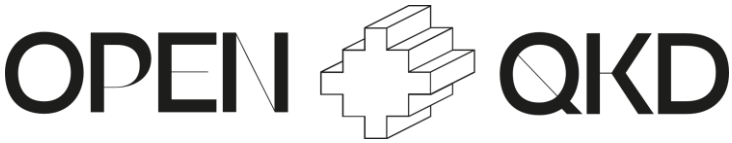
Call (part) identifier:	H2020-SU-ICT-2018-3
Topic:	SU-ICT-04-2019 Quantum Key Distribution testbed
Grant Agreement / Contract Number:	857156
Project Acronym:	OPENQKD

Open European Quantum Key Distribution Testbed



Second and Final Report on Field Trial Execution

Deliverable: **D8.7**	Lead: IDQ
Project month: M42	27. 02. 2023
Work package: WP08	Task: T8.4
Type: Report	Version: 2.0
Dissemination level: Public	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857156.

More information available at https://openqkd.eu/.

Copyright Statement

Document Information

Author List

Organization	Name	E-mail
IDQ	Jean-Sébastien Pegon	pegon@idquantique.com

Reviewer List

Organization	Name	E-mail
TEUR	Elisabetta Spigone	elisabetta.spigone@crl.toshiba.co.uk
MLNX	Giannis Patronas	giannisp@nvidia.com

Version History

Version	Date	Reason / Change	Editor
1.0	26.02.2023	Last draft	Jean-Sébastien Pegon
1.1	27.02.2023	Ready for review	Cristina Tamas
1.2	28.02.2023	Review from Elisabetta	Elisabetta Spigone
2.0	01.03.2023	Final version	Jean-Sébastien Pegon

Executive Summary

The report is aimed for public distribution, and anyone interested in the state-of-the-art of QKD and quantum communication. It collects reports received from use cases of QKD within the OPENQKD project, each describing the conditions of the individual projects, the deployment processes, results, KPIs and lessons learned during deployment and operation of several different QKD systems in various environments. This includes demonstrations in both scientific, as well as commercial settings.

Table of Contents

Abbreviations and Acronyms

This report uses the following abbreviations and acronyms:

QKD	Quantum Key Distribution
API	Application Programming Interface
QRNG	Quantum Random Number Generator
ETSI	European Telecommunications Standards Institute
ISO	International Organization for Standardization
EU	European Union
KPI	Key Performance Indicators
ITS	Information Technology Solutions
UC	Use Case
WP	Work Package

1 Introduction

1.1 Purpose and scope of the document

Deliverable D8.7 reports on use cases of QKD field trial execution within the OPENQKD project which were completed at the time of writing (February 2023). Among the points discussed are the conditions of the individual projects, the deployment processes, results, KPIs and lessons learned during deployment and operation of various QKD systems in various environments. This includes both scientific demonstrations, as well as demonstrations in a commercial setting.
OPENQKD brings together a multinational consortium with diverse expertise on quantum technology, communication, and security. It brings together providers of QKD devices and technology, both commercial and scientific, with providers of security and networking equipment, testbed providers, and, finally, end users, thus allowing them to experience the possibilities afforded by these technological advances and explore the new paradigms for securing data and communication made possible by quantum technology. We hope to increase awareness of the latest developments in the field and thus help further drive innovation and adoption of QKD, and that the testbeds and use cases described here can lead the way for quantum communication technology and cybersecurity in Europe and beyond.

1.2 Target audience

This report will be accessible publicly via the QPENQKD website. It aims to be of use for potential users of QKD and all wishing to keep informed about state-of-the-art development and adoption of QKD, such as decision makers in policy and industry. This is possible thanks to the diversity of use cases, which explore different technologies, as well as the space of potential applications of QKD in various sectors. This report also allows project partners, as well as all researchers and operators of QKD in general, to compare their systems, modes of operation and performance with these latest achievements and demonstrations.

1.3 Relation to other project work

This report is a result of task T8.4 (*Field Trial Execution and Repeatability)*. The deployment and evaluation, as well as KPIs considered here build upon WP6 (*Quantum Network Functionality*) and WP7 (*Deployment and Operation of QKD Testbeds*). The KPIs themselves are defined by task T6.5 (*Support for Performance Evaluation and Metrics*). Further information on the testbeds is available in D8.3 (T*estbed Replicability and Performance*).
Of further relevance for field trial execution tasks are the open calls (T3.3, *Monitoring the Implementation Phase of Mini-Projects*), as well as T7.4 (*Use-Case Demonstrations),* where the use cases are defined and approved. The requirements and implementation of use cases are informed by task T2.2 *(Derivation of Requirements and Recommendation for Implementation).*

Network performance metrics used to assess use cases are defined in task T8.1 (*Definition of Network Evaluation and Performance*) in coordination with task T6.1 (*Adoption, Extensions and Support for the Layered Networks Approach*).
Further use cases not completed by the time of this deliverable will be reported on in D8.7 (*Second and Final Report on Field Trial Execution*).

1.4 Structure of the report

This report is structured as follows:

- Section 2 comments on the use cases discussed in the report.
- Section 3 provides the information about each completed use case as provided from the operators.

1.5 Template report

Results suitable to be published in a public deliverable
Short description of use-case (10-15 lines) for dissemination (e.g. homepage): Our use-case successfully ….
Picture with the possibility to be published online
Lessons learned: •
KPI demo report: • We were able to encrypt 1GB of data per second using 256 bit AES keys refreshed by QKD once per minute •
Target sector demonstrated impact: • Airport management is now aware of the quantum computing threat and understands security strategies based on QKD and PQC •
AOB: • Other messages.

2 Remarks and Conclusions

In the following, use cases finished by February 2023 are detailed together with the achieved results and KPIs. More information on the definition of the KPIs and on the use cases can be found in D8.1, D8.3 and D8.4, respectively. The individual reports are given as received from the project partners operating the use cases.

Some use cases achieved to demonstrate the new possibilities enabled by quantum key distribution. They all achieved the planed quality and key rates. Mainly due to pandemic with limited access to test sites and deliverable problems, some of the use cases got delayed but most use cases were completed by February 2023 and are reported below.

3 Use Case Reports

3.1 Use Case 02

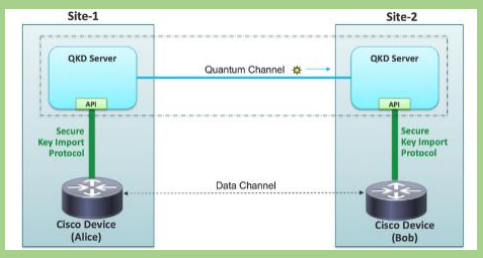
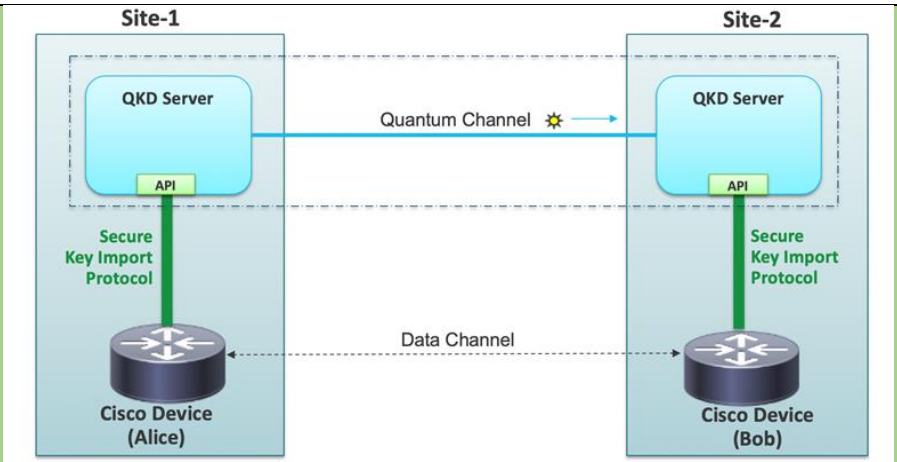
<table>
<tr><td colspan="2">UC: 02
Smart Grid</td><td rowspan="3"> 

Image credit: Cisco</td></tr>
<tr><td colspan="2">Target sector: Critical Infrastructure</td></tr>
<tr><td>Country: CH</td><td>Main site: Geneva</td></tr>
<tr><td colspan="3">Description from Proposal:
For the 7 years to come, SIG will create a Smart grid network to connect its power stations (over 800) in Geneva. Each power station will be connected in p2p fashion to the SIG Telecom optical fibre network and to SIG's Electricity NOC using L2/L3 transport services. To highly secure data transmission/detection intrusion (hackers taking control of the electricity distribution network), SIG would like to test Quantic technology in a real production and operational environment.
Towards this end, SIG will connect two power stations to the QKD testbed and asses available QKD technologies and services offered by our consortium.</td></tr>
<tr><td colspan="2">Partner</td><td>Role/Function</td></tr>
<tr><td colspan="2">ID Quantique (IDQ)</td><td>QKD System provider</td></tr>
<tr><td colspan="2">Services Industriels de Genève (SIG)</td><td>OTN provider and rack provider</td></tr>
<tr><td colspan="3">Impact</td></tr>
<tr><td colspan="2">Target sector planned impact:
Smartgrid communications

Companies attracted through use case:
- Electrical facilities</td><td>Planned KPI demonstrations:
- Measure Latency impact generated by Encryption + QKD
- Measure stability of the link
- Best practice about key rotation update and service continuity when the QKD link is down or the key exchange rate is too low compared to key request rate</td></tr>
<tr><td colspan="3">block diagram</td></tr>
<tr><td colspan="3"></td></tr>
</table>



Existing equipment
Telecom Lab : Use of 2 pairs of fibers, ¼ Rack, power **DIE Power station test**
QKD Systems
Manufacturers and Devices - IDQ: IDQ-02
Link details
List of links (see database): A link has two pairs of dark fibers one for the QKD system and one for classical channels.

Planned deployments

Phase 1 to start in January. Deployment of lab solution. Final deployment planned for March 21, planned to run for 10 months.

Interfaces between layers:

SKIP protocol

Impact

Target sector planned impact:

- Business customer point to point on dedicated link

Companies attracted through use case:

- Business customers (ONG, banking)

Achieved KPI demonstrations:

- QKD key exchange with Cisco IOS-XE equipment
- Stability of the link

Time of demonstration

Deployment:

- Deployment started on Oct 2021 and ran until Feb 2022

Time of demonstration:

- 1 month : Business link run with QKD for 1 month : mid Jan 22 – mid Feb 22

Results

Lessons learned:

- The use case went through several design changes due to technical blockers encountered, that we solved by evolution of the design. We learned that QKD key exchange equipment need as a prerequisite:
  - Dedicated fibre to be able to ensure QKD. No MPLS or active equipment in the middle can be passed through.
  - Fiber certifications need to be provided within precise values.

OTDR Measurements	SCH distance	
	SCH loss in dB	
	QCH distance	
	QCH loss in dB	max 12, 14, 16, 18 dB per model
	distance diff btw SCH and QCH in m	max 20m for auto-cal, 15km manual

  - Physical environment is a key factor for QKD in order to run properly, which implies a datacentre like environment: stable and cooled environment, clean room, rack mount facilities, stable electrical power supply or UPS.
    Environment requirements are :

Environmental	room temperature	15°C ~ 25°C
	dust-free condition 1	30mg/m3 of sand
	dust-free condition 2	0.2mg/m3 of dust
	dust-free condition 3	1.5mg/(m2h) of sedimentation
	proper chassis/rack ground	Must be grounded
	installation space	19" std telecom rack 6U

	voltage level	110 ~ 220 VAC
	outlet type	

- Deployment detailed procedure is needed to achieve a successful installation, including physical cabling, system prerequisites, access. This procedure is very useful for the team deploying the solution. Support from QKD expert is also a must to ensure a quick and efficient deployment.
- Operations team need specific support and expertise for the QKD maintenance. In case of QKD sync issue or key exchange issue, for example, QKD experts support is required to go back to a normal functioning.
- Monitoring of the QKD key exchange may be a challenge to be able to integrate it in a Telco environment. We encountered several changes in the QKD software release which did not allow a proper SNMP management though a telco NMS. We managed to successfully confirm the stability of the links from the customer service perspective.

3.2 Use Case 03

UC: 03

Quantum Vault

Target sector: *Finance (Digital Asset Custody, DAC)*

Country: CH	**Main site:** Geneva

Description from Proposal:

The use of crypto assets is currently increasing at an exponential rate. The secure generation, backup and storage (custody) of these crypto assets is an important issue. A modern solution of storing these assets is based on secret sharing protocols. This use case will exploit QRNGs for the so-called token generation in the key management node (KMN) and QKD for securing the data exchange with three key storage nodes (KSN). Each key storage node will only contain a piece of the original key in a way that you will need access to at least three nodes to reconstruct the key.

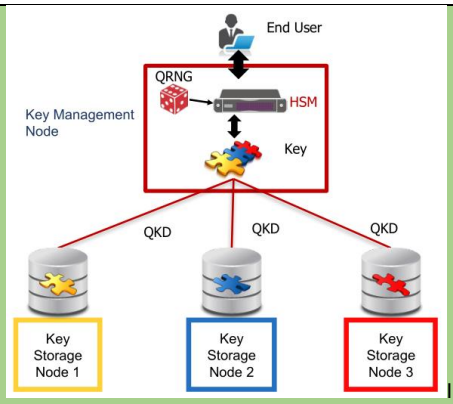


Image credit: IDQ, MTP

Partner	Role/Function
ID Quantique (IDQ)	QKD System provider
Mt Pelerin (MTP)	Service provider
Services Industriels de Genève (SIG)	OTN provider and rack provider
Poznan Supercomputing and Netw. Center (PSNC)	Rack provider
External partner: ATOS	HSM provider

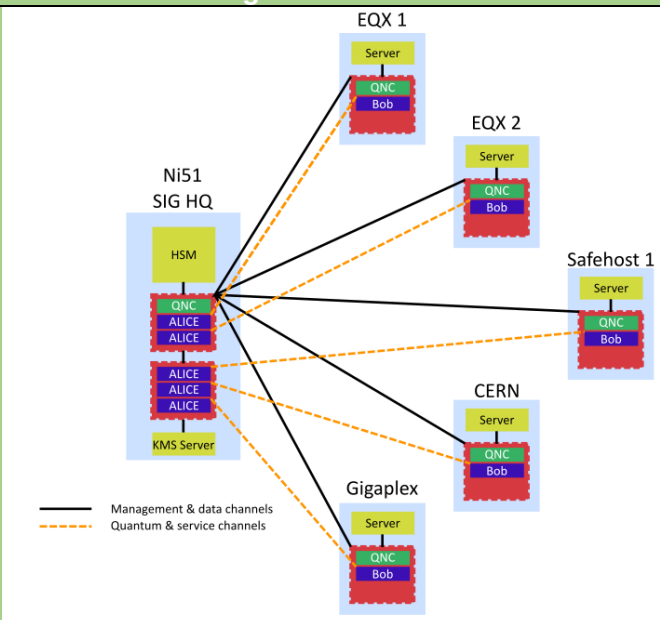
Impact

Target sector planned impact:	**Planned KPI demonstrations:**
Securing the storage of digital assets. **Companies attracted through use case:** - Banks, DAC service provider	1 Number of transaction signature per second 2 Latency of key dissemination 3 Latency of key reconstruction 4 Rate of key reconstitution failure when the system is overloaded 5 Key loss probability (probability of losing 3 pieces of the key which would lead to a loss of assets)

Implementation and block diagram

Work plan/TODO list:

4 Basic concept and topology
5 Find host partners
6 Develop DAC software + interface
7 Prepare QKD system and deployment
8 Schedule exact date for deployment with hardware and personnel
9 Perform deployment
10 Adjust deployment
11 Run use case
12 Offer network to other key users
13 Evaluate findings
14 Retrieve QKD devices
15 Write Report



Site access

- **Ni51** Unrestricted ☐ Restricted ☒
  If restricted how: accompanied by SIG
- **EQX 1** Unrestricted ☐ Restricted ☒
  If restricted how: accompanied by SIG
- **EQX 2** Unrestricted ☐ Restricted ☒
  If restricted how: accompanied by IDQ
- **Safehost 1** Unrestricted ☐ Restricted ☒
  If restricted how: accompanied by SIG
- **Gigaplex** Unrestricted ☐ Restricted ☒
  If restricted how: accompanied by SIG
- **CERN** Unrestricted ☐ Restricted ☒
  If restricted how: accompanied by CERN, SIG

Available power

What power delivery is available for telecom and quantum devices?

