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	

First Report on Field Trial Execution

Deliverable: **D8.6**	Lead: LMU
Project month: M33	31. 05. 2022
Work package: WP08	Task: T8.4
Type: Report	Version: 1.3
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/.

Document Information

Author List

Organization	Name	E-mail
LMU	Adomas Baliuka	A.Baliuka@physik.uni-muenchen.de
LMU	Lukas Knips	lukas.knips@mpq.mpg.de
LMU	Harald Weinfurter	h.w@lmu.de

Reviewer List

Organization	Name	E-mail
UNSA	Miralem Mehic	miralem.mehic@etf.unsa.ba

Version History

Version	Date	Reason / Change	Editor
1.0	30. 05. 2022	Last draft	Adomas Baliuka
1.1	31. 05. 2022	Small editorial changes	Andreas Poppe
1.2	03. 06. 2022	Comments by reviewers	Miralem Mehic
1.2a	03. 06. 2022	More use cases added	Harald Weinfurter
1.2b	07. 06. 2022	Review	Miralem Mehic
1.3	08. 06. 2022	Small editorial changes	Cristina Tamas

Executive Summary

The report is aimed at the general public and all interested in the state-of-the-art of QKD and quantum communication. It collects reports received from six finished 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 D8.6 reports on use cases of QKD field trial execution within the OPENQKD project which were completed at the time of writing (April 2022). 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 different 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. In particular, 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 to the *public* 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 afforded by the diversity of the use cases, which explore both 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:

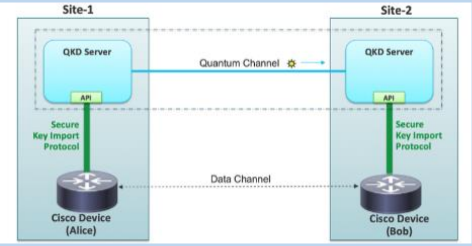
- Section 2 comments on the use cases discussed in the report.
- Section 3 provides the information about each completed use case as provided from the operators.
- Section 4 provides some concluding remarks.

2 Comments on Use Case Reports

In the following, use cases finished by April 2022 are detailed together with the achieved results and KPIs. More information on the definition of the KPIs and on the planned 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.

3 Use Case Reports

3.1 Use Case 02

ID: 02 **Smart Grid**	
Target sector: Critical Infrastructure	
Country: CH | **Main site:** Geneva	
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.*	Image credit: Cisco

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

Impact	
Target sector planned impact: Smartgrid communications **Companies attracted through use case:** - Electrical facilities	**Planned KPI demonstrations:** - Measure Latency impact generated by Encryption + QKD - Measure stability of the link - Best practise 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

Implementation and block diagram
Work plan/TODO list: 1. Link topology and design 2. List the inventory of hardware and planning 3. Request Cisco hardware and support (depending on SIG Cisco stock) 4. Prepare QKD system and deployment 5. Integrate the QKD pair with Cisco 6. Schedule exact date for deployment with hardware and personnel 7. Perform deployment in lab in order to test the configurations 8. Perform deployment on final sites 9. Adjust deployment 10. Run use case

11. Analyse link performance
12. Evaluate findings
13. Retrieve QKD devices
14. Write Report

Site access

- **SIG Lignon Telecom Lab** Unrestricted ☐ Restricted ☒
  If restricted how: accompanied by SIG

- **SIG Lignon DIE power station Test** Unrestricted ☐ Restricted ☒
  If restricted how: accompanied by SIG

