NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

Towards an Interoperable Quantum-Safe Network

National Quantum-Safe Network Testbed in Singapore

Hao Qin*

Senior Researcher

NUS ITU Focal Point

ETSI Official Contact

IMDA TSAC FA7 QCNTF Co-Chair

2024 HackTheon Sejong

Joint Conference Quantum Security Special Session

Sejong city , Korea
19 June, 2024

Centre for Quantum Technologies

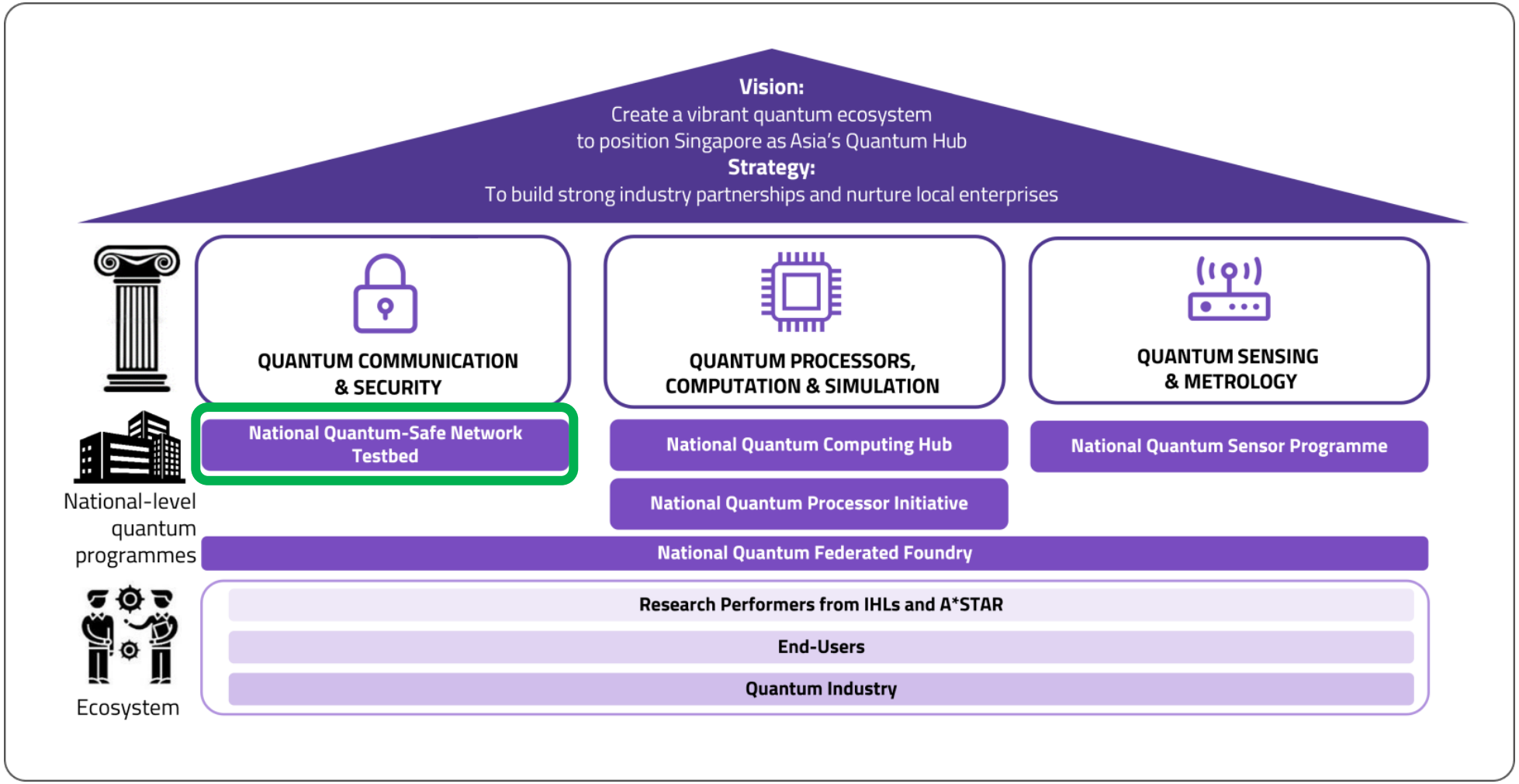
NUS National University of Singapore

Fraunhofer SINGAPORE

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

* hao.qin@nus.edu.sg

NATIONAL QUANTUM STRATEGY



[Innovation & Enterprise Partnerships - National Quantum Office (nqo.sg)]

SINGAPORE'S QUANTUM-SAFE COMMUNICATIONS INITIATIVES

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

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

2007 — Centre for Quantum Technologies

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

SPEQTRAL

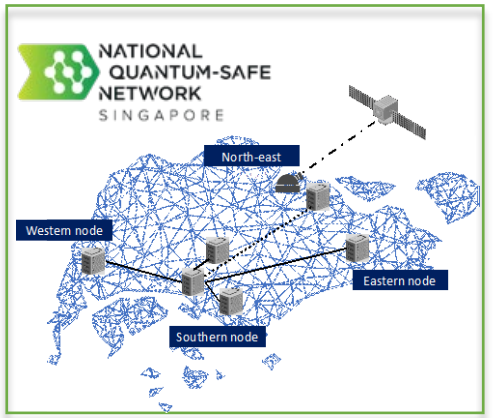
2017 — Quantum nanosatellite SpooQy-1 deployed from ISS

2019 — S15 Instruments

Entanglement-based QKD System

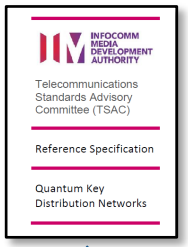
2020 — Entanglement over 10 km Metropolitan Fibre Network

Entanglement demonstration on nano-satellite



2022 — Led ITU-T work item on QKD protocol framework

2023 — Published Singapore's 1st standard on QKD Networks



Digital blueprint: vision of a quantum-safe nation in 10 years

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

Launched **NQSN+**, Southeast Asia's first quantum-safe network infrastructure

*Quantum Key Distribution (QKD)

IMPACT OF THE QUANTUM COMPUTING THREAT

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

Increasing data breaches of sensitive health & financial personal data

Threatening internet & message exchanges

Challenging the integrity of digital documents

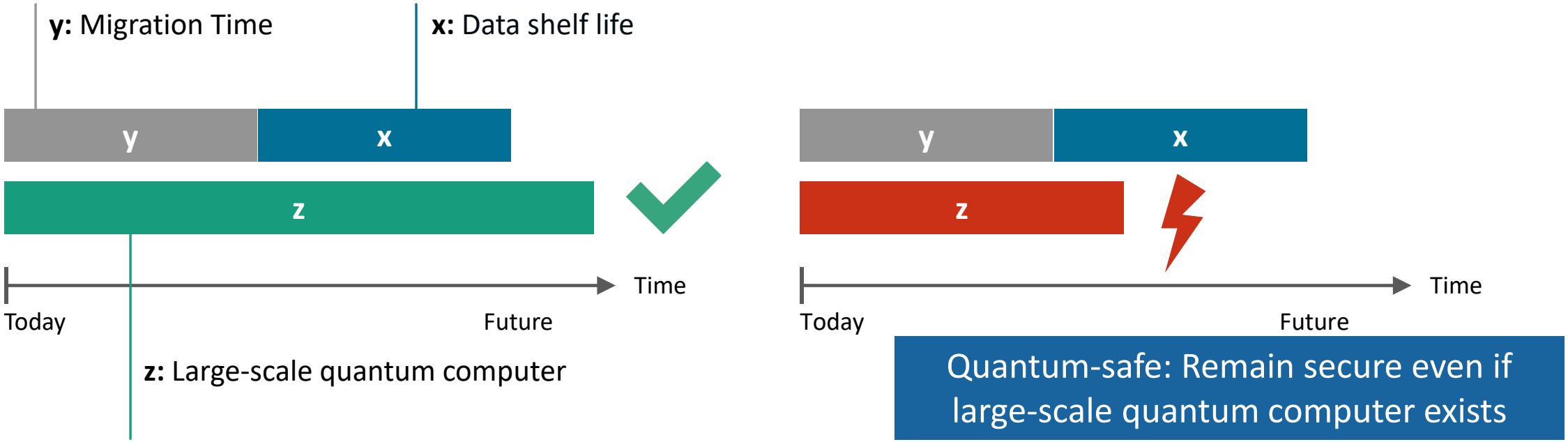
Breaking Cryptocurrencies

Risk of "harvest now, decrypt later" attacks

Act now to be Quantum-safe!