- **Ni51** AC 230 ☒ DC 48 ☐
- **EQX 1** AC 230 ☒ DC 48 ☐
- **EQX 2** AC 230 ☒ DC 48 ☐
- **Safehost 1** AC 230 ☒ DC 48 ☐
- **Gigaplex** AC 230 ☒ DC 48 ☐
- **CERN** AC 230 ☒ DC 48 ☐

Internet connection (closed LAN with remote access via VPN)

- **Ni51** Yes ☒ No ☐
- **EQX 1** Yes ☒ No ☐
- **EQX 2** Yes ☒ No ☐
- **Safehost 1** Yes ☒ No ☐
- **Gigaplex** Yes ☒ No ☐
- **CERN** Yes ☒ No ☐

Server

Manufacturers and Devices

- MTP
  o HSM (from ATOS)
  o 5x Raspberry Pi 4 (Server)
- IDQ
  o KMS Server

QKD Systems

Manufacturers and Devices
- IDQ
  o IDQ-02
  o IDQ-03
  o IDQ-04
  o IDQ-05
  o IDQ-06

Link details
List of links (see database): • GVA: SIG HQ – Gigaplex • GVA: SIG HQ - Safehost 1 • GVA: SIG HQ – CERN • GVA: SIG HQ - Equinix 2 • GVA: SIG HQ - Equinix 1 Every link has two dark fibers. The six-node network shares a proper LAN that is accessible via a VPN tunnel.
Interfaces
Interfaces between layers: - ETSI 014 interface between QKD and MTP HSM/Server

3.3 Use Case 12

UC: 12

QKD in Cloud Datacenters

Target sector: *Datacenters*

Country: **GR**	**Main site: Athens**

Description from Proposal:

Data security and privacy are among the top concerns in the datacenter environment. The

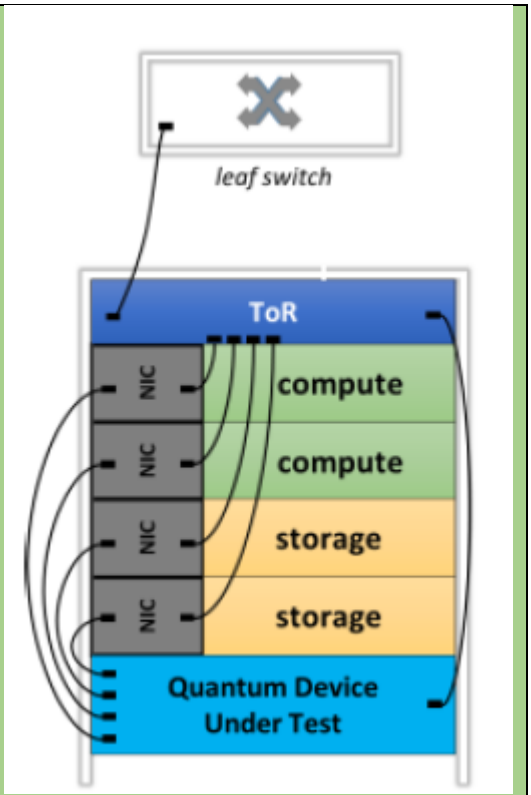
financial cost of a security breach can be substantial, especially when customer data is exposed.

Sensitive data has historically been protected by IP segmentation and firewalls with intrusion prevention systems that were simpler and faster than encryption. However, this model is now changing. As workloads in the corporate data center begin to migrate to the public cloud, the need to encrypt any data traversing the network becomes foundational. Hyperscale cloud service providers are increasingly enabling encryption across their massive DCI networks to meet customer expectations.

In order to eliminate vulnerabilities in the public cloud infrastructure all segments of the cloud datacenter network will need to be fortified with encryption.

New crypto acceleration devices are becoming available that mitigate the performance degradations imposed by encryption, thus laying inroads to the broad introduction of encryption in the datacenter.

The generalized introduction of encryption in the cloud datacenter can offer additional benefits in the flexibility and efficiency of the cloud infrastructure. If the encryption system being deployed can span multiple hybrid clouds, it allows the IT team to think about clouds simply as pools of capacity. End-to-end connections will be deployed using commercial datacenter networking equipment working in liaison with QKD infrastructure and will be evaluated in a realistic datacenter setting.



Partner	Role/Function
Mellanox Technologies (MLNX)	Testbed provider
Mellanox Technologies (MLNX)	End user
ID Quantique (IDQ)	QKD System provider
Toshiba (TEUR)	QKD System provider

Impact	
Target sector planned impact: -Provide true randomness to classical security in the DC -Provide end to end QKD inside DC **Companies attracted through use case:** - Mellanox, DC users/owners	**Planned KPI demonstrations:** - Providing a key rate high enough to support apps - QKD-exchanged key delivery latency to encryptors - Compliance with temperature and cost targets in the datacenter - Stability of the link

Implementation

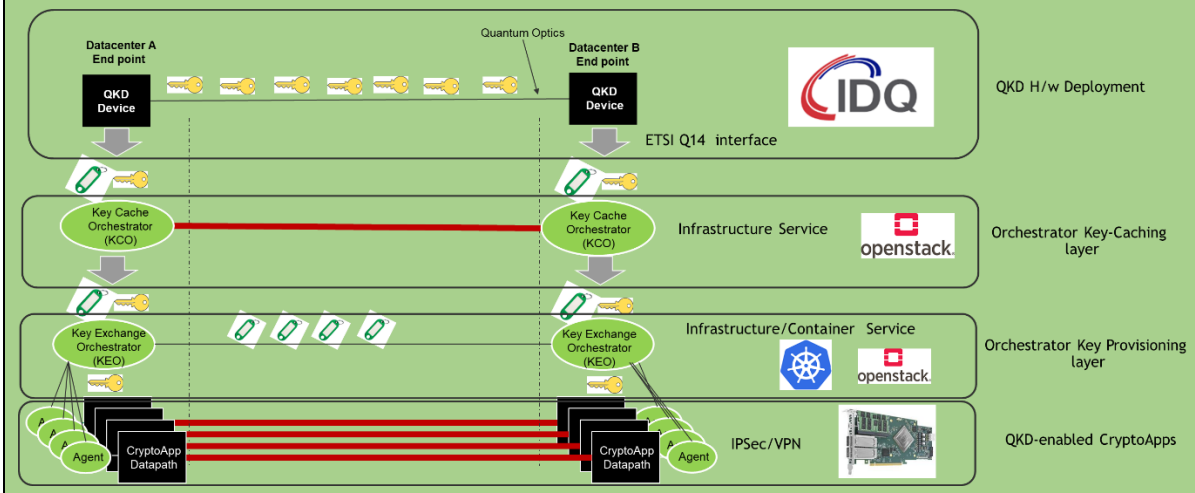
Work plan:

1. Software on MLNX NICs for receiving and using QKD-exchanged keys
2. Key management framework
3. Integration of QKD devices on the MLNX testbed

QRNG

4. Software on MLNX NICs for using the random numbers
5. Identify QRNGs with USB interface
6. Demonstrate high performance classical security with random numbers

Block diagram



Site access

- **Site1** Unrestricted ☒ Restricted ☐
  If restricted how:

Available power

What power delivery is available for telecom and quantum devices?

- **Site1** AC 230 ☒ DC 48 ☐
- **Site2** AC 230 ☐ DC 48 ☐
- **Site3** AC 230 ☐ DC 48 ☐

Internet connection

- **Site1** Yes ☒ No ☐

Existing equipment

What else is available and can be used?

Site1

- Bluefield SmartNICs
- Key management infrastructure (in progress)
- IDQ Cerberis 3 (C-band)
-

Encryptors

Manufacturers and Devices

- MLNX Bluefield SmartNIC

QKD Systems

Manufacturers and Devices

- ID Quantique (IDQ Cerberis 3, C-Band)
- Toshiba (Multiplexed, O-Band)

Link details

Please fill out the following list for each link (physical connection between two nodes):

Link1 (QRNGs)

- Classical encrypted link between the two Mellanox NICs
- USB for QRNG to host communication

Link2 (QKD system from Civiq)

- IPsec tunnel between MLNX endpoints using the QKD exchanged keys
- Dark fiber for QKD channel
- Co-existence for the sync & user channel (if exists)

Planned deployments

Deployment1 (QRNGs)

- Classical link and security protocols between two Mellanox NICs

Deployment2 (QKD system from Civiq)

- Link 1: 2x Bluefield SmartNICs, IDQ Cerberis 3 (C band)
- IPsec tunnel between two MLNX endpoints using the QKD exchanged keys

Interfaces between layers:

- USB interface for QRNG connection
- ETSI 14 interface for keys delivery
- Key management infrastructure

3.4 Use Case 14

UC: 14

Secured Datacenter Interconnection

Target sector: *Any sector using Datacenters (Telecom)*

Country: CH

Main site: Geneva

Description from Proposal:

The use of QKD combined with network encryption allows to propose quantum-safe connectivity. Indeed, today the private key exchange for AES-256 encryption uses RSA, Diffie-Hellman or Elliptic Curve which will be broken by quantum computers using Shor Algorithm. QKD provides the same secure key simultaneously in two locations where the data is encrypted / decrypted. This use case shows how IDQ QKD can be combined with ADVA FSP3K encryption using the standard ETSI interface (REST API QKD 014) in the case of datacenter interconnect, exchanging 10 Gbps of encrypted data.

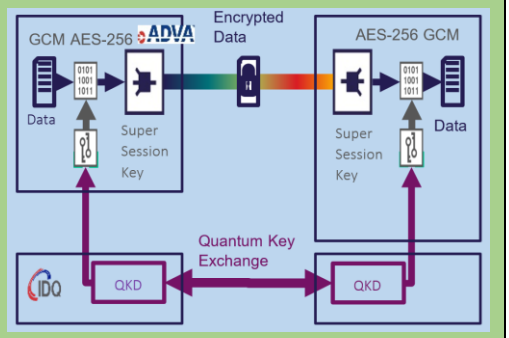


Image credit: IDQ, ADVA

Partner	Role/Function
ID Quantique (IDQ)	QKD System provider
ADVA (ADV)	Service provider
Services Industriels de Genève (SIG)	OTN provider and rack provider

Impact

Target sector planned impact:
Telecom Datacenter Interconnect.

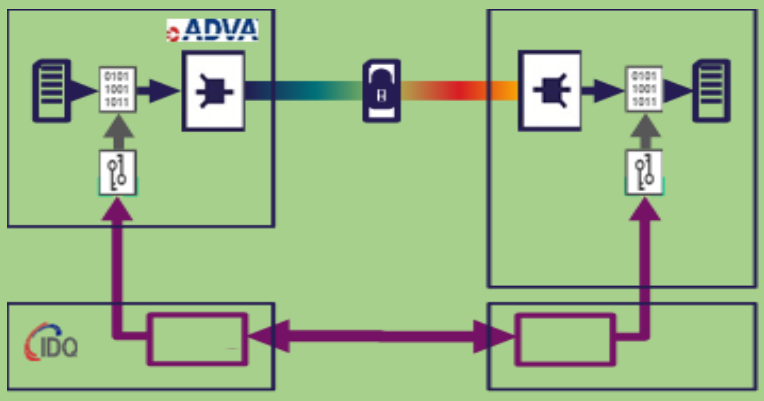
Companies attracted through use case:

- Service Providers
- Large companies with private Datacenters
- Cloud Providers

Planned KPI demonstrations:

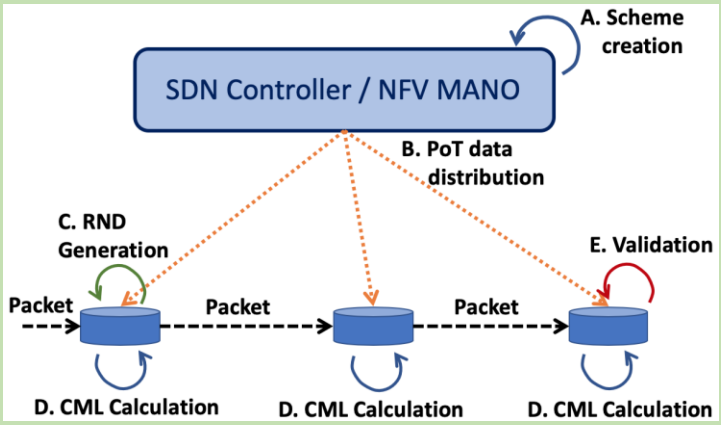
4 Measure Latency impact generated by Encryption + QKD
5 Measure stability of the link
6 Best practise about key rotation update
7 ADVA service continuity when the QKD link is down or the key exchange rate is too low compared to key request rate

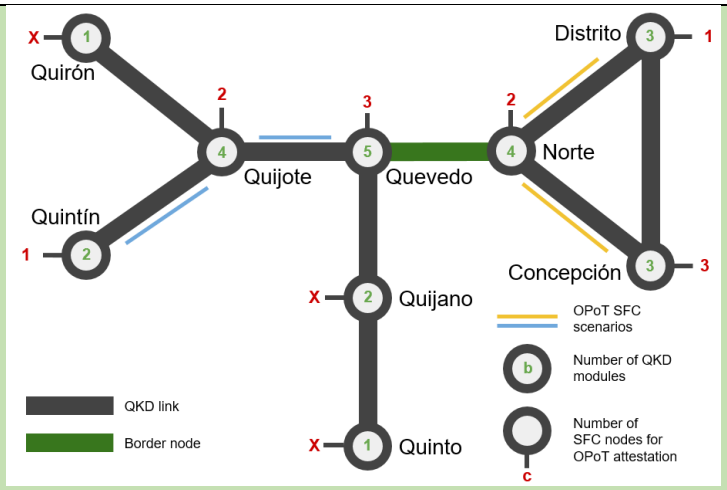
block diagram

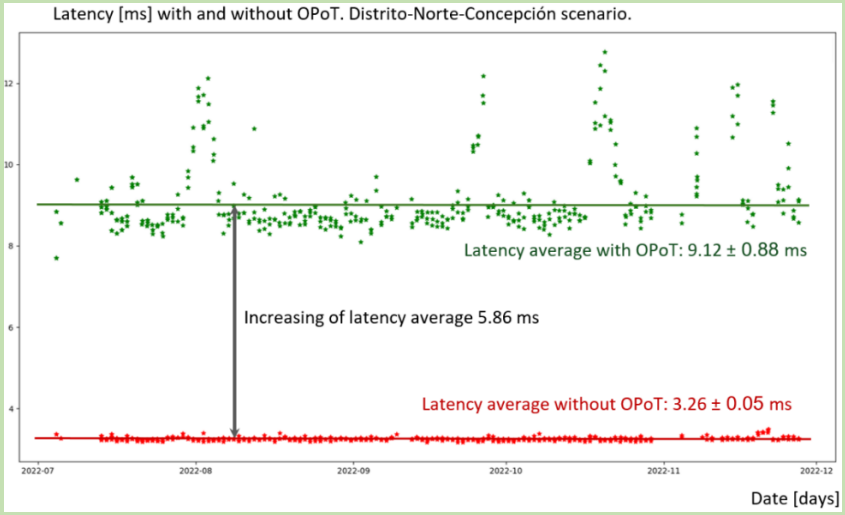


Existing equipment
What else is available and can be used? **Ni51:** Use of 2 pairs of fibers, ¼ Rack, power **IBM Gigaplex Datacenter:** Use of 2 pairs of fibers, ¼ Rack, power
MUX / DEMUX
Manufacturers and Devices - ADVA   o 1 MUX / DEMUX for classical channels
QKD Systems
Manufacturers and Devices - IDQ: IDQ-01
Link details
List of links (see database): - GVA: SIG HQ – IBM Gigaplex A link has two pairs of dark fibers one for the QKD system and one for classical channels. - ETSI 014 interface between QKD and ADVA FSP3K

3.5 Use Case 15

Use Case 15 – UPM Opot
Short description of use-case: Our use-case successfully demonstrates that the QKD services can be used for enhancing the security of technologies used in network security and attestation. Specifically, this use-case shows the ability to guarantee that a given network packet has passed through certain network functions and in a given order, namely ordered proof of transit (OPoT) for service function chaining (SFC). This technology is one of the most powerful mechanisms to ensure that the services in a network are working as expected and to make them resilient against attacks. Furthermore, it allows to attest the service or monitored behavior in case of legal issues. The solution tested in this use-case is proposes that the OPoT technology developed by UPM consumes the quantum-distributed keys as a resource and performs its functionality. However, given the threat to asymmetric cryptography that may be caused by quantum computing technologies, the information-theoretic secure (ITS) symmetric key provided by QKD ensures the delivery of a quantum-safe service resistant to that security concerns.
Picture: 
Lessons learned: - As the OPoT implementation is a software program, it needs enough computational power to perform the encryption of the communications relayed.
KPI demo report: - The following figures show a map of the network with the two scenarios where this use case has been evaluated and the increasing in the latency of delivering the service using the OPoT technology in one of them:





- We conclude that this latency increase allows using this solution without major penalties.

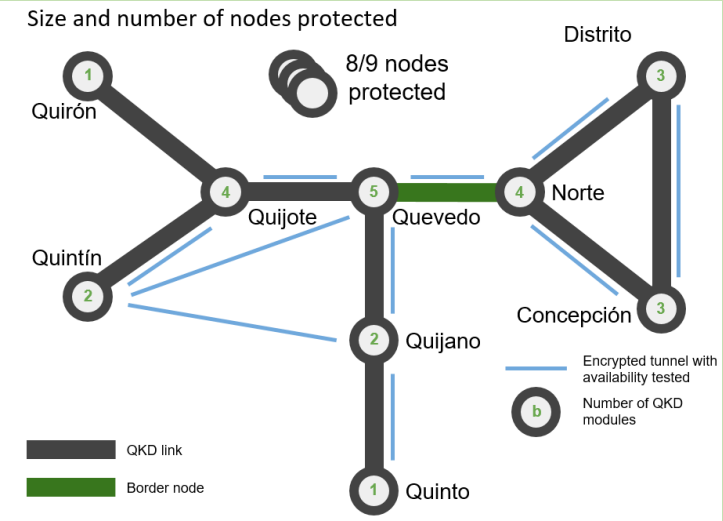
Target sector demonstrated impact:

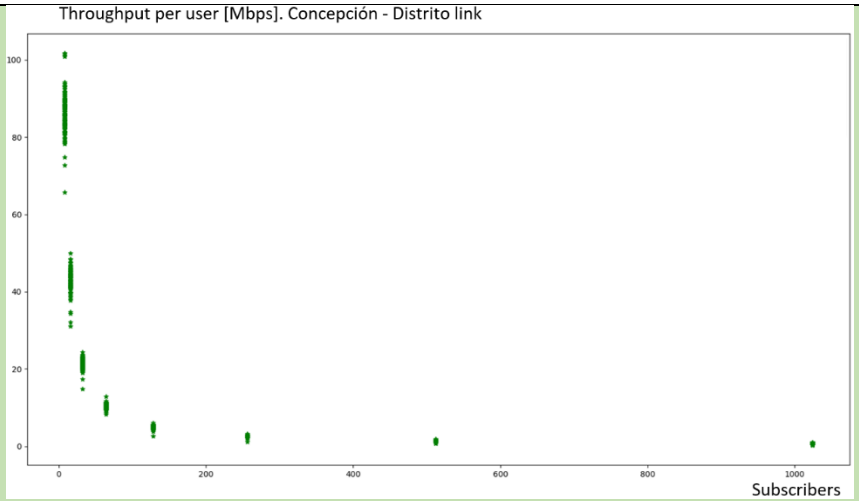
- Telco operators interested in services function chaining (SFC).
- Securing of telecommunication network providers.