Available power

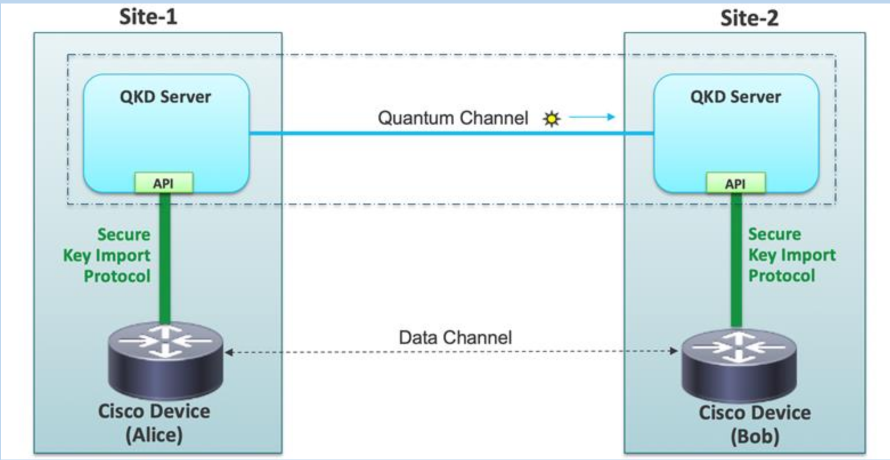
What power delivery is available for telecom and quantum devices?

- **SIG Telecom Lab** AC 230 ☒ DC 48 ☐
- **SIG Lignon power station Test** AC 230 ☒ DC 48 ☐

Internet connection (closed LAN with remote access via VPN)

- **SIG Telecom Lab** Yes ☒ No ☐
- **SIG DIE power station Test** Yes ☐ No ☒

block diagram



Existing equipment

Telecom Lab : Use of 2 pairs of fibers, ¼ Rack, power
DIE Power station test : TBD

MUX / DEMUX

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
Results
Lessons learned: -
Changes necessary to already deployed infrastructure: -
KPI demo report: -
Target sector demonstrated impact: -
Estimated cost of implementation: -

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 certification 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 :

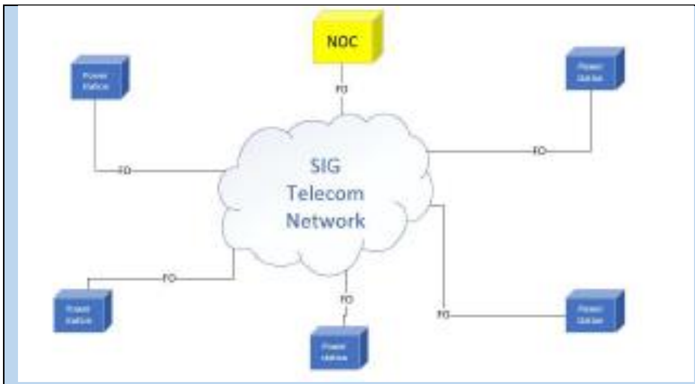
Environmental	room temperature	15°C ~ 25°C
	dust-free condition 1	30mg/m3 of sand
	dust-free condition 2	0.2mg/m3 of dust
	dust-free condition 3	1.5mg/(m2h) of sedimentation
	proper chassis/rack ground	Must be grounded
	installation space	19" std telecom rack 6U
	voltage level	110 ~ 220 VAC
	outlet type	

- 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 allowed a proper SNMP management though a telco NMS. We managed to successfully confirm the stability of the links from the customer service perspective.

Changes necessary to already deployed infrastructure:

UC Initial proposal : 5 power stations connected thought a telecom MPLS network

The initial version planned to connect 5 power stations with QKD. We discovered that QKD is not compliant with an active network, since QKD cannot “pass hardware and equipements”. QKD key exchange need dedicated fibers end to end between the devices.



Therefore we evolved the design to a point to point QKD link between 2 power stations :

- ### UC2 version 2 : point to point link version for SmartGrid

ID: 02

Smart Grid

Target sector: Critical Infrastructure

Country: CH | **Main site:** Geneva

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.

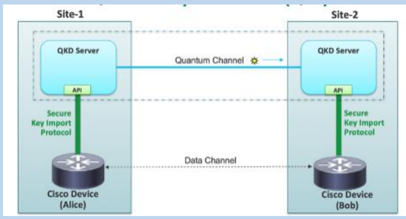


Image credit: Cisco

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

During the use case preparation we encountered physical environment challenges : temperature, rack space, cleanliness of the space.