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

THE QUANTUM THREAT TIMELINE



- **The Quantum Threat is a medium/long term threat but imminent**
- Deploy (support for) quantum-safe cryptography and quantum-safe communication infrastructure in time

Mosca, Michele and Marco Piani, Quantum Threat Timeline Report 2021, Global Risk Institute, January 2022, https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

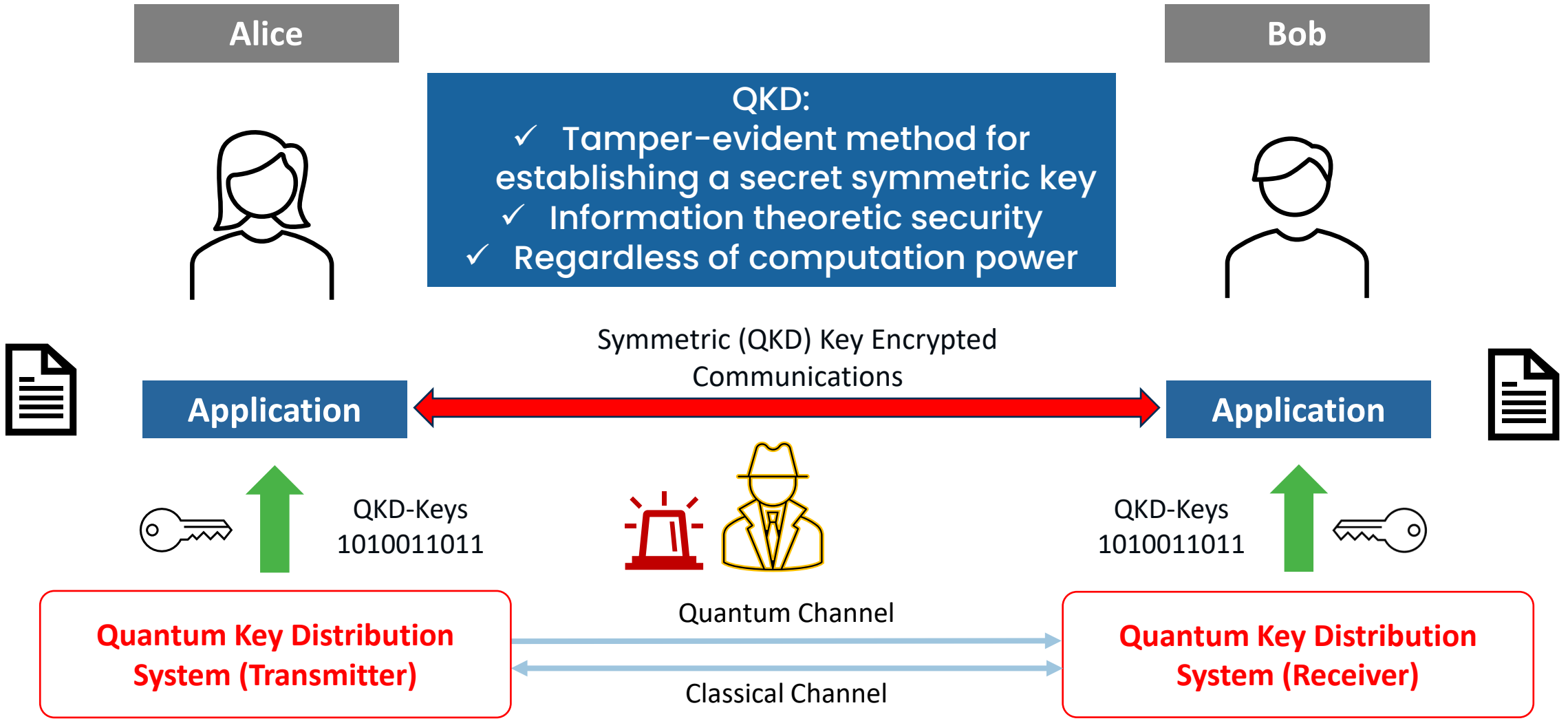
QUANTUM-SAFE TECNOLOGIES

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.
Replacing Quantum-vulnerable Asymmetric Encryption		True Randomness Source

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

QUANTUM KEY DISTRIBUTION TECHNOLOGY



QUANTUM-SAFE NETWORK TESTBED

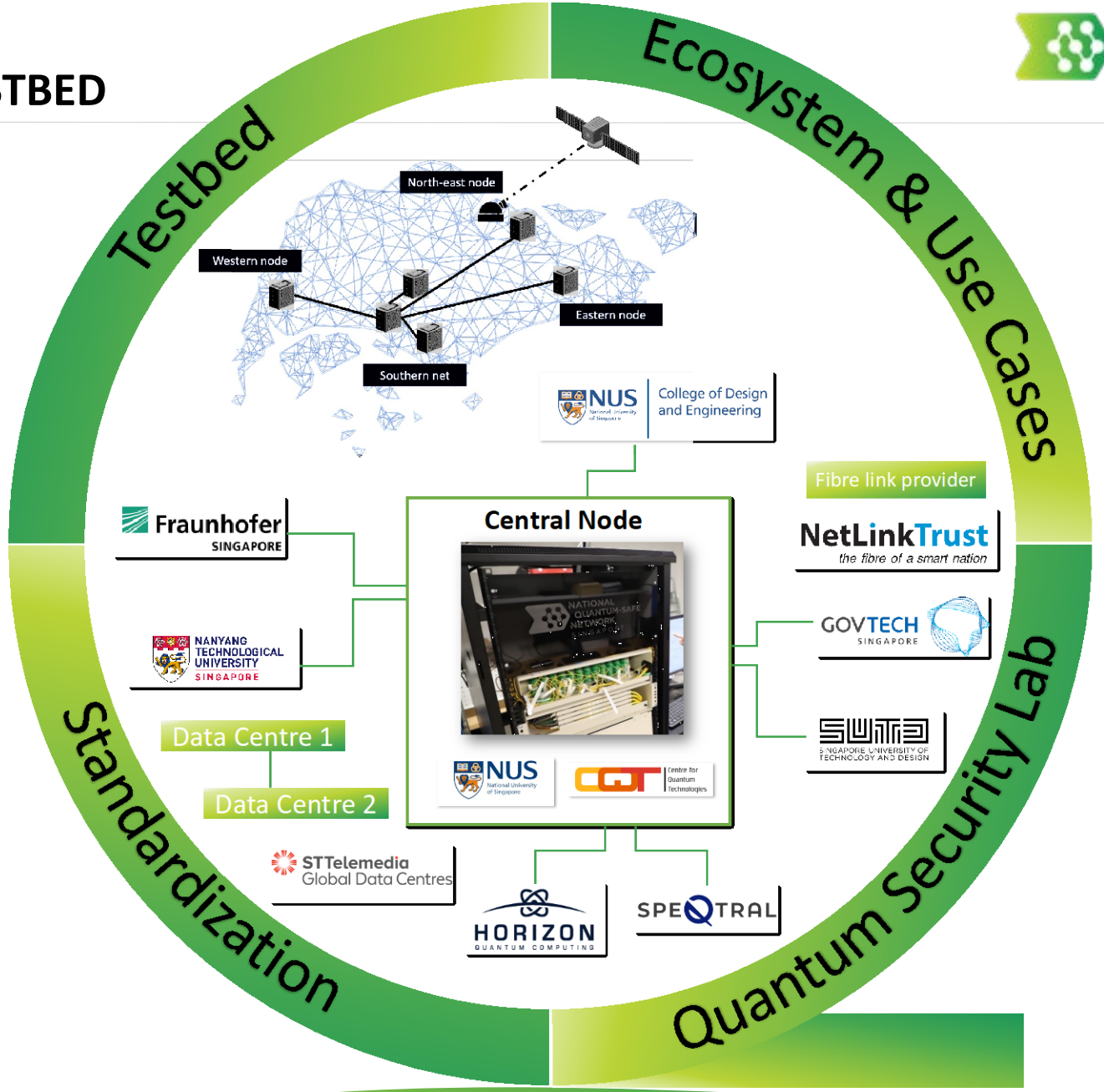
NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