AOB:

- The OPoT technology was successfully patented by the partner TID (…).

3.6 Use Case 16

Use Case 16 - UPM CIP
Short description of use-case: Our use-case successfully demonstrates that the QKD services can be used for enhancing the security of technologies used in critical infrastructures protection. Specifically, this use-case shows the ability to secure critical traffic such as the one generated when monitoring and managing industrial infrastructures remotely through the network. This kind of traffic, such as SCADA (Supervisory Control and Data Acquisition) is responsible for infrastructures that control systems ranging from the water supply to the electrical grid and are, thus, critical to our society. The solution tested in this use-case proposes that an IPSec tunnel consumes the quantum-distributed key as a resource and performs its functionality. SCADA data traffic is transmitted through this ITS protected tunnel. Given the threat to asymmetric cryptography that may be caused by quantum computing technologies, the information-theoretic secure (ITS) symmetric key provided by QKD ensures the delivery of a quantum-safe service resistant to that security concerns.
Lessons learned: - As the IPSec implementation is a software program, it needs enough computational power to perform the encryption of the communications relayed.
KPI demo report: - These figures show where the solution, IPSec encrypted tunnelling, has been deployed and tested among the network and an example of its scalability as a function of the number of subscribers: 

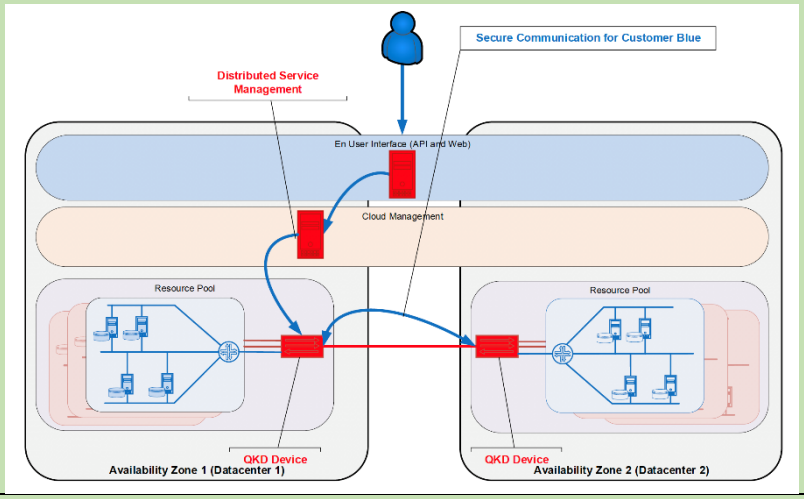


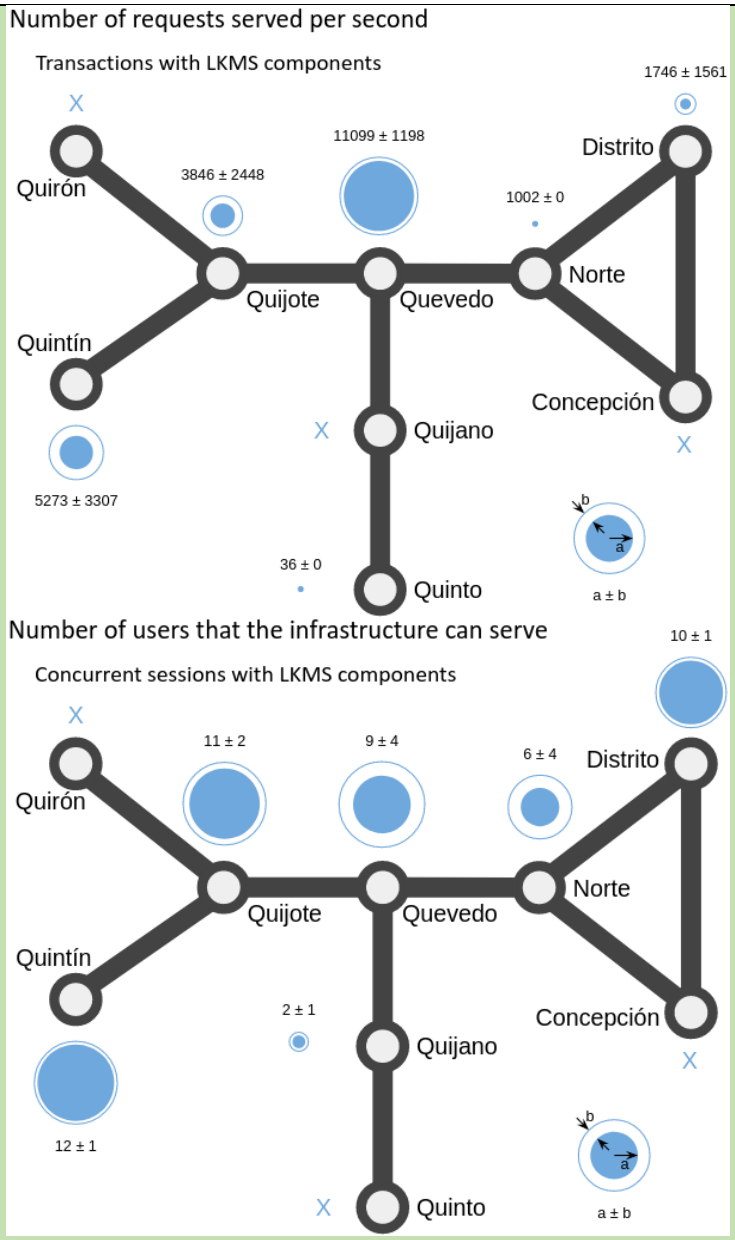
- We asses that the performance of the solution shows that it offers a quality-of-service equivalent to other solutions in the same range.

Target sector demonstrated impact:

- Securing critical infrastructures such as the central offices of telecommunication network providers.

3.7 Use Case 17

Use Case 17 – UPM QKD_Cloud
Our use-case successfully demonstrates that the QKD services can be delivered concurrently in a cloud environment to several hosted applications. Specifically, this use-case shows how the QKD network components can be used in such an environment, namely the local key management system (LKMS) in each node and the SDN control and operation system by UPM (SDN Stack). The solution tested in this use-case proposes that ach hosted application may consume the quantum-distributed key as a resource and performs its functionality. Given the threat to asymmetric cryptography that may be caused by quantum computing technologies, the information-theoretic secure (ITS) symmetric key provided by QKD ensures the delivery of a quantum-safe services resistant to that security concerns.
Picture: 
Lessons learned: - The QKD infrastructure is ready to support cloud services, but its performance depends on the environment chosen (e.g. OpenStack vs AWS).
KPI demo report: - The following figures show the performance of the network elements for supporting this use case. The first one measures how many key extractions can handle the key management system in each node (LKMS) while the second one measures the concurrent connections that the network can serve (both LKMS and the SDN controlling).

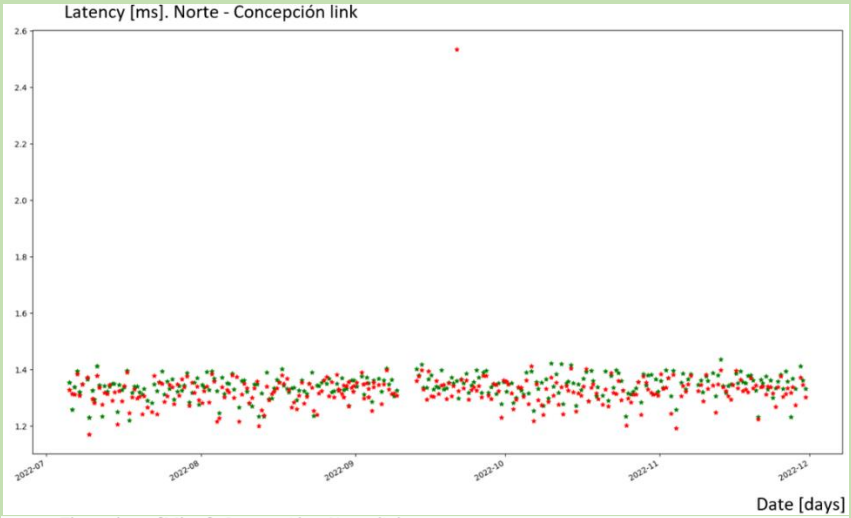
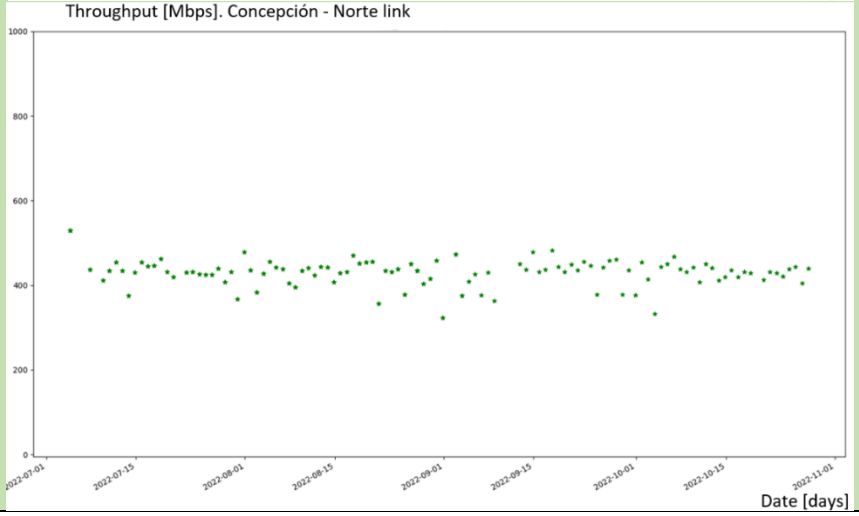


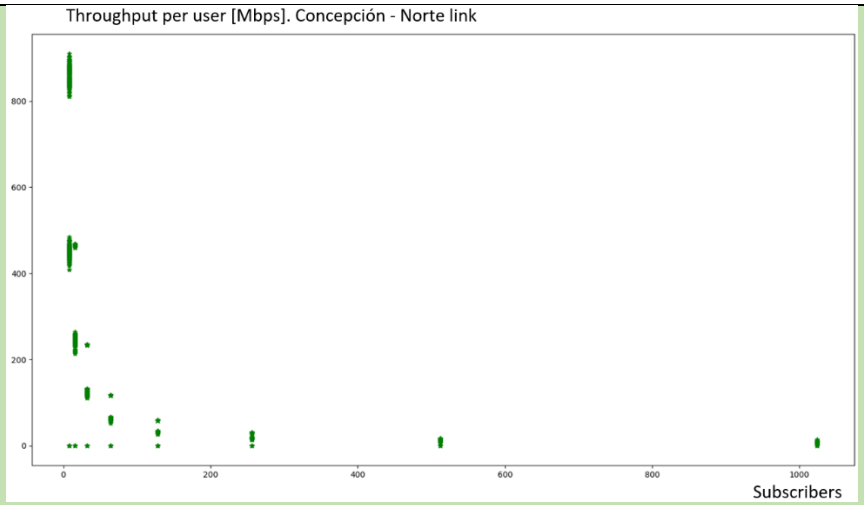
- We asses that the performance of the infrastructure allows concurrent access of several final applications hosted in a cloud environment.

Target sector demonstrated impact:

- Securing the communications of application programs hosted in a cloud infrastructure.

3.8 Use Case 18

Use Case 18 – UPM QKD_Cloud
Short description of use-case: Our use-case successfully demonstrates that the QKD services can be used for enhancing the security of technologies used to secure health related data and services. Specifically, this use-case shows the ability of securing the data traffic that supports e-Health services. This kind of traffic is often highly regulated since it may involve medical information and personal data of patients, so its securitization is critical using remote or distributed applications. The solution tested in this use-case proposes that an IPSec tunnel consumes the quantum-distributed key as a resource and performs its functionality. Through this ITS protected tunnel a special type of medical data is transmitted. Given the threat to asymmetric cryptography that may be caused by quantum computing technologies, the information-theoretic secure (ITS) symmetric key provided by QKD ensures the delivery of a quantum-safe service resistant to that security concerns.
Lessons learned: - As the IPSec implementation is a software program, it needs enough computational power to perform the encryption of the communications relayed.
KPI demo report: - The following pictures show the performance of the solution, IPSec encrypted tunnelling, in Norte-Concepción link in terms of latency, throughput and throughput as a function of subscribers:    

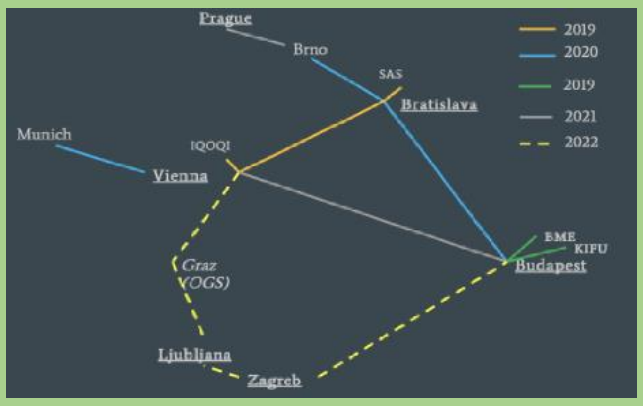


- We asses that the performance of the solution shows that it offers a quality-of-service equivalent to other solutions in the same range.

Target sector demonstrated impact:

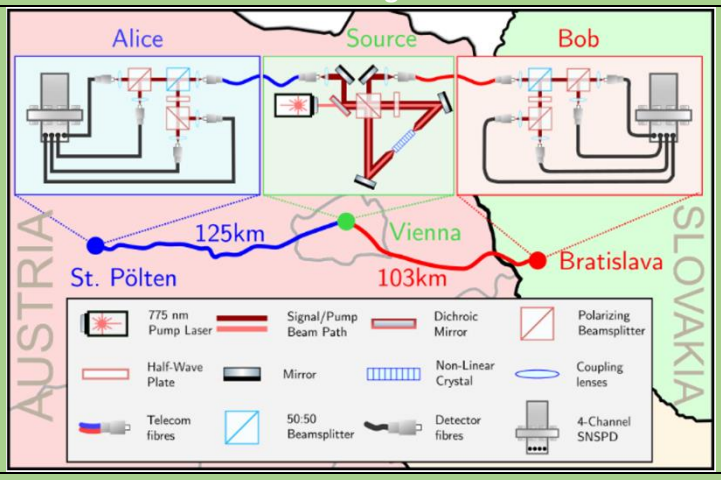
- Securing the traffic of health institutions.

3.9 Use Case 19

UC: 19 **Building a European quantum internet**	
Target sector: Research & Education	
Country: AT	**Main site:** IQOQI Vienna
Description from Proposal: With use case #19 we intend to connect capital cities in the European Union over a quantum link, thus enabling the production of a shared secret random key. The cities will be connected via classical telecommunication fibers with a wavelength of 1550 nm. This trusted-node free QKD system will allow 24/7 key generation.	

