QUANTUM CYBER SECURITY

Quantum Cryptography Technology
Migration Strategy and Global use cases.

Sangyun Uhm

25/06/2024

01

About us

ID Quantique

Founded in 2001

Geneva, Switzerland
Seoul, Bundang, South Korea
Boston, USA

By 4 quantum physicists from the University of Geneva

120+ employees, including 50 engineers/scientists

Investments in 2018 by SK Telecom & Deutsche Telekom

Develops technologies and products based on quantum physics within 2 business units:

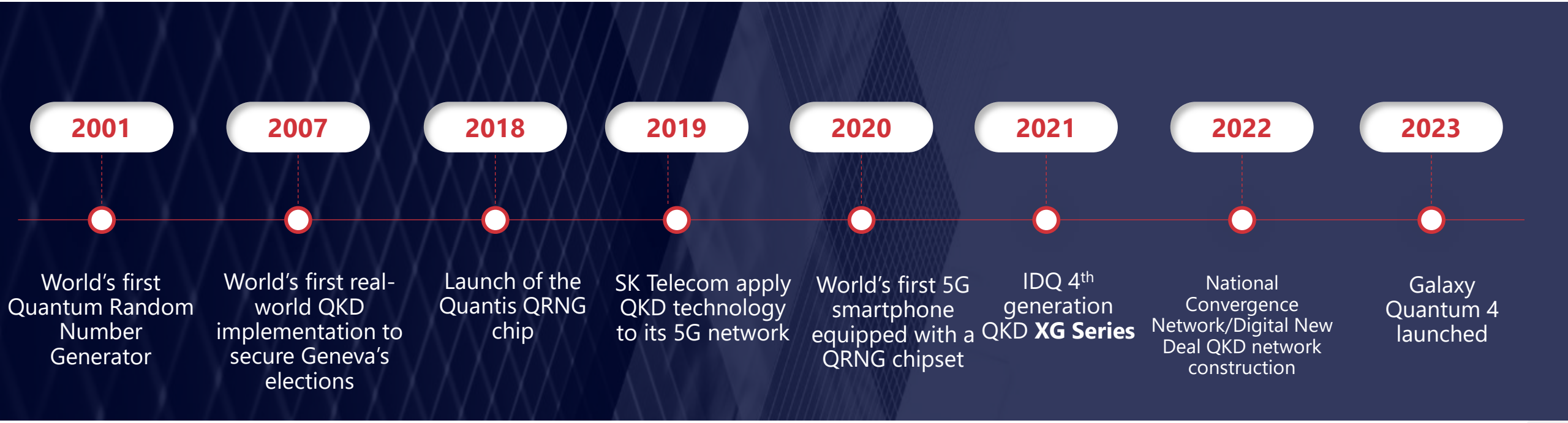
- Quantum-Safe Security
- Quantum Photonic Sensing

Performs R&D, production, professional services, integration, support

Clients: Governments / Banks / Gaming Industry / Universities / IT Security

ID Quantique – 23 years of experience, innovation & trust

Global leader in quantum randonmness and security solutions



Quantum-Safe Security

Quantum Cyber Security tools to enable unbreakable communications

QRNG

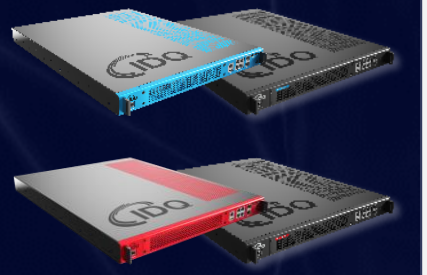
Quantum Random Number Generation

- USB
- PCIe card
- Appliance
- Chips

QKD

Quantum Key Distribution

- For commercial production environments
- For academia, research institutes & innovation labs



Selected Case Studies

- Samsung Galaxy Quantum 5G smartphones, powered by QRNG

- First nation-wide QKD network in Korea, linking 48 government organizations over 800 km

Quantum Sensing

Enabling Quantum Technologies
through Photonic Sensing Solutions

Low-light level sensing

SPADs & SNSPDs

Precision timing & control

Time Controller & Pulsed Lasers

Selected Applications

- Quantum Communications
- Photonic Quantum Computing
- Integrated Circuit Inspection
- Fluorescence Lifetime Measurement

02

Quantum Computer Opportunities and Risks

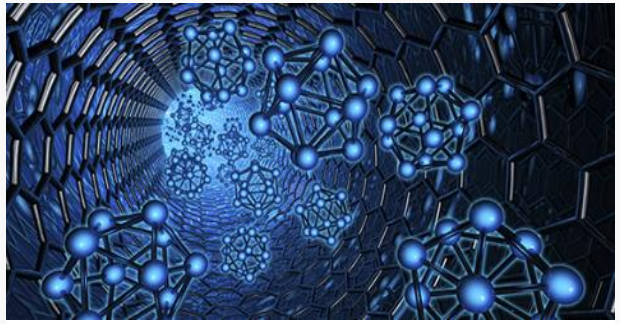
Quantum Computer Opportunities and Risks

Quantum Vs Classical

1st Flight of Wright Flyer I
December 17, 1903

Horsepower
December 17, 1903

A new realm of possibilities



Material Design

Cryptography

Big Data

Weather Services

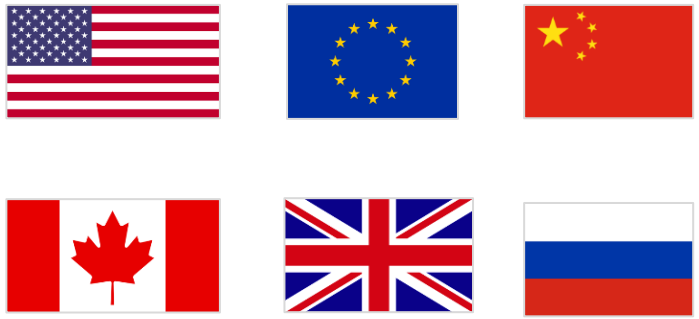
Chemistry

Machine Learning

The Quantum race is on

Public initiatives

Global quantum effort



Private initiatives

Private quantum computing firms (not exhaustive)

IBM, Google, Microsoft, aws, Atos, intel, D-Wave, IONQ, ORCA Computing, 本源量子 ORIGIN QUANTUM, PASQAL, QUANDELA, QUANTWARE, QUANTINUUM, rigetti, 图灵量子 TURINGQ, XANADU, PsiQuantum, QILIMANJARO QUANTUM TECH

Quantum Technology Monitor 2024 overview (1/2)

Private and corporate funding for QT start-ups slowed from prior years, while a strong flow of public funding was announced by several governments, totaling ~$42 billion. The ecosystem continues to progress toward unlocking an estimated economic value of ~$2 trillion by 2035.

+XX% Compared to previous year

Investments and ecosystem

$8.5B +25% YOY
total cumulative global QT start-up investment

367 +5% YOY
start-ups in the QT ecosystem

$42B +26% YOY
total government investment announced

Quantum technology market size scenarios for 2035 and 2040

Based on existing development road maps and assumed adoption curve

	Quantum computing	Quantum communication	Quantum sensing
2035	$28B–$72B	$11B–$15B	$0.5B–$2.7B
2040	$45B–$131B	$24B–$36B	$1B–$6B

Potential economic value from quantum computing in 2035

~$0.9T–$2T

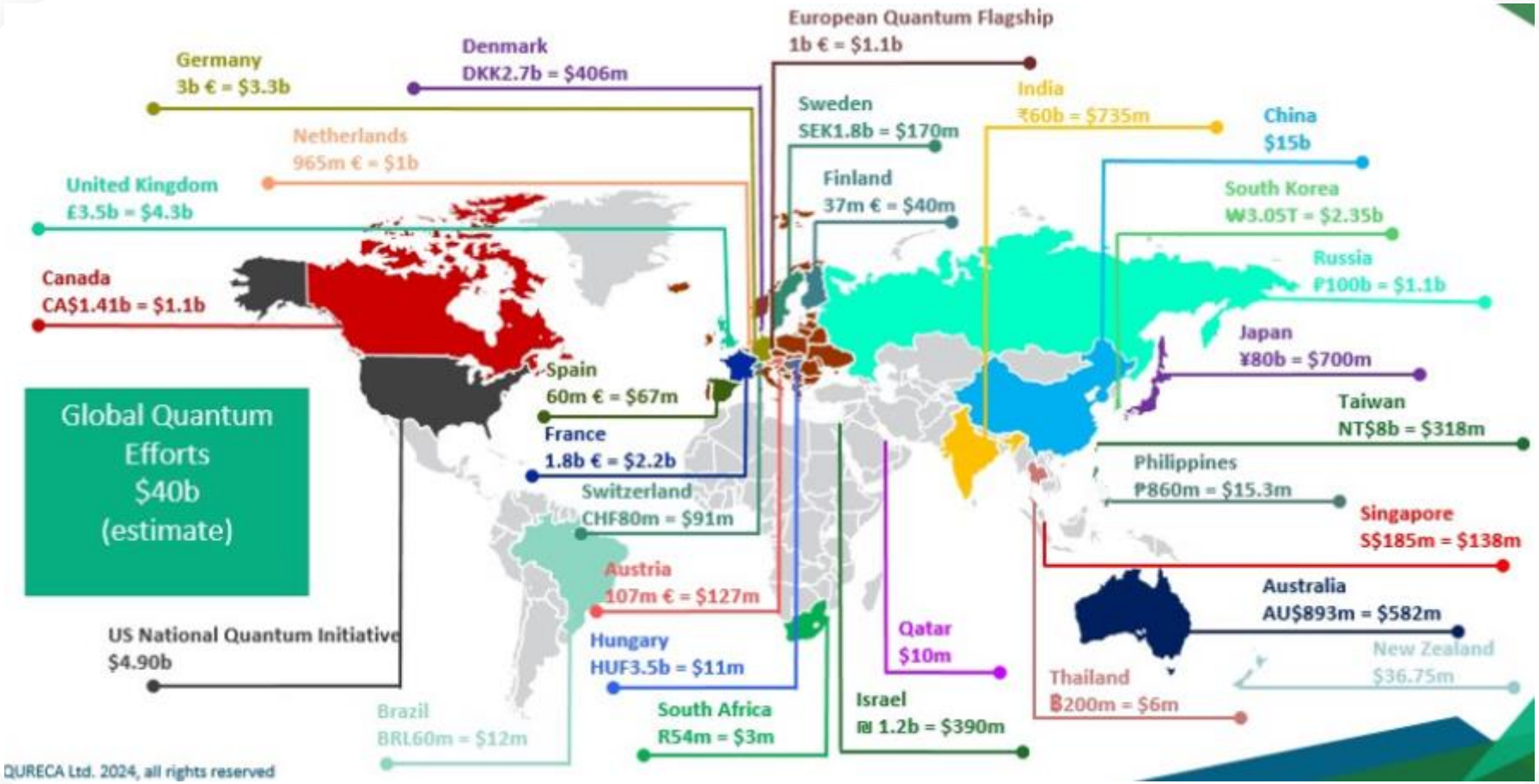
potential economic value across four industries by 2035: chemicals, life sciences, finance, and mobility[1]