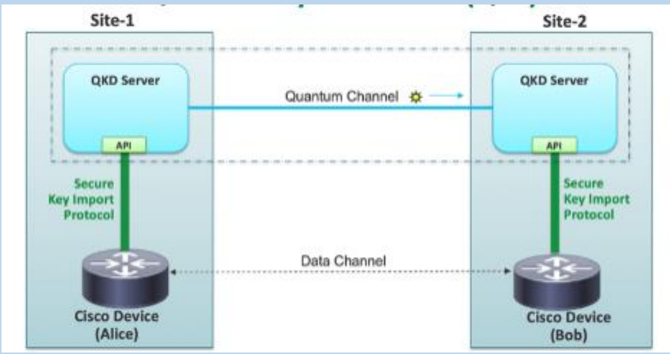
The power stations have very different environment from a datacenter. There is not air conditioning, and no racks mount. QKD needs a proper datacenter like environment with a cooled room, clean environment to manipulate the fibers and rack space. QKD key exchange is extremely sensitive to the environment it runs thought.

The use case was nevertheless interesting in terms of vendors involved : Key exchange with Cisco business equipment used in Geneva for delivering MPLS services.

Therefore we worked on a new version of the use case that would meet the physical environment needs and propose a benefit to the project.

UC2 version 3 : demo version : point to point MPLS business customer link

We prepared a use case for a customer point to point link for the last mile in Geneva, using Cisco equipment on both end that we install on customer Telecom premises, with Datacenter standards.



- We managed to configure and run the use case on a SIG business customer point to point link on dedicated fiber successfully.

Target sector demonstrated impact:

- Business customer last mile link successfully ran with QKD key

Estimated cost of implementation:

- Cisco hardware is standard running IOS-XE
- QKD hardware and software : 100K EUR

Use case design description hardware :

- 2 QKD hardware equipment running Cerberis3
- 2 Cisco hardware running IOS- XE >=17.2
- QKD NMS system to configure the QKD hardware (requirements : Linux server running either CentOS7 (not 8) or Ubuntu20. The newest management software (QMS) ideally should have 16G RAM and 8 CPU cores and 100G disk space).

Configuration and monitoring details :

- We monitored the customer link stability in terms of traffic and tunnel stability.

Below the checks for operations :

QKD enabled check

```
openqkd_router1#sh crypto ikev2 sa detailed
 IPv4 Crypto IKEv2  SA
Tunnel-id Local                 Remote                fvrf/ivrf            Status
```

```
6         10.1.0.1/500          10.1.0.2/500          none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK,
Auth verify: PSK, QR
      Life/Active Time: 3000/615 sec
      CE id: 0, Session-id: 2
      Status Description: Negotiation done
      Local spi: 08D3B120306CF5DE       Remote spi: 6F39A6E05DAB40E0
      Local id: 10.1.0.1
      Remote id: 10.1.0.2
      Local req msg id:  6              Remote req msg id:  0
      Local next msg id: 6              Remote next msg id: 0
      Local req queued:  6              Remote req queued:  0
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      Fragmentation not  configured.
      Dynamic Route Update: enabled
      Extended Authentication not configured.
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes
      Quantum Resistance Enabled          <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
      Local Sys Id: encASIG  Remote Sys Id: encBSIG
 IPv6 Crypto IKEv2  SA
```

QKD crypto tunnel statistics

```
openqkd_router1#sh crypto ipsec sa
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 10.1.0.1
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.1.0.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.1.0.2/255.255.255.255/47/0)
   current_peer 10.1.0.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 17049975, #pkts encrypt: 17049975, #pkts digest: 17049975
    #pkts decaps: 16042625, #pkts decrypt: 16042625, #pkts verify: 16042625
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
```

QKD crpto tunnel statistics details

```
openqkd_router1#sh crypto ipsec sa detail
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 10.1.0.1
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.1.0.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.1.0.2/255.255.255.255/47/0)
   current_peer 10.1.0.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 17049975, #pkts encrypt: 17049975, #pkts digest: 17049975
    #pkts decaps: 16042625, #pkts decrypt: 16042625, #pkts verify: 16042625
```