Partner	Role/Function
OEAW	QKD System provider
Slovak Academy of Sciences	Partner in Bratislava
Türk Telekom International AT AG	Glass Fiber Provider

Impact	
Target sector planned impact: Connecting academic institutions between Vienna and Bratislava with a reliable QKD system (Austrian and Slovak Academia of Sciences). St. Pölten was chosen because of its vicinity to Germany for future collaborations.	**Planned KPI demonstrations:** - Entanglement based 24/7 operation of QKD-secured long-distance links over several months without readjusting the setup - Developing a publicly accessible online-dashboard with real-time data updates and key generation - Optimized dispersion compensation - Low bandwidth polarization compensation

Block diagram

Existing equipment
What else is available and can be used? **St. Pölten** - Data warehouse room with 230V and AC - Glass fiber to connect the Receiver-module - Receiver-module - Superconducting nanowire (four channel) detector **Vienna** - Fully operational laboratory - EPR Source - Optical spare parts **Bratislava** - Glass fiber to connect the Receiver-module - Receiver-module - Superconducting nanowire detector

Encryptors
Manufacturers and Devices - IQOQI-made algorithms
QKD Systems

Manufacturers and Devices
- Single Quantum
  o SNSPD
- Toptica Photonics
  o High-power Laser
- PPLN based Telecommunication-band source

Link details

Please fill out the following list for each link (physical connection between two nodes):
 	
St. Pölten – Vienna
- Number of parallel fibers: **2**
- Optical fiber details: length of fiber, attenuations in dB, type of fiber, quality of connection (heavily spliced, old, direct connection) constraints/add-ons (e.g. filters or dispersion compensation)
  o Length: **123 660 m**
  o **0,23 dB/km**
  o measured attenuation for fiber 1: **25,73 dB**
  o measured attenuation for fiber 2: **26,03 dB**
  o Type of fiber: **Dark Fiber**
  o Constraints: **None**
  o Add-ons: **Dispersion compensation**
 	
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
  ○ For classical communication LTE will be used
  ○ For QKD Channel occupied wavelengths are ITU Ch 28 (1554.94 nm) & Ch 40 (1545.32 nm)
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
  ○ **Dark Fiber**
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)
  ○ **None**
 	
Vienna - Bratislava
- Number of parallel fibers: **2**
- Optical fiber details: length of fiber, attenuations in dB, type of fiber, quality of connection (spliced, old, direct connection) constraints/add-ons (e.g. filters or dispersion compensation)
  o Length: **100 880 m**
  o **0,23 dB/km**
  o measured attenuation for fiber 1: **22,07 dB**
  o measured attenuation for fiber 2: **22,43 dB**
  o Type of fiber: **Dark Fiber**
  o Constraints: **None**
  o Add-ons: **Dispersion compensation**

- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
  - For classical communication LTE will be used
  - For QKD Channel occupied wavelengths are ITU Ch 28 (1554.94 nm) & Ch 40 (1545.32 nm)

- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
  - **Dark**
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)
  - **Restricted to 1550.12 to 1552.12 nm in one channel and 1548.12 to 1550.12 nm due to dispersion compensation module**

Planned deployments

- St. Pölten - Vienna, 3243 Phyrra (AUT), Sebastian Neumann, Lukas Achatz, February 2020 - March 2020
- Vienna - Bratislava, 851 01 Bratislava (SVK), Sebastian Neumann, Lukas Achatz, February 2020 – March 2020

Interfaces between layers:

- Employing IQOQI-written software between all layers
- Implementing communication APIs between IQOQI-written and external software

Results

KPI demo report:

- Establishment of 24/7 quantum connections over altogether several weeks, longest uninterrupted time: 8 days
- Optimized dispersion compensation has been achieved, temporal detection precision limited by electronics only
- Polarization compensation successful, with 75% duty cycle

Target sector demonstrated impact:

- Connected academic institutions between Vienna and Bratislava with a reliable QKD system (Austrian and Slovak Academia of Sciences)
- Scientific publications submitted to high-impact journals

Impact

Target sector planned impact:

- Connecting members of the European Union by implementing a trusted-node free QKD System to allow secure communication between research facilities has been successful

Companies attracted through use case:

- N.a. (Scientific research demonstration)

Achieved KPI demonstrations:

- Establishment of 24/7 quantum connections over altogether several weeks, longest uninterrupted time: 8 days
- QKD-secured and stable communication between European research facilities successful
- Optimized dispersion compensation has been achieved, temporal detection precision limited by electronics only
- Polarization compensation successful, with 75% duty cycle

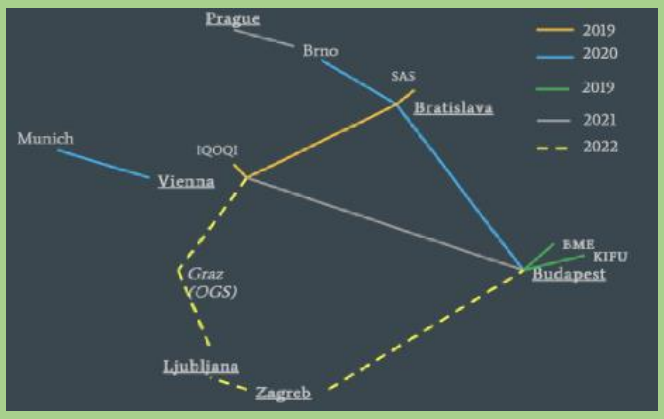
Time of demonstration

Deployment:

- Start of deployment: June 2019, ready for experiments: July 2021

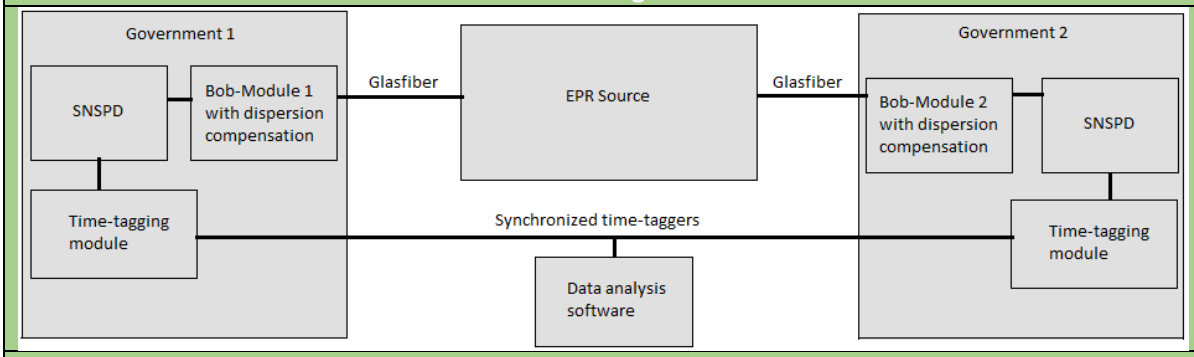
Time of demonstration: - July 2021 – December 2021, QKD-runs starting in September, 3 successful runs of 3 days, 8 days, 4 days
Results
Lessons learned: - Automatized polarization compensation is substantially slowed down by high loss and therefore low detection rates due to the long integration times necessary for determining the actual quality of entanglement - PMD in the fibers is not a problem for 100 GHz broad channels around 1550 nm - Classical internet connections less stable than our quantum ones, especially if one has to rely on the mobile network - More information can be inquired from our open-access publication: https://arxiv.org/abs/2203.12417
Changes necessary to already deployed infrastructure: - All overland fiber stretches had to be spliced together rather than passing optical amplifiers in every (classical) repeater station - Air-condition in receiver stations had to be enhanced in order to compensate for excess heat from helium compressor
Target sector demonstrated impact: - Connected academic institutions between Vienna and Bratislava with a reliable QKD system (Austrian and Slovak Academia of Sciences) - Scientific publications submitted to high-impact journals: https://arxiv.org/ftp/arxiv/papers/2203/2203.12417.pdf https://arxiv.org/pdf/2107.07756v2.pdf https://journals.aps.org/pra/pdf/10.1103/PhysRevA.104.022406 https://iopscience.iop.org/article/10.1088/2058-9565/abe5ee

3.10 Use Case 20

UC: 20 **Building a European quantum internet**	
Target sector: Research & Education	
Country: AT | **Main site:** IQOQI Vienna	
Description from Proposal: With use case #20 we intend to implement a QKD network between members of the European Union. The network will be implemented between Vienna (AT), Prague (CZ), Bratislava (SK), Budapest (HU) and potentially Zagreb (CR) and Ljubljana (SI). With this, the respective governments will be able to communicate in full secrecy without having to trust third parties.	

Partner	Role/Function
OEAW	QKD System provider
Slovak Academy of Sciences	Partner in Bratislava
Ruder Boskovic Institute	Partner in Zagreb
Department of Telecommunication and Media Informatics	Partner in Budapest
Cesnet	Technical support
Türk Telekom International AT AG	Glass Fiber Provider

Impact	
Target sector planned impact: Connecting members of the European Union by implementing a trusted-node free QKD System to allow secure inter-government communication.	**Planned KPI demonstrations:** - Entanglement based 24/7 operation of QKD-secured long-distance links over several months without readjusting the setup - Low bandwidth polarization compensation - QKD-secured and stable communication between European embassies and governments

Block diagram

Existing equipment
What else is available and can be used? **St. Pölten** - Glass fiber to connect the Receiver-module - Receiver-module - Superconducting nanowire detector **Vienna** - Fully operational laboratory - EPR Source - Optical spare parts **Bratislava** - Glass fiber to connect the Receiver-module - Receiver-module - Superconducting nanowire detector
Encryptors
Manufacturers and Devices o IQOQI-made algorithms

QKD Systems

Manufacturers and Devices

- Single Quantum
  - SNSPD
- Toptica Photonics
  - High-power Laser
  - PPLN based Telecommunication-band source

Link details

Please fill out the following list for each link (physical connection between two nodes):

St. Pölten – Vienna

- Number of parallel fibers: **2**
- Optical fiber details: length of fiber, attenuations in dB, type of fiber, quality of connection (heavily spliced, old, direct connection) constraints/add-ons (e.g. filters or dispersion compensation)
  - Length: **123 660 m**
  - **0,23 dB/km**
  - measured attenuation for fiber 1: **25,73 dB**
  - measured attenuation for fiber 2: **26,03 dB**
  - Type of fiber: **Dark Fiber**
  - Constraints: **None**
  - Add-ons: **Dispersion compensation**

- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
  - For classical communication LTE will be used
  - For QKD Channel occupied wavelengths are ITU Ch 28 (1554.94 nm) & Ch 40 (1545.32 nm)
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
  - **Dark Fiber**
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)
  - **None**

Vienna - Bratislava

- Number of parallel fibers: **2**
- Optical fiber details: length of fiber, attenuations in dB, type of fiber, quality of connection (heavily spliced, old, direct connection) constraints/add-ons (e.g. filters or dispersion compensation)
  - Length: **100 880 m**
  - **0,23 dB/km**
  - measured attenuation for fiber 1: **22,07 dB**
  - measured attenuation for fiber 2: **22,43 dB**
  - Type of fiber: **Dark Fiber**
  - Constraints: **None**
  - Add-ons: **Dispersion compensation**

- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
  - For classical communication LTE will be used

○ For QKD Channel occupied wavelengths are ITU Ch 28 (1554.94 nm) & Ch 40 (1545.32 nm) - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed ○ **Dark** - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) ○ **None** -
Planned deployments
- Vienna - Bratislava, 851 01 Bratislava (SVK), Sebastian Neumann, Lukas Achatz, February 2020 – March 2020
Interfaces between layers: - Employing IQOQI-written software between all layers - Implementing communication APIs between IQOQI-written and external software
Results
Lessons learned: - Automatized polarization compensation is substantially slowed down by high loss and therefore low detection rates due to the long integration times necessary for determining the actual quality of entanglement - PMD in the fibers is not a problem for 100 GHz broad channels around 1550 nm - Classical internet connections less stable than our quantum ones, especially if one has to rely on the mobile network - More information can be inquired from our open-access publication: https://arxiv.org/abs/2203.12417
Changes necessary to already deployed infrastructure: - All overland fiber stretches had to be spliced together rather than passing optical amplifiers in every (classical) repeater station - Air-condition in receiver stations had to be enhanced in order to compensate for excess heat from helium compressor
KPI demo report: - Entanglement based 24/7 operation of QKD-secured long-distance links over several weeks (instead months) without readjusting the setup - Low bandwidth polarization compensation successful, 75% duty cycle
Target sector demonstrated impact: - Connecting members of the European Union by implementing a trusted-node free QKD System to allow secure communication (between research facilities) has been successful

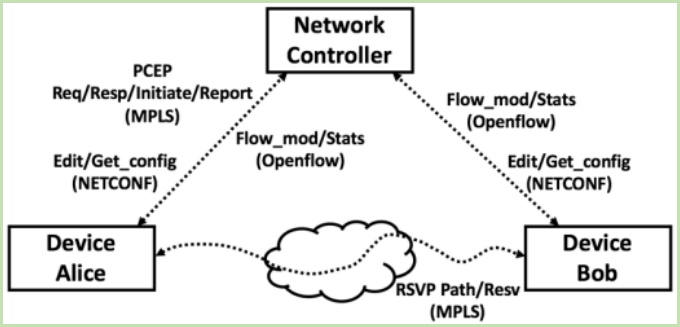
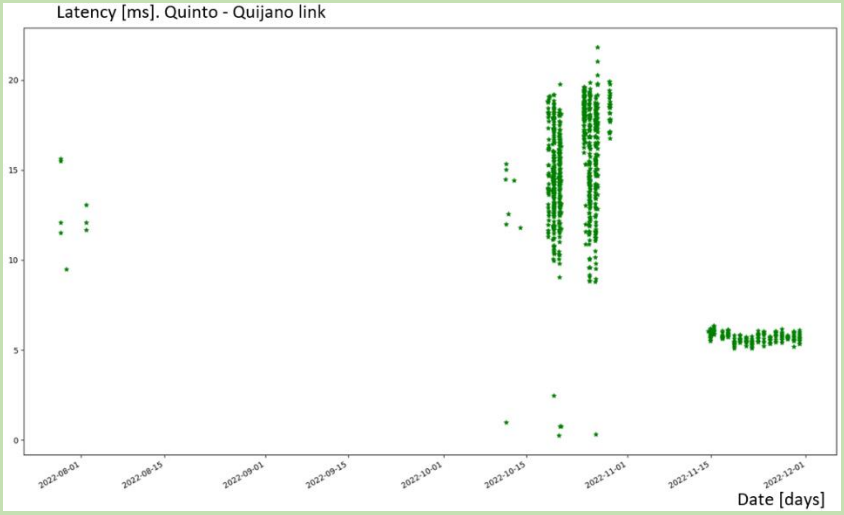
3.11 Use Case 23

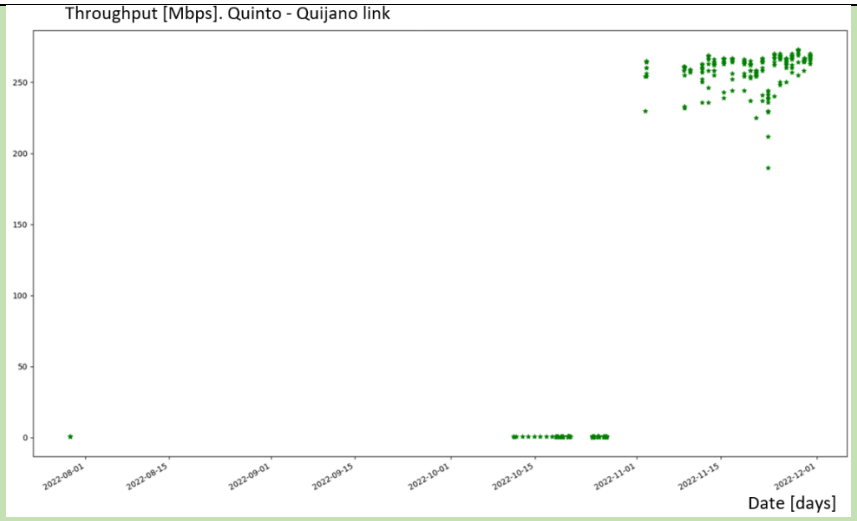
Use Case 23: Globally securing space and ground infrastructure

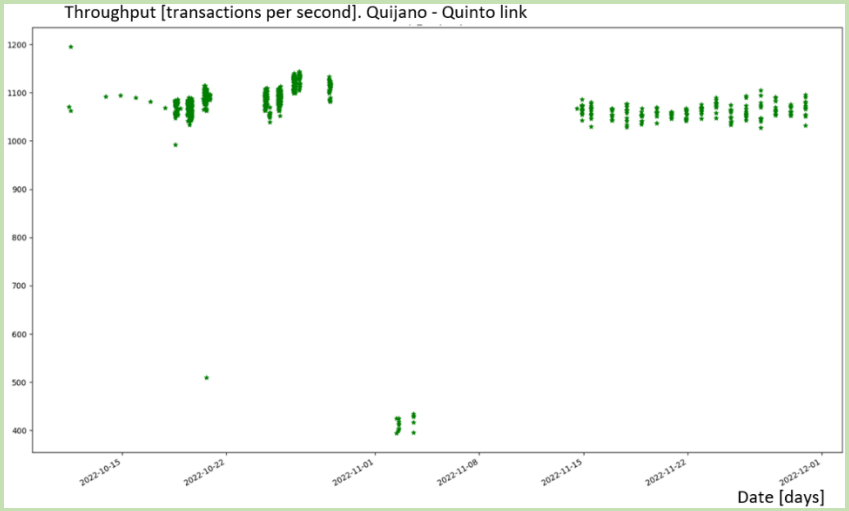
Lessons learned:
- Network connection is the trickiest part, setting the internet connection required a day and a half of debugging (while QKD devices were functional in 30 min and clock data logging and transmission were tested beforehand).
- The firewall got in the way 3 times.
  o Router problem 1: data was blocked by DLR-KN general firewall, due to wrong interface configuration. Internal interface rules were set on the virtual WAN interface (from outside to inside) but not virtual LABOR interface (from inside to outside). As a result, pinging between the device was possible, but TCP and UDP traffic was blocked by the firewall rules.
  o Router problem 2: the firewall in Matera had unclear markings of the required IP addresses, different IP settings had to be tried out before one finally worked.
  o Router problem 3: the Windows firewall on the acquisition PC was also blocking the data in the virtual subnet spanning across Matera and DLR-KN. The data transfer between PCs got tested beforehand locally, but then it did not work when the subnet between the two labs was established. This is probably due to the MTU sizes – the encryptors add extra headers/data to the frames and the packages are chopped by the network devices afterwards, and this chopping breaks the functionality. Turning off the Windows firewall on the clock data acquisition PC solved the issue.
- Router selection: using openWrt may be advisable, it is a Linux distribution that allows package retrieval via a package manager, which is allows for faster and easier debugging.

Changes necessary to already deployed infrastructure: - IT support will be required for setup of real-world application. Achieving practical security (e.g., against DOS attacks) has a large overhead over to the deployment of the QKD devices alone.
KPI demo report: - We were able to establish quantum keys simultaneously in the MLRO laboratories in Matera and in DLR site in Oberpfaffenhofen (using 4 devices in total: a QKD transmitter and a QKD receiver in each of the two locations); these were used to forward a quantum key with one-time padding, as required for last-mile connections in real QKD applications. - We were able to collect clock and GNSS data simultaneously in both locations for almost two days – with short interruptions due to the unintended resetting of one of the GNSS receivers. - We have encrypted the clock data and GPS data and transfer it over the internet (sent from MLRO to DLR)
Target sector demonstrated impact: - Establishing and securing a precise UTC by synchronising clocks in different labs - Synchronisation of clocks in Precise Timing Facilities for reliable and secure operation of GNSS constellations
AOB: - In future application, a satellite capable of establishing QKD link may become available and the use case may be implemented including also the space segment – rather than emulating it.

