, K., Haw, J. Y., Qin, H., Ng, N. H., Kasper, M., & Ling, A. (2024). Quantum-Secured Data Centre Interconnect in a field environment. Journal of Surveillance, Security and Safety, 5(3), 184-197.

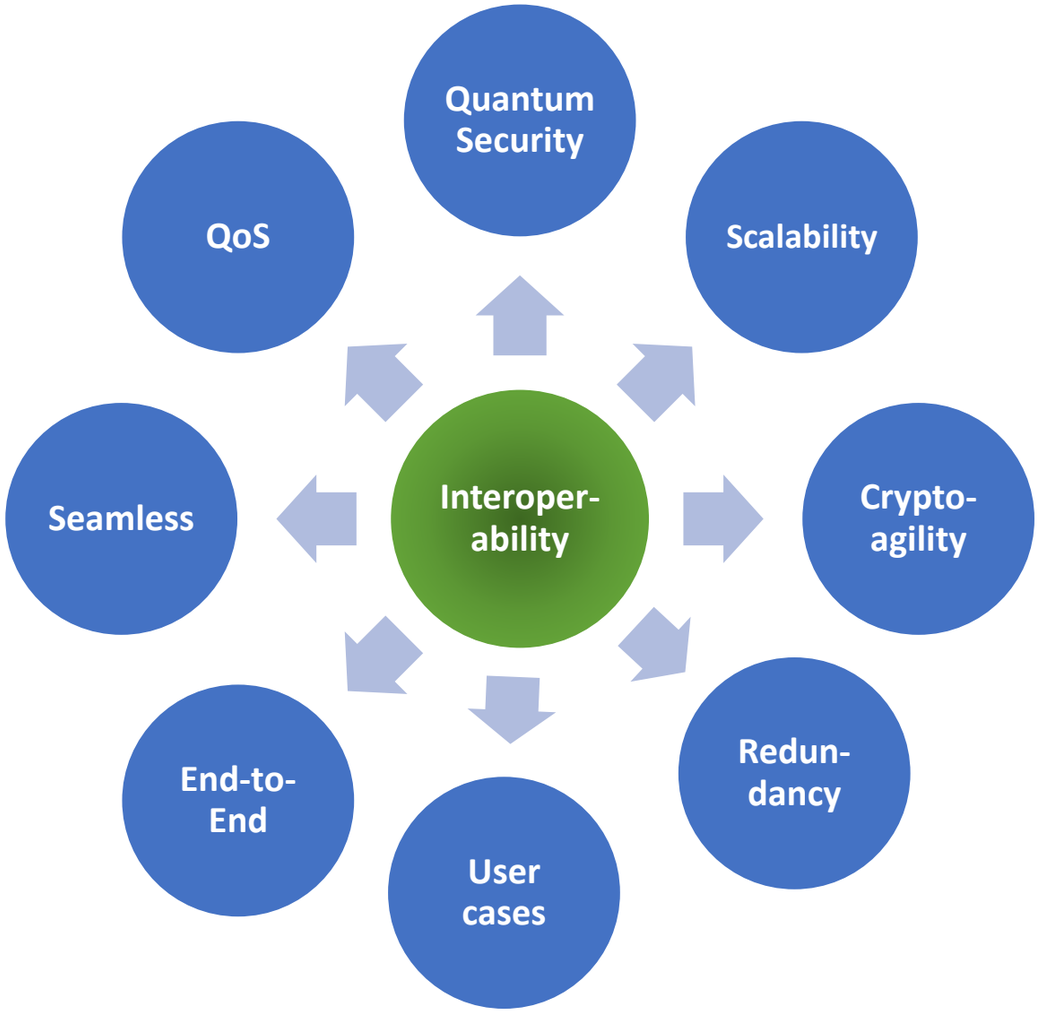
MOTIVATION & OBJECTIVES

TESTBED INFRASTRUCTURE & USE CASES

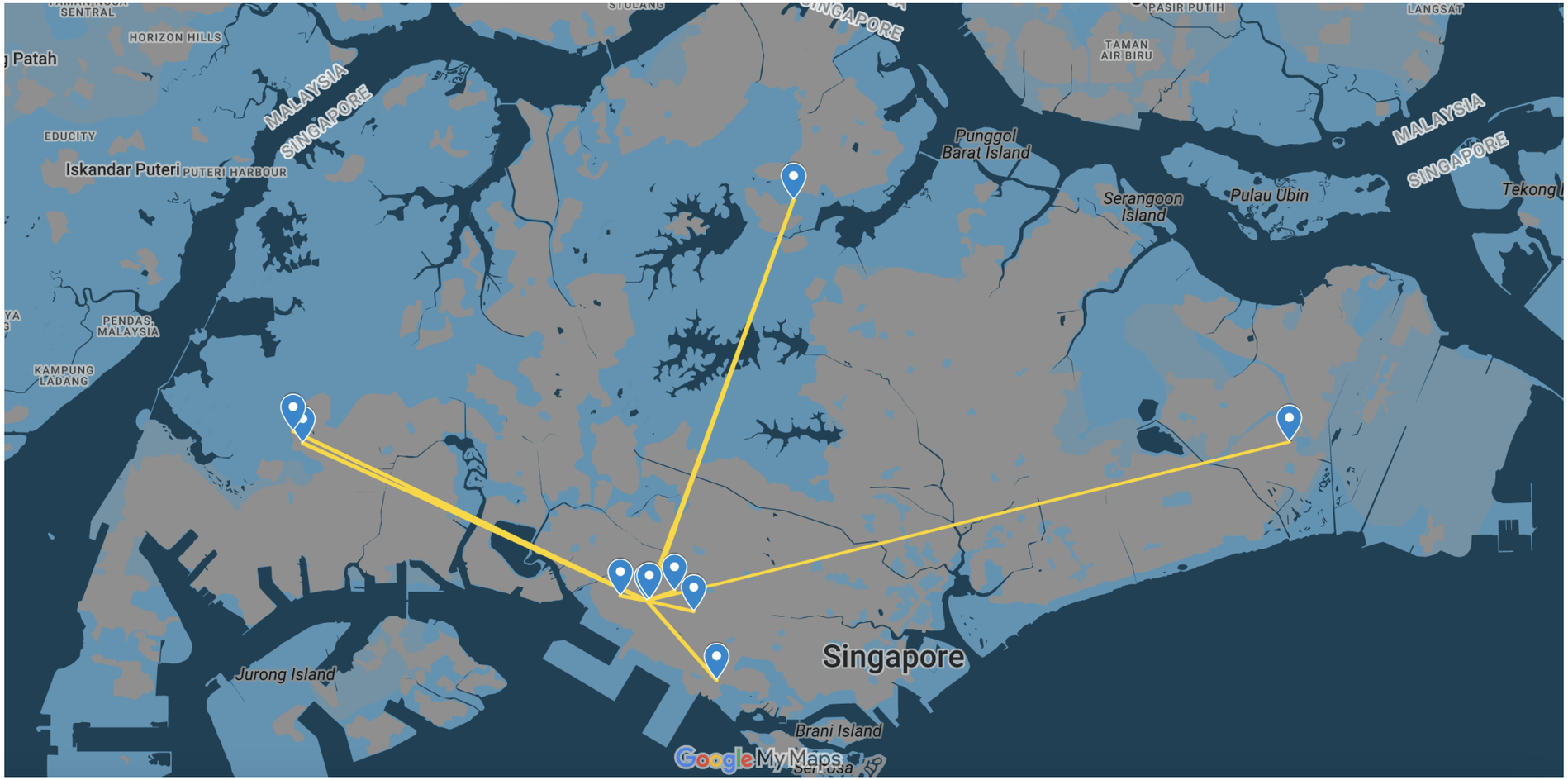
- Nation-wide terrestrial network (+ optical ground station)
- Public-private collaborations & use cases with >30 companies & govt agencies
- **Vendor neutral** and **multiprotocol**
- Hybrid Quantum-Safe Technologies, e.g. QKD and PQC (Post-quantum cryptography)
- **Interoperability** of quantum-safe technologies and applications

SECURITY FRAMEWORK & GUIDELINES

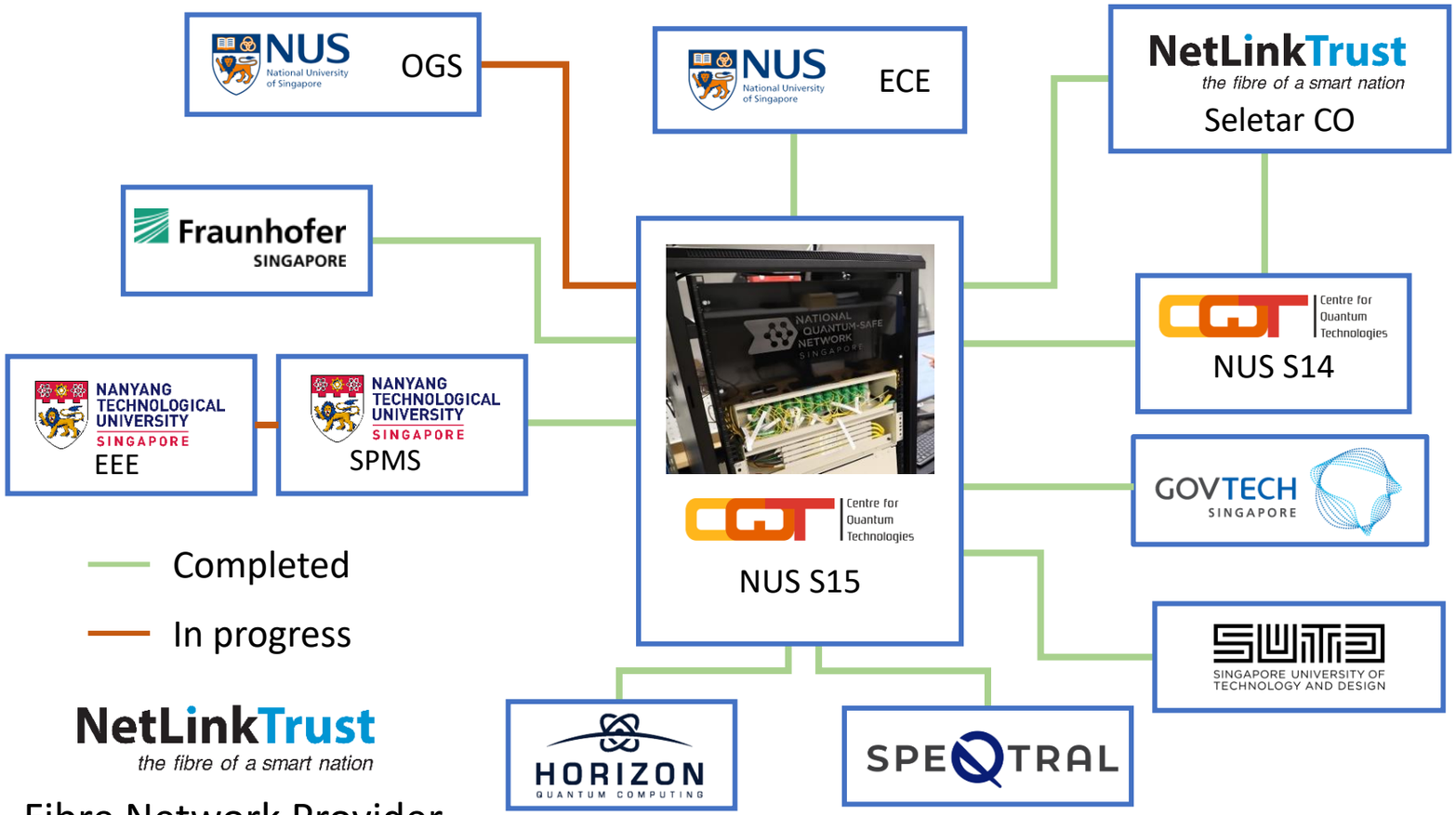
- In-depth **functional & security evaluation** of Quantum-safe technologies to seed certification
- Build readiness by developing **national and international standards**