[1]Economic value is defined as the additional revenue and saved costs that the application of QC can unlock in all industries. These four industries are the most likely to realize this value earlier than other industries; therefore, they are examined in more depth.

03

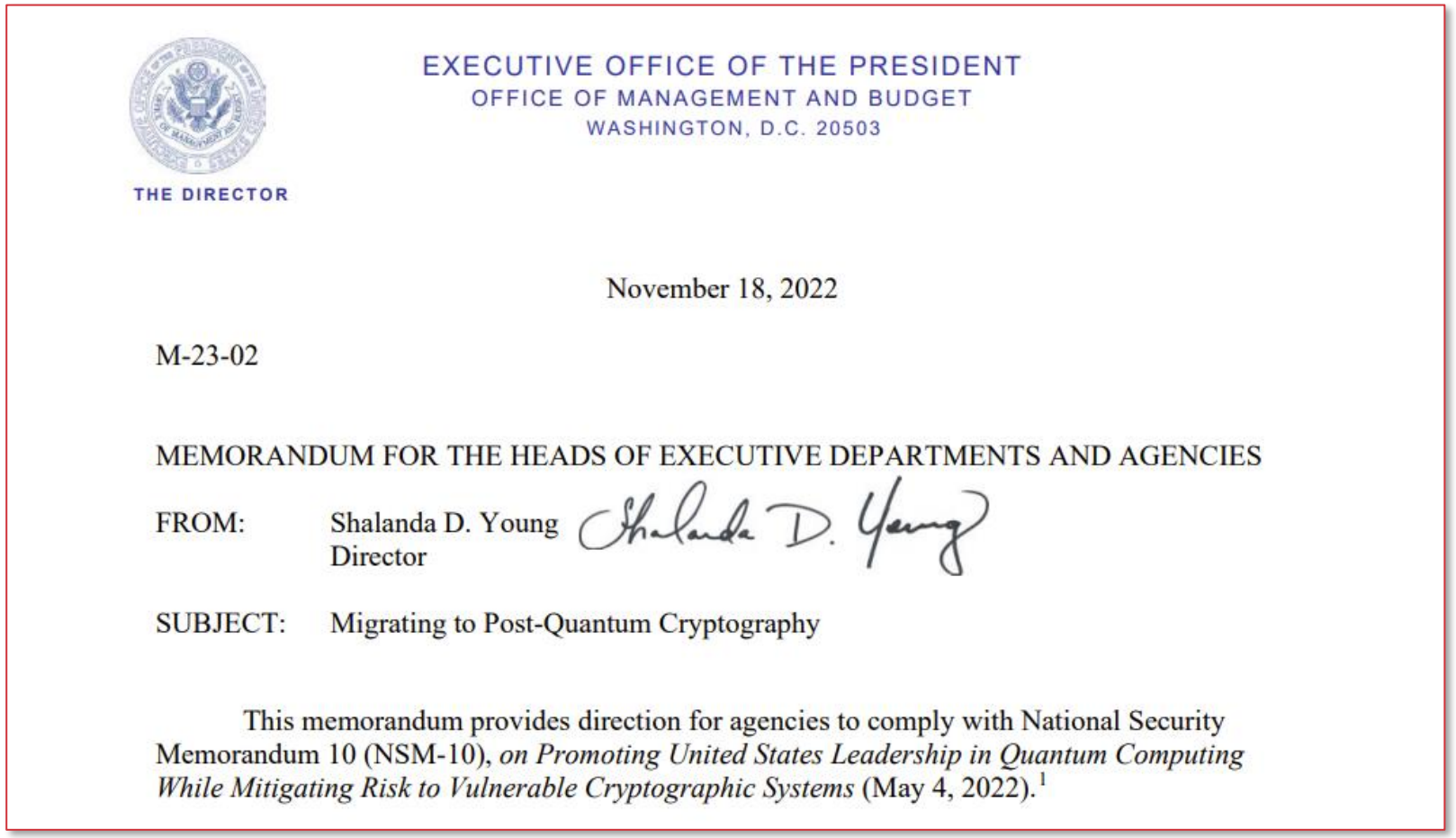
International momentum

Quantum effort worldwide



Case 1: US Government Executive Order

The goal is to complete quantum-resistant cryptography migration within major U.S. government systems by 2030.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography

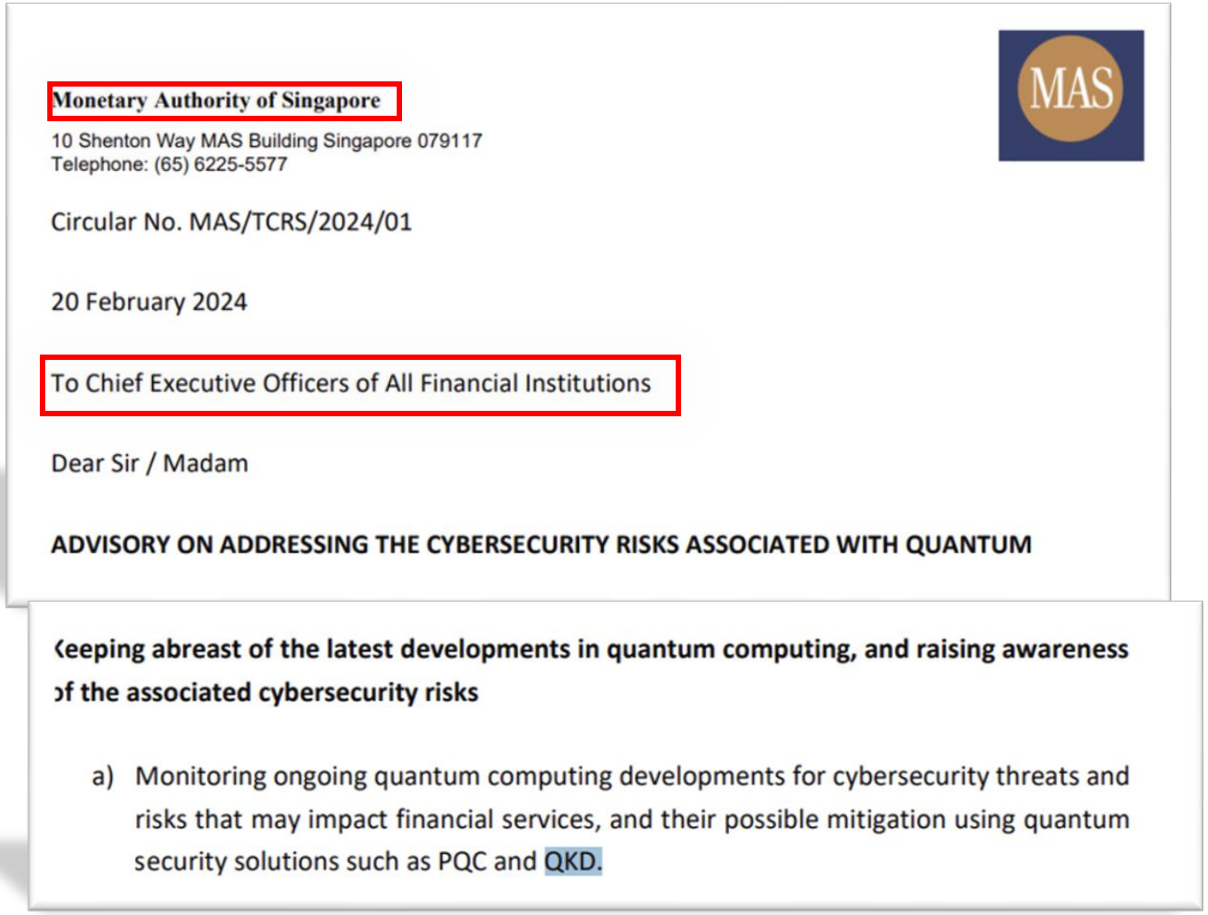
This memorandum provides direction for agencies to comply with National Security Memorandum 10 (NSM-10), *on Promoting United States Leadership in Quantum Computing While Mitigating Risk to Vulnerable Cryptographic Systems* (May 4, 2022).[1]