3.12 Use Case 25

Use Case 25 – UPM B2-5G
Our use-case successfully demonstrates that the QKD services can be used for enhancing the security of technologies used in business to business (B2B) communications, specially through the 5G access network. Specifically, this use-case shows the ability of securing the data traffic of services on top of the transport network to incorporate quantum-safe security for end users communications: VPNs or connectivity from 5G base stations to core or data centre premises, for instance. The solution tested in this use-case proposes an IPSec tunnel that consumes the quantum-distributed key as a resource and performs its functionality through the simulated 5G infra-structure. Given the threat to asymmetric cryptography that may be caused by quantum computing technologies, the information-theoretic secure (ITS) symmetric key provided by QKD ensures the delivery of a quantum-safe service resistant to that security concerns.
Picture: 
Lessons learned: - As the IPSec implementation is a software program, it needs enough computational power to perform the encryption of the communications relayed.
KPI demo report: - The following pictures show the performance of the solution, IPSec encrypted tun-nelling through a 5G access network, in Quinto-Quijano link in terms of latency, throughput and transactions as a function of time: 



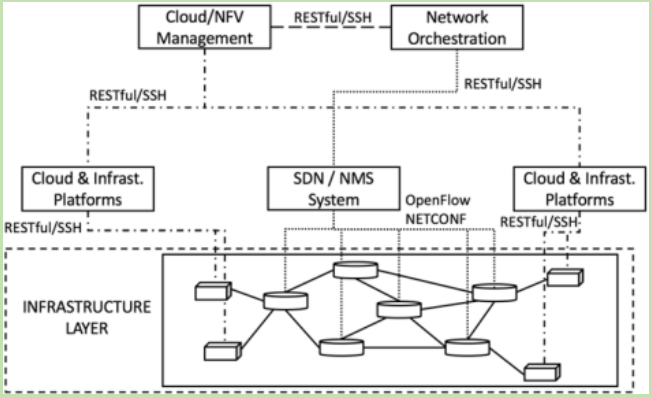
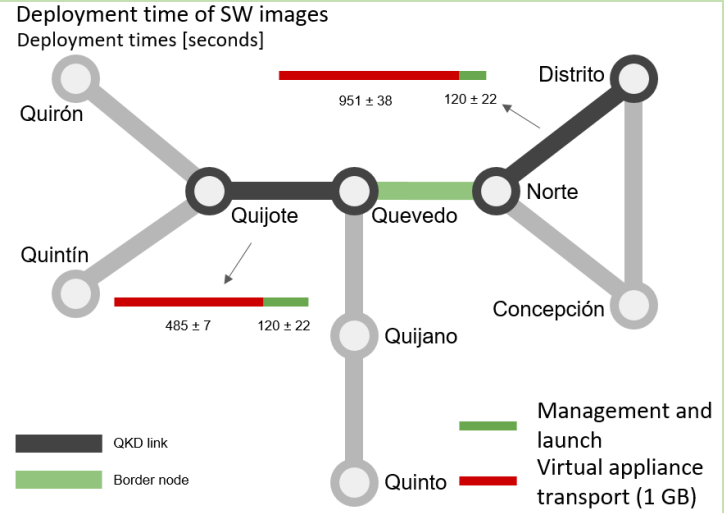


- We asses that the performance of the solution shows that it offers a quality of service equivalent to other solutions in the same range.

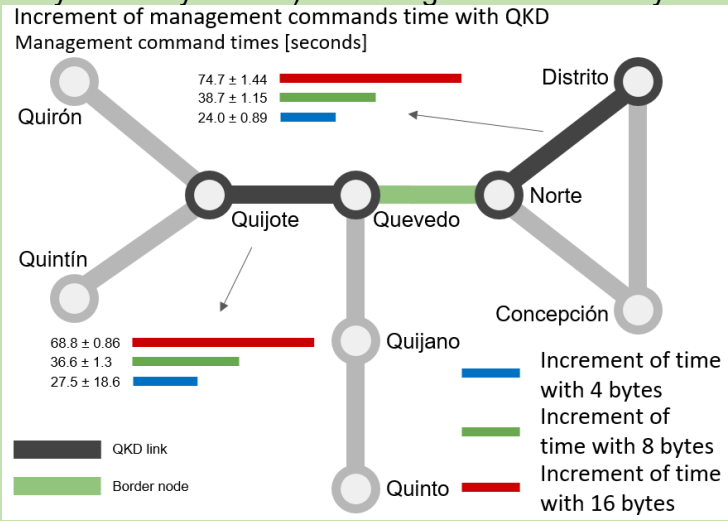
Target sector demonstrated impact:

- Business to business communications through 5G.

3.13 Use Case 26

Use Case 26 - UPM-Self Healed Network Management
Short description of use-case: Our use-case successfully demonstrates that the QKD services can be used for enhancing the security of infrastructures with virtualized network functions (NFV). Specifically, this use-case shows the ability of delivery and deploy software images in a secure manner. When deployed, this kind of software images perform the network functionality itself, so they are a fundamental piece of some modern networking approaches to ensure a self-healed behavior. The solution tested in this use-case proposes that the NFV delivery technology consumes the quantum-distributed key as a resource and performs its functionality. Given the threat to asymmetric cryptography that may be caused by quantum computing technologies, the information-theoretic secure (ITS) symmetric key provided by QKD ensures the delivery of a quantum-safe service resistant to that security concerns.
Picture: 
KPI demo report: - The following figure show the encrypted delivery and deployment time of software images for network function virtualization (NFV) in two different scenarios in the network: 

- Also, the following picture depicts the increment of latency when delivering the command controls for deploying the virtual appliances. It uses several qualities of service (several bytes of key reused) for testing it's the scalability of the solution:



Target sector demonstrated impact:

- Securing the communications of the network management in NFV operations.

3.14 Use Case 27

UC27: Using PQC/QRA to additionally secure the QKD Key Management Layer, the transport layer and to extend the network to a 5G radio cell	
Target sector: *Communication Infrastructure*	
Country: **DE** / **Main site: Berlin**	
Description from Proposal: While QKD and symmetric encryption is used to secure the communication among applications along the core fiber networks, the communication across future 5G wireless networks is not included. This use case investigates an integration of core fiber and 5G access networks, where the fiber sections are secured by QKD and the 5G services are secured by post-quantum cryptography (PQC). As a result, telecommunication services (voice, video, data or chat) will be secured by both quantum secure encryption methods to allow telco operators to make use of the optimum security level to secure their confidentiality asset.	

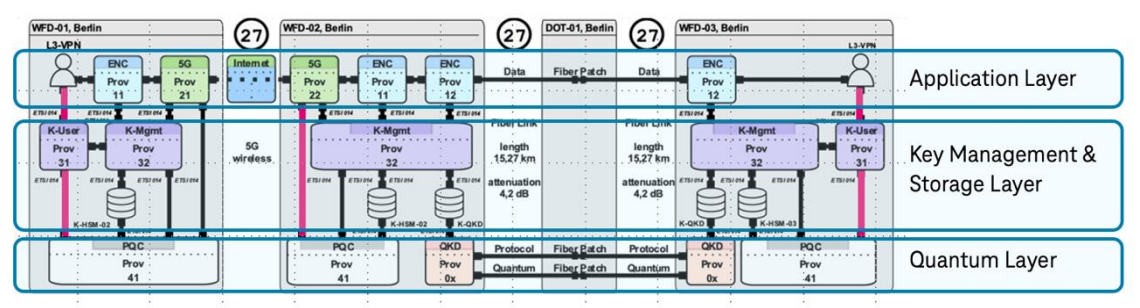
Partner	Role/Function
ID Quantique, Toshiba	QKD / systems
Deutsche Telekom	PQC / systems
Adva Optical, Thales	Encryptor / systems
Deutsche Telekom	5G / systems
Deutsche Telekom	HSM / systems
Deutsche Telekom	Key control / Key management
Deutsche Telekom	Friendly User / applications

Impact

Target sector planned impact:	Planned KPI demonstrations:
Securing the QKD intra-node communication stack, securing 5G peering points, securing end2end communication **Companies attracted through use case:** - Network provider (network, 5G) - QKD provider - PQC provider	- Establishing PQC protocols in QKD key management and PQC fallback on transport layer - Architecture of an integration point of 5G wireless / fiber based communication lines - Demonstration of end2end communication across wireless / fiber channel secured by QKD/PQC as defined by architecture.

- Encryption provider - HSM provider - Key control provider - End user	

Block diagram



Fokus area: quantum secure 5G wireless and PQC encryption / authentication on QKD KMS systems.

Existing equipment

5G:

- 5G Access Point / Hotspot

WFD:

- TestNet environment (optical and IP), computing, server, diagnostics, fiber loops

HSR:

- Show Room Facility, network node, representative events

Network links between sites:

- Fiber Network connectivity between sites

Measurement equipment:

- Optical measurement equipment, e.g. OTDR, OSA, power meter, etc.
- IP and higher layer network performance measurement equipment

Encryptors

Manufacturers and Devices

- Encryptors (as in OpenQKD DB):
  - Encryptor1: Thales Mistral IP Encryptor 01 (IP VPN)
  - Encryptor2: Thales Mistral IP Encryptor 02 (IP VPN)
  - Encryptor3: Thales Mistral IP Encryptor 03 (IP VPN)
  - Encryptor5: Thales Mistral IP Encryptor 04 (IP VPN)
  - Encryptor6: Adva Optical BSI certified AES encryptor (10GE loan)
  - Encryptor7: Adva Optical BSI certified AES encryptor (10GE loan)
  - Encryptor8: Adva Optical BSI certified AES encryptor (100GE DT)
  - Encryptor9: Adva Optical BSI certified AES encryptor (100GE DT)
  - Encryptor10: Adva Optical BSI certified AES encryptor (100GE DT)
  - Encryptor11: Adva Optical BSI certified AES encryptor (100GE DT)

- Encryptor12: Software encryptor (in virtual machine)
- Encryptor13: Software encryptor (in virtual machine)
- Encryptor14: Software encryptor (in virtual machine)

QKD Systems

Manufacturers and Devices

- **QKD Devices (as in OpenQKD DB):**
  - QKD-System1: ID Quantique 1550nm, IDQ-12
  - QKD-System2: ID Quantique 1310nm, IDQ-14
- **QKD Devices (as in OpenQKD DB):**
  - QKD-System1: Toshiba 1550nm, TRL-04
  - QKD-System2: Toshiba 1310nm, TRL-03

PQC Systems

Manufacturers and Devices

- PQC systems (Deutsche Telekom & OpenSource)
  - Open Quantum Safe (OQC PQC Library) on HP Server with KVM hyper-visor

5G Systems

Manufacturers and Devices

- 5G systems (Deutsche Telekom with commercial Huawei equipment)
  - Access Point Hotspot

HSM systems

Manufacturers and Devices

- HSM systems (Deutsche Telekom and Gemalto KeyStore 250)
  - Hardware Security Modules and Trust Master of QKD node

Link details

Link1: 5G – WFD:

- Number of parallel fibers:
  - Minimum 4 fibers
- Optical fiber details:
  - length of fiber: City, < 5 km
  - attenuations in dB: < 5 dB
  - type of fiber: standard single mode fiber
  - quality of connection (heavily spliced, old, direct connection): normal SSMF
  - constraints/add-ons (e.g. filters or dispersion compensation): none
- Telecom connection:
  - Client data rates (1/10/100GB): 1/10/100G
  - Client format: Ethernet, 1/10/100GBASE
  - Line data rates: 10/100G
  - Line format (Ethernet, OTN, Fiber Channel): OTN

- Quantum link:
  - Fiber for QKD system (dark/shared): both possible
  - if shared: define wavelength, launch power, crosstalk limitations

Link2: WFD – HSR:

- Number of parallel fibers:
  - Minimum 4 fibers
- Optical fiber details:
  - length of fiber: City, < 5 km
  - attenuations in dB: < 5 dB
  - type of fiber: standard single mode fiber
  - quality of connection (heavily spliced, old, direct connection): normal SSMF
  - constraints/add-ons (e.g. filters or dispersion compensation): none
- Telecom connection:
  - Client data rates (1/10/100GB): 1/10/100G
  - Client format: Ethernet, 1/10/100GBASE
  - Line data rates: 100G
  - Line format (Ethernet, OTN, Fiber Channel): OTN
- Quantum link:
  - Fiber for QKD system (dark/shared): both possible
  - if shared: define wavelength, launch power, crosstalk limitations
    wavelength defined by QKD systems (1310 nm, 1550 nm)
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)
  - Adjacent channel distortions
-

Planned deployments

- Link1, QKDSystem1, Encryptor1+2, WFD - WFD, Personnel1, Okt 2020 - Feb 2022
- Link2, QKDSystem2, Encryptor3+4, 5G, WFD – MacOS, Personnel1, Okt 2020 - Jun 2022

Interfaces between layers:

- Employing PQC enabled KMS between Quantum Layer, Key Management Layer and Application Layer (if supported by vendor).
- Employing PQC fallback key exchange (as alternative or fallback to QKD)
- Integration of PQC key exchange to the Key Management system.
- Integration of wireless 5G access point
- PQC secured QKD Key Forwarding mechanism
- Development and deployment of hybrid QKD & PQC key exchange protocols

Results

Lessons learned:

- Improving the Telco QKD architecture (see block diagram) as depicted by UC28 by PQC.
- Provider key management system developed, installed, executed, proof of concept
  - Supporting the layered and modular network architecture
    - including 3 fiber connected network nodes, and

        - three 5G connections to the Internet
    - Using standardized ETSI 014 protocols
    - Between all subsystems including KMS, QKD systems, HSMs / memories, Encryptors, Application based Client Systems (Thales IP VPN)
- PQC key exchange based on libOQS is stable, scalable and robust.
- A PQC enabled version of the KMS is highly appreciated because it opposed internal fraud and reduces the requirements on trusted QKD nodes.
- Hybrid QKD & PQC protocols strengthen the security of a key exchange platform, because they compensate the potential weaknesses of either key exchange method. This is the missing security proof or possible implementation flaws of PQC, on the other hand the possibility of technical side channels, a missing certification or the need of the trusted node concept of QKD.
- A combination of classical / quantum key exchange mechanisms using disjoint network paths, i.e. satellite / terrestical or competing mobile provider networks, raises the overall system security to a higher level.
- The robust combination of classical / quantum keys at the endpoints of the network, where the keys are exchanged via disjoint network paths and secured by different classical / quantum key exchange methods (QKD, different PQC algorithms on either network path) seems to be the design goal for a high security key exchange platform.

Changes necessary to already deployed infrastructure:

- Dedicated mobile access node to integrate into a quantum key exchange platform.
- Vendors need to support PQC encryption & authentication to integrate into a PQC key management system.
- Alternative / disjoint network paths between the network end points are required.

KPI demo report:

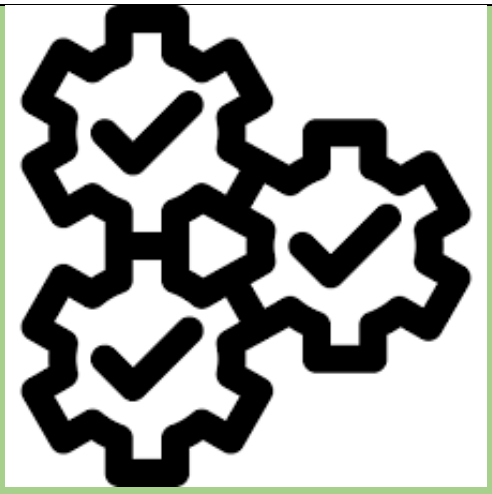
Establishing PQC protocols in QKD key management

- Establishing PQC protocols in QKD key management ✓
- Integration point of 5G wireless / fiber based communication lines ✓
- Demonstration of end2end communication across wireless / fiber channel secured by QKD/PQC as defined by architecture. ✓
- PQC Key Creation Rates: up to 1 kBit/sek Key by Key (on a HP Gen8 Server with Python)
- Compatibility with existing infrastructure ✓
- PQC Link Stability: stable operation w/o failure ✓
- Resistance to Failure: no measured outage of the PQC key exchange ✓

Target sector demonstrated impact:

- PQC KMS has been proven to be operational
- Key exchange via a 5G network between fixed and / or mobile clients. 5G key exchange has been demonstrated with various PQC encryption and authentication algorithms and with a number of combinations of the latter.
- Hybrid QKD / PQC and PQC / PQC key exchange via disjoint network paths and using different PQC algorithms has been demonstrated.
- A hybrid QKD / PQC key forwarding mechanism through trusted QKD nodes has been demonstrated, yielding a reduction of security requirements of a trusted node.

3.15 Use Case 28

UC28: Integration of QKD to telecoms core network architecture	
Target sector: *Communication Infrastructure*	
Country: **DE** / **Main site: Berlin**	
Description from Proposal: The challenge of telecommunication providers is to integrate QKD systems into existing network architecture comprising multiple vendors and technologies. This includes minimum disturbance of the existing network and cost efficient QKD implementation. Furthermore, the key management has to support various connections to be secured, including e.g. management, data, national, international, access, and peering connections. This use case accounts for the implementation of QKD systems in an existing carrier network. This use case is based on the ansatz to protect the network itself. The threat scenario is that of an "almighty Eve" who targets not at a single financial transaction or tries to decipher a certain encrypted communication relation. Instead, Eve is assumed to attack the communication network as part of a critical infrastructure. From an IT integration point of view, the challenges are similar, because there already exists an (security) eco-system of legacy systems and applications. While for the management of the QKD layer one can adopt unification strategies well known from promising network abstraction approaches, it is much harder to define the correct interfaces between established and rather rigid systems, which were never meant to actually undergo such a change of paradigms as it is imposed by QKD.	

