IDQ

20 YEARS QUANTUM INNOVATION

QUANTUM-SAFE SECURITY

Building a trusted future through quantum technologies

Pejman Panahi

Senior Director, Global Market & Business development

17/03/2021

ID Quantique

Founded in 2001

Geneva, Switzerland
Seoul, South Korea
Boston, USA

By 4 quantum physicists from the University of Geneva

100+ 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:

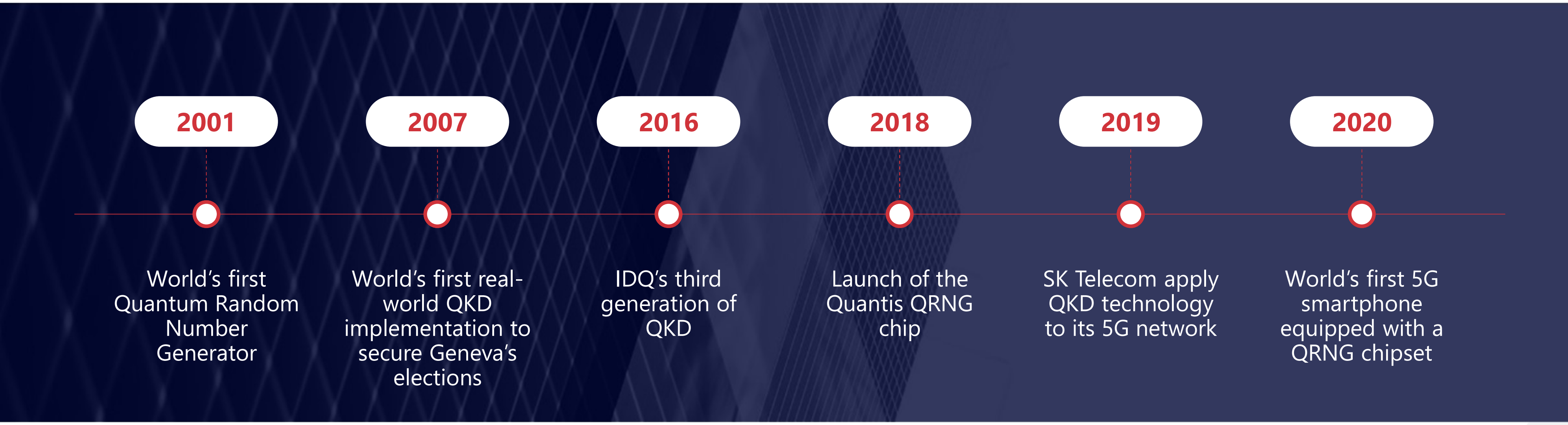
- Quantum-Safe Security
- Quantum Sensing