KPI Groups (Unique and Sorted)	KPI name	
Rates	Key creation rates	Not measures, since link point to point.
	Key consumption rates	Key required each 3000 sec
	Key transmission rate	Not measures, since link point to point.
	QBER / excess noise	N/A
Throughput	Data Transactions	N/A
	Data Throughput	Customer standard traffic of 50 top 100 Mbps
Latency	Quantum network latency	3ms on Geneva local loop. QKD did not impacted the latency of AES 256 encrypted on Cisco IOS-XE cisco equipment
	classical network latency	3ms on Geneva local loop.
Compatibility with existing Infrastructure	Modularity	Compliant with Datacenter environment or equivalent.
	Equipment Size	Half rack to be provided
	Deployment (Size & Automation)	Rack space to be planned in advance. QKD evolution tend to lower down Rack units, but not the needed physical environment.
	Scalability	N/A
Security & certification	Security & certification	Not measured, only stability of the link was measured.
Resistance to Failure & Link stability	Resistance to Failure	Not measured, only stability of the link was measured.
	Link stability	Link has been up and running fully for 1 month.

3.2 Use Case 03

ID: 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.

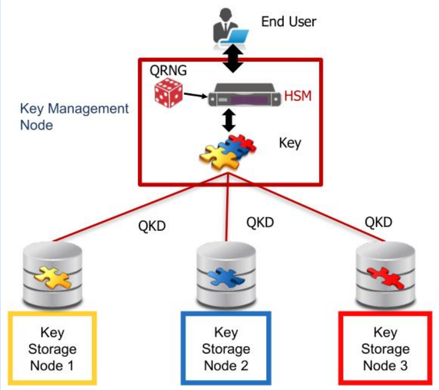


Image credit: IDQ, MTP

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

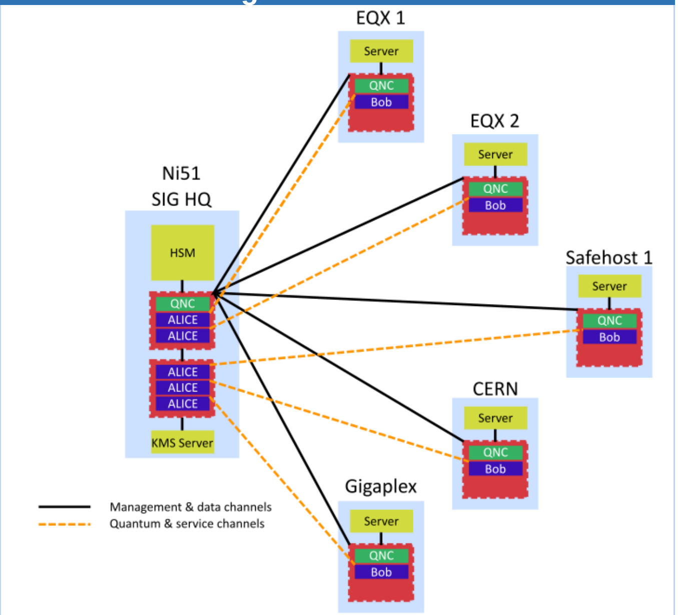
Impact

Target sector planned impact:
Securing the storage of digital assets.
Companies attracted through use case:
- Banks, DAC service provider

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

Existing equipment

What else is available and can be used?

Site1

-
Site2
-
Site3
-

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.
Planned deployments
All links will be deployed in January 2020. The use case is planned to run for ten months. **Interfaces between layers:** - ETSI 014 interface between QKD and MTP HSM/Server
Results
Lessons learned: - **Changes necessary to already deployed infrastructure:** - **KPI demo report:** - **Target sector demonstrated impact:** - **Estimated cost of implementation:** - QKD systems: 475 k€ - HSM: 10 k€ - Personnel for installation and maintenance: 30 k€ - Other equipment used: 5 k€ - Total cost: 520 k€ - Target costs: 200 k€