PILOT INFRASTRUCTURE

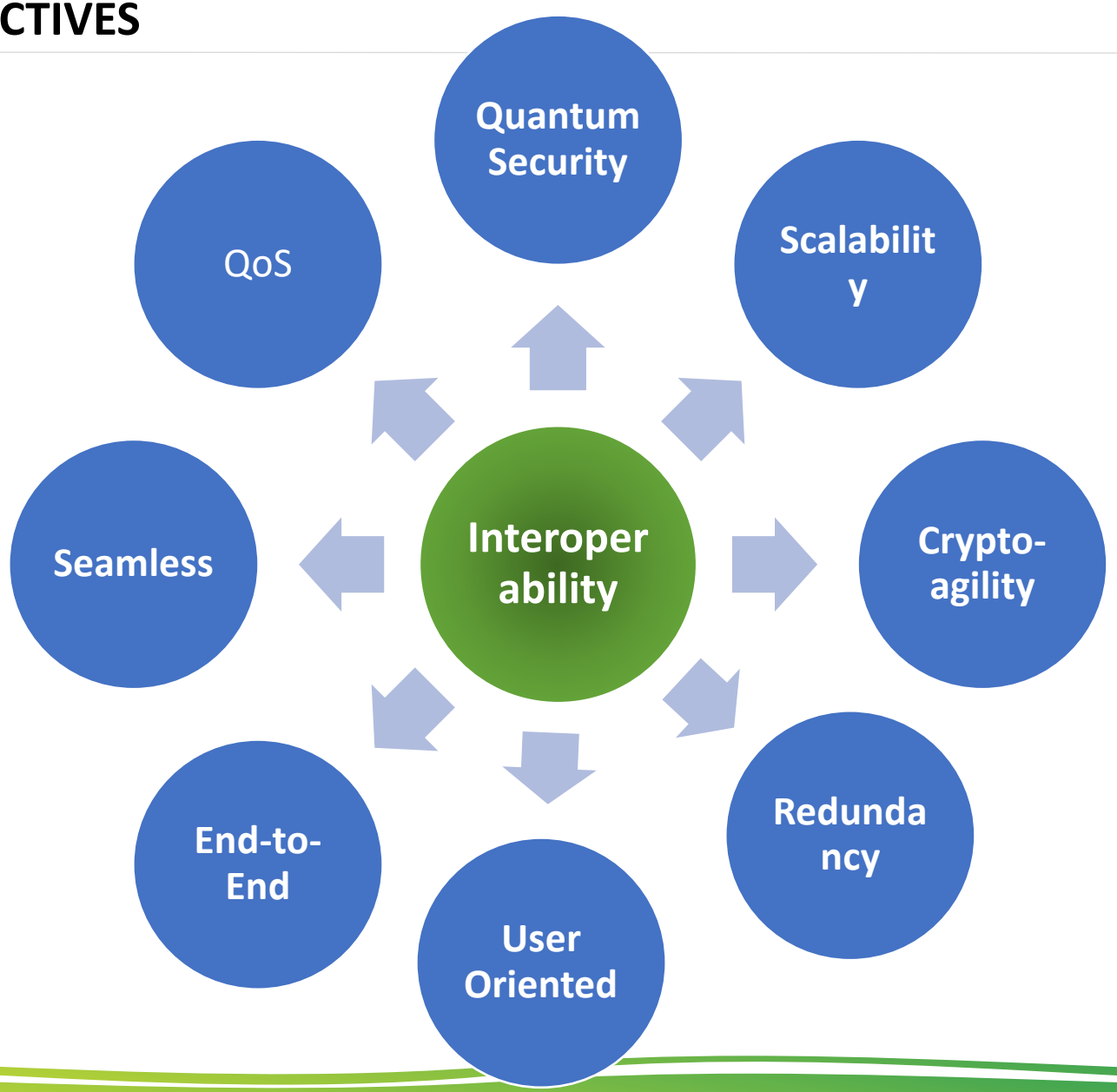
- Star-type Quantum Key Distribution (QKD) network topology
- Public-private collaborations with >20 companies & govt agencies
- **Vendor neutral** and **multiprotocol**
- Hybrid QKD/PQC (Post-quantum cryptography) approach

SECURITY FRAMEWORK & GUIDELINES

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

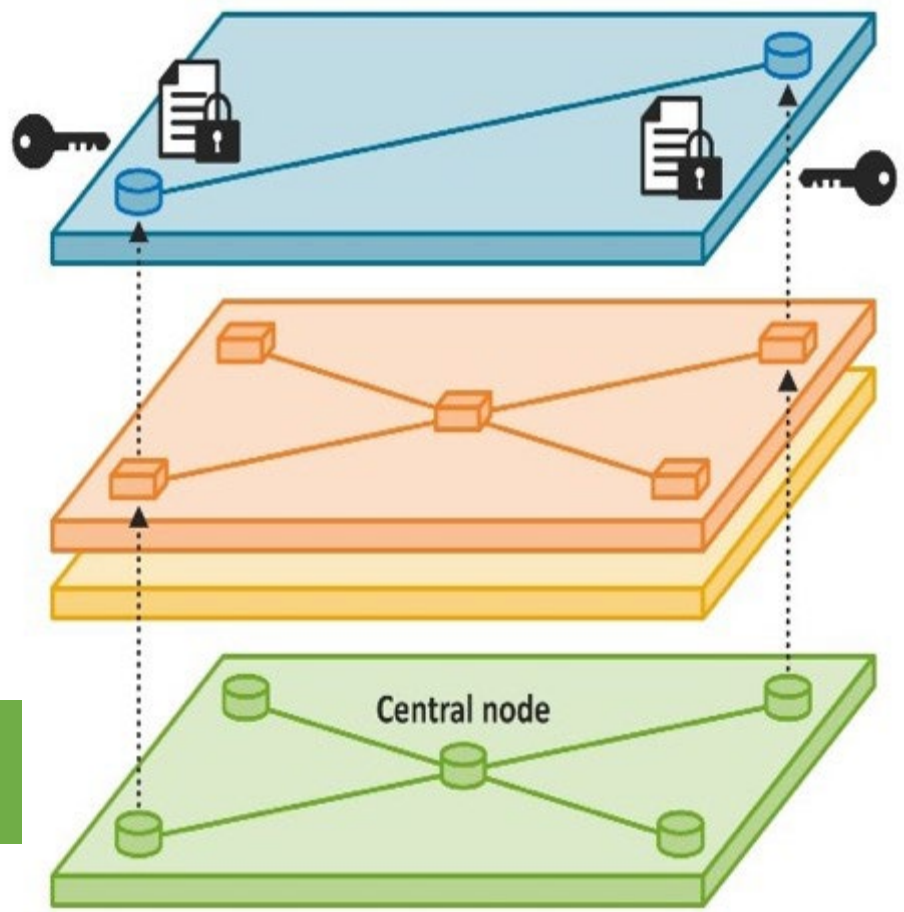


MOTIVATION & OBJECTIVES



TESTBED – DIFFERENT LAYERS IN NQSN

- Encryptors & Quantum-Safe Applications
- Interoperability
- Scalability
- Multi QKD protocol
- Production-grade link



Application layer

Network management layer

Key management layer

Quantum layer

Open Systems Interconnection (OSI) Layers

- Layer 4-7 Session Presentation Application
- Layer 3 Network
- Layer 2.5 MPLS
- Layer 2 Data Link
- Layer 1 Physical