TESTBED – NATION-WIDE FIBRE NETWORK



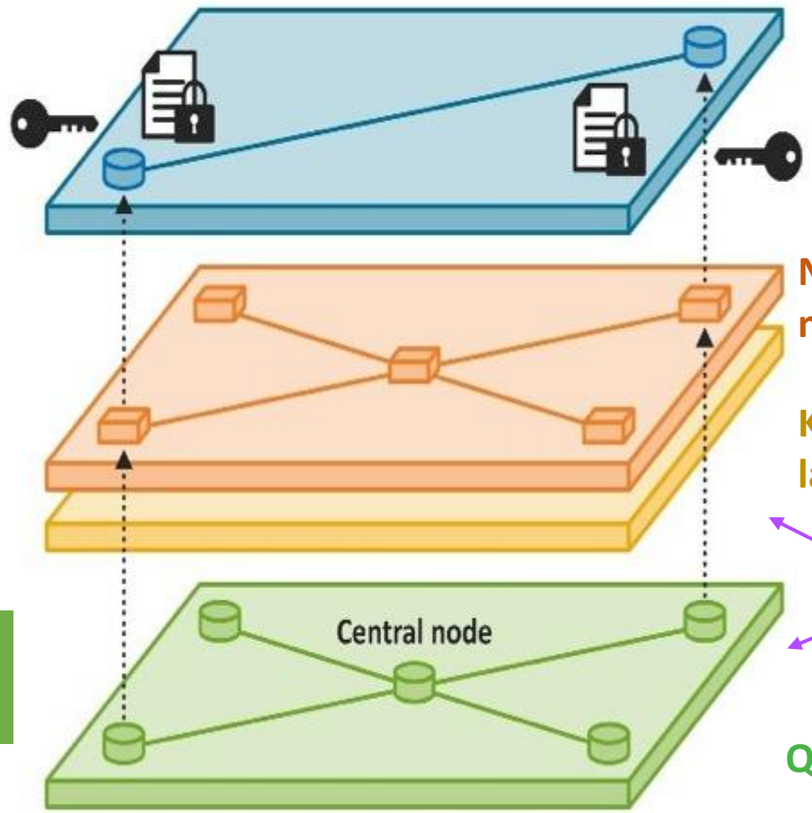
TESTBED - FIBRE NETWORK FEATURES



- 12-node **Star-Mesh** Network
- Total dark fibres: **> 75 fibres**
- Total fibres length: **> 1500 km**
- Distance range: **0.45 km – 47 km**

TESTBED – DIFFERENT LAYERS IN NQSN

- ❑ Encryptors & Quantum-Safe Applications
- ❑ Interoperability
- ❑ Scalability
- ❑ Multi QKD protocols
- ❑ Existing Fiber infra



Application layer

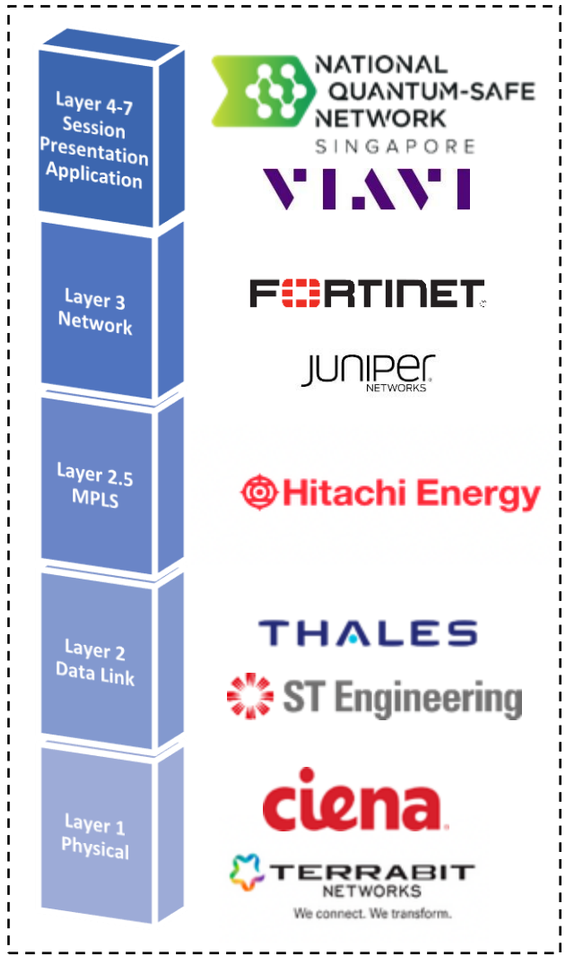
ETSI GS QKD 014

Network management layer

Key management layer

Testing

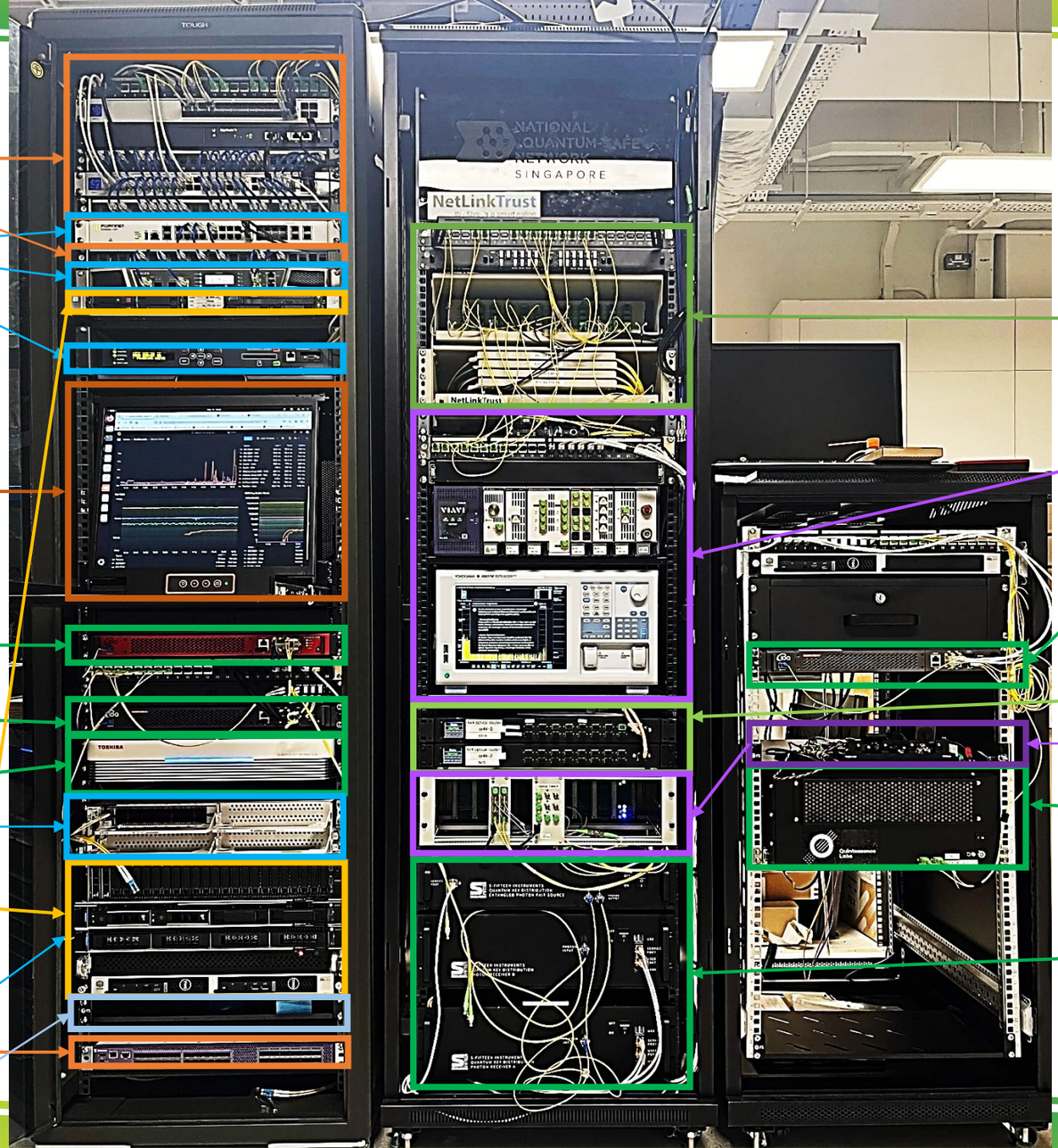
Quantum layer



Open Systems Interconnection (OSI) Layers

- Compliance with ITU-T Y.3800; IMDA TSAC RS QKDN

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE



Network

Encryptor

QKDN Manage.

IDQ COW

IDQ BB84

Toshiba BB84

KMS & QKDN Manage.

Software App

Quantum Randomness Beacon (S15 QRNG)

Fiber panel

QKD & Fiber Testing Viavi etc.