KPI Groups (Unique and Sorted)	KPI name	
Rates	Key creation rates	≈ 4 keys per second (1 key = 256 bits)
	Key consumption rates	Depending on test configuration; could be arbitrarily high (e.g., 100 keys per second)
	Key transmission rate	Depending on the QKD-internal buffers. If filled, transmission rate can be as high as consumption rate for a limited time even if the consumption rate exceeds the creation rate
	QBER / excess noise	Typically, between 1% and 2%
Throughput	Data Transactions	Data was encrypted with OTP method, hence the data transactions equal the key consumption rate
	Data Throughput	Each transaction consists of a 256 bit string.
Latency	Quantum network latency	No latency if key request rate was on average at most 4 keys per second
	classical network latency	Distribution and recovery: 1.5s and 0.25s respectively. (Distribution was slower due to consistency checks)
Compatibility with existing Infrastructure	Modularity	QKD and key consumers are interoperable
	Equipment Size	13u at central node, 6u at peripheric nodes
	Deployment (Size & Automation)	More attention on
	Scalability	Can be embedded in future shared QKD networks of datacentre interconnect links
Security & certification	Security & certification	ITS thanks to OTN
Resistance to Failure & Link stability	Resistance to Failure	Shamir Secret Sharing exhibits redundancy per design
	Link stability	After setup, no issues with the link stability.
Use Case or Testbed specific features	Use Case or Testbed specific features	Use case testing operating in several contemporary datacentres, which was a good experience for all participants

3.3 Use Case 12

ID: 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

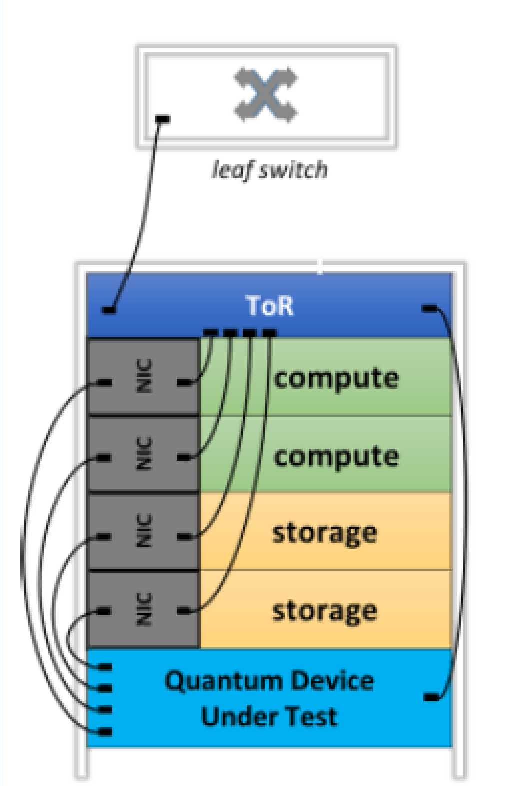
financial cost of a security breach can be substantial, especially when customer data is exposed.

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 (TREL)	QKD System provider

Impact

Target sector planned impact:	Planned KPI demonstrations:
-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	- 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:

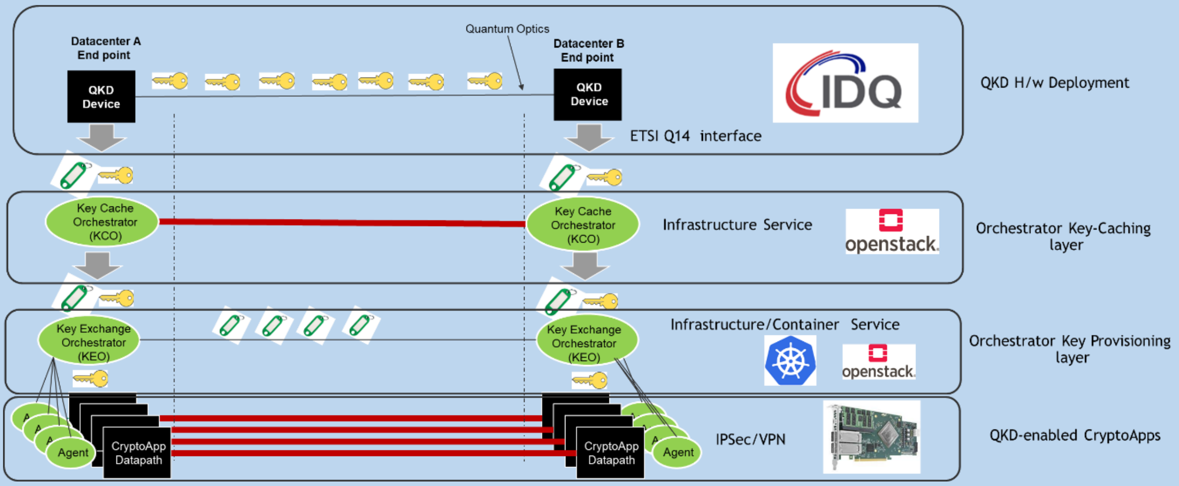
QKD

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) **Site2** - **Site3** -
Encryptors
Manufacturers and Devices ○ MLNX Bluefield SmartNIC
QKD Systems
Manufacturers and Devices ○ IDQuantique (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
Results
Lessons learned: -
Changes necessary to already deployed infrastructure: -

KPI demo report: -
Target sector demonstrated impact: -
Estimated cost of implementation: -

Impact

Target sector planned impact:
- Data Center

Companies attracted through use case:
- Mellanox/ Nvidia

Achieved KPI demonstrations:
- Key rate: 4 keys/s (256-bit keys)
- Latency: 100 ms
- Compliance with temperature standards: yes
- Stability: Key error rate = $\sim10^{-2}$

Time of demonstration

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

Time of demonstration:
- June 2021 – Dec 2021

Results

Lessons learned:
-

Changes necessary to already deployed infrastructure:
- Allocate space in the Racks for the QKD equipment
-

Target sector demonstrated impact:
- Replaced IKE with a safer alternative
-

Estimated cost of implementation:
-

Further comments:
-

KPI Groups (Unique and Sorted)	KPI name	
Rates	Key creation rates	4 keys/s (256-bit keys)
	Key consumption rates	4 key/s
	Key transmission rate	4 key/s
	QBER / excess noise	
Throughput	Data Transactions	
	Data Throughput	5 GB/s
Latency	Quantum network latency	100ms (to get the keys from the quantum device)
	classical network latency	10 us
Compatibility with existing Infrastructure	Modularity	
	Equipment Size	Should be miniaturized
	Deployment (Size & Automation)	Point to point servers
	Scalability	
Security & certification	Security & certification	
Resistance to Failure & Link stability	Resistance to Failure	Ok
	Link stability	Ok
Use Case or Testbed specific features	Use Case or Testbed specific features	

3.4 Use Case 14

ID: 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.

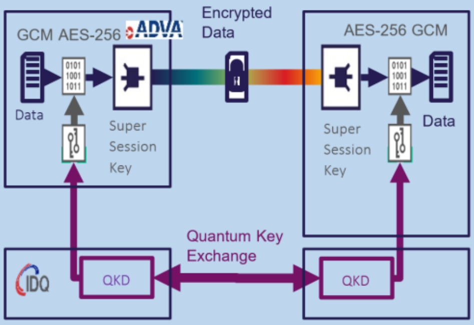


Image credit: IDQ, ADVA

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

Implementation and block diagram

Work plan/TODO list:

6 Link topology and design
7 Prepare QKD system and deployment
8 Integrate the QKD pair with ADVA FSP3K
9 Schedule exact date for deployment with hardware and personnel
10 Perform deployment
11 Adjust deployment
12 Run use case
13 Analyze link performance
14 Evaluate findings
15 Retrieve QKD devices
16 Write Report

Site access

- **SIG Ni51** Unrestricted ☐ Restricted ☒
  If restricted how: accompanied by SIG
- **IBM Gigaplex** Unrestricted ☐ Restricted ☒
  If restricted how: accompanied by SIG