TESTBED – QUANTUM LAYER

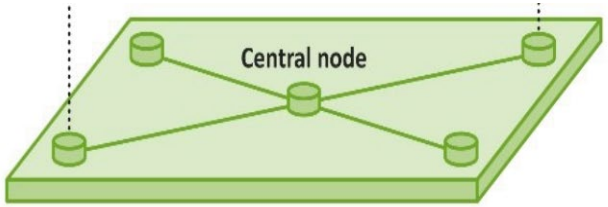
Prepare-&-Measure Discrete-Variable (DV) QKD

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

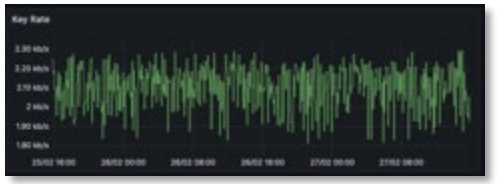
Entanglement-based (EB) QKD

*From respective public websites. Non-exhaustive list

- **Multi-protocol, vendor-neutral QKD network testbed**
- **Evaluation of DV & CV QKD protocols: BB84, COW, GMCS, BBM92 etc**



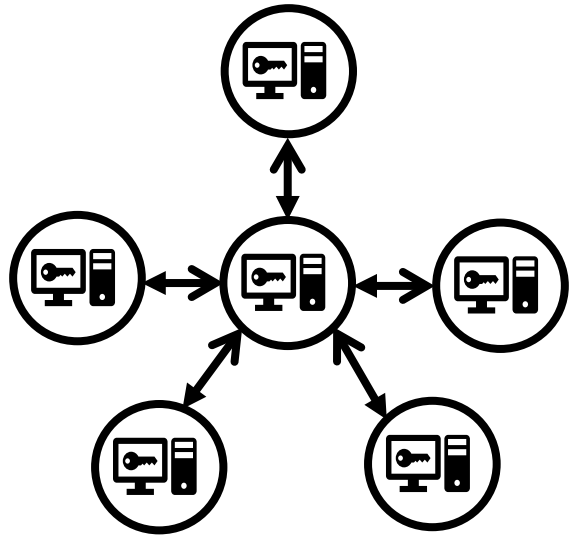
Quantum layer



TESTBED – KEY MANAGEMENT & NETWORK MANAGEMENT LAYER

Key Management Layer

- ITU-T and ETSI compliance
- **Interoperable** with different QKD providers
- Multi-input &-output key interface with high **scalability**
- Enable & integrated with PQC technology

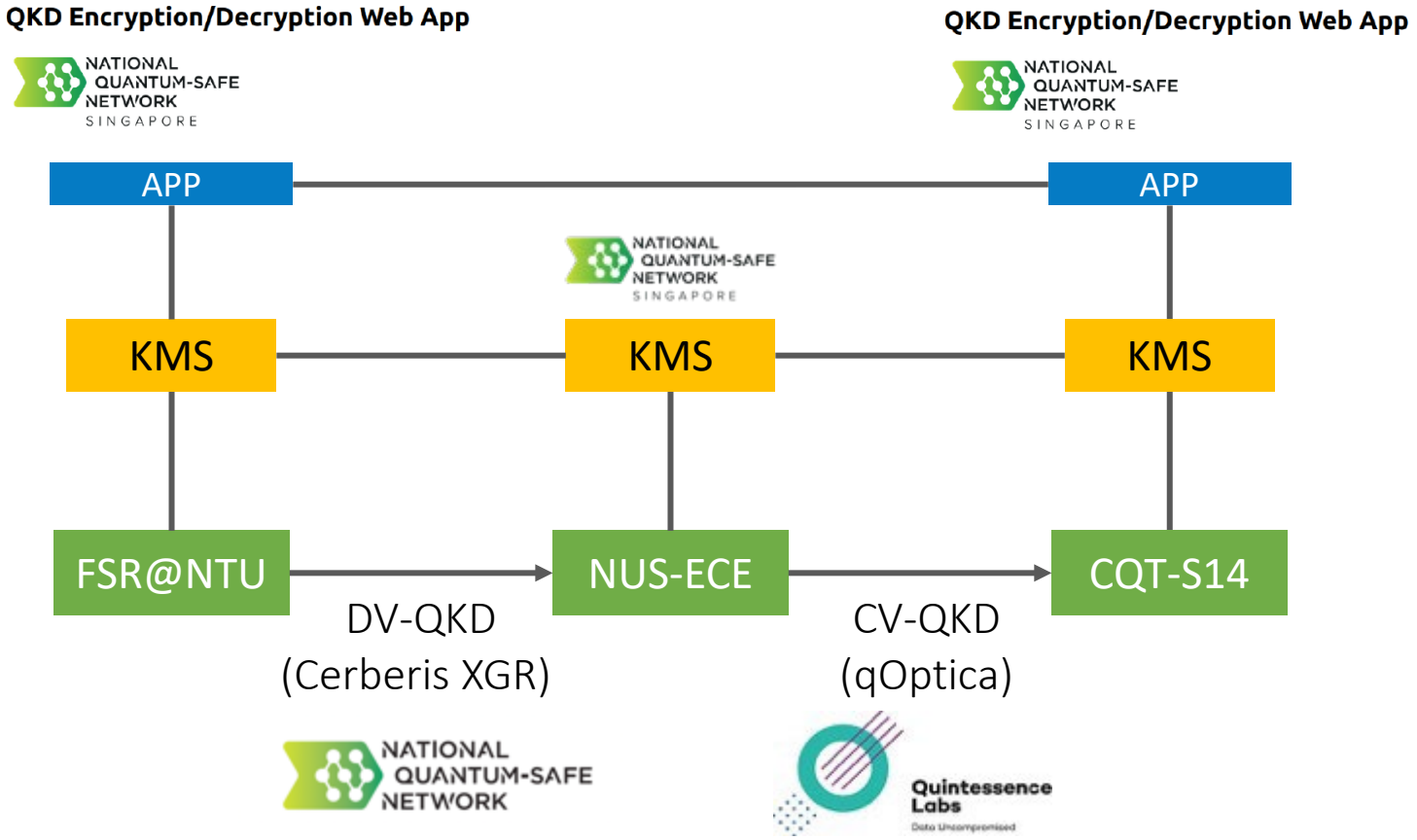


Network Management Layer

- A **centralized** network management on QKD Network (QKDN)
- Control Function:
  - Instructs the key delivery path across QKDN
  - Configure network components
  - Resource optimization
- Management functions
  - QKDN monitoring
  - Quality of Service (QoS)
  - Fault detection & reporting

KEY MANAGEMENT SYSTEM & PoCs

NQSN Key Management System



- ✓ Key relay over 3 nodes with NQSN QKD-PQC Web Application
- ✓ End-to-End symmetric QKD key encryption (AES)

Multi-hops, Multi-vendor KMS

evolution

Key Management layer

- ❑ Quantum Key Management for multi-hops (5 nodes), multi-vendor QKDs (DV, CV, EB, QKD Sim) with evolutionQ Basejump software

Symmetric Key Distribution

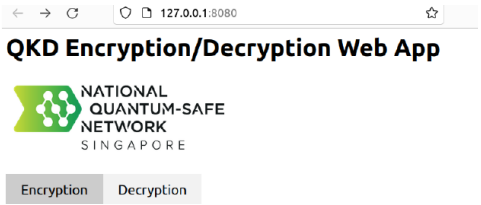
Quantum Bridge

DSKE Protocol

- ❑ Distributed Symmetric Key Exchange (DSKE) Protocol on NQSN Testbed based on secret sharing

TESTBED – APPLICATIONS LAYER

- ✓ NQSN **Quantum-safe software**
  - One-Time Pad (OTP) & PQC secured data transfer
- ✓ Quantum-secured **VPN**
  - Fortinet Firewall L3 Appliances
- ✓ Quantum-secured **video surveillance**
  - Hitachi Energy L2.5 Hardware Encryptor
- ❑ GovTech **data link** quantum Encryption
  - ST Engineering L2 encryptor
- ❑ Quantum-encrypted **5G infrastructure**
  - Thales SENETAS L2 encryptor on SUTD 5G Testbed
- ❑ **OTN Layer** quantum encryption
  - Ciena L1 hardware encryptor