Case 2: Singapore Recommendation

From: Monetary Authority of Singapore (MAS)

To: Chief executive officer of a financial institution

Quantum Security Advisory Statement on Cybersecurity Risks Due to Latest Advances in Quantum Computers



Monetary Authority of Singapore
10 Shenton Way MAS Building Singapore 079117
Telephone: (65) 6225-5577

Circular No. MAS/TCRS/2024/01

20 February 2024

To Chief Executive Officers of All Financial Institutions

Dear Sir / Madam

ADVISORY ON ADDRESSING THE CYBERSECURITY RISKS ASSOCIATED WITH QUANTUM

‹eeping abreast of the latest developments in quantum computing, and raising awareness ›f the associated cybersecurity risks

a) Monitoring ongoing quantum computing developments for cybersecurity threats and risks that may impact financial services, and their possible mitigation using quantum security solutions such as PQC and QKD.

Case 3: U.S. National Security Agency (NSA: National Security Agency)

NSA Commander-in-Chief: Concerns About Adversaries' Advances in Quantum Computing

NSA fears quantum computing surprise: 'If this black swan event happens, then we're really screwed'

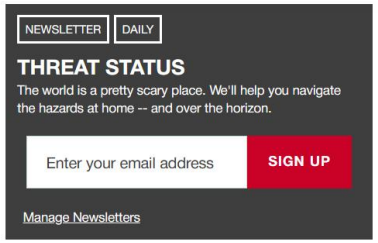
Intelligence fears mount that China, other adversaries could surge ahead in key technology

U.S. Cyber Command Commander Gen. Paul Nakasone testifies before the House Armed Services Subcommittee hearing on cyberspace operations, on Capitol Hill in Washington, March 30, 2023. The National Security Agency is starting an artificial intelligence security center — a crucial ... more >

Americans could suffer consequences from such a quantum leap in several ways. Mr. Herrera said the world economy, and the U.S. market in particular, are vulnerable because most financial transactions are secured by encryption systems that can't be cracked by non-quantum means.

Technological advancements in quantum computing leave the global economy, particularly the U.S. market, vulnerable, he said, because most financial transactions are protected by mathematical classical encryption systems.

Link : NSA fears quantum surprise: 'If this black swan event happens, then we're really screwed' - Washington Times

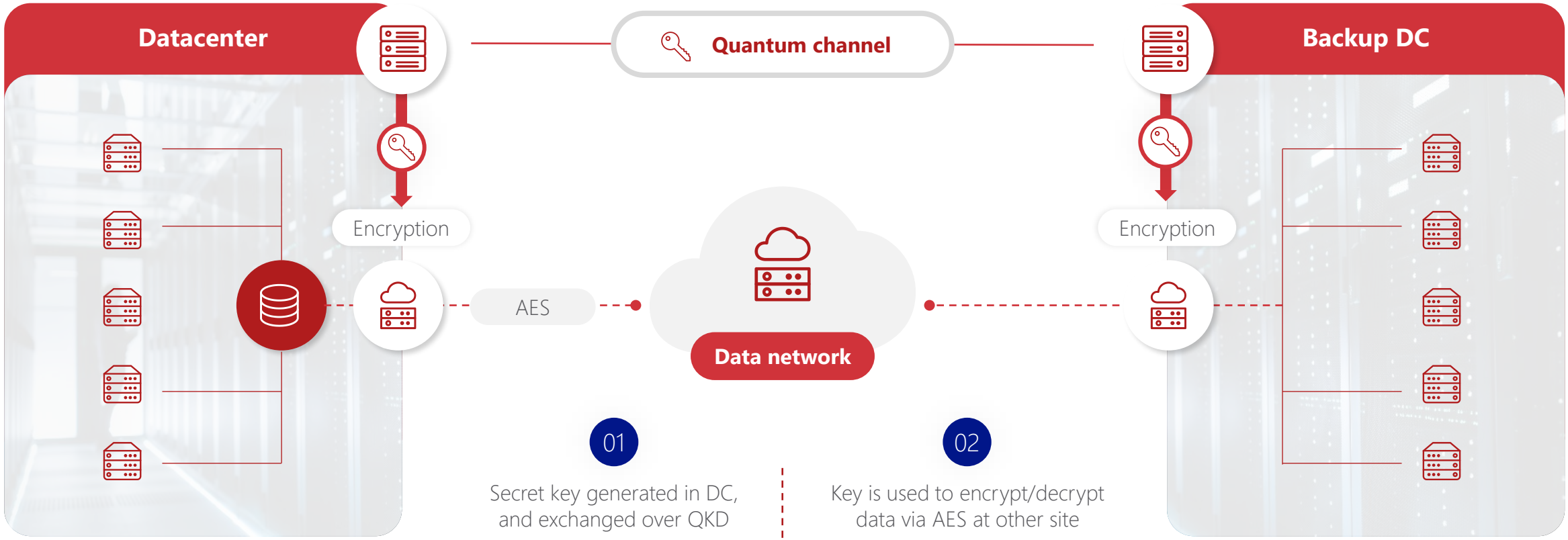


04

Quantum computer threat response plan

Quantum computing threat response plan

Step 1 : Apply a QKD layer



Quantum computing threat response plan

Step 2: Building a Hybrid End-to-End System (QKD+PQC)

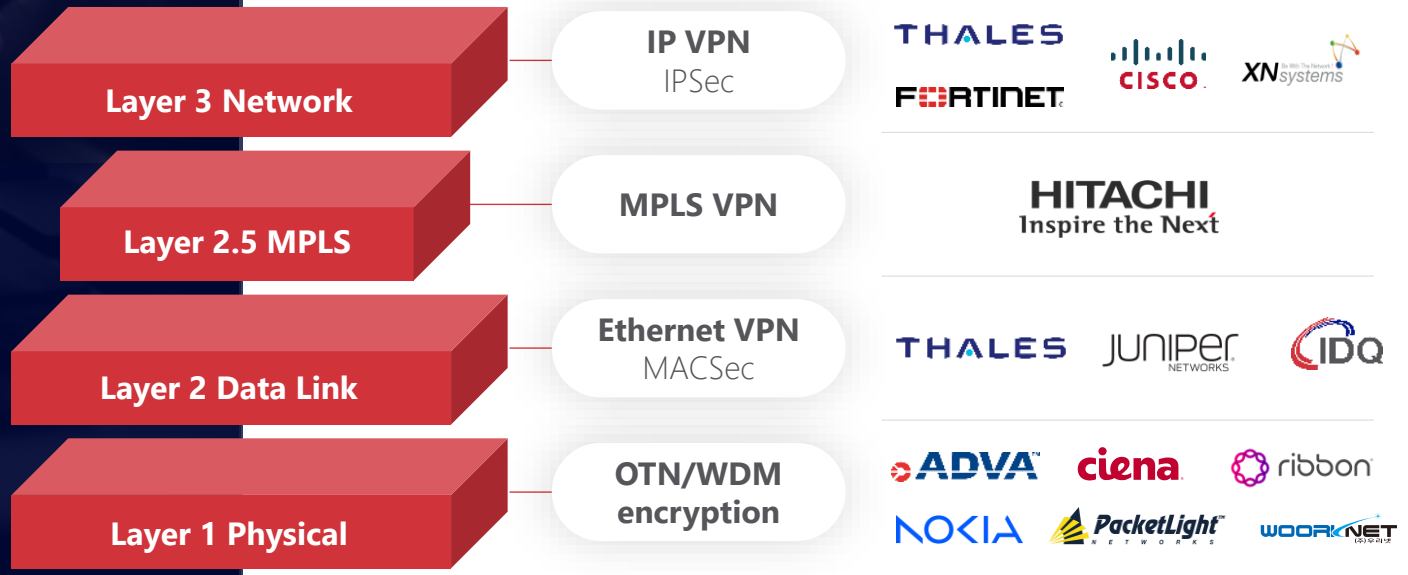
Integrating QKD with existing encryption solutions

IDQ works with different network encryption solutions which may be upgraded with QKD to be Quantum-safe

Benefits of overlaying QKD:

1. Securing your organization in the post-quantum era
2. Reaching long-term confidentiality and aiding data integrity
3. Improving the TCO & ROI of your incumbent encryption solution
4. Acting as a 'value-add', demonstrating your cybersecurity commitments to stakeholders