IDQ BB84 Bob

Optical switch

Quintessencelabs GMCS CV QKD

S15 BBM95 Source, Receiver A, and Receiver B

QUANTUM LAYER – QKD SYSTEMS EVALUATED

- **Multi-QKD protocol, vendor-neutral QKD network testbed**
- **Evaluation of different QKD protocols: BB84, COW, GMCS, BBM92**
- **SKR between 0.2kbps – 0.1 Mbps**

Prepare-&-Measure Discrete-Variable (DV) QKD

Cerberis XG & XGR

Clavis XGR

LD- QKD

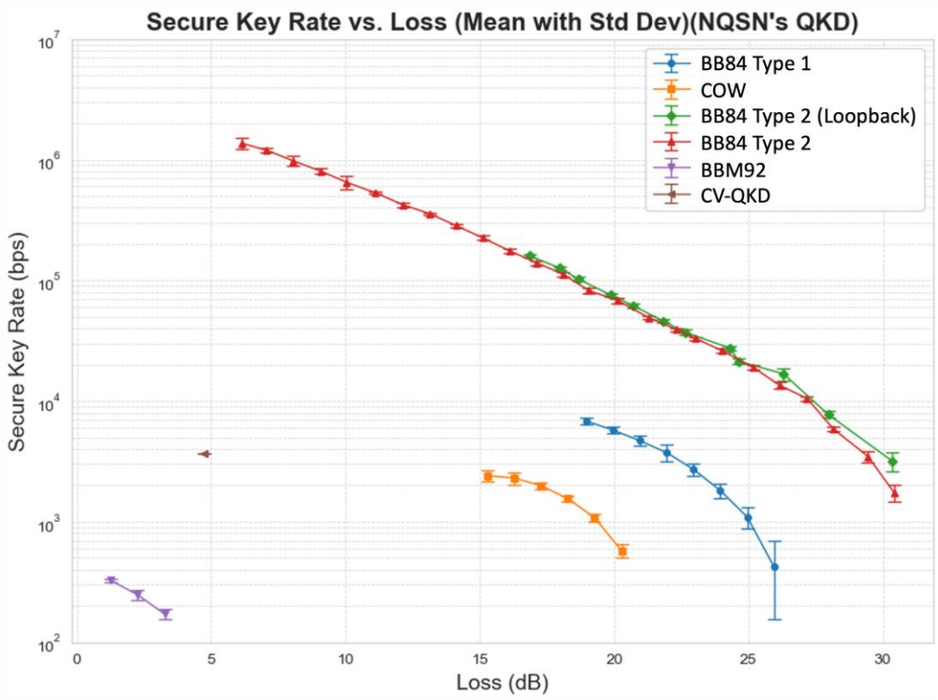
Prepare-&-Measure Continuous-Variable (CV) QKD

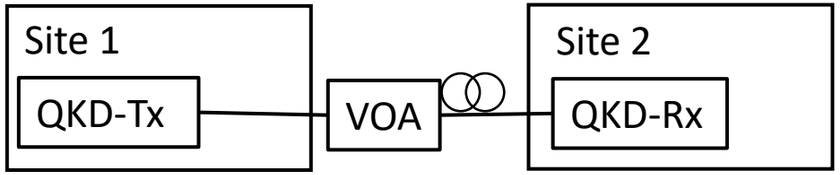
qOptica 100

Entanglement-based (EB) QKD

QKD System V0.2

QKD System with asymmetric setting





Performance evaluation & SKR verification

KEY MANAGEMENT LAYER

- **Interoperable Key Management System (KMS)**
- **Key interface development & evaluation**

Key Management System (KMS)

- **Interoperable** with different QKD systems and apps
- Multi-input &-output key interface with **scalability**
- KMS link secure by TLS 1.3 with X25519MLKEM768 for key exchange (PQC) and X.509 PKI certificate for authentication

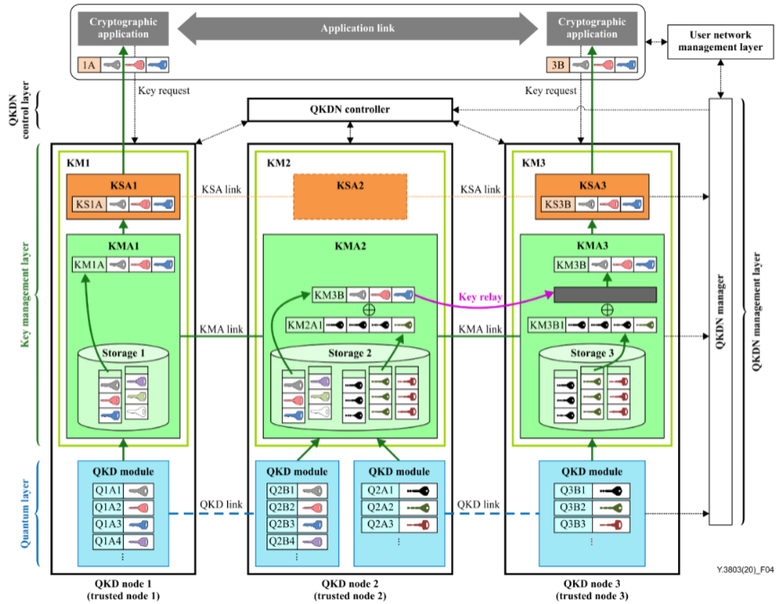
Key Management Agent (KMA)

- Key buffer for integrity check
- KMA key storage: Key data base
- Proactive key relay with OTP and AES
- Hybrid key capability under development

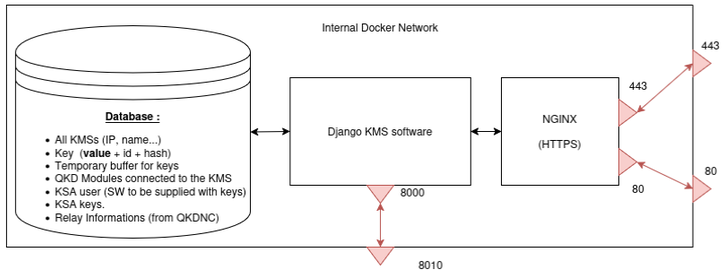
Key Supply Agent (KSA)

- Key supply to cryptographic application
- KSA key storge: Key data base
- Key Interface**: ETSI GS QKD 014**

*** Follow ITU-T Y.3803, X.1712; ETSI GS QKD 014; IMDA TSAC RS QKDN**



ITU-T Y.3803 Quantum key distribution networks – Key management
(NQSN KMS: Modified version of Case 2)



NQSN KMS V1 software architecture

QKD NETWORK MANAGEMENT LAYER

• QKDN Controller & QKDN Manager

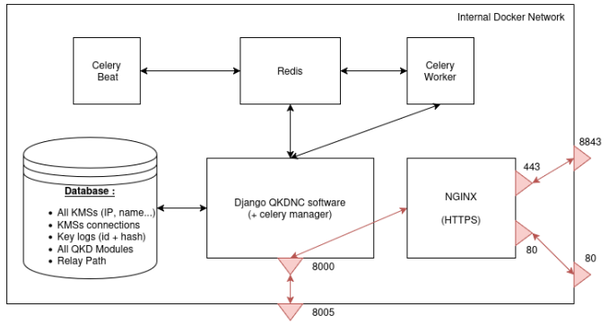
- A **centralized** QKD network management system consists of QKDN controller and manager

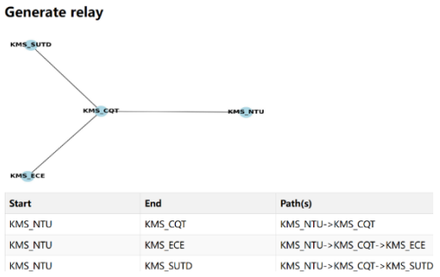
Controller Function

- Network configure control
- Routing control for key relay
- Configuration control
- KMS policy and other policy control
- Access control & session control
- Periodic task control

Management Function

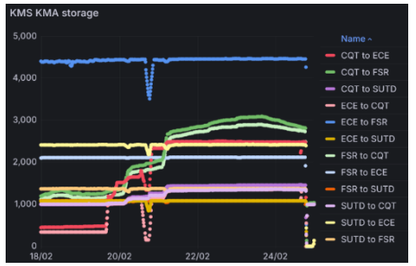
- QKDN parameters monitoring: QKD, KMS, interfaces…
- Entity authentication
- Quality of Service (QoS)
- Fault detection & reporting



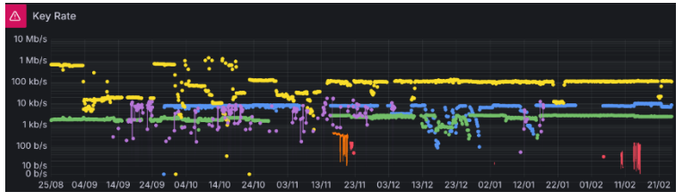


NQSN QKDN control & management system software V1 architecture

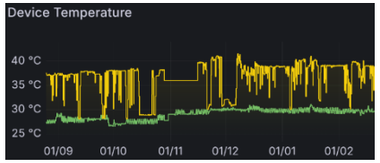
QKD link status



KMS storage



QKD-Key rate log



QKD device temp.