NQSN OTP-PQC Software

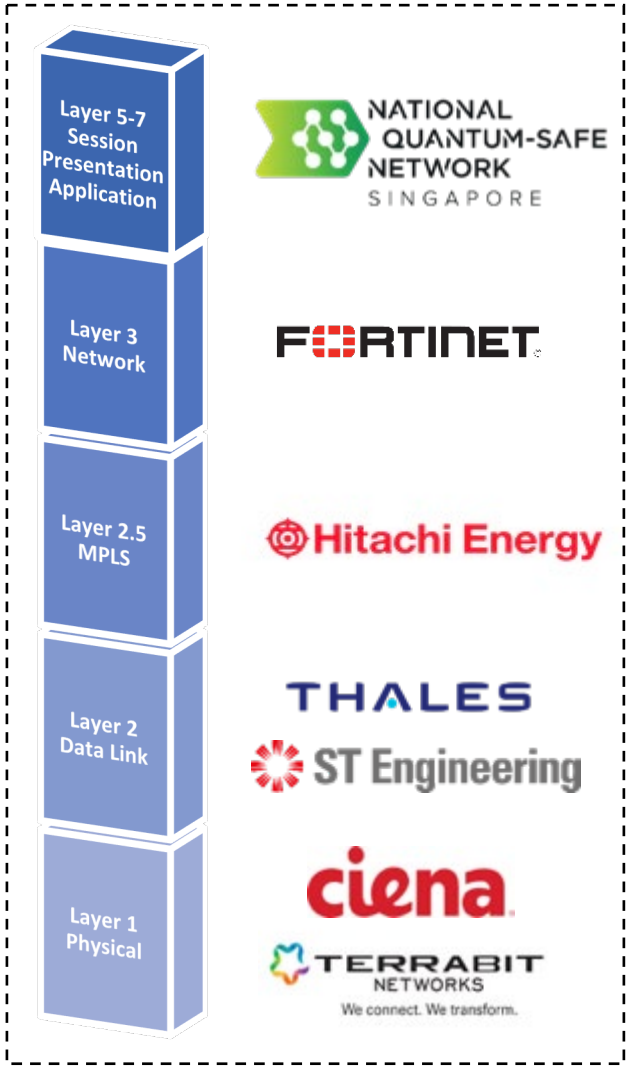
Fortinet FGT-100F

Hitachi FOX615 Encryptor

Thales SENETAS

Ciena Waveserver 5

OSI Layers



USE CASES – QKD LINK IN NQSN TESTBED

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

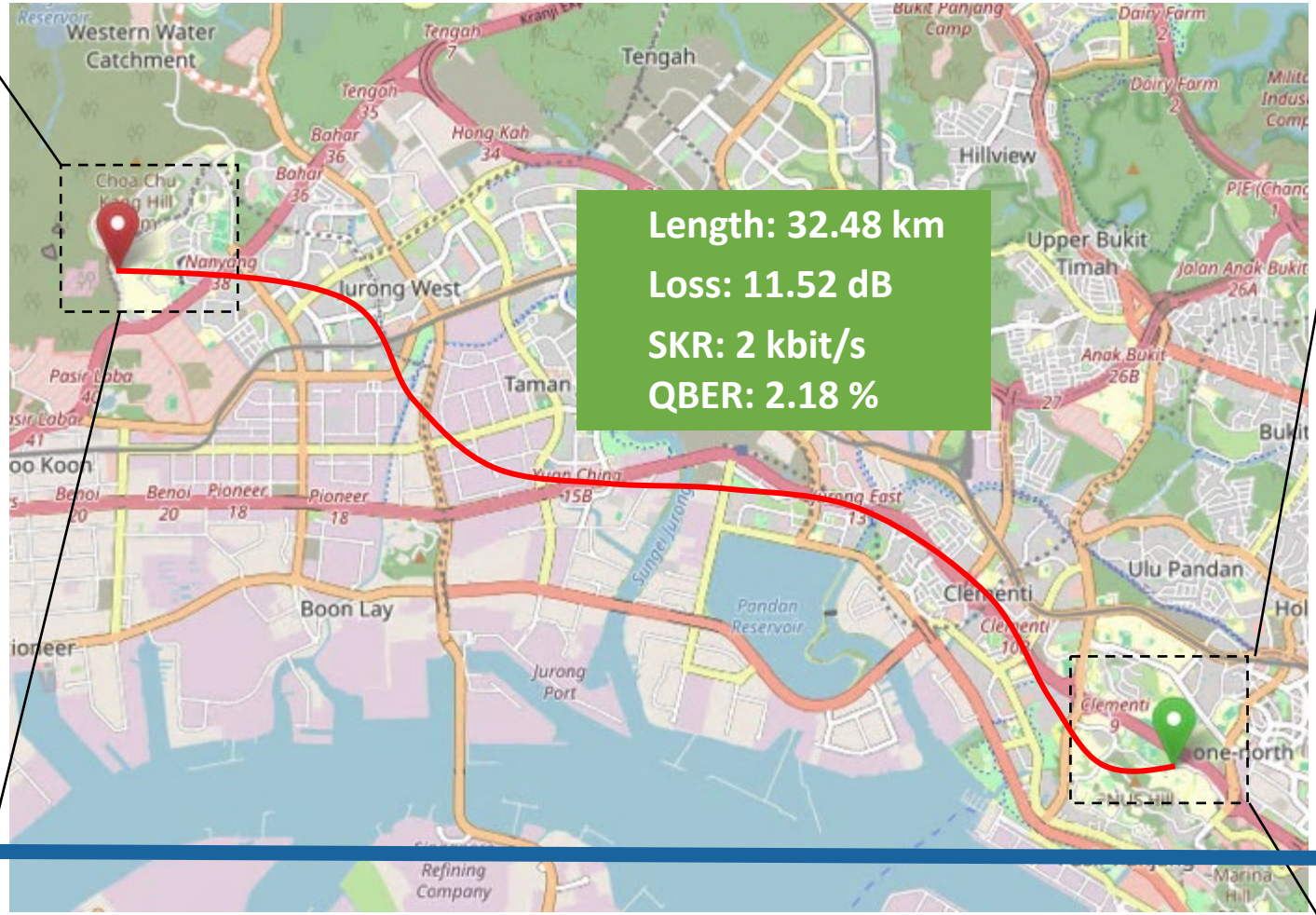
NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Fraunhofer SINGAPORE

QKD Key

Hitachi Energy

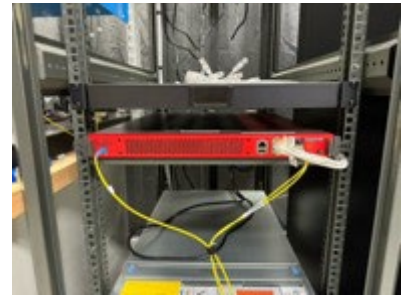
FORTINET



- QKD-secured Video app demo (Hitachi & Fortinet)
- Fully commercial-off-the-shelves equipment