Supported/PoC Vendors

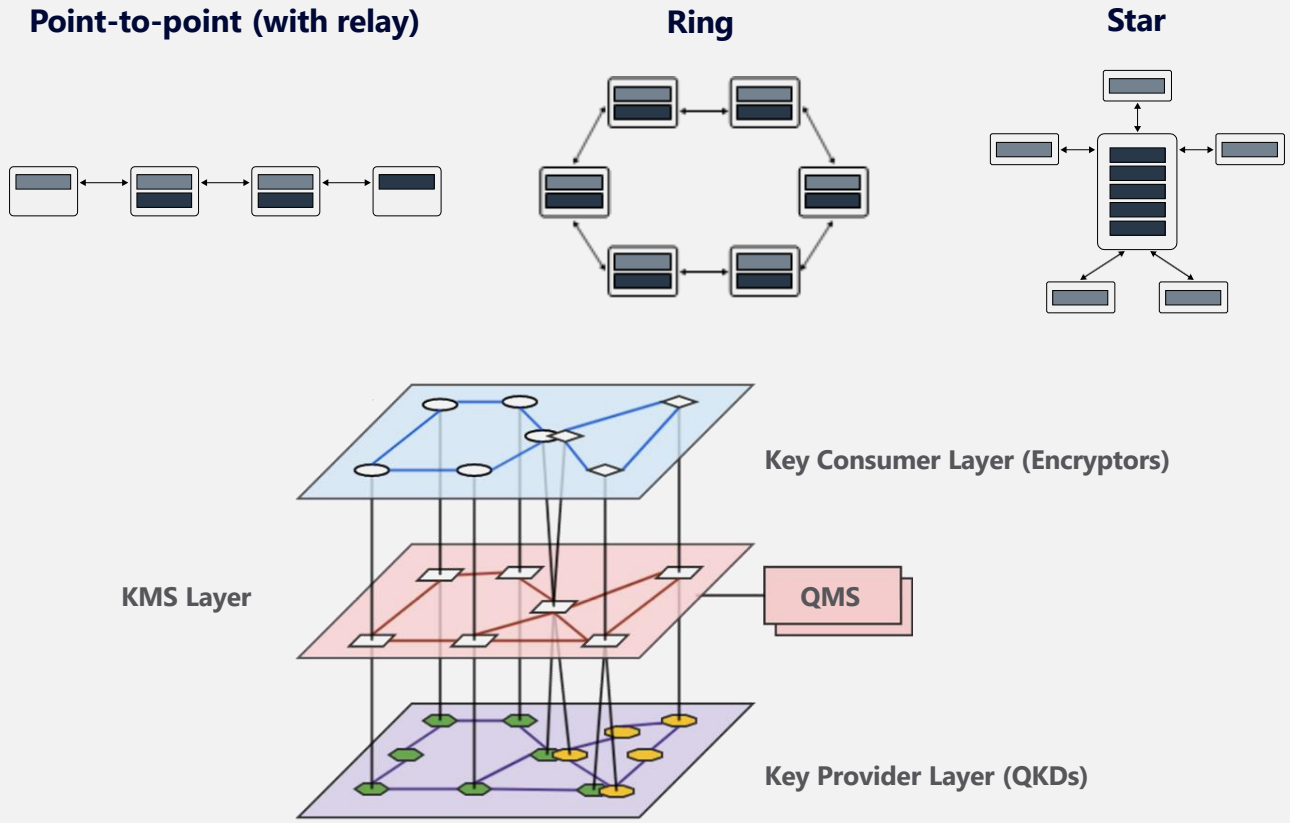


Key Management System – QNET & KMS Software

XG Series' systems can be deployed in any network configurations:

- Point to Point with Key Relay
- Ring
- Star
- Mesh

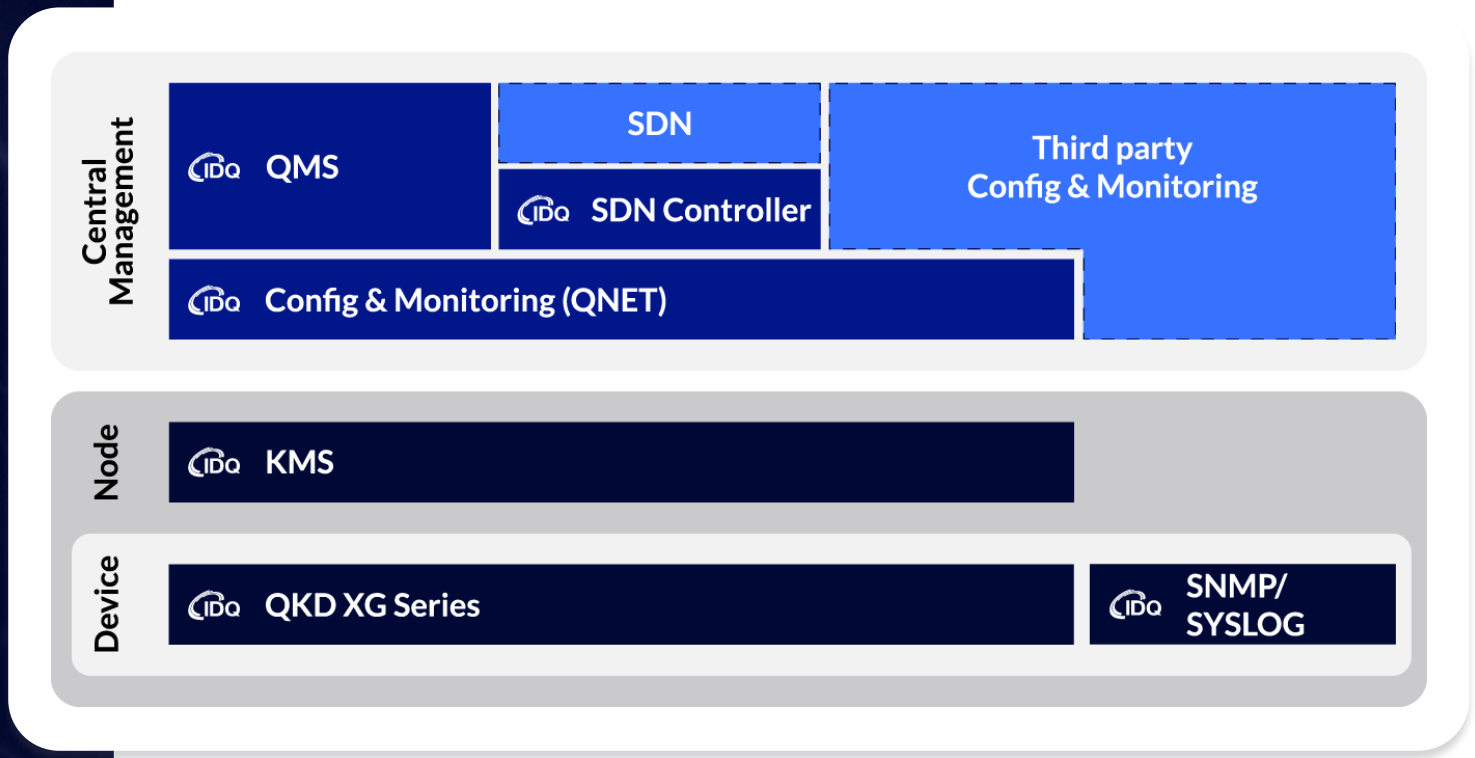
At each QKD node, an embedded **Key Management System (KMS)** software arbitrates the key distribution between QKD and manages key requests and key transfers between QKD optical systems and external encryptors.



IDQ's QKD management and monitoring framework

Facilitate large scale QKD network deployment

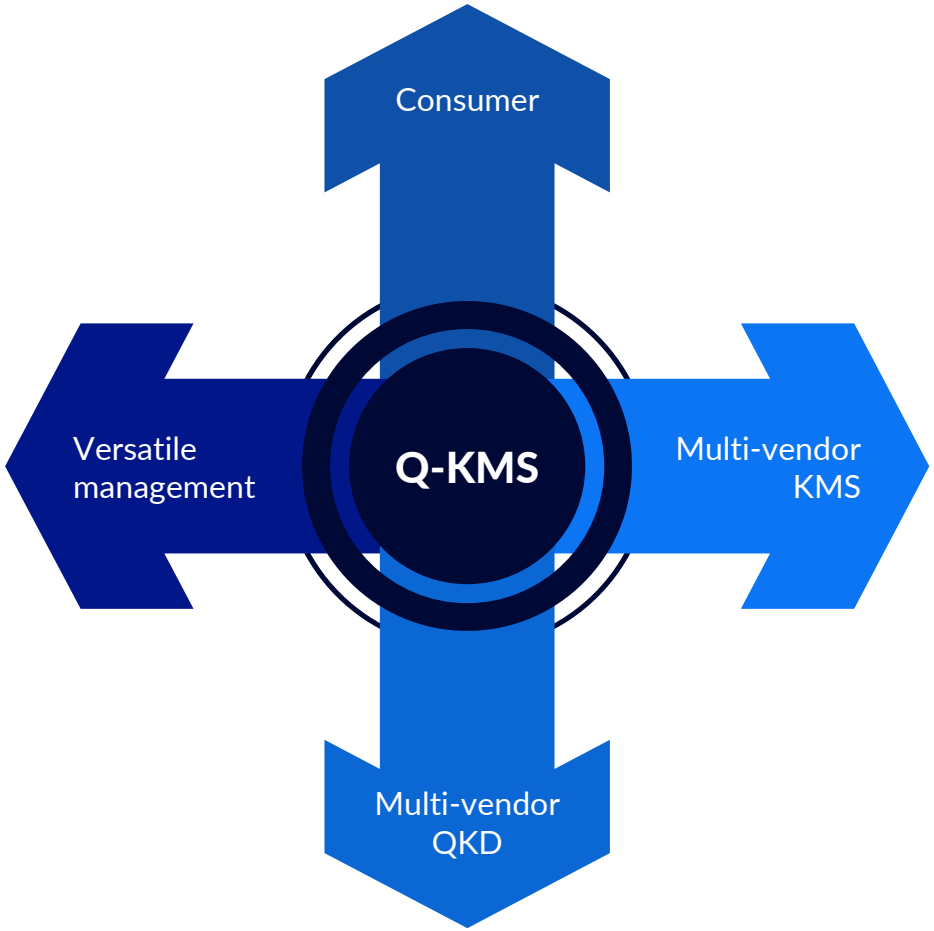
- Integrates current Software-Defined Network (SDN)
- **Intuitive** Quantum Management System
- **Seamless** integration in existing infrastructure