Partner	Role/Function
ID Quantique, Toshiba	QKD System provider
Adva Optical, Thales	Encryptor provider
Gemalto / Thales	HSM / LKS Provider
Deutsche Telekom	Key control / Key management
Deutsche Telekom	Friendly User / applications

Impact	
Target sector planned impact:	**Planned KPI demonstrations:**

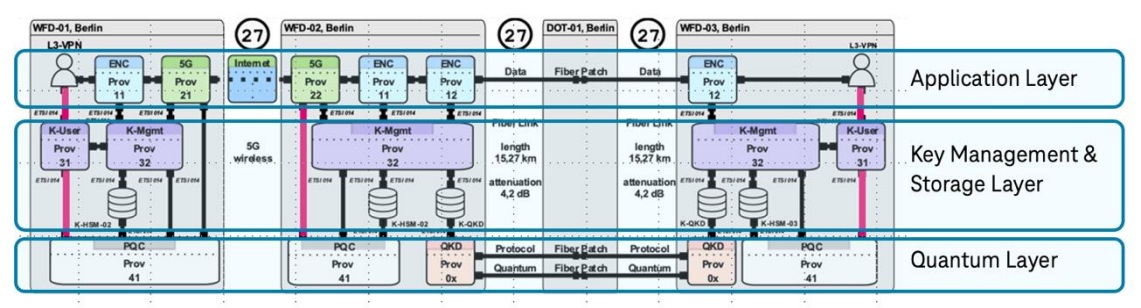
Demonstrate a working QKD integration into Telco networks. **Companies attracted through use case:** - Network provider - QKD provider - Encryption provider - HSM provider - Key control provider - End user	- Implementing and demonstrating an architecture as closed as possible to standard to support the requirements of a telecom provider. - Demonstration of end2end communication across wireless / fiber channel secured by QKD defined by architecture. - QKD Key Creation Rates - QKD QBER - Compatibility with existing infrastructure - Link Stability - Resistance to Failure

Implementation

Work plan:

1. Define the QKD / KMS / LKS architecture as close as possible to standard ✓
2. Implement the QKD / KMS / LKS architecture ✓
3. Deploy QKD links, KMS, LKS with APIs ✓
4. Test and Demonstrate protocol flows as defined ✓
5. Evaluate findings, measure KPIs ✓
6. Write Report ✓

Block diagram



Existing equipment

DTI / KST:

- Terminated fiber, rack space

WFD:

- Computing, Network diagnostics and automation, various fiber loops
- Loop to Strausberg (100km link)

HSR:

- Show Room Facility, fiber end point

Encryptors

Manufacturers and Devices

- Encryptors (as in OpenQKD DB):
  - Encryptor1: Mistral IP Encryptor 01
  - Encryptor2: Mistral IP Encryptor 02
  - Encryptor3: Mistral IP Encryptor 03
  - Encryptor4: Adva AES 10G Encryptor 01 (ADVA)
  - Encryptor4: Adva AES 100G Encryptor 02 (ADVA)
  - Encryptor4: Adva BSI certified AES 100G Encryptor 03 (Deutsche Telekom)
  - Encryptor5: Adva BSI certified AES 100G Encryptor 04 (Deutsche Telekom)
  - Encryptor6: Adva BSI certified AES 100G Encryptor 05 (Deutsche Telekom)

QKD Systems

Manufacturers and Devices

- QKD systems (as in OpenQKD DB):
  - QKD-System1: IDQ 1550nm (IDQ-12)
  - QKD-System2: IDQ 1310nm (IDQ-14)
  - QKD-System3: Toshiba 1550nm (TRL-04)
  - QKD-System4: Toshiba 1310nm (TRL-03)

HSM systems

Manufacturers and Devices

- HSM systems
  - 3xGemalto KeySecure 250 (by Deutsche Telekom)

Link details

Link1: WFD - KST – WFD:

- Number of parallel fibers:
  - Minimum 4 fibers
- Optical fiber details:
  - length of fiber: City, < 5 km
  - attenuations in dB: < 5 dB
  - type of fiber: standard single mode fiber
  - quality of connection (heavily spliced, old, direct connection): normal SSMF
  - constraints/add-ons (e.g. filters or dispersion compensation): none
- Telecom connection:
  - Client data rates (1/10/100GB): 1/10/100G
  - Client format: Ethernet, 1/10/100GBASE
  - Line data rates: 10/100G
  - Line format (Ethernet, OTN, Fiber Channel): OTN
- Quantum link:
  - Fiber for QKD system (dark/shared): both possible
  - if shared: define wavelength, launch power, crosstalk limitations
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range):
  none
  - Adjacent channel distortions.

Link2: WFD - DTI – WFD:

- Number of parallel fibers:
  - Minimum 4 fibers
- Optical fiber details:
  - length of fiber: City, < 5 km
  - attenuations in dB: < 5 dB
  - type of fiber: standard single mode fiber
  - quality of connection (heavily spliced, old, direct connection): normal SSMF
  - constraints/add-ons (e.g. filters or dispersion compensation): none
- Telecom connection:
  - Client data rates (1/10/100GB): 1/10/100G
  - Client format: Ethernet, 1/10/100GBASE
  - Line data rates: 100G
  - Line format (Ethernet, OTN, Fiber Channel): OTN
- Quantum link:
  - Fiber for QKD system (dark/shared): both possible
  - if shared: define wavelength, launch power, crosstalk limitations wavelength defined by QKD systems (1310 nm, 1550 nm)
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)
  - Adjacent channel distortions.

Link3: WFD – HSR - WFD:

- Number of parallel fibers:
  - Minimum 4 fibers
- Optical fiber details:
  - length of fiber: City, < 5 km
  - attenuations in dB: < 5 dB
  - type of fiber: standard single mode fiber
  - quality of connection (heavily spliced, old, direct connection): normal SSMF
  - constraints/add-ons (e.g. filters or dispersion compensation): none
- Telecom connection:
  - Client data rates (1/10/100GB): 1/10/100G
  - Client format: Ethernet, 1/10/100GBASE
  - Line data rates: 100G
  - Line format (Ethernet, OTN, Fiber Channel): OTN
- Quantum link:
  - Fiber for QKD system (dark/shared): both possible
  - if shared: define wavelength, launch power, crosstalk limitations
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)
  - Adjacent channel distortions

Deployments

- Link1, QKDSystem1, Encryptor1+2, WFD - WFD, Personnel1, Oct 2020 - Jun 2022
- Link2, QKDSystem2, Encryptor3+4, WFD - WFD, Personnel1, Oct 2020 - Jun 2022
- Link3, QKDSystem3, Encryptor5+6, WFD - WFD, Personnel1, Oct 2020 - Feb 2022

- Link4, QKDSystem4, Encryptor7+8, WFD - WFD, Personnel1, Oct 2020 - Feb 2022
Interfaces between layers: - Employing KMS between QKD, LKS (HSM), neighbor KMS and application layer (ETSI 0014) - Employing Interfaces as close to standard as possible (ETSI 0014)
Results
Lessons learned: - Installation procedures and operations of QKD systems, encryptors and HSMs. - Required working environments (especially temperature) - How to deploy a self-contained rack as network node setup including compute, network and storage systems. - Proof of the ideated QKD integration architecture for a Telco key exchange platform. - Key Managements Processes (Extraction, Forwarding, Usage - Usage of keys by L1, L3 encryptors and applications - Integration of mobile networks and mobile network clients into the key exchange platform (together with UC27)
Changes necessary to already deployed infrastructure: - QKD requires a more dedicated operating environment especially with temperature control.
KPI demo report: - Implementing and demonstrating an architecture as closed as possible to standard to support the requirements of a telecom provider. ☑ - Demonstration of end2end communication across wireless / fiber channel secured by QKD defined by architecture. ☑ - QKD Key Creation Rates: 1,8kBit/s (see AIT DB) ☑ - QKD QBER: 3% (see AIT DB) ☑ - Compatibility with existing infrastructure ☑ - Link Stability: stable operation w/o failure (if within temperature limits <25°C) - Resistance to Failure: unstable systems after high temperature period (>25°C)
Target sector demonstrated impact: - First integrated QKD system infrastructure at DT - Demonstrated long term QKD key exchange in varying operational environments

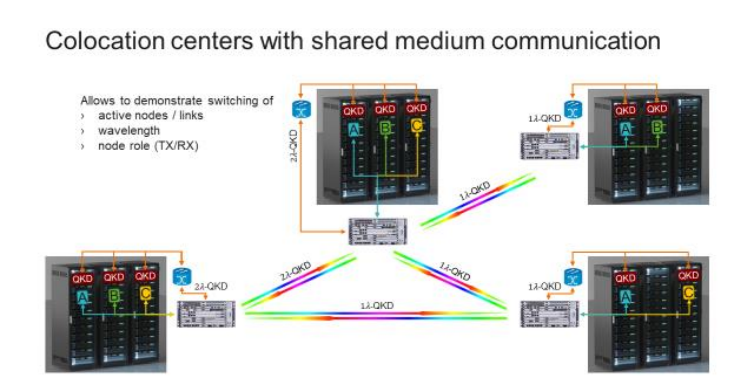
3.16 Use Case 31

Use Case 31: Long span quantum links
Lessons learned: - The main outcome is a positive one: we learned that QKD can co-exist with 100G classical data on very long (>120 km; >28 dB) telecom backbone links. This demonstration is a new record for off-the-shelf QKD technology in the field and demonstrates that QKD is suitable for securing telecom backbones (with sufficient secure bit rate for regular AES-encryptor rekeying), even when quantum and classical signals must share a fibre. - Gaining access to data centre racks was difficult due to strict regulations. The equipment was located in a major carrier-neutral colocation, information and communications technology services centre. The same floor housed many production server racks for other users – hence the tight security. Access visits were carefully planned and we developed a management LAN with VPN to enable remote access to our rack for remote monitoring. - ADVA encryptors were updated to the latest software version during the trial, which included changes to the certificates format for pulling QKD keys by ETSI 014. This temporarily broke key pulling functionality, but we fixed it by liaising with ADVA to understand what certificate fields were needed, then re-generated TLS certificates. For production use of QKD, it is advisable to not update encryptor firmware without testing in a non-production area first.
Changes necessary to already deployed infrastructure: - Fibre link initially included EDFAs due to the long length (and classical telecom application). We had to bypass these to avoid the quantum channel going through the amplifier and instead, we included EDFAs at the end nodes.
KPI demo report: - We were able to encrypt 100G of data per second using 256-bit AES keys refreshed by QKD once per minute (the QKD secure bit rate was actually sufficient to support rekeying faster than once per second, but the encryptors did not support faster rekeying than once a minute), for a comms channel with length >120 km and loss > 28 dB. - Despite the long distance of >120 km, QKD signals co-existed with -5 dBm launched classical signals carrying the encrypted data, achieving <6% QBER and >2 kbps secure bit rate.
Target sector demonstrated impact: - Demonstrated compatibility of QKD with long-distance telecom operator backbones. - Demonstrated deployment into major carrier-neutral colocation, information and communications technology services centre, with QKD operating alongside standard IT equipment and withstanding the environment. - Demonstrated secure solution for back-up of large enterprise datasets to off-site storage

3.17 Use Case 32

Use Case 32: Secured video transmission
Lessons learned: - Access to the data processing center of the CTTI (Center for Telecommunications and Information Technology of Catalonia) is limited thus it is important to have full remote control and telemetry of the system. - Due to administrative and security regulations. it might take a significant time to set up VPN connection for remote control and monitoring of the QKD systems. - As optical losses are critical for QKD, it is important to clean the fiber connectors carefully, which in some cases, might not be part of the standard procedures of the operators. - Dissemination of the results to the public in a live demonstration was challenging as QKD key generation happens at a layer that is not visible by the users. For instance, a videoconference should look the same as a standard video conference as the users do not have visibility on how data is encrypted. To this end, we have to develop specific videoconference software with labels for dissemination that highlight the quantum technology underneath.
Changes necessary to already deployed infrastructure: - Extra fiber (100m) had to be deployed to reach the data centers of ICFO and CTTC and use an already deployed fiber of 25 km.
KPI demo report: - Results from the field test of a CVQKD prototype with Gaussian modulation, true local oscillator and QRNG integration (provided by QUSIDE) - Excess noise: 0.0138 snu - QKD demonstration: 112 kbps (5.5 dB losses) asymptotic - Error correction and privacy amplification performed offline (rate 5kbps without GPU, 70kbps with GPU). - Extracted secret bits: 4.2 Mbits (considering finite size analysis with security parameter 10^-10) - Live demonstration was performed of a video conference with key requested by ETSI 004 API and custom software that uses AES for encryption and WebRTC based videoconference.
Target sector demonstrated impact: - Critical infrastructure - Government

3.18 Use Case 33

Use Case 33 UPM – Minimum Resources
Our use-case successfully distil quantum-distributed key using a minimum set of QKD modules. These can be emitters or receivers, so that one emitter can operate with several receivers with the correct configuration of the optical network. Here the SDN capabilities by UPM of the Madrid test bed are combined with the optical capabilities of the QKD systems by HWDU for configuring jointly the QKD and optical network domains and performs that optimized key distil.
Picture: 
Lessons learned: - QKD optical switching could be used as a medium to optimize the QKD resources of interconnecting independent users, companies, CPDs etc. operating at collocated computing centers, who utilize independent QKD devices.
KPI demo report: Table listing link losses and key rates as measured by the QKD devices and configured trusted transmit (TX) losses for each link, respectively. The table includes back-to-back configurations in Norte, Quevedo, and Quijote. Five links have a too high loss for key generation.

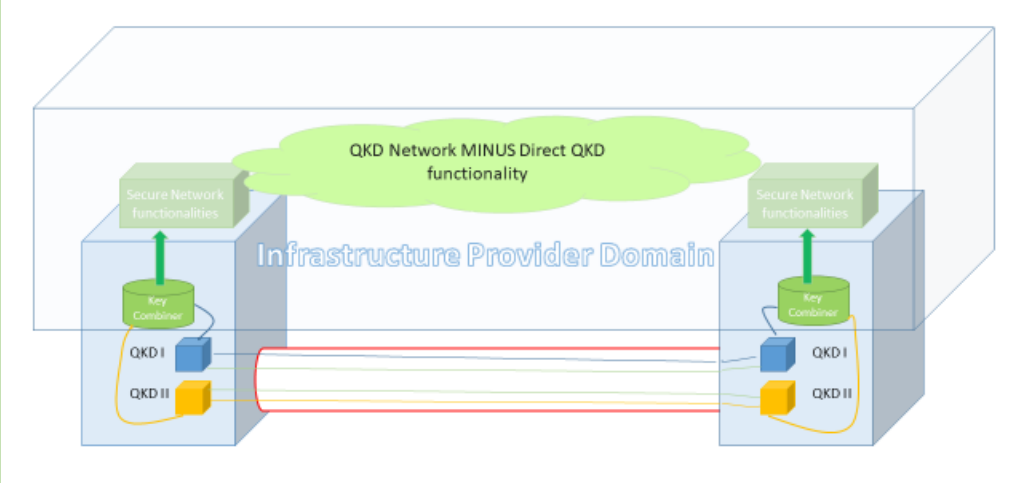
sender	receiver	optical channel [THz]	trusted TX loss [dB]	channel loss [dB]	key rate b/s
Concepción	Distrito	193,4	3,3	19,8	9,0E+01
	(- via Norte -)	193,7	5,3	20,1	1,1E+02
	Norte	193,7	5,3	11,1	7,4E+03
	Quevedo	193,7	5,3	15,3	2,4E+03
	Quijote	193,7		too high	no key
	Quintin	193,7		too high	no key
Norte	Distrito	193,7	1,1	10,2	8,4E+03
		193,8	1,1	10,5	8,1E+03
	Norte	193,7	0,5	1,6	1,7E+04
		193,8	0,5	1,7	1,7E+04
	Quevedo	193,7	1,4	5,1	9,0E+03
		193,8	1,4	5,2	3,2E+03

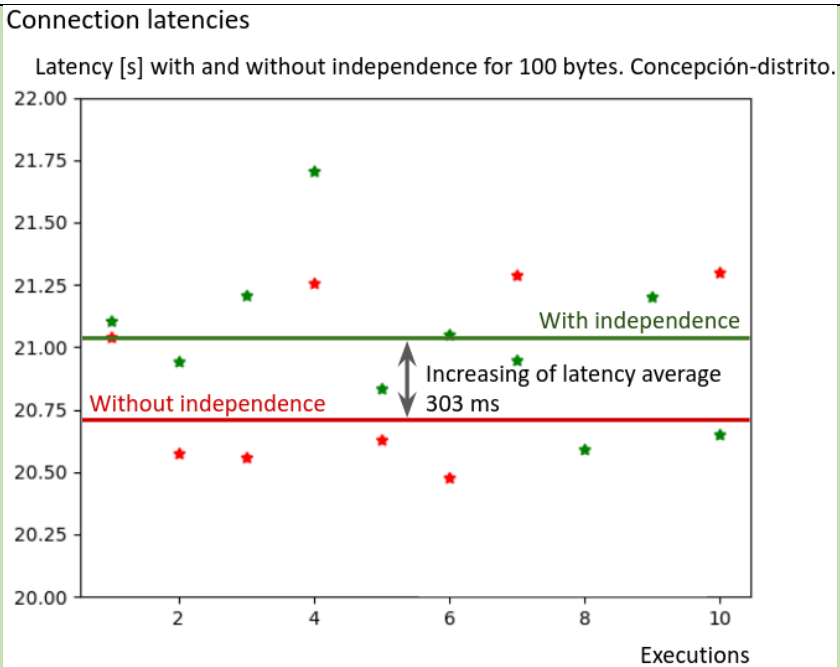
	Quijote	193,7	1,4	10,3	7,1E+03
		193,8	1,4	12,1	5,2E+03
	Quintin	193,7	1,4	20,9	7,2E+01
		193,8	1,4	22,8	3,6E+01
Quevedo	Distrito	193,7	1,4	13,3	4,3E+03
		193,8	1,4	13,3	4,3E+03
	Norte	193,7	1,4	3,8	8,7E+03
		193,8	1,4	4,3	1,2E+04
	Quevedo	193,7	0,5	0,1	1,4E+04
		193,8	0,5	0,2	1,4E+04
	Quijote	193,7	1,4	4,8	1,1E+04
		193,8	1,4	5,9	7,8E+03
	Quintin	193,7	1,4	15,5	1,8E+03
		193,8	1,4	17,3	7,0E+02
Quijote	Distrito	193,7	1,4	21,0	4,1E+01
		139,8	1,4	20,9	4,1E+01
	Norte	193,7	1,4	11,5	6,0E+03
		139,8	1,4	11,5	6,6E+03
	Quevedo	193,7	1,4	6,6	4,5E+03
		139,8	1,4	6,9	1,0E+04
	Quijote	193,7	0,5	1,2	1,2E+04
		139,8	0,5	1,3	1,6E+04
	Quintin	193,7	1,1	11,4	5,5E+03
		139,8	1,1	11,8	6,2E+03
Quirón	Distrito	193,7		too high	no key
	Norte	193,7		too high	no key
	Quevedo	193,7	3,3	19,0	7,3E+01
	Quijote	193,7	3,3	12,1	3,3E+03
	Quintin	193,7		too high	no key

Target sector demonstrated impact:

- Security and privacy in distributed computing centres.