AD-HOC QUANTUM APPLICATION

- **Quantum Randomness Beacon Service**

- Developed in "SpooQy Lab“ in CQT and operation under NQSN Testbed

Randomness Source

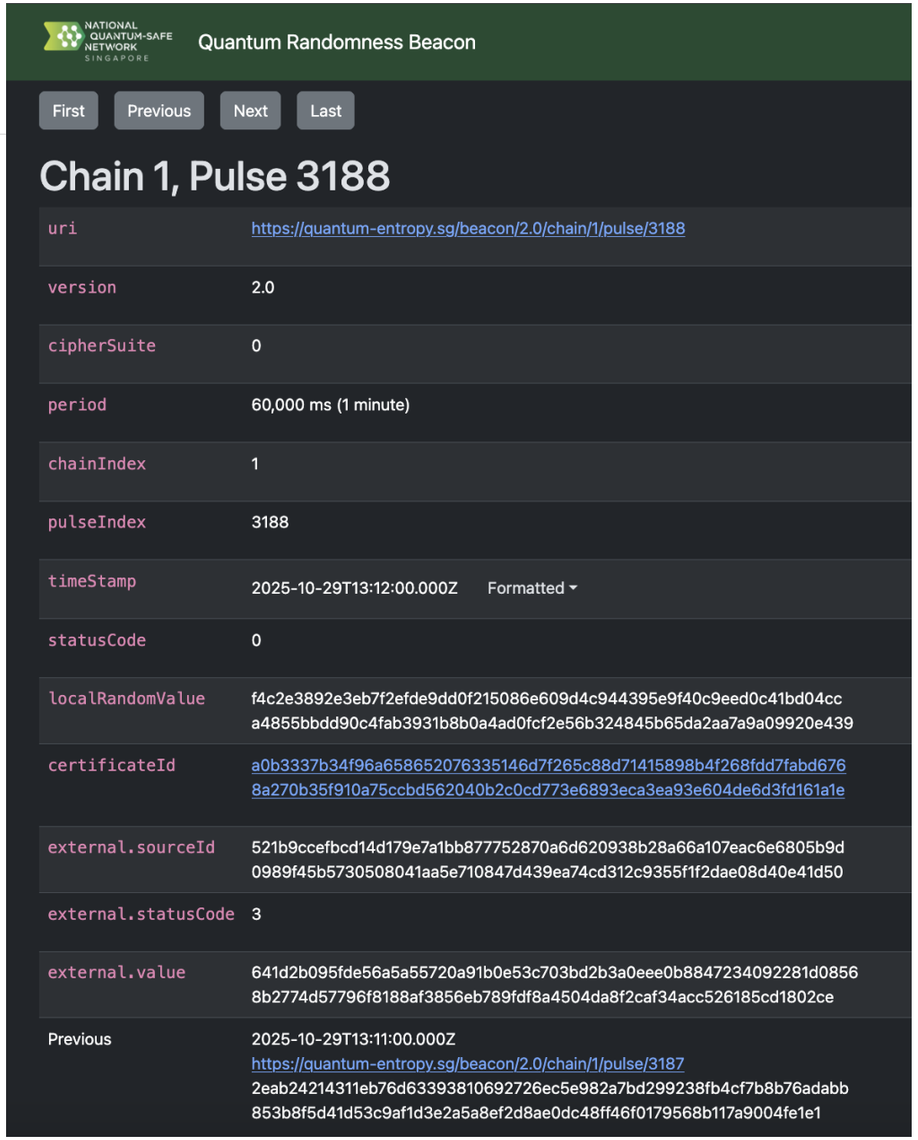
- Based on Quantum Random Number Generator (QRNG) from S-Fifteen Instruments
- Vacuum fluctuation with homodyne detection

Randomness Beacon Service

- Randomness service as in **NIST IR 8213**
- Random string bits on a fixed interval
- Real-time randomness without a formatting framework

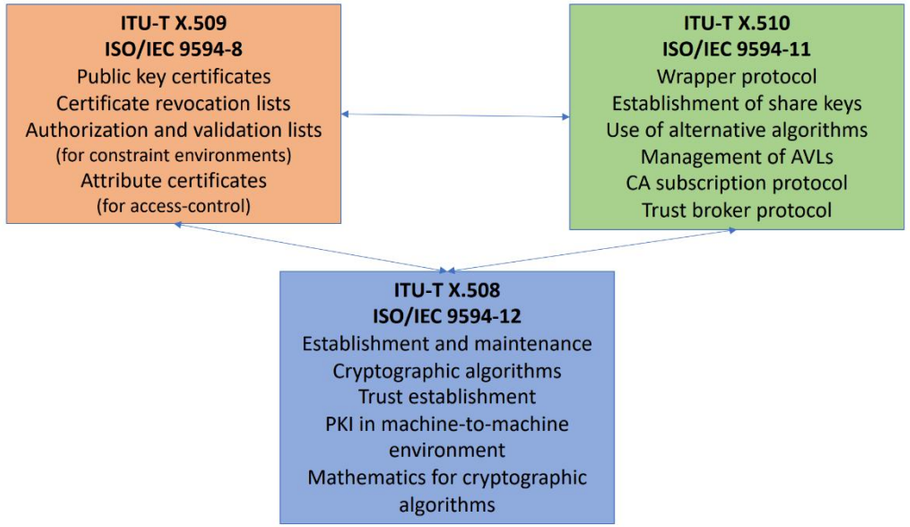
https://quantum-entropy.sg/

QRNG1



PUBLIC KEY INFRASTRUCTURE (PKI) STANDARD QUANTUM-SAFE MIGRATION STATUS

ITU-T Recommendation	Title	ISO/IEC reference
X.508 (04/2025)	Information technology - Open Systems Interconnection - The Directory: Public-key infrastructure: Establishment and maintenance	ISO/IEC 9594-12
X.509 Amendment 1 Corr.2 (11/2023)	Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks	ISO/IEC 9594-8
X.510 Amendment 1 (08/2025)	Information technology - Open Systems Interconnection - The Directory: Protocol specifications for secure operations	ISO/IEC 9594-11



- X.508, X.509 and X.510 belong to the X.500 series (directory) and the ASN.1 modules imports definitions from other parts of X.500 series recommendations often related to directory service.
- Plan to reorganize ASN.1 definitions to have three categories of module: Modules common to Directory Service and Cybersecurity (example: UsefulDefinitions), Modules dedicated to Directory Service, Modules dedicated to Cybersecurity

❑ **Plans for X.508, X.509,X.510**

- ➢ Usage of Authority and Validation lists for IoT devices which have limited capacity.
- ➢ Usage of quantum safe algorithms. A migration mechanism using specific extensions has already been added to the last Edition of X.509 Recommendation.
- ➢ Split ITU-T X.509 to separate Public Key Infrastructure and Privilege Management infrastructure used for access control.

Jean-Paul Lemaire, Plans for X.508, X.509, X.510 Recommendations 3rd ITU-T X.509 Day, 9 May 2024

PUBLIC KEY INFRASTRUCTURE (PKI) STANDARD QUANTUM-SAFE MIGRATION STATUS

WP1/17	**Digital identity, Quantum based security, PKI and Fundamental security technologies**	
Q10/17	Identity management and telebiometrics architecture and mechanisms Continuation of Q10/17, update by ITU-T SG17 (Geneva, 8-17 April 2025) and endorsed by TSAG (Geneva, 26-30 May 2025)	
Q11/17	Generic technologies to support secure applications Continuation of Q11/17	PKI standard, X.509, X.500 series
Q15/17	Quantum-based security Continuation of Q15/17	QKD related WIs, NQSN involved

❑ PKI standards are now under revision

- Under development in **ITU-T SG 17 WP1 Q11/17** and ISO/IEC JTC1 SC6
- PQC considerations will be gradually updated in the X.508, X.509, X.510
- ITU celebrates ITU-T X.509 Day every year on 9 May or 5 Sept

❑ X.508 (Published 04/2025)

- Some considerations on migration to PQC
- ✓ Quantum computers and cryptographic algorithm migration
- ✓ Possible attacks by use of quantum computers

❑ X.510 Amd.1 (Published 08/2025)

- ✓ The wrapper protocol includes a migration path for cryptographic algorithms allowing for smooth migration to stronger cryptographic algorithms as such requirements evolve. This will allow migration to PQC algorithms.
- ✓ Annex H Migration of cryptographic algorithms: quantum computer threat; migration tools/approaches

MyWorksp... Home ITU-T Assistant Community

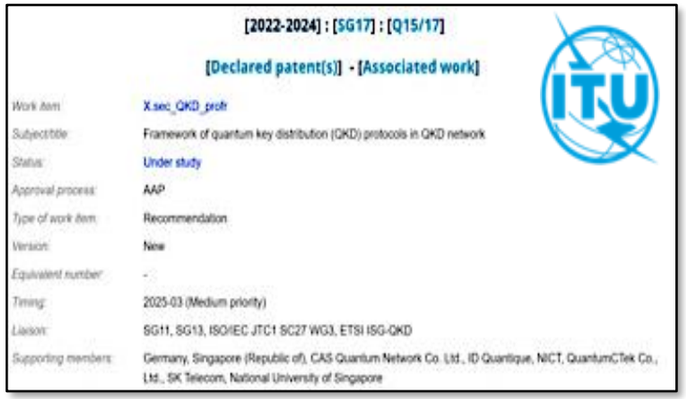
X.509Amd.2 - The Directory: Public-key and attribute certificate frameworks

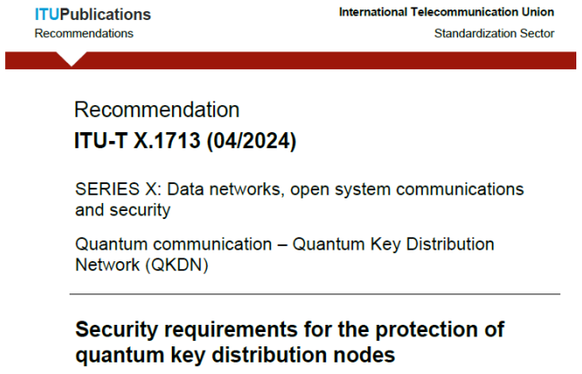
Study Period:	2025-2028
Study Group:	SG17
Question:	Q11/17
Status:	Under study [Issued from previous study period]
Approval process:	AAP
Type of work item:	Recommendation

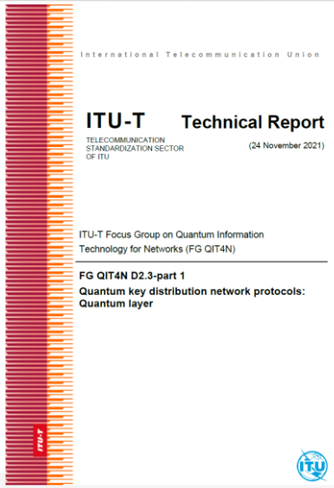
❑ X.509amd.1 Corr. 2 (Published 10/23)

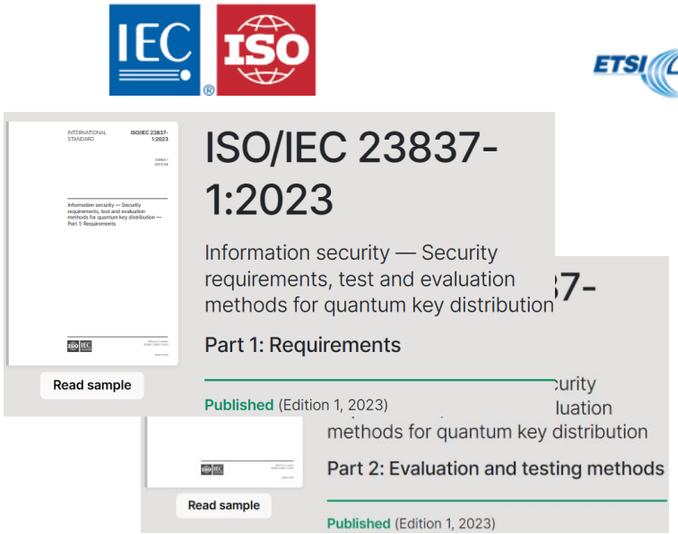
- A migration mechanism using specific extensions has already been added to the last edition of X.509.
- Usage of PQC algorithms will be updated in following editions and maybe in the **X.509amd.2**