IDQ's QKD versatile KMS

IDQ-KMS implement open standard on most interface

- Easy to Control & Orchestrate via Q-SDN
- IDQ KMS support one of the largest set of QKD Key consumers
- Support multi KMS networks



Quantum Safe PaaS

Model & service

Platform-aaS
for all networks

Quantum-Safe Bandwidth

Enterprise client

Quantum-Safe bandwidth Layer 1-3

Any network

Encryption

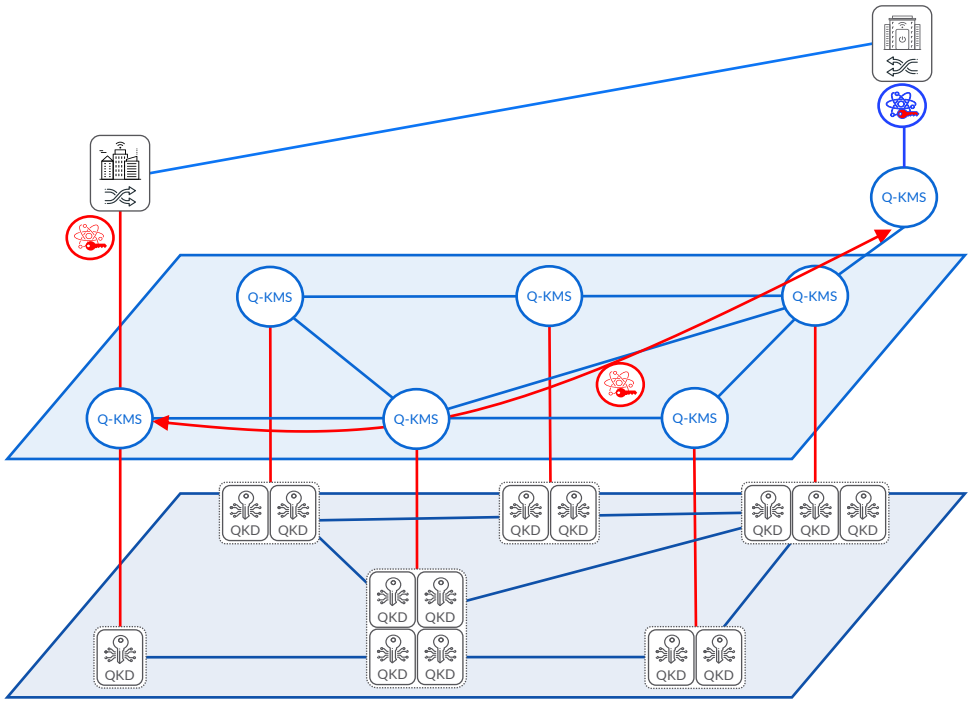
Telecom operator

Quantum Enhanced KMS

Open ETSI interface

Fiber

QKD



Secure Application Layer

Quantum Key Management System Layer

IDQ - Clarion KX

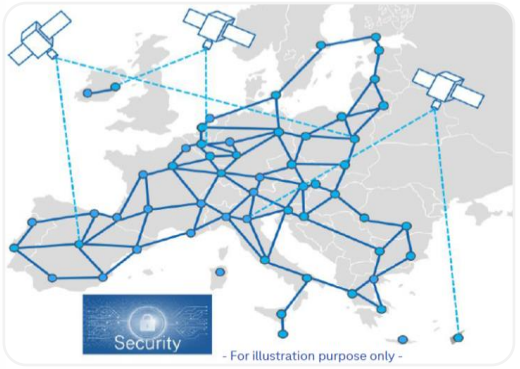
Quantum Key Distribution Layer

IDQ - QKD XG Series

The XG Series: QKDaaS ready

Altice presents security solution based on Quantum Information Technology, with quantum keys-as-a-service

altice warpcom



EuroQCI: the foundation for a future QKD-as-a-service offering?

European Commission

SK Telecom launches a brand-new subscription-based Quantum-Safe-as-a-Service offering

SK telecom NOKIA EQUINIX

Singtel to develop Singapore's first Nationwide Quantum-Safe Network Plus for enterprises

Singtel

05

Main application cases

South Korean Leadership in QKD

2019-2022 projects: more than 2,000 km of QKD links

QKD implemented in SK Telecom 5G network in 2019
330km

SKT applied QKD to Sungsoo-Dunsan section of its LTE and 5G network to prevent hacking.

2022 G-Project

800km of QKD links

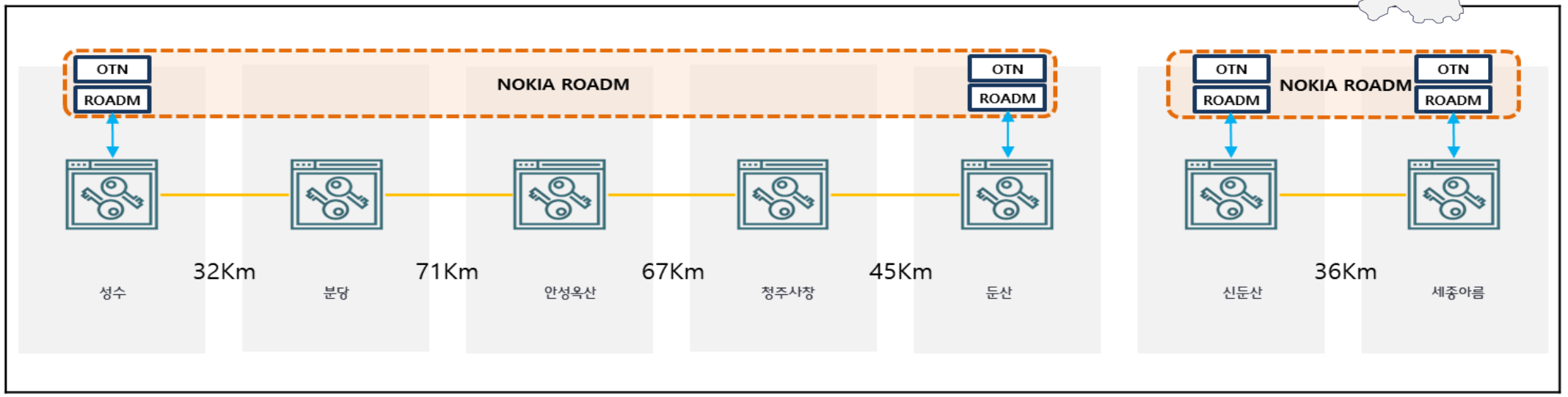
SKT 5G network QKD backbone network

In 2023 SK Telecom deployed the Clavis XG

SKT applies Clavis XG to enhance 5G backbone network reliability

Collaboration with NOKIA

SK telecom



1,770 km-long intercity QKD infrastructure in Poland

Building a QKD Network as part of the Polish Quantum Communication Infrrastructure (EuroQCI) for digital science, economy and social innovations.

Business need

- Poznan Supercomputing and Networking Center (PSNC) was looking to establish a QKD infrastructure to provide secure links for a series of use cases and applications.

Solution

- Used IDQ's XG Series QKD over a dedicated fiber network, on a total length of 1770 km
- Trusted nodes in main cities of Poland and ready for metro QKD system installations with different topologies

Results

- Interconnect all High Performance Computing Centers in Poland and establish common access layers to QKD services.
- Pan-European cross-border QKD infrastructure

> Launching the QKD link between Poznan and Warsaw was the first stage to building a nationwide quantum communication network, providing access to modern technology to companies and organizations seeking to protect their assets in the post quantum era.
>
> Artur Binczewski, Director of Network Technologies Division at PSNC