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

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

ID Quantique

The world leader in Quantum Randomness and Quantum-Safe Security



2001
World's first Quantum Random Number Generator

2007
World's first real-world QKD implementation to secure Geneva's elections

2016
IDQ's third generation of QKD

2018
Launch of the Quantis QRNG chip

2019
SK Telecom apply QKD technology to its 5G network

2020
World's first 5G smartphone equipped with a QRNG chipset

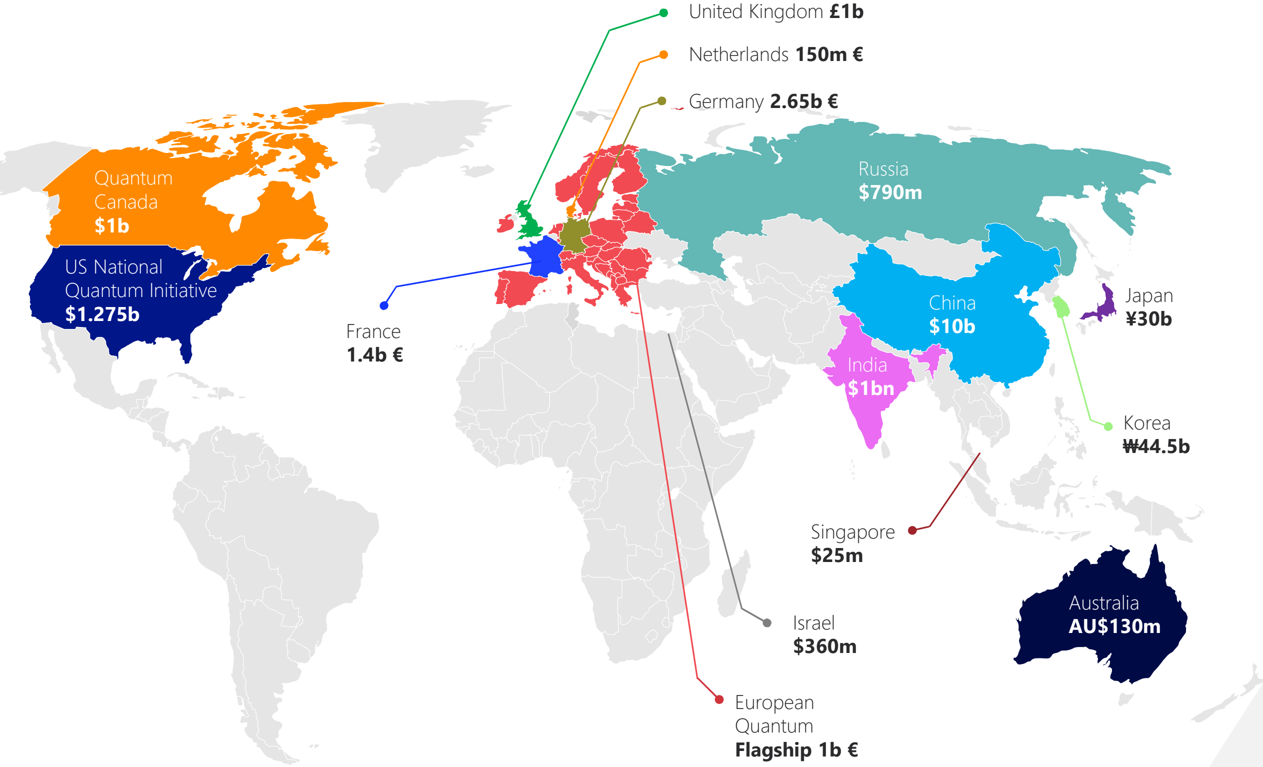
ID Quantique

ID Quantique celebrates its 20 years anniversary

Quantum funding: Public investments

More than a quantum race, the world is building a **global ecosystem around quantum technologies.**

Global effort 2020 $21b (estimate)

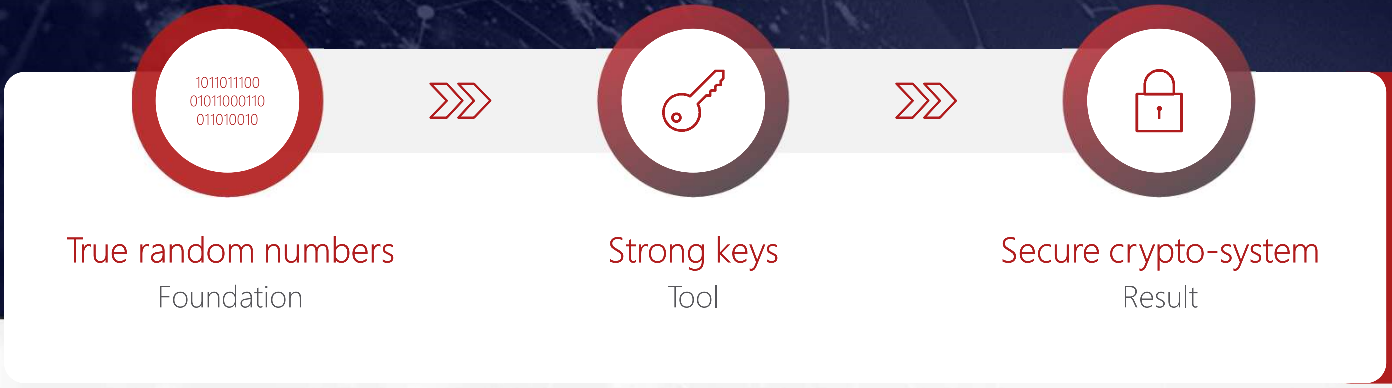


© 2020 QURECA Ltd – Confidential and Proprietary

1

QUANTUM RANDOM NUMBER GENERATION

Feed your security systems with quantum randomness



True random numbers
Foundation

Strong keys
Tool

Secure crypto-system
Result

QRNG is the only solution offering provable entropy thanks to the laws of quantum physics which makes it invulnerable to prediction or bias

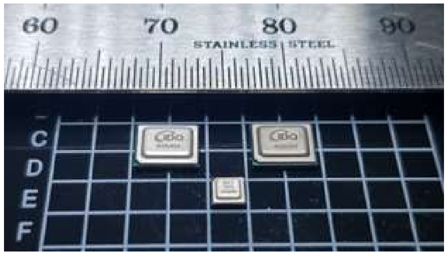
The security of any cryptographic system is determined by the security of its keys…

Which rely on random numbers.