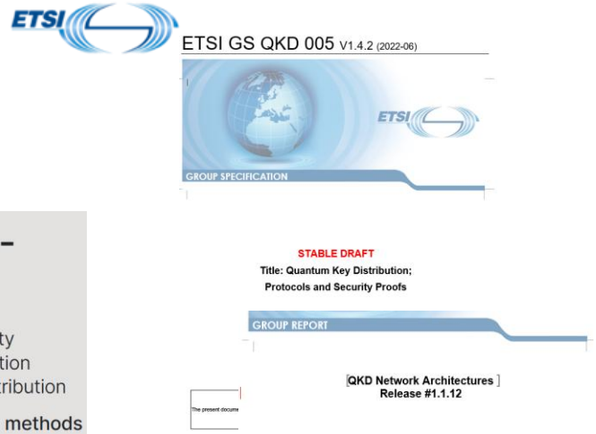
STANDARDIZATION – INTERNATIONAL







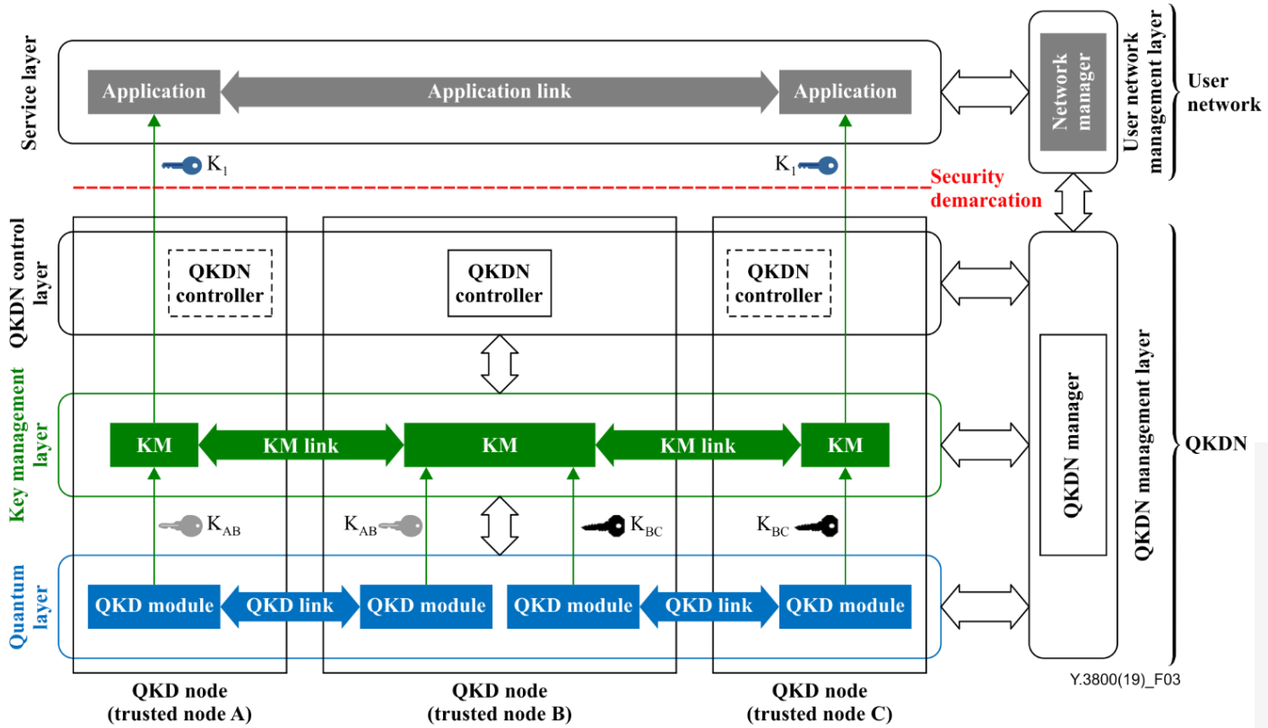




❑ International standards

- Led and established the work item for **1st standard on QKD protocol framework** in ITU-T (With IMDA)
- Editor ITU-T X.1713; FGQIT4N D2.3.1 & 2.3.2
- **ITU-T** JCA QKDN Vice Chair; Q15/17 Asso. Rapporteur
- Liaison officer & Contributor **ISO/IEC** 23837
- Contributor **ETSI** GR QKD 017, Revision GS QKD 005
- Participation & Monitor in ITU-T SG17, SG 13, SG11, JCA-QKDN; ETSI ISG QKD; ISO/IEC JTC1 SC 27 WG3

STANDARDIZATION –LOCAL



- **Figure 2 in Rec. ITU-T Y.3800 Corr.1 (2020);**
- **Figure 2 in IMDA RS QKDN 2023(referenced);**

*** Conceptual structure of a QKDN and a user network**

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

Telecommunications Standards Advisory Committee (TSAC)

Reference Specification

Quantum Key Distribution Networks

QKDN Framework & Functions

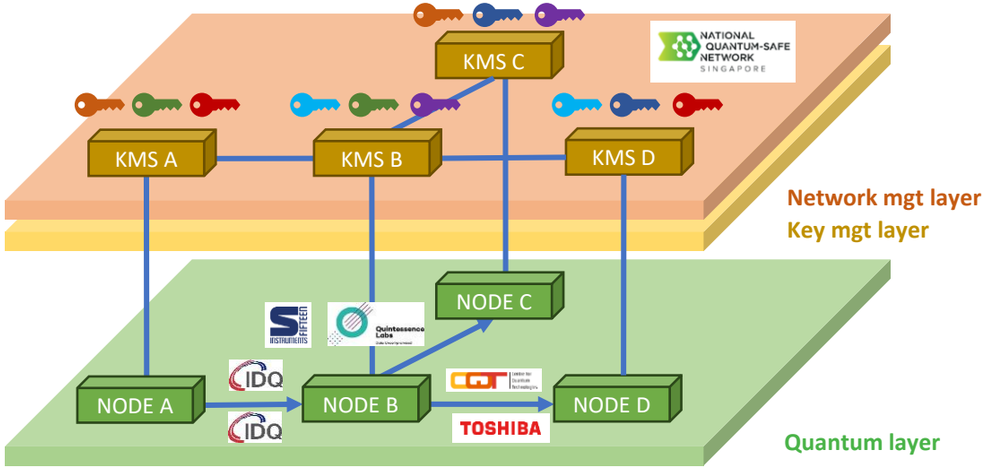
- QKDN Use Cases & Considerations
- QKDN Management Layer & QKDN Control Layer
- QKDN Key Management Layer
- Quantum Layer: QKD Modules & Links

IMDA RS

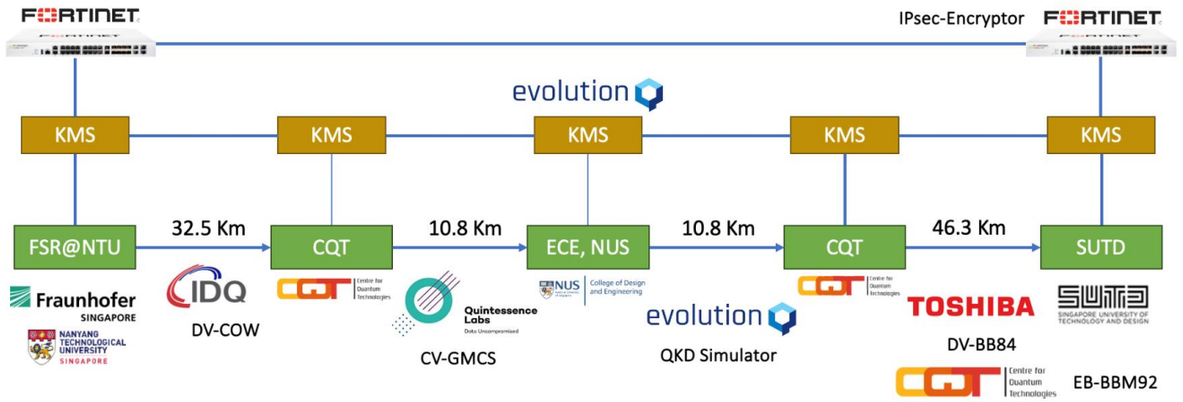
❑ **Local standards**

1. IMDA TSAC **Quantum Communications Network Task Force**, with chairs & editors from NQSN, consolidated the contributions from 20 partners
2. Singapore's **1st standard (Reference Specification)** on **QKD Networks** published on June 2023, with high level descriptions of QKDN & aligned with SDOs on QKDN, e.g. ITU-T, ETSI
3. 2nd phase study on QKD modules & networks **evaluation & certification**
4. 3rd phase study to update RS QKDN, e.g. **PQC**, interworking