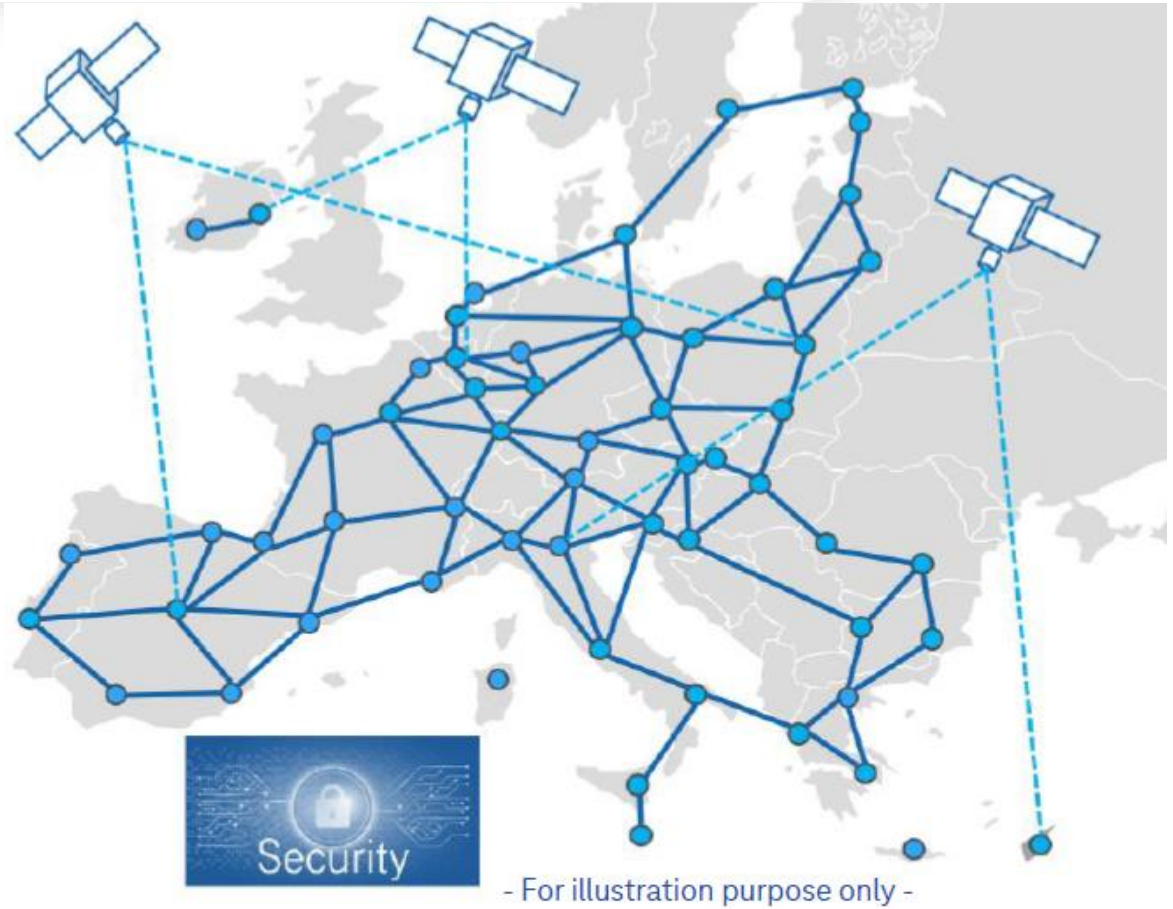
The EuroQCI Initiative

Cybersecurity Strategy for the coming decades.

Aiming at safeguarding sensitive data and critical infrastructures by integrating quantum-based systems into existing communication infrastructures.

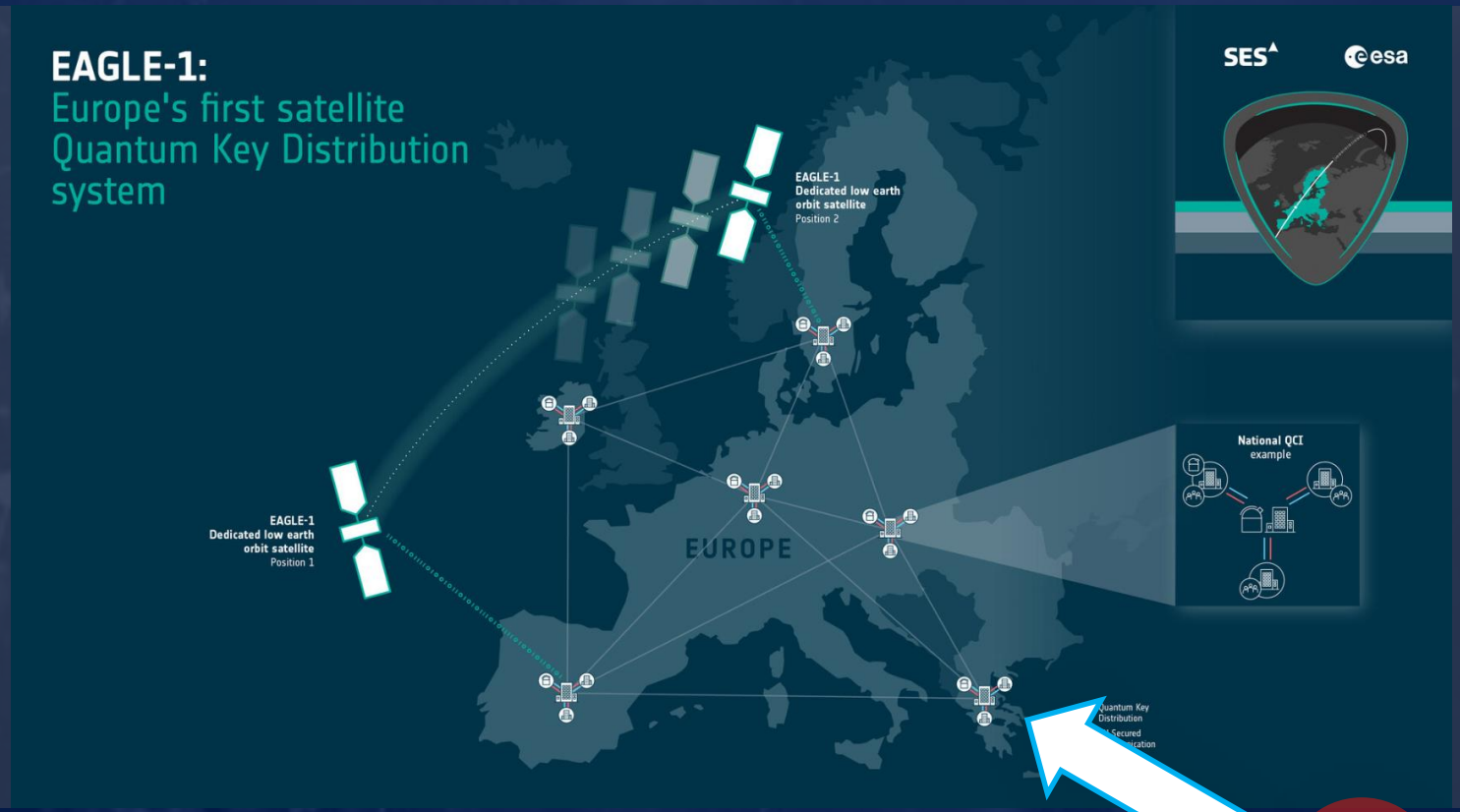
- First phase 2022-2023 National Phases
- Second phase 2024 any beyond – roll out
- Fully operational by 2027

EU Quantum Communication Infrastructure



Quantum networks in 2024

Long-distance QKD with satellites



- The first space-based quantum key distribution system to be developed under ESA, the European Commission and 20 companies in Europe.
- Several ground stations across Europe
- To be launched in 2024
- IDQ is a proud project partner

Portability, efficiency, time precision

Quantum networks in 2024

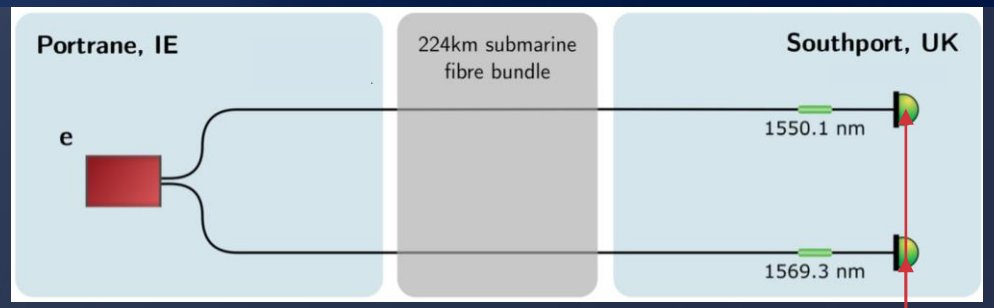
Long-distance using entanglement and low-noise detection

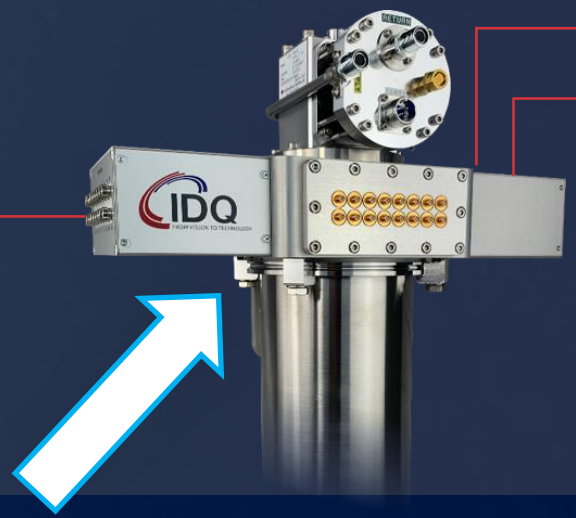
Article

Quantum Communications Feasibility Tests over a UK-Ireland 224 km Undersea Link

Ben Amies-King [1,*,†], Karolina P. Schatz [1,*,†], Haofan Duan [1,†], Ayan Biswas [1], Jack Bailey [2], Adrian Felvinti [2], Jaimes Winward [2], Mike Dixon [2], Mariella Minder [1,3], Rupesh Kumar [1], Sophie Albosh [1] and Marco Lucamarini [1,*]