NUS National University of Singapore

CQT Centre for Quantum Technologies



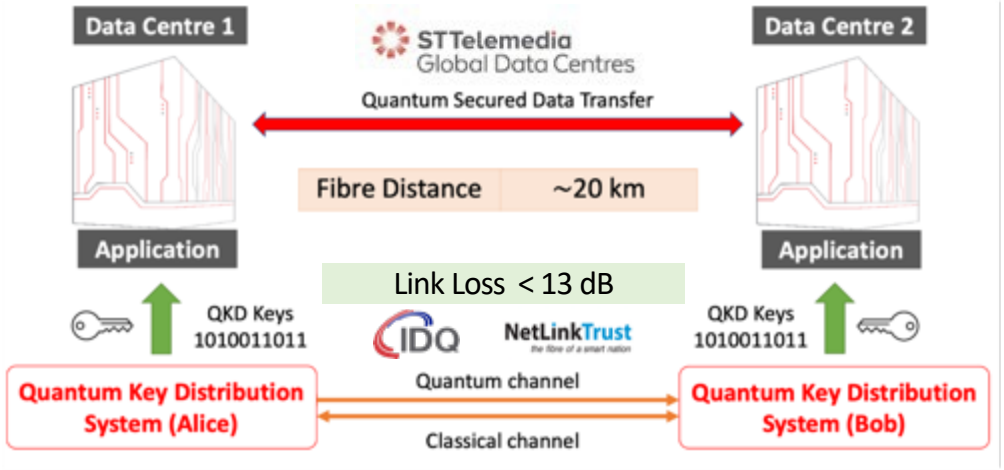
QKD Key

Hitachi Energy

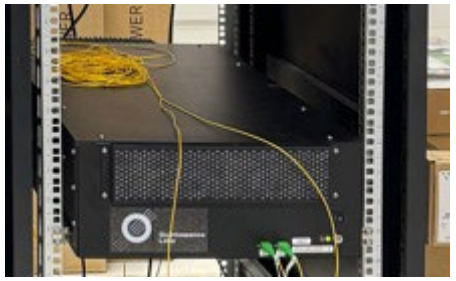
FORTINET

USE CASES – REFERENCE APPLICATIONS

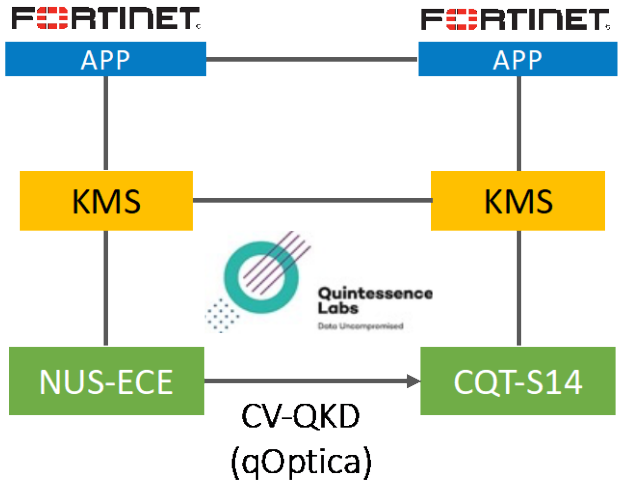
QKD-secured Data Centre Interconnect (STT-GDC)



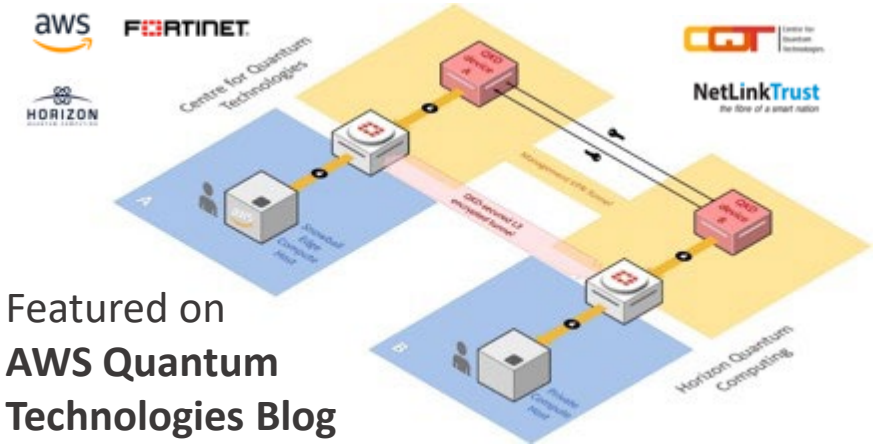
Continuous-Variable QKD with Application (QLabs & Fortinet)



Secret Key Rate
40 kb/s



Quantum-Secured VPN (AWS-Fortinet-Horizon QC)



Featured on
AWS Quantum Technologies Blog

Presentation at **Q2B 22**

QKD over Diverse Fibre Network (SpeQtral-ST Eng-SpTel)

SPTel, SpeQtral and ST Engineering Held Successful Trial for Quantum-Secure Networks to Enable Robustly Secure Digital Communications

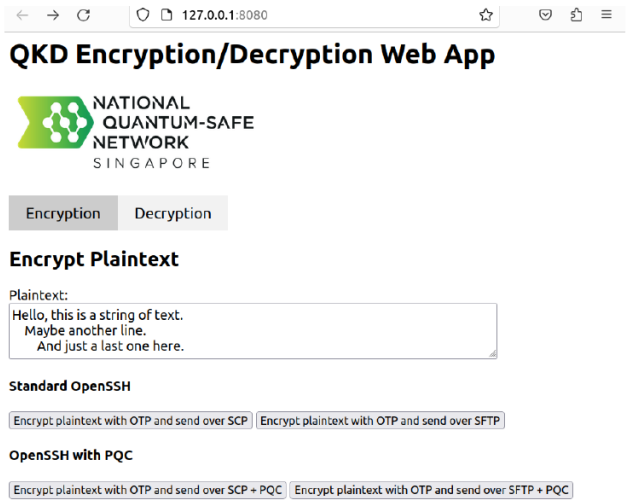
SINGAPORE – 10 November 2022 – SPTel and SpeQtral announced today their success on initial trials toward setting up Quantum-Secure Networks on SPTel's diverse fibre network, in the first among such trials in Singapore. SpeQtral conducted the trial using ST Engineering's quantum-enabled encryptors and Toshiba Digital Solutions' ("Toshiba") Quantum Key Distribution ("QKD") system over SPTel's diverse fibre network. The successful trial paves the way for robustly secure digital communications.

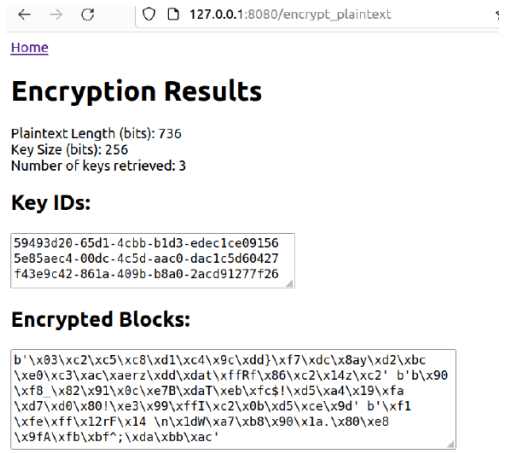
NQSN Advisory

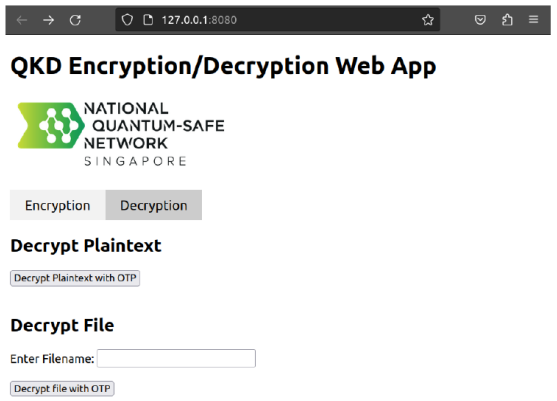
USE CASES – NQSN HYBRID QKD-PQC APPLICATION

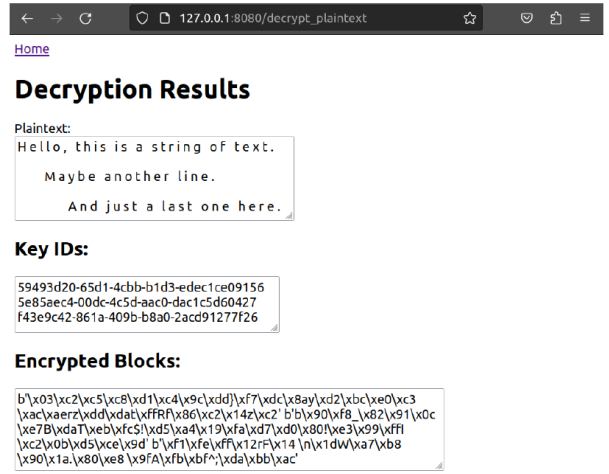
Hybrid Quantum Safe application

- **Two-layer quantum safe encryption**
- One Time Pad (OTP) encryption with QKD keys plus Quantum-safe OPEN-SSH*
- Kyber for key exchange (NIST Post quantum cryptography standard selection) + AES encryption
- **For short messages & high confidentiality use cases**