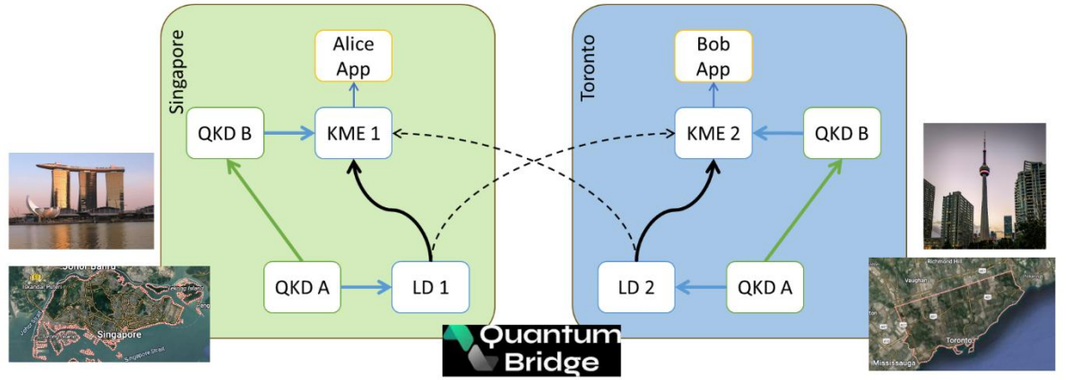
KEY MANAGEMENT LAYER USE CASES



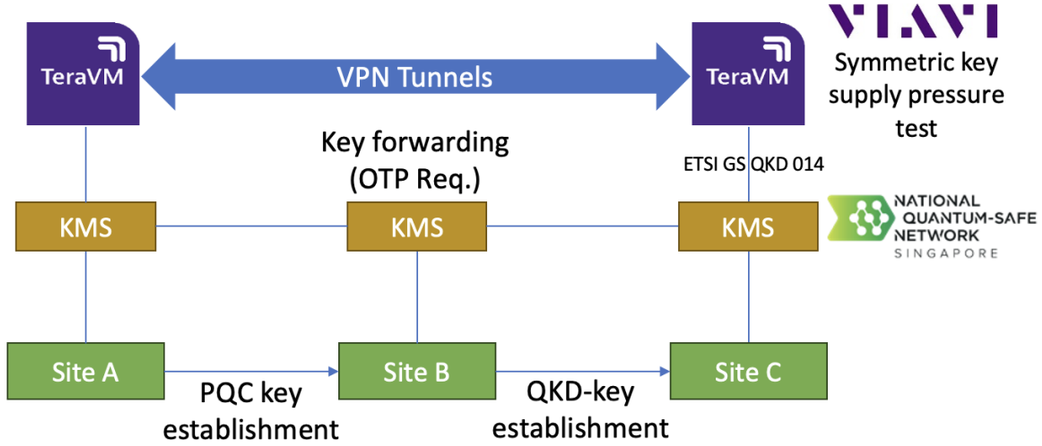
NQSN KMS for Multi-node, Multi-QKD Key Relay



Multi-hop, Multi-QKD Over 5 Nodes

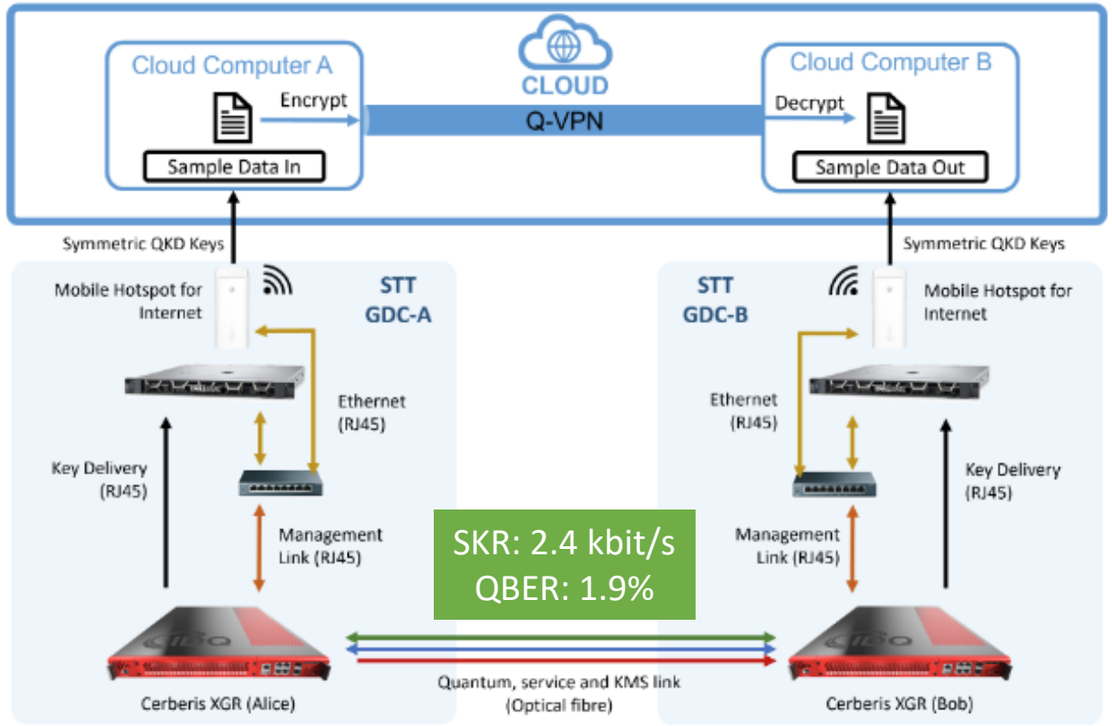


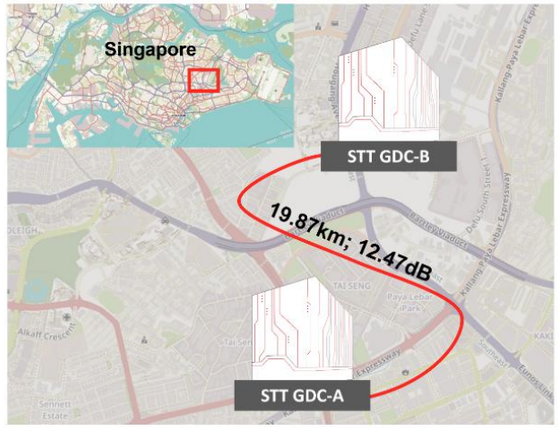
Cross-border Distributed Symmetric Key Exchange (with QKD)



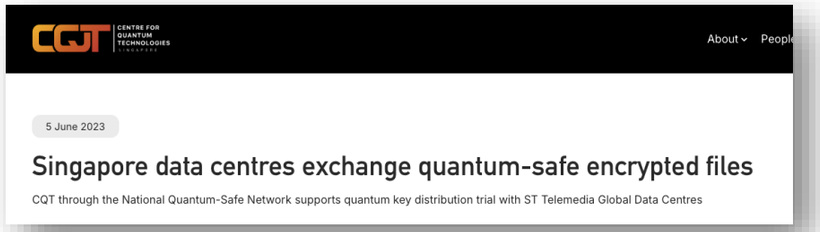
QKDN KMS Robust Test with TeraVM

QKD-SECURED DATA CENTRE INTERCONNECT

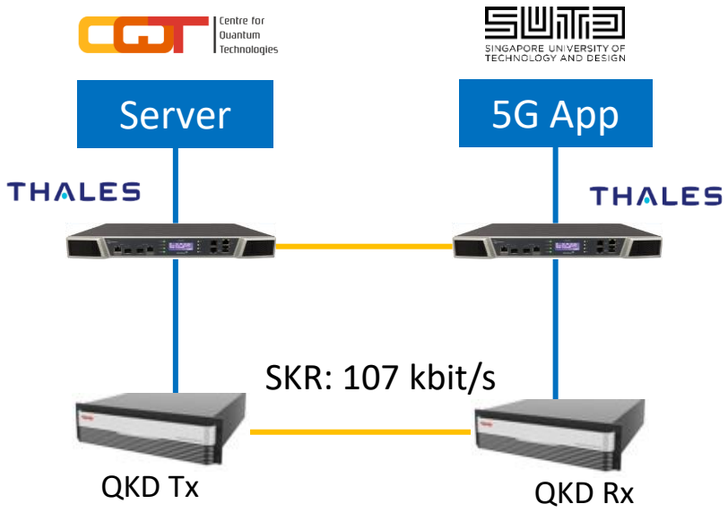


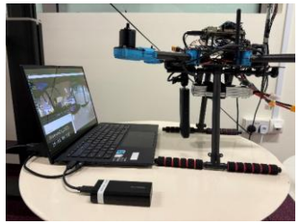


- QKD system (IDQ) operated **stably & continuously** over commercial-grade fibre (Netlink Trust)
- Demonstration of **secure data transfer** over VPN with QKD keys



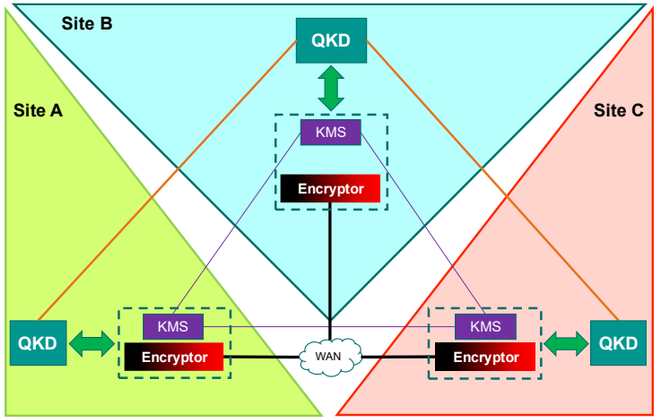
QUANTUM-SAFE 5G & GOVERNMENTAL INFRASTRUCTURE



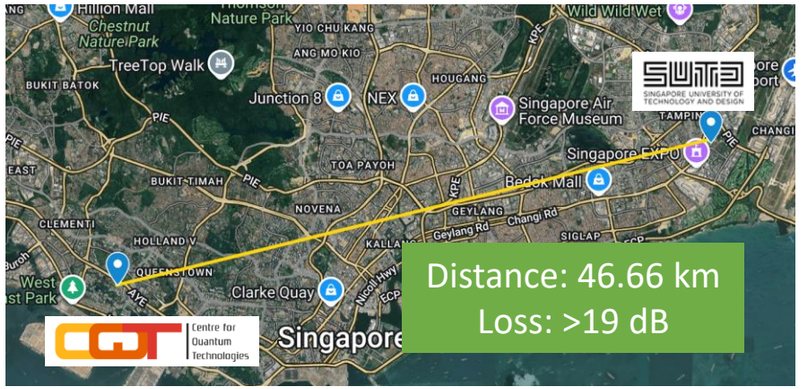


Drone & 360 Camera

Streaming



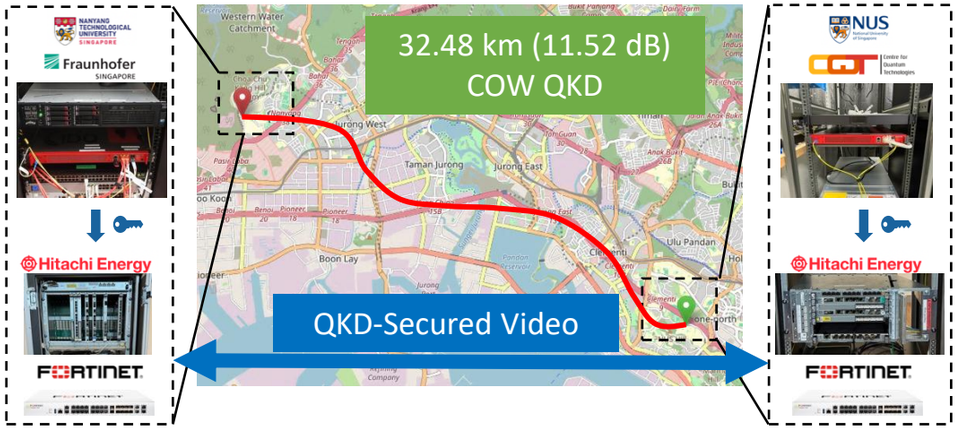
- 3-node Encryptor
- 3-node KMS
- 2 types of QKD