Entropy **2023**, *25*, 1572. https://doi.org/10.3390/e25121572





High-efficiency and low-noise detection

Quantum networks in 2024

Entanglement-based QKD in metropolitan quantum network

Operational entanglement-based quantum key distribution over 50 km of field-deployed optical fibers

Yoann Pelet, Grégory Sauder, Mathis Cohen, Laurent Labonté, Olivier Alibart, Anthony Martin, and Sébastien Tanzilli

Phys. Rev. Applied **20**, 044006 – Published 3 October 2023

High-performance low-noise detection

Portability, efficiency, low-noise

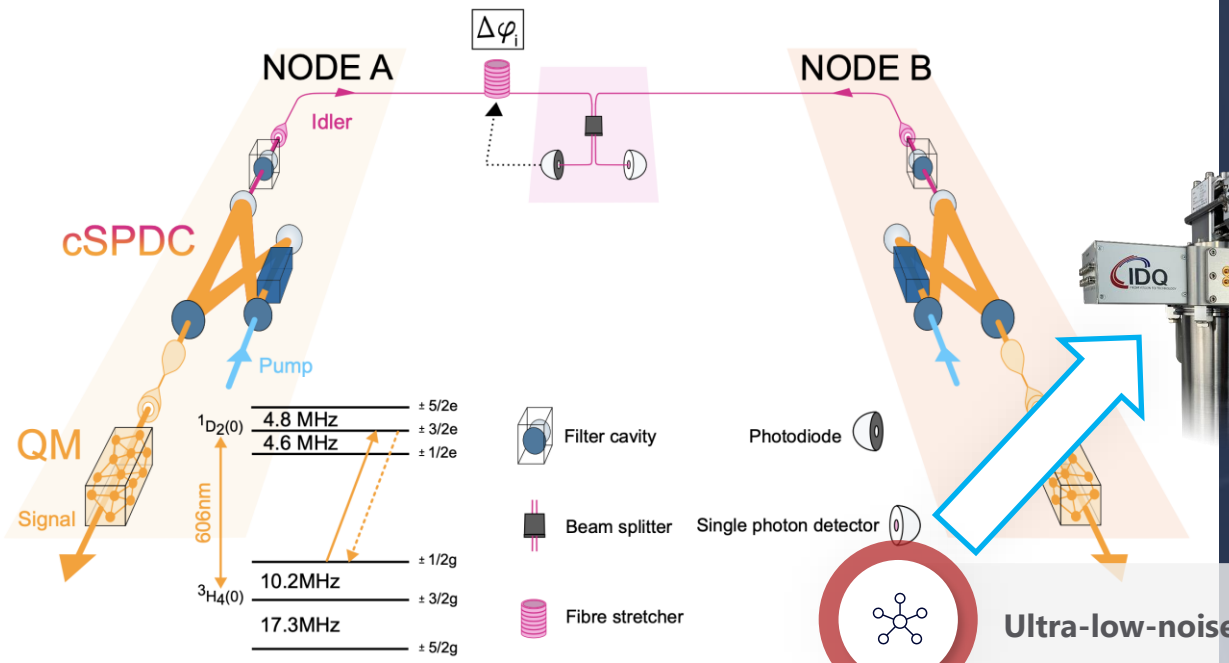
Quantum networks in 2024

Adding entanglement and quantum memories to synchronize quantum information

Telecom-heralded entanglement between multimode solid-state quantum memories

Dario Lago-Rivera, Samuele Grandi, Jelena V. Rakonjac, Alessandro Seri & Hugues de Riedmatten

Nature **594**, 37–40 (2021) | Cite this article

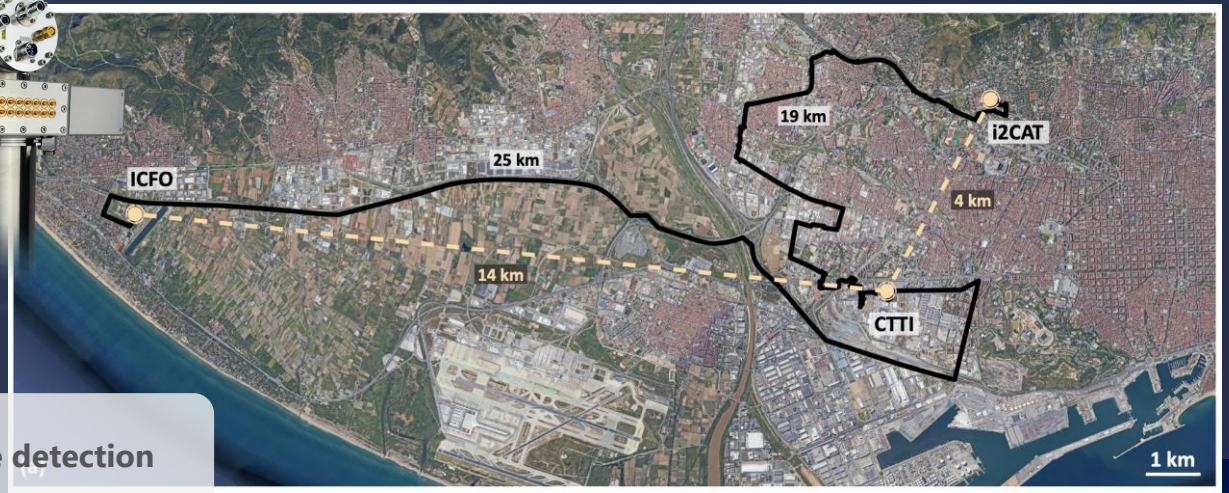


94 Vol. 1, No. 2 / 25 December 2023 / *Optica Quantum* Research Article

OPTICA QUANTUM

Transmission of light–matter entanglement over a metropolitan network

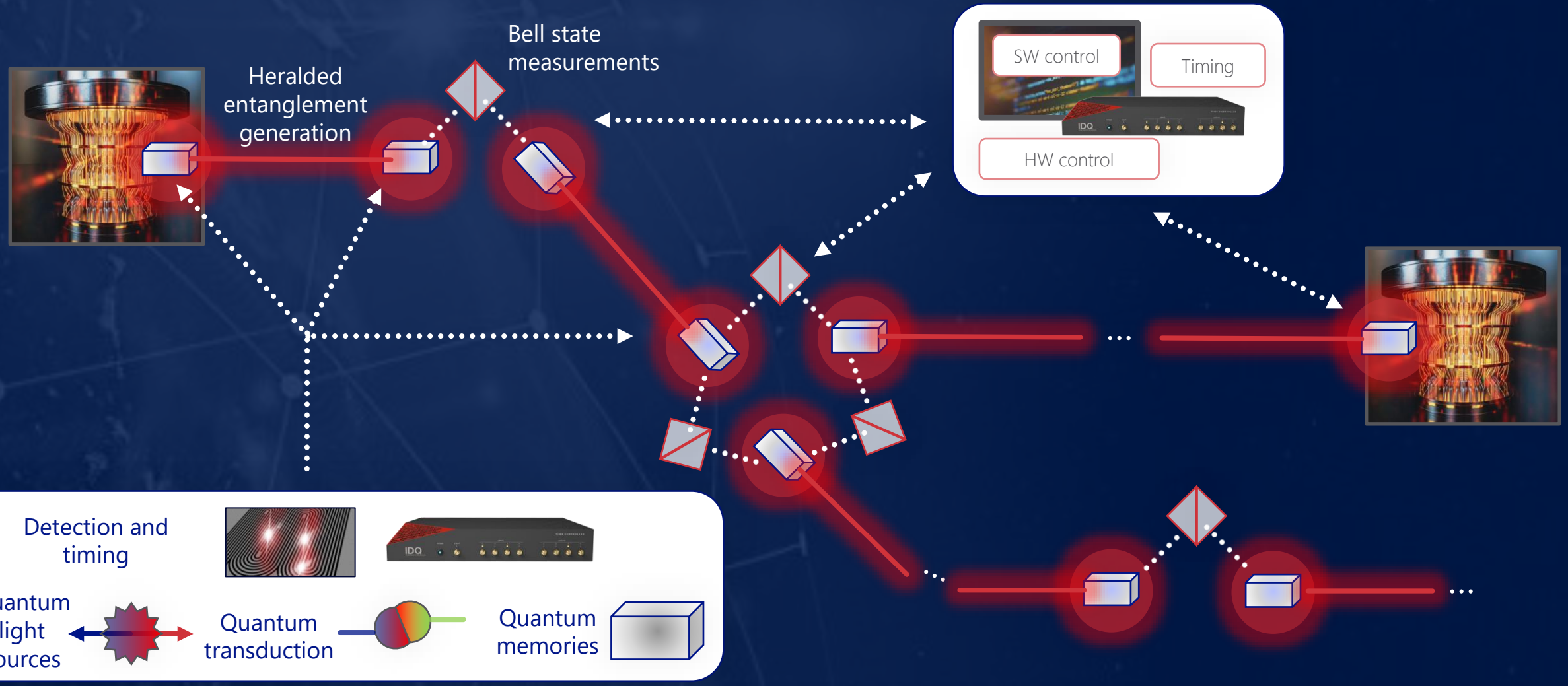
Jelena V. Rakonjac,[1,†] Samuele Grandi,[1,†*] Sören Wengerowsky,[1,†] Dario Lago-Rivera,[1] Félicien Appas,[1] and Hugues de Riedmatten[1,2]