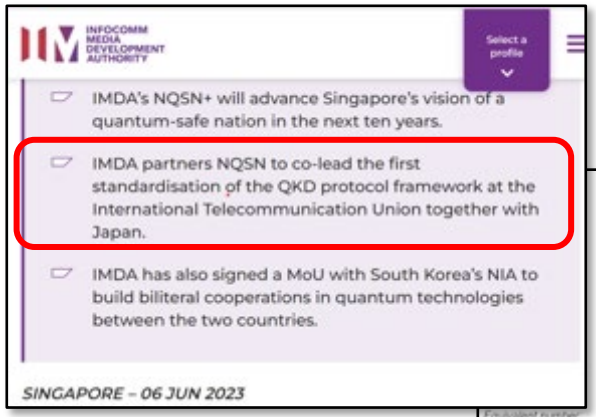


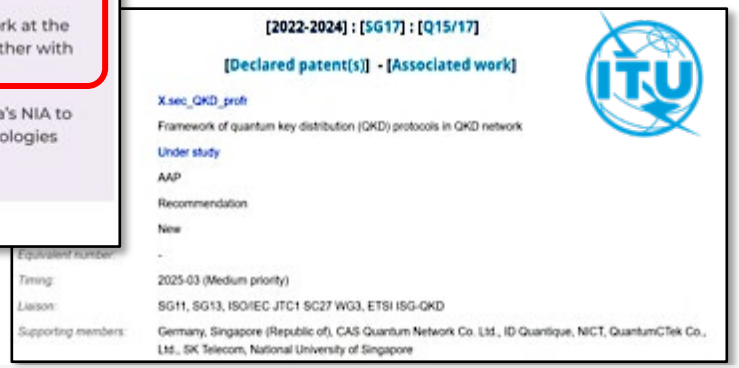


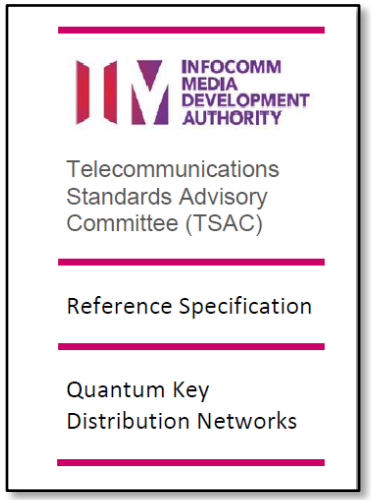


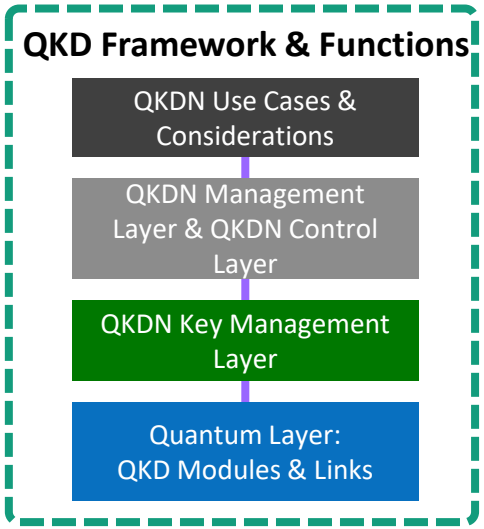
*SSH | Open Quantum Safe (openquantumsafe.org)

STANDARDISATION – INTERNATIONAL & LOCAL









IMDA RS

❑ International standards

1. Led and established the work item for **1st standard on QKD protocol framework** in ITU-T
2. Liaison officer ISO/IEC 23837: Security requirements, test and evaluation methods for quantum key distribution; Editor: ISO/IEC PWI 22061: Investigation of the effect of transmission media on QKD security evaluation and possible modifications to ISO/IEC 23837
3. Participation & Contribution in ITU-T SG17, SG 13, SG11, JCA-QKDN; ETSI ISG QKD; ISO/IEC JTC1 SC 27

❑ Local standards

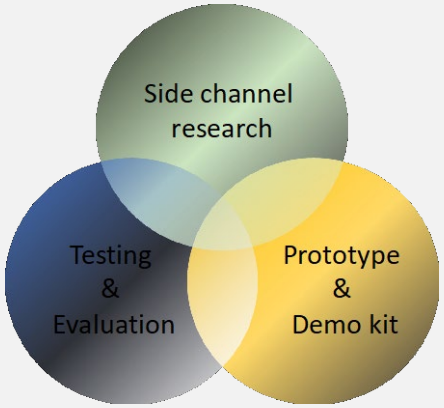
1. IMDA TSAC **Quantum Communications Network Task Force**, with chairs & editors from NQSN, consolidated the contributions from 20 partners
2. Singapore's **1st standard (Reference Specification)** on **QKD Networks** published, with high level descriptions of QKDN & aligned with SDOs on QKDN, e.g.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

STANDARDZATION EVENTS HOSTED BY NQSN/CQT

- ✓ Q15/17 interim meeting in 11/2022
- ✓ Q15/17 interim meeting in 06/2023

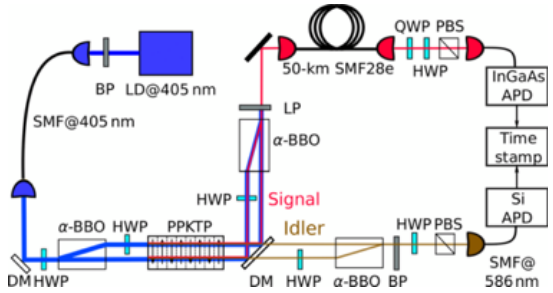
* In partnership with IMDA

QUANTUM SECURITY LAB

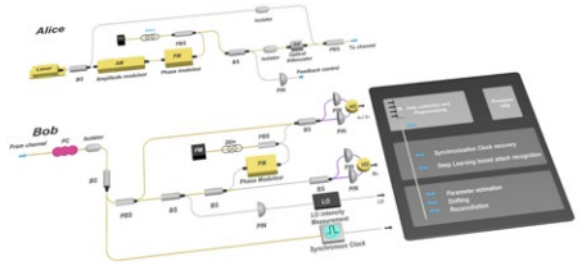


Functionality & Security Evaluation on QKD Module & QKD Networks

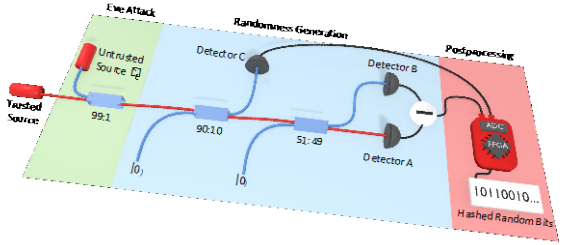
NQSN reviewed Germany BSI's "Implementation Attacks against QKD Systems"



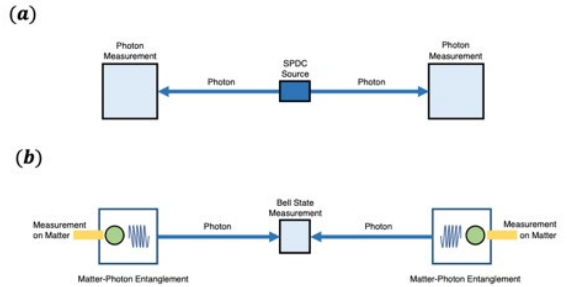
Physical Review Applied, *18*(4), 044075 (2022)



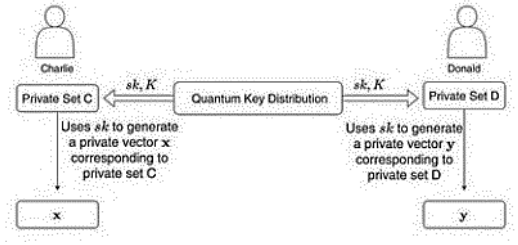
Physical Review A 105, 042411 (2022)