Getting the foundation right is crucial.

The solution?
Quantum Random Number Generation (QRNG)

The Quantis family



Quantis Chips

IDQ6MC1
IDQ20MC1
IDQ250C2

Quantis Modules

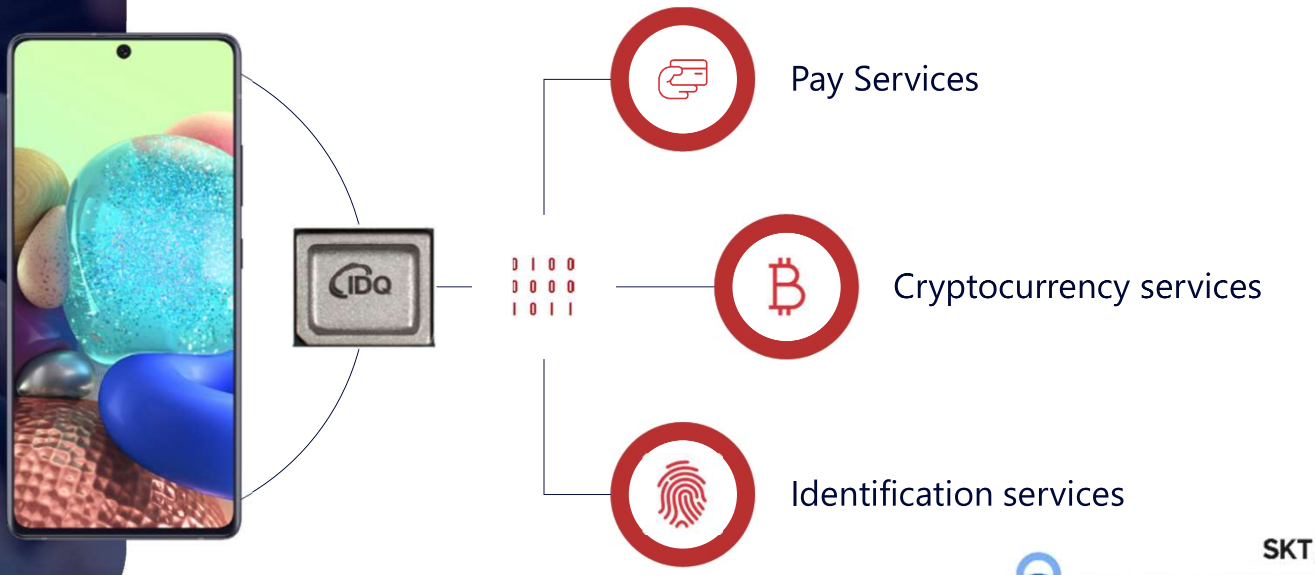
USB 4M
PCIe 4M
PCIe 16M
PCIe 40M
PCIe 240M

Quantis Appliance 2.0

QRNG chip – Mobile Application

IDQ brings a new level of Quantum enhanced phone security allowing differentiated security solutions for ICT services.

Phone Applications and Services use Security Algorithms



Pay Services

Cryptocurrency services

Identification services

SKT 5GX QUANTUM

Secured by Swiss Quantum

The Quantum decade has begun

IDQ

Quantis QRNG chip integrated into Vsmart Aris 5G smartphones

- Enhanced security of user data
- Unique differentiation through a much higher level of trust to users
- Basis for new revenue streams especially in combination with e-sim and quantum-secured datacenters

2

QUANTUM KEY DISTRIBUTION

Industries benefiting from QKD

Government & Defense

Financial services and Banks

Telco & MSP

Healthcare & Pharma

Datacenter & Cloud

Critical Infrastructure

Clavis^3 QKD Platform

Clavis^3

Quantum Key Distribution for academic and research labs

- Open QKD platform for R&D applications
- Interface to external detectors
- Interface to external encryptors
- User interface for technology evaluation and testing

Cerberis^3 QKD System

Cerberis^3

Quantum Key Distribution for enterprise, government and telco production environments

- Complex network topologies (ring, hub and spoke)
- Interoperability with major Ethernet and OTN encryptors
- Easy integration in any data center
- Centrally monitored solution
- Multiplexing of all channels on single fiber for metropolitan area. DWDM