3.19 Use Case 34

Results suitable to be published in a public deliverable
Short description of use-case: Our use-case successfully deliver a vendor-independent key material, which enhances both the security of the final application and the trustiness of the QKD infrastructure. Furthermore, the increase of latency do not modify the quality of the quantum service. The quantum-distributed keys must fulfil several requirements to enhance the security of the final applications. First, the quality of both the generated and distributed keys must be quantum-grade", so that the different operations for its distribution maintain its theoretical security. But, also, the infrastructure must offer a certain level of trustiness to all the involved parties, so that the trusted forwarding of the key can be accomplished. This use case helps with this latest issue.
Picture: 
Lessons learned: - The vendors involved on this UC are on logically segregated networks. Therefore, it has been necessary to combine these networks (through a common gateway) to give the SDN application access to the different QKD vendors. - As the SDN applications that consume and combine (e.g. XOR) the key are software programs, they need enough computational power to perform the encryption of the communications relayed.
KPI demo report: - The following figure shows the detail of the impact of this procedure with respect the normal operation of the QKD network:



- We asses that the increase of latency do not modify the final quality of the quantum service.

Target sector demonstrated impact:

- Delivered vendor-independent secure key in QKD networks.

AOB:

- *Other messages and statements maybe interesting or relevant for the consortium, the co-ordinator or the EC (e.g. project officer).*

3.20 Use Case 35

ID: 35

Private transactions and permissioning in DLT networks.

Target sector: *Commercial and infrastructure*

Country: SP	**Main site: Madrid**

Description from Proposal:

The integration of QKD in private and permissioned DLT networks can significantly improve the security and performance of private transactions.

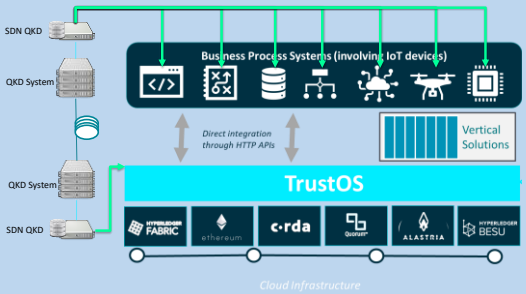
Blockchain adoption to deliver trust in corporate environments leverage in deploying private networks. Telefonica has developed **TrustOS (https://aiofthings.telefonicatech.com/en/technology-services/blockchain-services/trust-os)**, a kind of middleware that makes business applications and solutions agnostic of the underlying blockchain technology, but leverage all the advantages, including the traceability, certification, reconciliation and tokenisation features. Instead of talking the blockchain language, applications just must invoke easy plug and play HTTP APIs modeling the asset they want to trace in blockchain.

For industrial deployments, some of the data gathered by IoT devices are critical for the business. To ensure data integrity, it is desirable that the data be loaded to the blockchain (and become immutable and verifiable) as quickly as possible and **as close to the source as possible**. The first point where this can be done is the IoT device.

QKD allows the IoT devices sending encrypted information with a QKD generated key to improve the security of both the transmission channel and the key integrity. Between the potential IoT sectors we can envision:

- -Telco: Audit data information for about infrastructure sites or devices, such as mobile communication towers or terminal logistic chain
- -E-health: IoT areas related with privacy and confidentiality of the information
- -Defense: Military IoT equipment with strong security demands.

In this use case, a common framework integration to support any kind of IoT device to protect HTTP transactions with TrustOS has been implemented to address any scenario demand.



Partner	Role/Function
IDQ	QKD System provider

TEUR	QKD System provider
TID	Testbed and SW provider
UPM	SW provider
RM	Testbed provider
Other	QKD experimental System provider

Impact

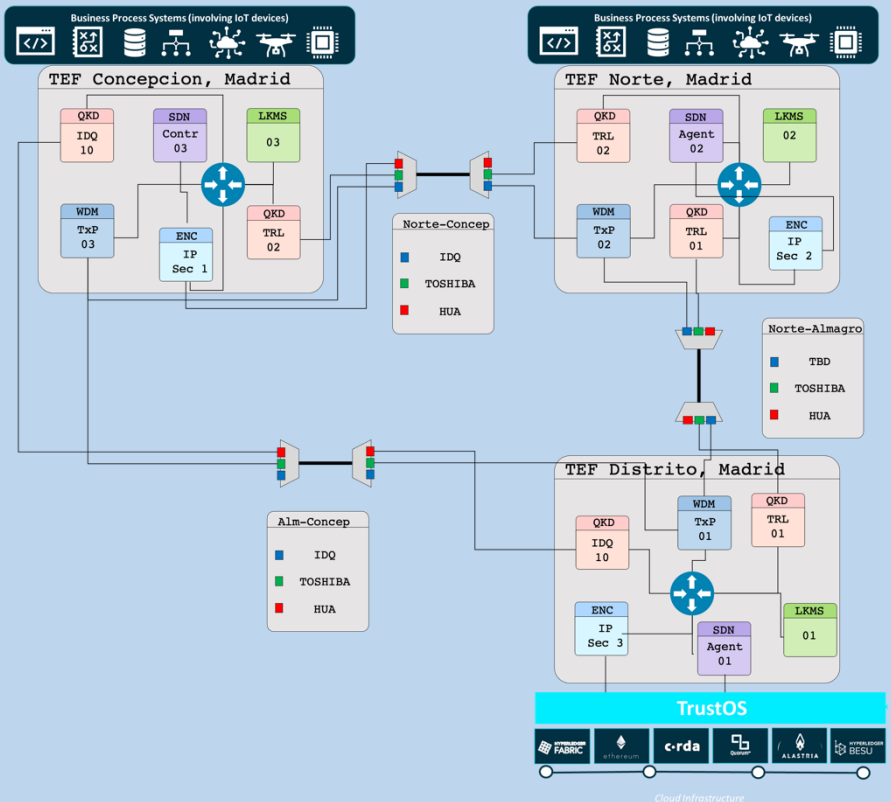
Target sector planned impact: Enhanced security distributed systems. **Companies attracted through use case:** - Telefónica - BT - DT - Verticals	**Planned KPI demonstrations:** - Use of QKD in DLT service - Integration existing systems. NB: Metrics defined in WP8, D8.1

Implementation

Work plan/TODO list:

1. Define parameters for the test.
2. Prepare QKD systems and SW deployment
3. Schedule exact date for deployment with hardware and personnel
4. Perform deployment: HW and SW.
5. Adjust deployment
6. Finalize deployment and retrieve devices
7. Evaluate findings
8. Write Report

Block diagram



Deployment

Site access

Note: Eleven possible places can be used for this test, eight of them are in the RM network and they can be accessed with less restrictions and the other three are within the Telefonica production network, with more restricted access. Ideally, all the sites (with a topology that imply eight links -three of them in a star with a central node and several hops in one of the branches(IMDEASW/UPM-RMCIEMAT, RMCIEMAT-UAM, RMCIEMAT-CSIC, CSIC-UC3M, UC3M-IMDEANW, IMDEANW-URJC, URJC-RMCIEMAT), three of them in a ring (Telefonica production network, DISTRITO-NORTE, DISTRITO-CONCEPCION, CONCEP-CION-NORTE) and another link connecting both (CSIC-NORTE) topologies (ring and star) could be used. All RM nodes are in production and have to provide classical communications at the same time. Network operator requires also that every node has to have a redundant link where no quantum communications are taking place at the same time than the classical in order to safeguard classical communications from any possible problem coming from the QKD equipment or associated devices.

For this case we selected the use of Telefónica's Quantum Ring for a three nodes DLT network setup. This infrastructure would be ready close to the end of the project. For the testbed, each node will run an instance of a TrustOS DLT solution enabling IoT transactions. Whenever one of the nodes running IoT devices (NORTE or CONCEPCION) wants to send a private IoT related data transaction with the TrusOS Cloud production (DISTRITO) a QKD exchange will be performed between both of them. The exchanged key will be used to en-crypt the transaction and it will be stored in the enclaves of Party A and B. Thus, any of the nodes involved in the key exchange will have access to the content of the private transaction and will be able to dencrypt the information in the blockchain if they have the key.

The RM network and the Telefonica production have different access requirements:

- **RM Sites** Unrestricted ☐ Restricted ☒
  If restricted how: RM permission
- **Telefónica Production:** Unrestricted ☐ Restricted ☒
  If restricted how: restricted to trained persons only

Restricted access examples: with passport; with short training; with trained person; restricted to trained persons only

Available power

What power delivery is available for telecom and quantum devices?

All TID sites have both, AC 230 and DC 48 under request. RM sites have AC 230.

Internet connection

TID sites, only Distrito has internet connection. All RM sites have internet connections (in-ternet connection= equipment can be accessed from the outside)

Existing equipment

TID and RM have in their facilities transmission equipment for classical channels. Moreover, they have routers to provide connectivity among the sites and IT resources for small VM deployments.

DLT nodes

Manufacturers and Devices

- TrustOS service from Telefonica (https://aiofthings.telefonicatech.com/en/technology-services/blockchain-services/trust-os).
- Simulated IoT devices

QKD Systems

Manufacturers and Devices

- 3 links (Norte-Concepción, Concepción-Almagro and Almagro-Norte)
- Devices: IDQ, TOSHIBA, ADVA

Link details

The available links in the Madrid NW and their characteristics are:

Description	Distanceinkm	Lossindb	Node1	Node2
Almagro - Norte	3.9	6	MAD-03	MAD-04
Norte - Concepcion	5.5	7	MAD-04	MAD-05
Concepcion - Almagro	6.4	7	MAD-05	MAD-03
CIEMAT-UAM	24.5	8	MAD-02	MAD-01
CIEMAT-IMDEA SW	24.2	6	MAD-02	MAD-08
CSIC-UCM	6.5	3.5	MAD-06	MAD-07
CIEMAT-UCM	0.92	1.9	MAD-02	MAD-07
CSIC-UC3M	33.1	10.3	MAD-06	MAD-09
UC3M-IMDEA Networks	1.91	0.4	MAD-09	MAD-10
CIEMAT - URJC	40.68	11.93	MAD-02	MAD-11
URJC - IMDEA Networks	22.47	6.10	MAD-11	MAD-10

- Additionally, a CSIC-Norte link is currently being commissioned. It is a short link of about 1km and losses are expected to be in the range of 2dB. This link is important since it will be the connection between the two infrastructure providers.
- Other intermediate nodes can be used if required.
- Other two links UAH-UAM and UAH-CIEMAT (not listed, of about 50-60 Km) are in the process of being formally approved and might be available by the end of the project.

The details of the different links follow:

Telefónica Quantum Ring (Distrito-Norte-Concepción)

The current network is a ring network in downtown Madrid (16 km perimeter). It joins three central offices of Telefónica Spain (Norte, Concepción and Distrito -Nodes MAD03, MAD04 and MAD05-, and crosses several others PoPs in between (not listed). This means that the ring could be, in principle, easily extended to have 5 to 7 Points of Presence). Losses are relatively high due to connectors and, possibly, bending the fiber when going through the PoPs, however they are always within the reach of the QKD systems (always less than 12 dB losses). The network could be used during the whole duration of the project and it has been tested and used already with quantum equipment. These nodes are in production facilities, which means that the access is restricted and follows strict procedures. The nodes are linked by a pair of dark fibres that can be used exclusively for the quantum channels if needed. All nodes can be accessed through an VPN.

Below there is a map of the Telefónica Quantum Ring used for this testbed.

Deployment

- 3 links. Dec. 2021 - March 2023

Interfaces between layers:

- All SW will be running using ETSI 004 (because of QoS and expected latencies). If 004 is not available in a native way but ETSI 014 is provided, then a wrapper on top of 014 to provide the 004 will be implemented.

Results

KPI demo report:

- Separate document

Impact

Target sector planned impact:

- Blockchain transactions
- Internet of Things

Companies attracted through use case:

- Telefónica de España

Achieved KPI demonstrations:

- KPI_1: Number of IoT devices connected simultaneously
- KPI_2: Rate of measurements sent per device per second
- KPI_3: Time it takes to get a QKD key

Note: This are preliminary results, and additional test will be made once final setup is ready.

Time of demonstration

Deployment:

- Initial development an adaptation of the Madrid Network. 3 months.
- Note that this deployment assumes that all the SDN stack of the Madrid Quantum Network is fully deployed and operative. It uses 1 link between Distrito and Norte nodes. In Norte node resides IoT devices and use case clients and in Distrito resides the Telefónica TrustOS service.
- The QKD secure transfer proposed on this UC will protect a set of sensitive IoT data delivered and stored in the blockchain. The information is managed through ciphering at application layer.

Time of demonstration:

- This is the first version of this UC fully functional. June 2022.
- This demonstrator is being run on the Madrid Network over a virtualized environment and it can be deployed physically close to any IoT device. The current demonstrator is running over the Telefonica nodes, so it can use the Telefonica's TrusOS Permissioned Distributed Ledger (PDL) platform **(https://aiofthings.telefonicatech.com/en/technology-services/blockchain-services/trust-os)**

Results

Lessons learned:

- QKD Stack thorugh API 004 provides a constant source of keys, suitable for encryption periodic IoT messages, that demands private information. For example data related IPR industrial information, medical sensors.
- Solution is based on light REST API protocol optimized for IoT devices. The solution is design to have co-located IoT devices with QKD Node. E.g.: Military building, hospital, Factory, etc.
- Remote IoT devices should combine PQC as a solution to access QKD keys when there is no co-location. Future plans involves to link remote IoT combining PQC

Changes necessary to already deployed infrastructure:

- IT resources and virtualization software was added to cover the use case and provide connectivity with SDN stack over ETSI ISG QKD 004.

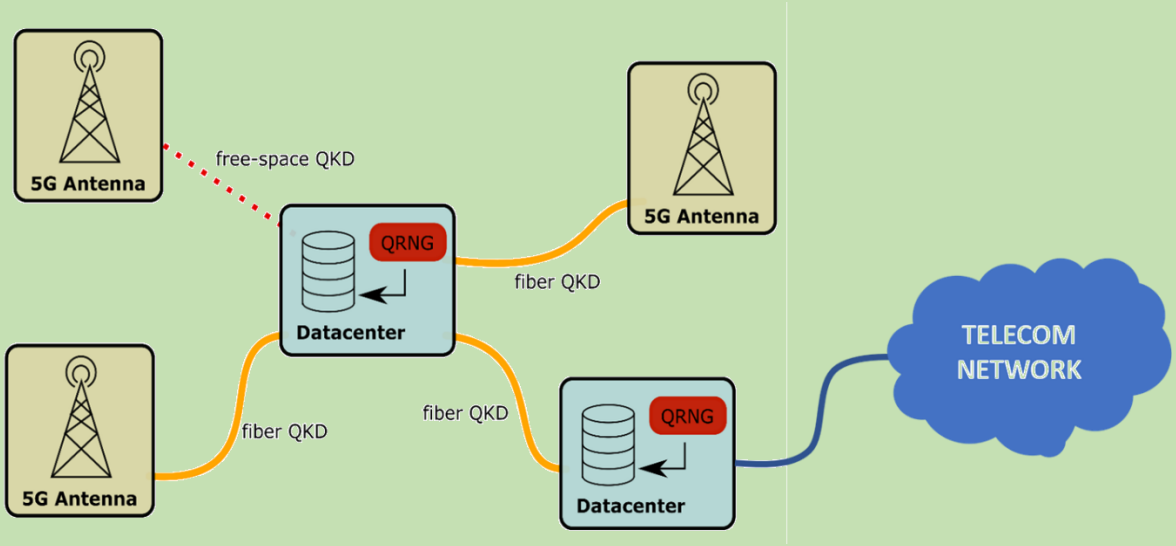
.