AQIS 2023 & *IPS* 2023



Quantum, *7*, 932 (2023)



IEEE Internet of Things Journal (2023)

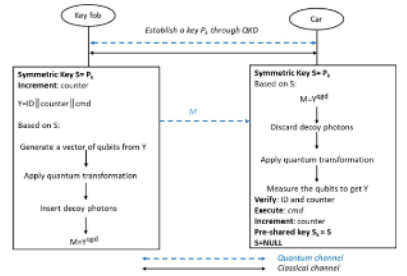
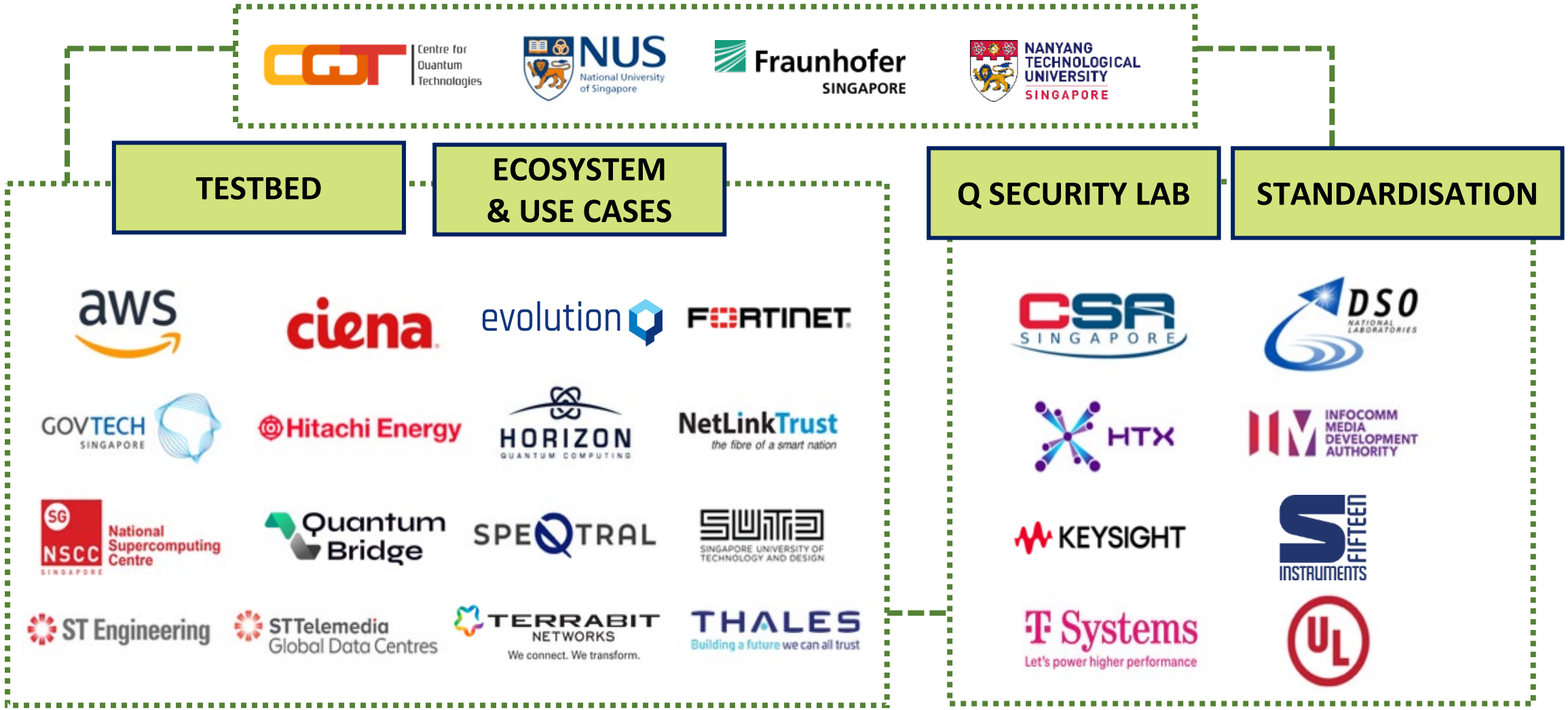


Fig. 1: The key fob authentication phase.

IEEE 98th Vehicular Technology Conference (2023)

ECOSYSTEM – NQSN PARTNERS & COLLABORATORS (2024)

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE



ECOSYSTEM – INTERNATIONAL & LOCAL

AsiaTech x SG (Jun 2022)


MCI visit to CQT (Oct 2022)

SGI Quantum Safe Workshop (Nov 2022)


ETSI-IQC Quantum Safe Cryptography (Feb 2023)


ITU-T QKD Workshop (Nov 2022)

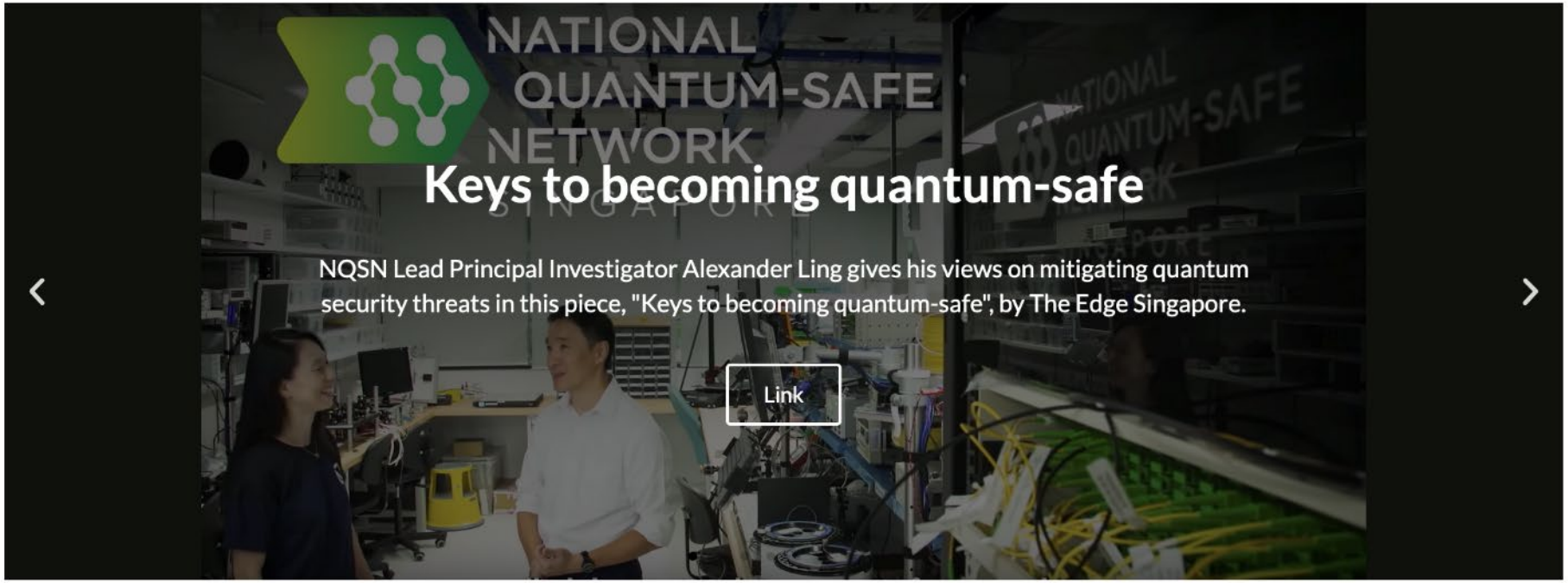

IMDA Brown Bag (Mar 2023)

1st SG Quantum Industry Day (Feb 2023)

Quantum.Tech APAC (Apr 2023)


49th ECOC (Oct 2023)

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE



NQSN

nqsn.sg

IMDA RS

IMDA RS QKDN