Ultra-low-noise detection

Quantum networks in 20…

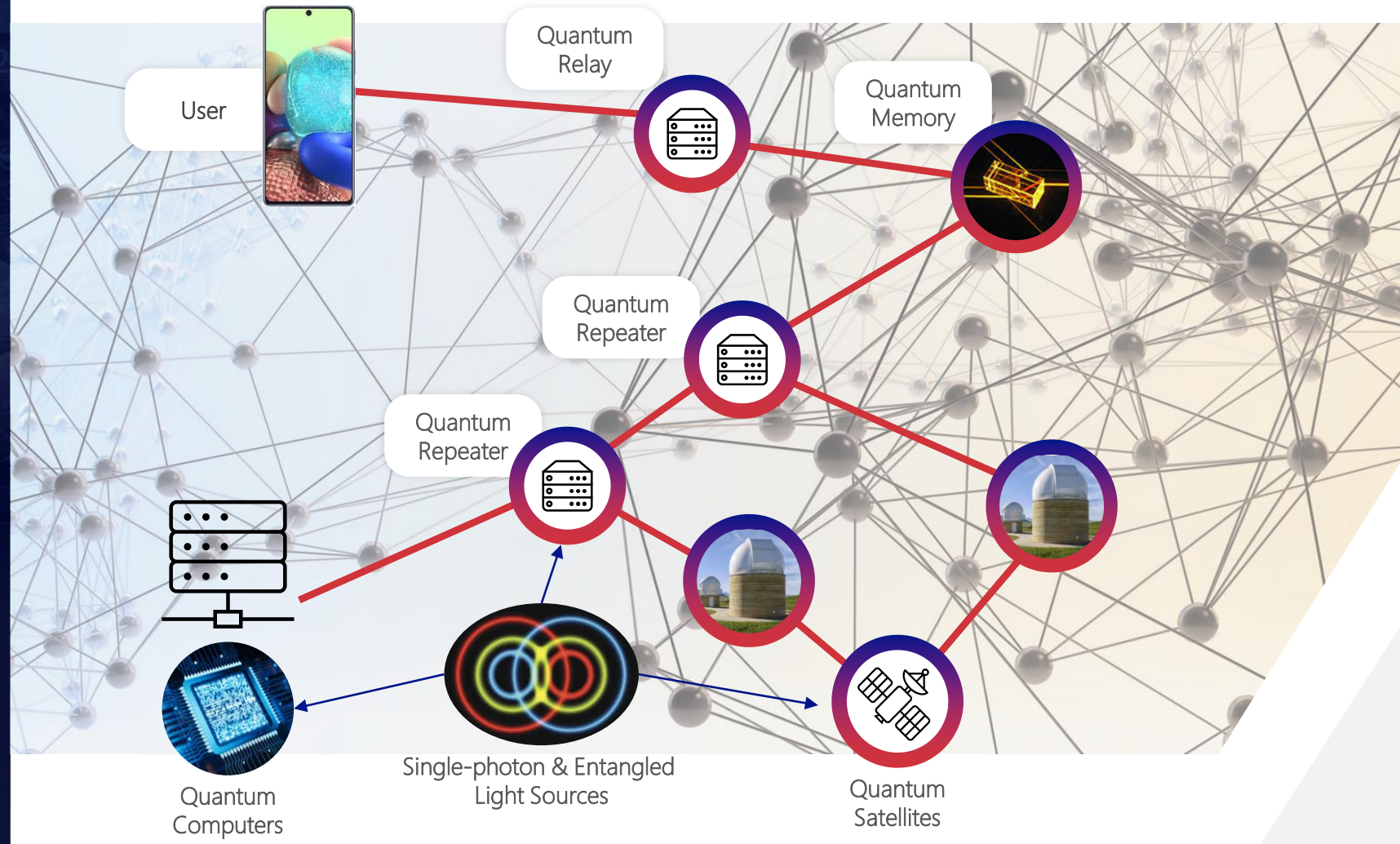
Towards a generalized “Quantum Internet” to distribute and use entanglement



Topology of the Quantum Internet

Today, we distribute keys.

Tomorrow, we will distribute **entanglement**.

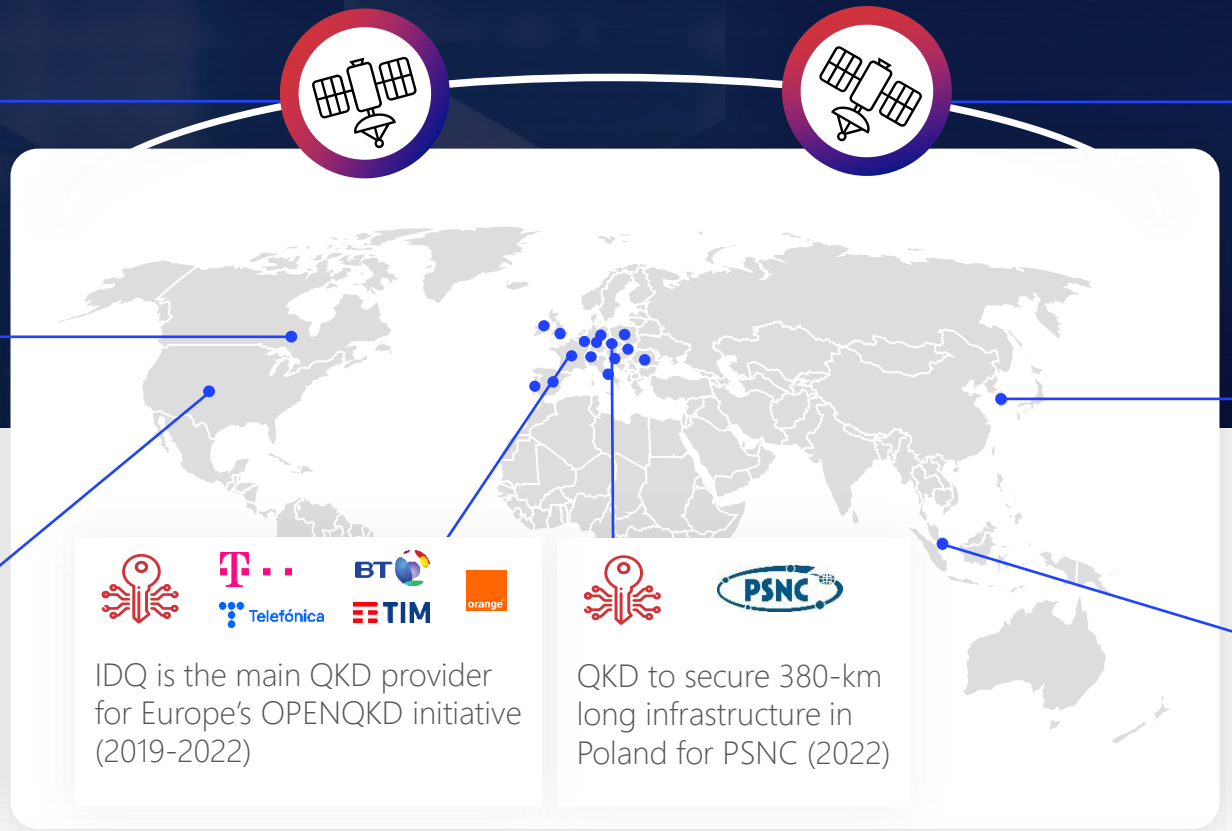


IDQ Quantum-Safe global reach – Snapshot

QRNG for EAGLE-1 Satellite QKD initiative (2022)

Quantum communication infrastructure project between Montreal, Sherbrooke and Quebec (2022)

DocuSign QSCD appliance embedding a QRNG is FIPS 140-2 level 3 approved (2022)



IDQ is the main QKD provider for Europe's OPENQKD initiative (2019-2022)

QKD to secure 380-km long infrastructure in Poland for PSNC (2022)

Boosting Galileo's performance and cybersecurity (initial launch 2024)

Deployment of an 800-km QKD network linking 48 government organizations (2022)

IDQ and Singtel launch the first nationwide Quantum Safe Network in Singapore (2023)

Leading Quantum Safe technology adoption through close collaboration

Key takeaways

1

Do not delay

(Crypto)
Winter is coming!

It will take time to implement solutions.

Start now!

2

Know Your Data

Where are your vulnerabilities?

What needs to be protected?

For how long?

3

Improve key generation

Use QRNG as a first, easy step to instantly strengthen your crypto systems

4

Pursue crypto-agility

Be prepared to switch to alternative crypto primitives and algorithms

Protect any kind of investment you made so far by overlaying QKD to your existing infrastructure

5

One size does not fit all

Adapt the solution to the case.

Hybrid systems can improve security.

Use QKD on mission-critical links & data center interconnect

ID Quantique

Quantum.
Trust enabled for the future

Q & A

info@idquantique.com | www.idquantique.co.kr

ID Quantique

Founded in 2001

3 Product lines:

1. Quantum Random Number Generation
2. Quantum-Safe Security
3. Quantum Sensing

High-quality engineering

Best-in-class performance

Trust

Operational simplicity