Target sector demonstrated impact:

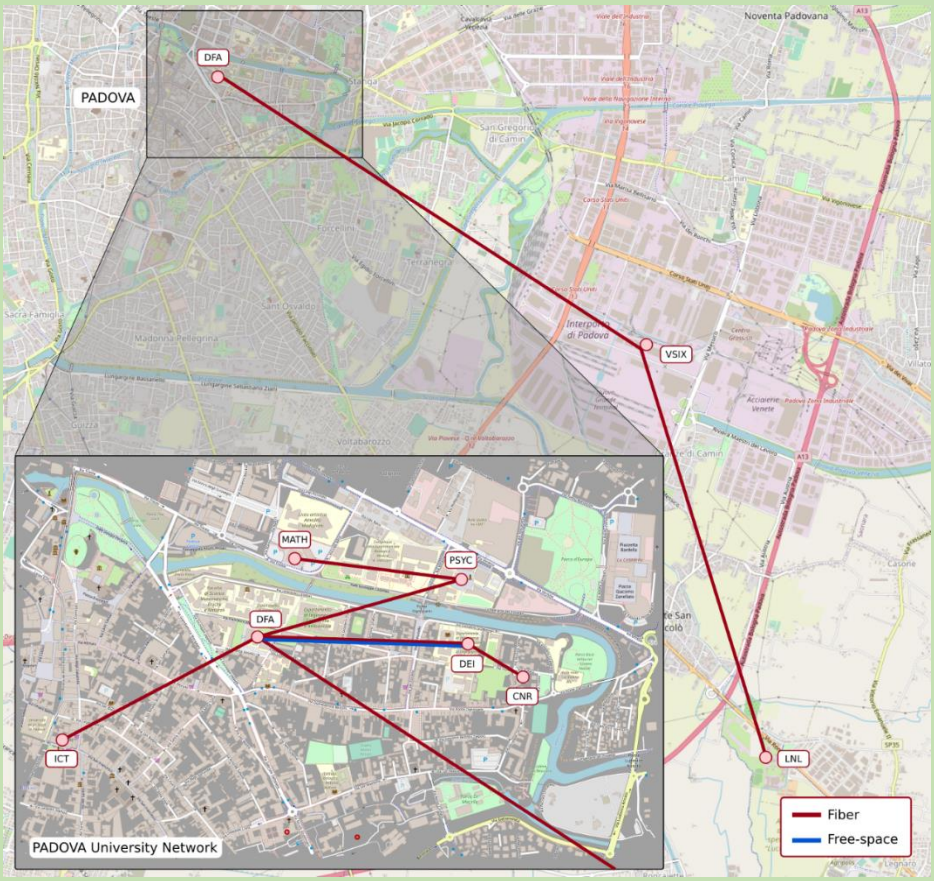
Commercial and Infrastructure related to IoT market.

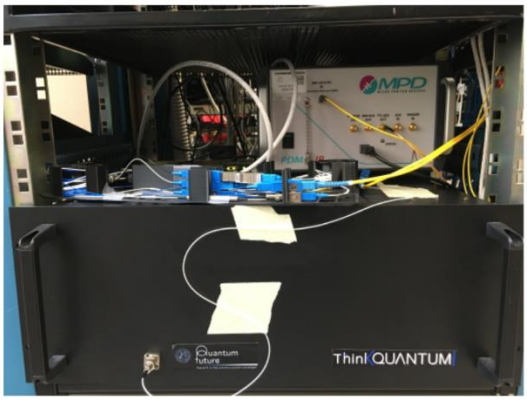
KPIs	
Number of IoT devices connected simultaneously	10 devices
Rate of measurements sent per device per second	1 x 60 seconds
Time it takes to get a QKD key	21.7537 seconds

3.21 Use Case 42 – Open Call

Use Case 42 – CEQUAM – 5G Security
Turin use-case successfully demonstrated the use of QKD to protect data transmitted over the network connecting mobile radio sites (spread over the territory often at not secure locations) to local and central aggregation nodes. Point-to-point and point-to-multipoint configurations were realized using both fibre and free space optical channels. Both the radio sites and aggregation nodes were simulated using laboratory and/or field trial installations. The central location was further protected via a point-to-point QKD link to a higher hierarchical level location. The coexistence of the data and quantum channels on the same fibre link, for cost savings, was also successfully demonstrated.
 CEQUAM architecture
Lessons learned: - Interference of the data onto the quantum channel, caused both by crosstalk and non-linear effects (Raman), can cause big limitations unless the link is very carefully engineered; transmission at low levels in combination with strong filtering and use of optical amplifiers at the receiving side were successfully tested - A network operator must consider the main planning and operational differences between the telecom equipment and links he is used to operate on one side and the more delicate QKD system and associated quantum channel on the other side
KPI demo report: - Achievable QKD key rate was acceptable in the range of attenuations of interest - Crosstalk (especially if sharing the same optical band) and Raman effect (especially on long links) may cause serious impairments to the QKD performance - The free space link performance was similar to the fibre one on a short link - The PTP link was inserted in an ORAN setup for the connection between DU (Distributed Unit) and CU (Core Unit) with negligible impact on the service throughput and latency performance
Target sector demonstrated impact: - QKD could be beneficial to secure critical network segments and it can also be offered as a service to the customers
Dissemination (press releases, conference contribution, webinar…): - An invited paper was submitted to ECOC'22 including some considerations and results of experiments carried out on the Turin CEQUAM testbed

3.22 Use Case 43 – Open Call

Use Case 43 - UNIPD
Short description of use-case (10-15 lines) for dissemination (e.g. homepage): UNIPD realized in Padova a QKD network with 8 nodes and 6 different links and developed in-house different QKD devices based on polarization encoding. UNIPD focused on the development of free-space/fiber inter-modal QKD (IM-QKD), in which a free-space link is used as an extension of an optical single-mode-fiber, like a fiber patch cord but realized through two telescopes. IM-QKD requires coupling the optical free-space signal into a single-mode fiber and to route the signal to the to QKD device which may be located in another building with respect to the free-space telescope. The use of SMF coupling allows to move the "trusted zone" of QKD systems (i.e., the physical secure area around the transmitter and receiver systems is not accessible for eavesdroppers) from the optical telescopes to the QKD devices using fiber links. This is useful when different QKD receivers share the same optical telescope or when it is hard to establish the trusted zone near the latter. Beyond IM-QKD, UNIPD realized various QKD tests and demonstrations over the Padova University network, including a QKD experiment with coexistence of classical and quantum signals in the same fiber.
Picture      Map of the Padova testbed



Pictures of the QKD devices for fiber, free-space and inter-modal QKD used in Padova testbed.

Lessons learned:

- Finding suitable locations for free-space links demonstrations can be hard
- The physical access to some testbed nodes can be very limited, so the QKD devices must be easy to be deployed

KPI demo report:

- We were able to encrypt 1GB of data per second using 256 bit AES keys via Rohde & Schwarz (ETSI-004) and ADVA (ETSI-014) encryptors
- Coexistence of quantum/classical signal into the same fiber demonstrated on a 13km-long deployed fiber
- Daylight QKD realized along free-space link up to 600 m with portable telescopes

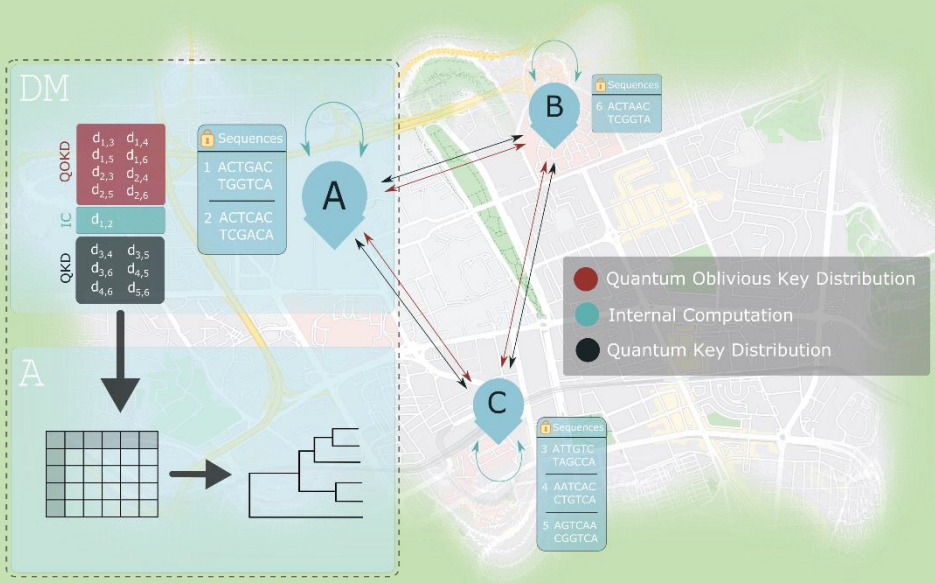
Target sector demonstrated impact:

- Hybrid free-space/fiber quantum network
- Free-space/satellite QKD

AOB:

- The UNIPD group founded in 2021 a spin-off company based in Italy and called ThinkQuantum srl thanks also to the research activities performed within the OPENQKD project

3.23 Use Case 44 – Open Call

Use case 44 – QuGenome - SMC
The use case demonstrates a quantum secure multiparty computation (SMC) of phylogenetic trees, involving three private genome databases placed at three distinct nodes in the Madrid quantum network. Such SMC service enables distributed parties in a network to jointly compute arbitrary genome trees without revealing their private genome sequences. In the use case, the three Nodes run a quantum-enabled SMC procedure to jointly compute the *matrix distance* of the genome sequences present in the private databases. For that purpose, the different Node pairs (e.g., Node A – Node C; Node A – Node B; and Node B – Node C) consume oblivious keys to compute the *matrix distance* entries corresponding to the genome sequences belonging to different databases. Such oblivious keys are generated through an implemented QODK protocol, which uses raw keys obtained from continuous-variables quantum key distribution (CV-QKD) systems. After the computation of the *matrix distance* entries corresponding to the sequences from the same database, the three Nodes share the missing *matrix distance* entries via encrypted messages with symmetric keys obtained from discrete-variables quantum key distribution (DV-QKD) systems. Once the full matrix distance is obtained, the three nodes can iteratively group the genes with the fewest differences between them. The final output, shared by the three Nodes, will be the phylogenetic tree corresponding to the genome sequences belonging to the three private genome databases.
Picture

Lessons learned: - Access to the raw keys was a challenge as the different installed QKD systems do not provide raw keys by default. - Standardization of a key management layer that allows access to raw keys and that also incorporates oblivious keys will facilitate the implementation of secure multiparty computation services based on quantum technologies.

KPI demo report:

- We were able to run the QOKD protocol using raw keys from Huawei's CV-QKD system.
- We were able to run a two-party secure computation to compute the distance matrix of the genes using the QOKD keys.
- We were able to iteratively group the gene distances between the different parties, which were encrypted with symmetric keys generated through the ID Quantique's DV-QKD systems.
- We were able to perform a private computation of phylogenetic trees based on quantum technologies, with 3 parties and 30 SARS-CoV-2 genome sequences with 32 000 length taken from GISAID.

Target sector demonstrated impact:

- Data in healthcare is an asset of high value, so the consortium has established contacts with SMEs in the sector and one of them decided to join the QuGenome;
- Cooperative health research activities require sharing of highly sensitive data, therefore players are implementing multiparty systems to share data, without disclosing the data. This boosts trust and fosters collaborative research, with a strong positive impact on health knowledge and consequently, on healthcare services to end-users.

3.24 Use Case 45 – Open Call - BerlinaleQ

USE CASE 45 – BerlinaleQ - film festival with QKD-secured movie distribution

In the scope of this OpenQKD-project, Fraunhofer HHI, Colt, ADVA and ID Quantique successfully demonstrated and validated a new use case for QKD that provides highest protection in the realm of digital movie data distribution during the Berlin International Film Festival "Berlinale" in February 2022. As during previous years, the festival's premiere movie data was distributed from a central distribution hub to the movie theaters over Colt's dedicated fiber and service network, while network encryption and transport equipment was provided by ADVA. Our concept extended this established architecture by seamlessly and transparently adding a commercial point-to-point QKD link from ID Quantique into the existing infrastructure. Thus, for the first time, the premiere movie data was successfully protected by encryption with highly secure QKD keys during distribution from the Berlinale film distribution hub and the festival's main movie theater "Berlinale Palace" in the city center of Berlin. During the whole duration of the Berlinale Film Festival between 10.-20.02.2022, the QKD link ran autonomously, continuously and without any perturbation or interference, and provided QKD keys to the ADVA network encryptors for protecting the distribution of the festival's movie data between both sites.

Picture

Figure 1: Left: The network of the 72th Berlin International Film Festival. The QKD-protected fiber link between the Digital Cinema Distribution Center and the Berlinale Palace is shown in red. Right: Photo of the whole node comprising the QKD system, network encryptor and transport system as installed in the Berlinale Palace stage environment.

Lessons learned:

- Today's commercial QKD systems can be seamlessly integrated into an existing and operational inner-city network infrastructure
- After an initial hands-on introduction, the deployment and operation of all systems could be replicated by employees of the network equipment supplier as well as the fiber infrastructure- and professional services provider
- Most challenging and time-consuming was the configuration of the overall network topology and correct initialization of the security certificates on all devices, which required remote support by the QKD manufacturer

KPI demo report:

- During the eleven days of the film festival, the QKD link ran autonomously and continuously with a mean QBER of 2.1 % and a mean secret key rate of 2.72 kbps
- A total of 2.35 Gbit of secret keys was distributed and used to encrypt 37 festival movies with a total volume of over 11.8 TB of digital movie data

Target sector demonstrated impact:

- Network equipment supplier and fiber infrastructure- and professional services provider are aware of the quantum computing threat and understands security strategies based on QKD and PQC
- Despite the successful demonstration, currently no further use of QKD is planned during one of the next film festivals

3.25 Use Case 46 – Open Call - QGov

USE CASE 46 – QGov

The QGov project aimed at integrating, demonstrating and assessing the use of QKD for secure key distribution between governmental agencies. The project was jointly implemented by Space Hellas S.A. and the National and Kapodistrian University of Athens. The involved end-user is the Hellenic National Intelligence Service (NIS), officially in charge of producing and distributing national cryptographic keys.

Picture

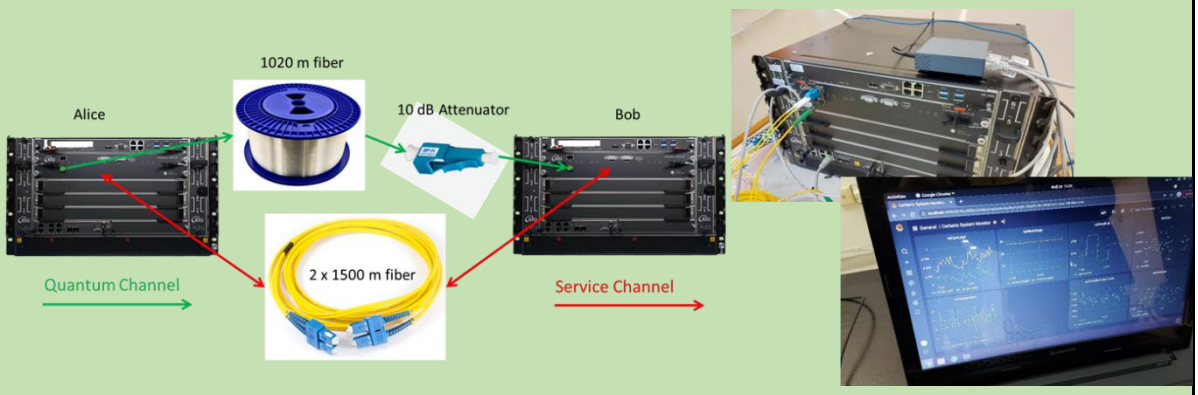


Figure 1. Baseline QKD demonstrator configuration installed at end user's premises

Lessons learned:

- The unconditional security offered by a quantum key distribution system is invaluable as it is based on fundamental principles of physics.
- The technical maturity of the implementations of the above systems is at a very good level while they continue to be constantly improved.
- There is an absolute need to complete the standardization and subsequent verification of these systems so that they can be used by state authorities
- It would be particularly useful to explore the possibilities of interoperability of these systems with existing crypto devices.
- Given the high cost of QKD systems, it would be particularly desirable to design network topologies as well as system variants that allow their optimal performance in terms of performance but mainly cost.

KPI demo report:

- A 1.5 GBps payload (sample random key) was encrypted using AES-256 and securely transmitted over an shared channel using QKD keys.
- Key output remained constant at a few Kbps and QBER at 2-3% under different conditions:
    - Insertion of optical elements (polarization controllers and optical isolators) to emulate a real transmission network
    - Various star and tree topologies
    - Length difference between service and data channel up to 1 Km max

Target sector demonstrated impact:

- The QGov project successfully implemented, tested and validated a proof-of-concept system for Quantum Key Distribution for the needs of Greek public agencies. It is deduced that, in the short term, QKD technology could, even partially, replace the traditional in-person delivery of cryptographic keys.
- The brief feasibility study carried out in the frame of the project identifies the steps for a wider pilot QKD implementation involving four Greek public agencies directly involved in national security operations.

AOB:

- Nation-wide QKD piloting in Greece is currently being implemented under the HellasQCI project recently started, co-funded under the EU Digital Europe programme.