Clavis^{300} Quantum Cryptography Platform

Clavis^{300}

Integrated QKD & LEA Encryption System

- 6U 19” chassis
- Key distribution protocol BB84+ decoy
- Transmission loss (typ.): 18db
  (longer range available upon request)
- Secret key rate (typ.): 10 kb/s after 50km
- Point to Point Relay Node configuration
- Embedded high speed LEA L1 encryptor

3

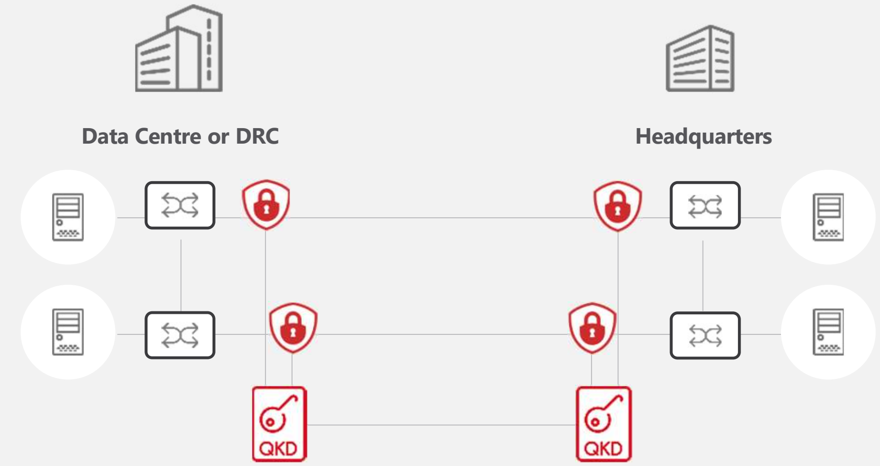
QUANTUM KEY DISTRIBUTION

Use cases and Applications

Secure data center interconnect

Point-to-Point QKD combined with L1 to L4 encryption

- Hybrid approach
- Generate highly secret keys
- Secure daily backup & database replication
- Assure business continuity and protect against data loss