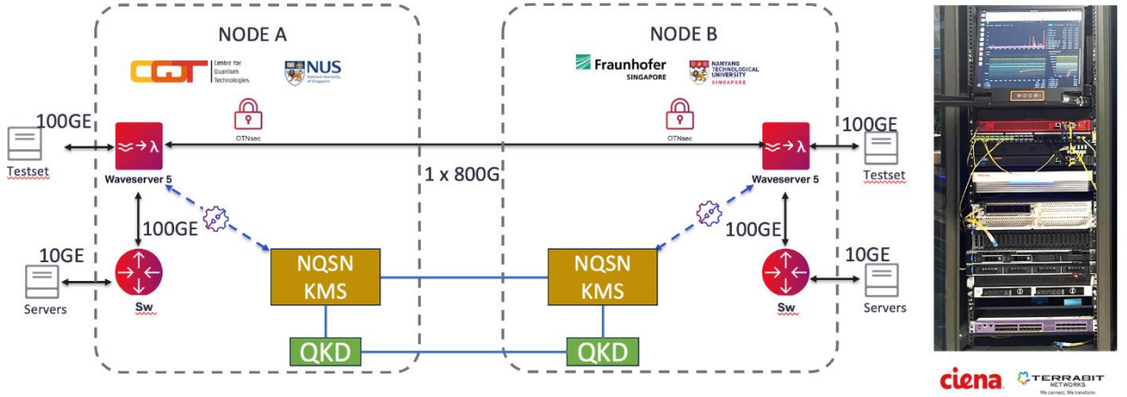
QKD/PQC-encrypted 5G Infrastructure

3-node GovTech-ST Engineering QKD-Encryption

OTHER QUANTUM-SAFE REFERENCE USE CASES

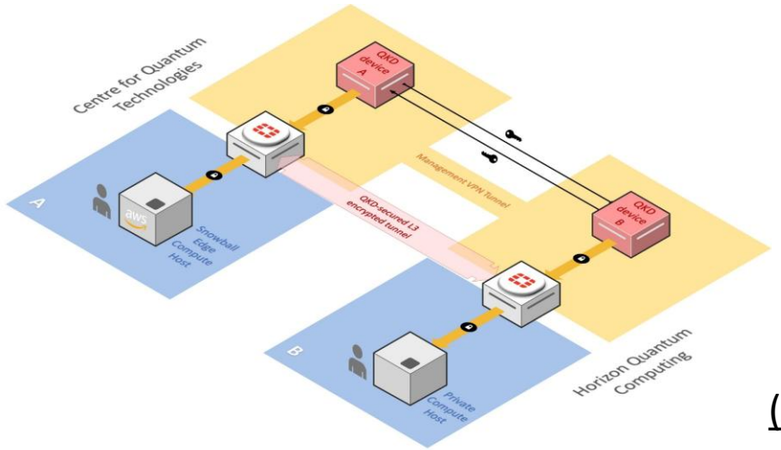


Hitachi Energy MPLS QKD Integration (L2.5)/Fortinet VPN (L3)

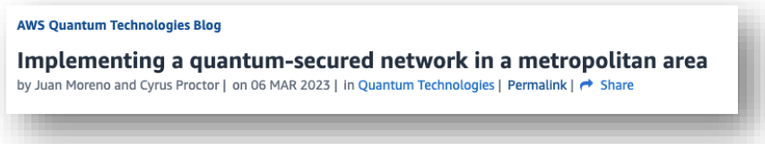


OTN Layer Quantum Encryption (Ciena L1 Encryptor)*

*In Progress



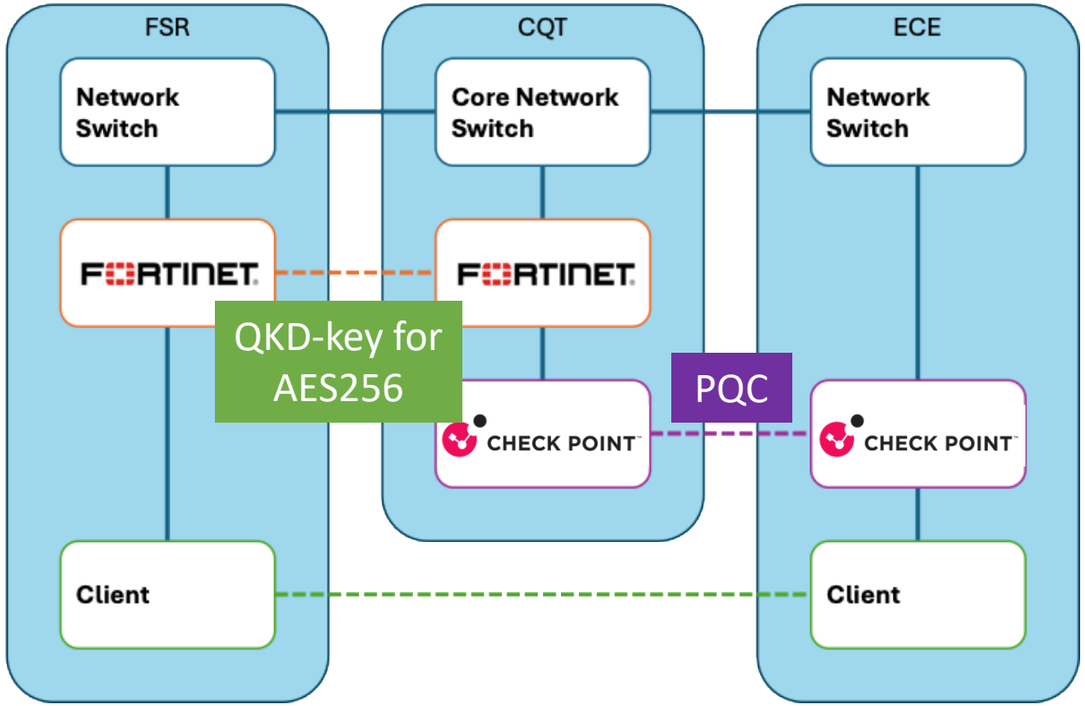
Quantum-secured VPN link
(AWS Edge Compute & Fortinet hardware)



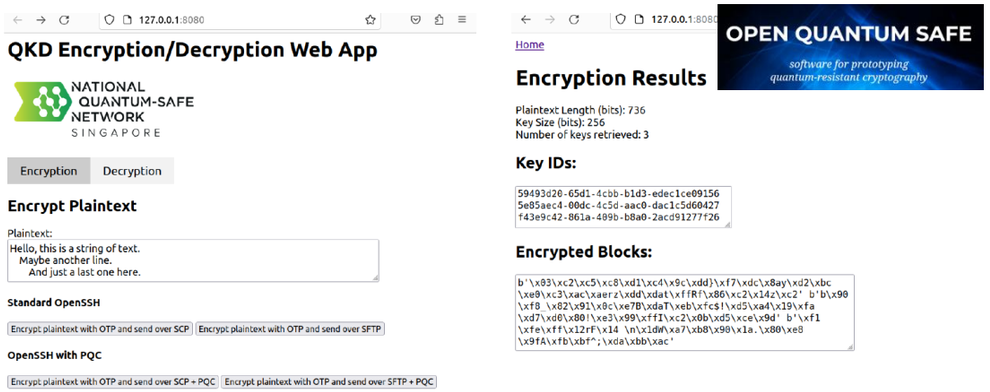
Featured on
AWS Quantum Technologies Blog

https://aws.amazon.com/blogs/quantum-computing/implementing-a-quantum-secured-network-in-a-metropolitan-area/

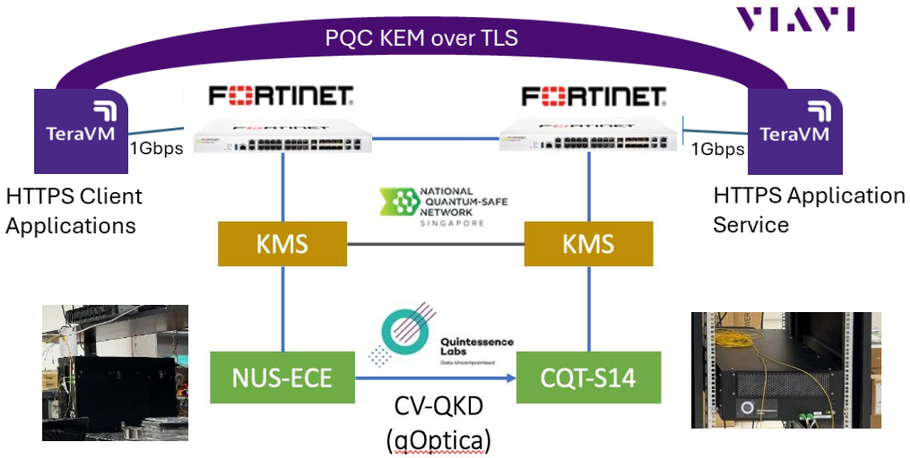
HYBRID QKD-PQC SECURED USE CASES



Hybrid QKD-PQC VPN (Fortinet, Check Point) between 3 nodes

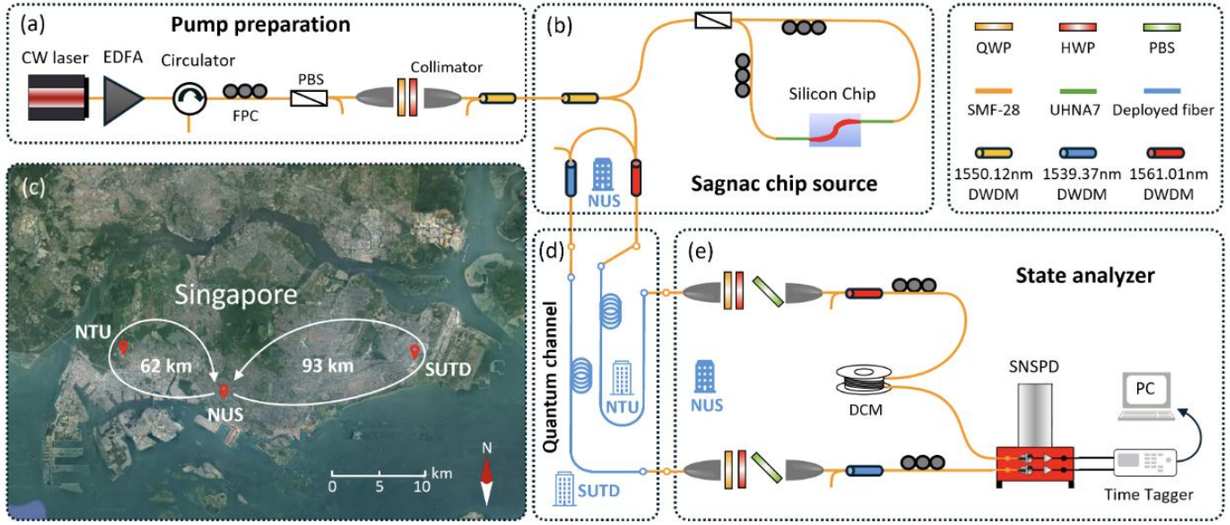


Hybrid QKD-OTP with PQC-OpenSSH Encryption

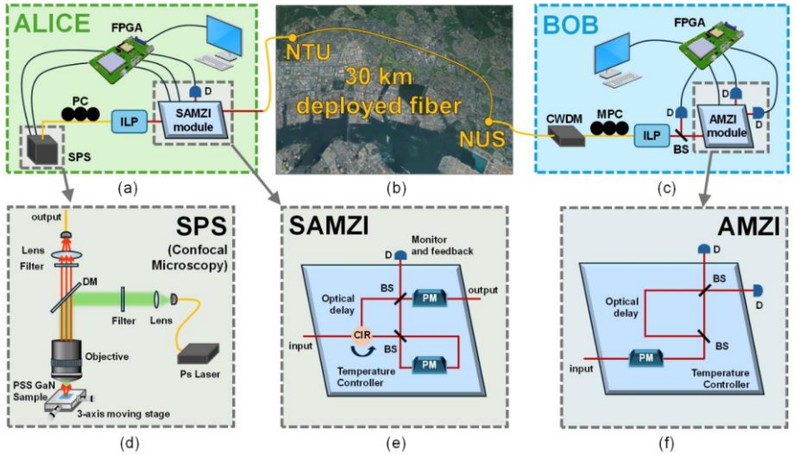


QKD-PQC Defence in Depth (QuintessenceLabs, Fortinet, Viavi)

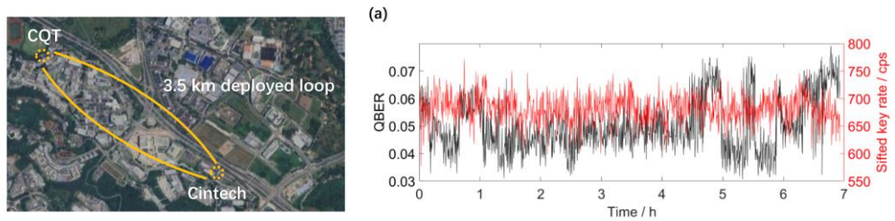
QUANTUM NETWORK RESEARCH ON NQSN TESTBED



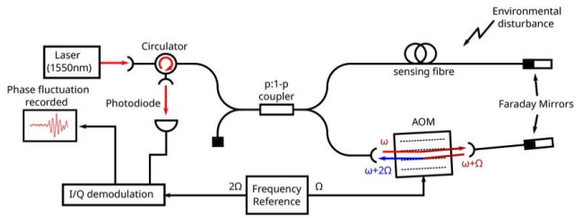
Entanglement Distribution with Silicon Photonic Chip over **155 km**



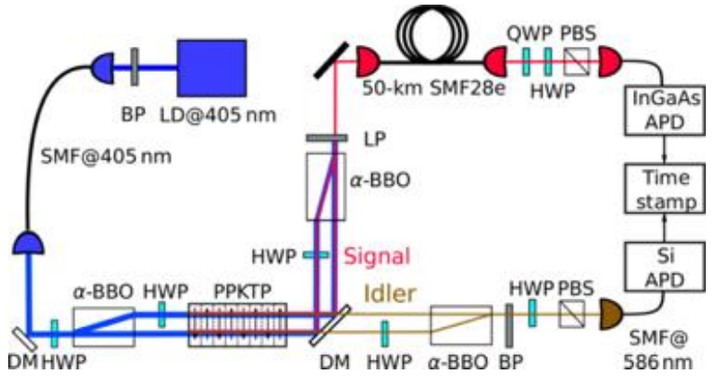
QKD with Single-photon Source



Polarization QKD With Single-photon Emitter



Interferometic Fibre-Sensing



Polarization Entangled Photon Pairs

RECENT QUANTUM-SAFE INITIATIVE IN SINGAPORE

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

Biz-Tech IMDA INFOCOMM MEDIA DEVELOPMENT AUTHORITY

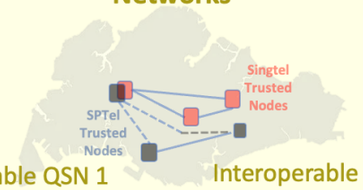
Acceleration Singapore's Quantum-Safe Transition

As global quantum adoption advances, Singapore has prioritized enabling quantum-safe solutions to stay ahead.

- **National Quantum-Safe Network Plus (NQSN+)** was launched to enable businesses to adopt quantum-safe technologies (agnostic to both QKD and PQC) in real-world applications. Builds up and mature capabilities in technical, operations and business in this area.

Key Developments:

Commercial Quantum Safe Networks



Interoperable QSN 1 (Singtel)

Interoperable QSN 2 (Sptel, SpeQtral)

A platform integrating QKD into networks

Standards Collaboration

Co-leading QKD protocol standards and interoperability

Industry Pilots and Adoption

Ongoing pilots and adoption in the industry

National Quantum-Safe Network Plus

https://www.imda.gov.sg/about-imda/emerging-technologies-and-research/national-quantum-safe-network-plus

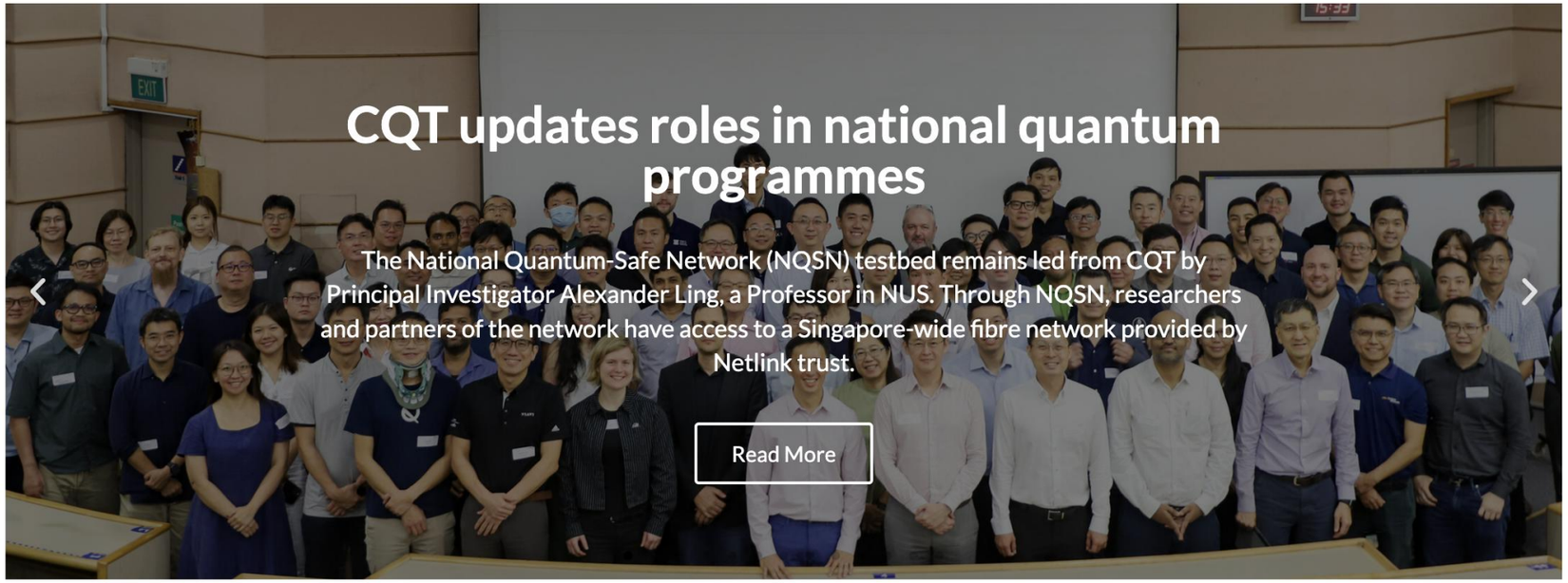
MAS Quantum-Safe Communications Sandbox

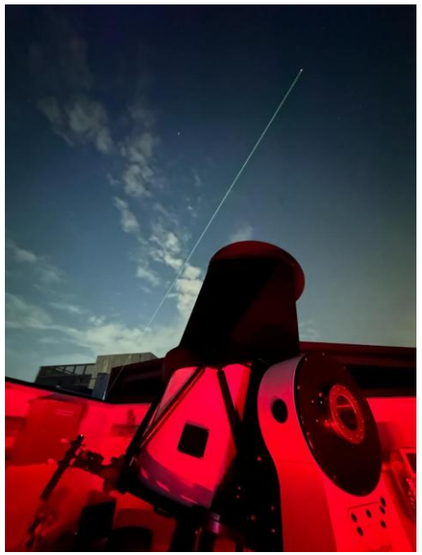
https://www.mas.gov.sg/news/media-releases/2025/mas-and-industry-partners-publish-technical-report-on-proof-of-concept-sandbox

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

ABOUT NQSN | TEAM | COLLABORATION | NEWS | PUBLICATIONS | JOIN US | Contact Us

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE





NQSN Testbed (2025-2029)

Supported by

NRF SINGAPORE | NATIONAL QUANTUM OFFICE SINGAPORE | QUANTUM ENGINEERING PROGRAMME SINGAPORE | INFOCOMM MEDIA DEVELOPMENT AUTHORITY | NetLinkTrust the fibre of a smart nation (Fibre Network)

Email: nqsn_contact@groups.nus.edu.sg

nqsn.sg