Integrating QKD with existing encryption solutions

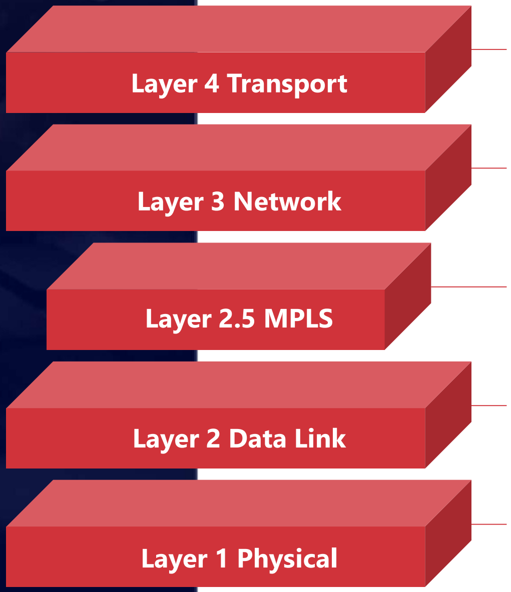
IDQ

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

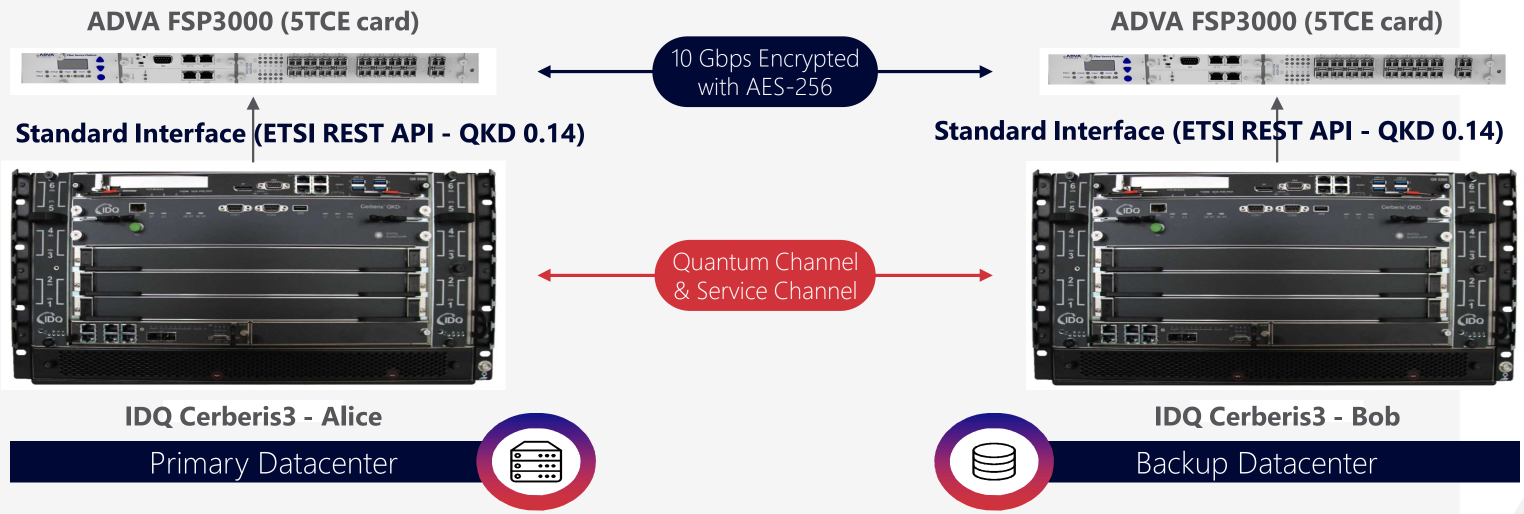


Layer 4 Transport	**SSL VPN** SSL/TLS	Available soon
Layer 3 Network	**IP VPN** IPSec	THALES FORTINET CISCO
Layer 2.5 MPLS	**MPLS VPN**	HITACHI ABB
Layer 2 Data Link	**Ethernet VPN** MACSec	IDQ THALES
Layer 1 Physical	**OTN/WDM encryption**	ADVA

Secure data center interconnect – OPEN QKD

OPEN QKD

OPEN QKD
SIG/ ADVA/ IDQ



ADVA FSP3000 (5TCE card)

ADVA FSP3000 (5TCE card)

10 Gbps Encrypted with AES-256

Standard Interface (ETSI REST API - QKD 0.14)

Standard Interface (ETSI REST API - QKD 0.14)

Quantum Channel & Service Channel

IDQ Cerberis3 - Alice

IDQ Cerberis3 - Bob

Primary Datacenter

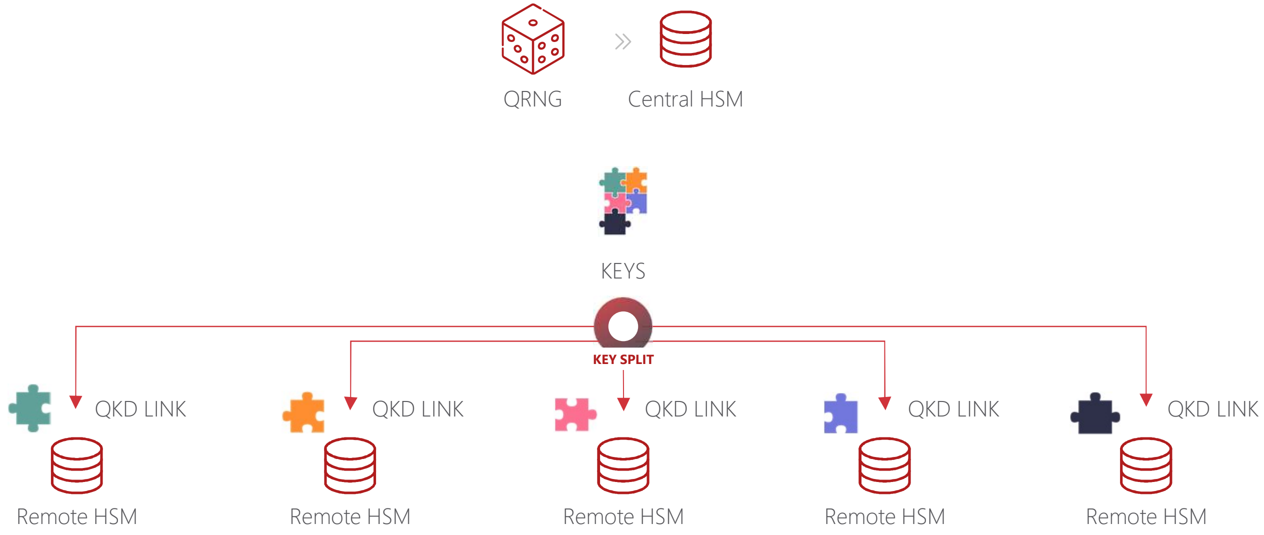
Backup Datacenter

The Quantum Vault

Principle:

1. Generate keys with QRNG
2. Use Shamir Secret Sharing for distributed safe storage
3. QKD for secure transmission
4. 3 out 5 nodes needed to recover the key

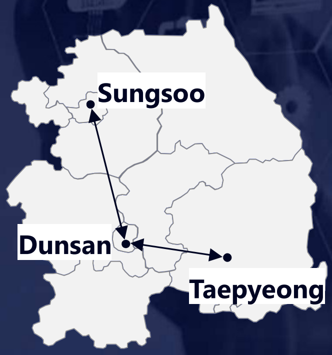
Ultimate security for digital assets custody



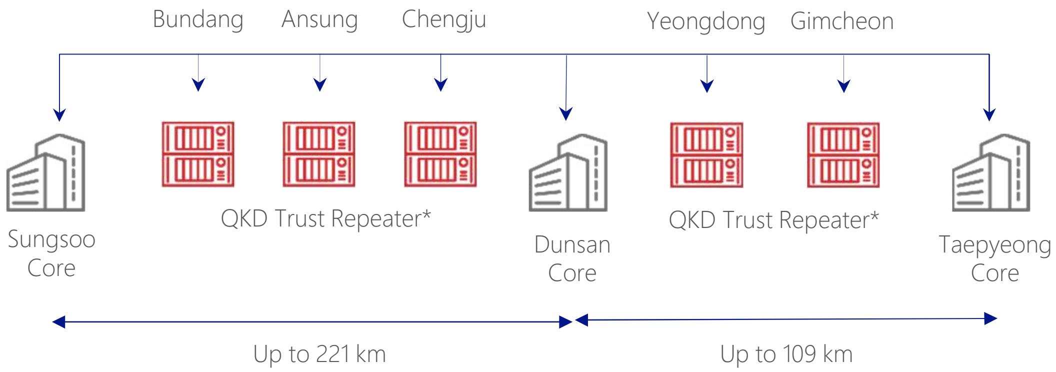
QKD on a 5G network

QKD implemented in SK Telecom network in 2019

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



Cryptography based on QKD



The National Convergence Network Project

IDQ and SK Broadband selected for the construction of the first nation-wide QKD network in Korea

2000 kilometers

The two companies will protect major areas of public networks with QKD on a section of up to 2000 km. It will constitute the largest operational QKD network in the world outside of China.

48 government organizations

Across a communication network of 48 government organizations, including the Ministry of Employment and Labor, the Ministry of Economy and Finance, the Ministry of Education and local governments.

Security, stability & efficiency

The National Convergence Network Project will strengthen security and stability, as well as increase the efficiency of the operation and budget of national institutions.

QKD on a telecom network

Implementation of UK's ultra-secure Quantum Network Link

New high-speed link that uses over 125km of standard BT optical fiber between Cambridge and Adastral park.

Worked with BT, Uni York & Uni Cambridge for deployment of system

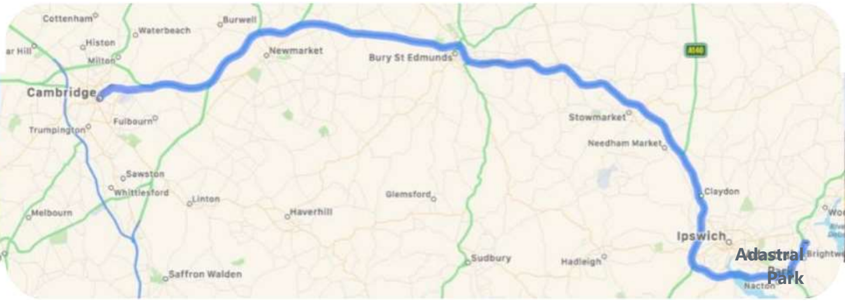
QKD interfaced with ADVA's FSP 3000 encryption

Works with Trusted Nodes for distance extension

Uses single fiber multiplexing quantum and data channels

Long distance QKD with Trusted Nodes

Cambridge University



BT's Adastral park campus

Cambridge University → Cambridge Exchange → Ipswich Exchange → BT's Adastral park campus

ID Quantique

Quantum.
Trust enabled for the future

info@idquantique.com | www.idquantique.com

IDQ

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