Available power

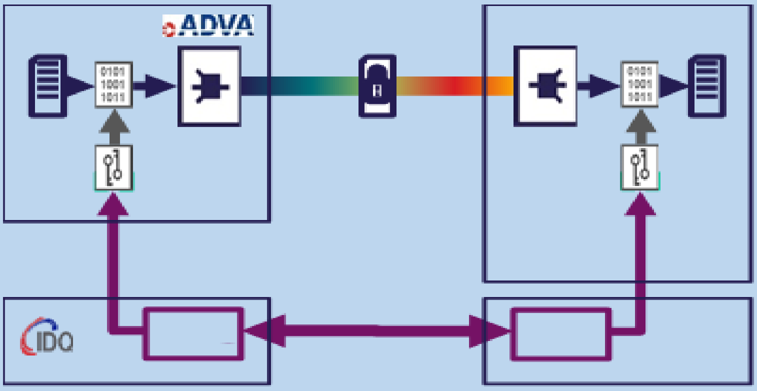
What power delivery is available for telecom and quantum devices?

- **SIG Ni51** AC 230 ☒ DC 48 ☐
- **IBM Gigaplex** AC 230 ☒ DC 48 ☐

Internet connection (closed LAN with remote access via VPN)

- **Ni51** Yes ☒ No ☐
- **IBM Gigaplex** Yes ☒ No ☐

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
  - 1 MUX / DEMUX for classical channels

QKD Systems

Manufacturers and Devices

- IDQ: IDQ-01

Link details

List of links (see database):

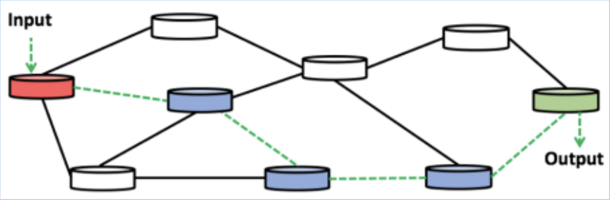
- GVA: SIG HQ – IBM Gigaplex

A link has two pairs of dark fibers one for the QKD system and one for classical channels.

Planned deployments
QKD and ADVA equipment are produced and available mid-December 2019 and will be installed on site in January 2020. The use case is planned to run for ten months. **Interfaces between layers:** - ETSI 014 interface between QKD and ADVA FSP3K
Results
Lessons learned: - **Changes necessary to already deployed infrastructure:** - **KPI demo report:** - **Target sector demonstrated impact:** - **Estimated cost of implementation:** - QKD systems: 95k€ - Personnel for installation and maintenance: 5 k€ - Other equipment used: 25k€ - Total cost: 125 k€ - Target costs: 50 k€

KPI Groups (Unique and Sorted)	KPI name	
Rates	Key creation rates	≈ 4 keys per second (1 key = 256 bits)
	Key consumption rates	1 key every 10 min
	Key transmission rate	1 key every 10 min
	QBER / excess noise	Typically, around 1%
Throughput	Data Transactions	Continuous
	Data Throughput	10 Gbps
Latency	Quantum network latency	No measurable impact
	classical network latency	No measurable impact
Compatibility with existing Infrastructure	Modularity	Interoperability between QKD and encryptor thanks to ETSI 014
	Equipment Size	7u on each site
	Deployment (Size & Automation)	Rack space to be planned in advance. QKD evolution tend to lower down Rack units, but not the needed physical environment.
	Scalability	P2P
Security & certification	Security & certification	QKD keys combined with legacy key exchange method to encrypt data via AES 256.
Resistance to Failure & Link stability	Resistance to Failure	By default, ADVA FSP3000 continue the data encryption communication using the standard mode DH for key exchange in case of QKD link down.
	Link stability	Up and running for two months without interruption
Use Case or Testbed specific features	Use Case or Testbed specific features	Used in production

3.5 Use Case 15

ID: 15 Network security and attestation	
Target sector: *Telecommunication, Critical Infrastructure protection*	
Country: SP | **Main site: Madrid**	
Description from Proposal: The ability to guarantee that a given network packet has passed through certain nodes and in a given order 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. It also allows to attest the service or monitored behavior in case of legal problems. Here we will be using a novel protocol based on QKD that is currently going through a standardization process at IETF to enforce OPoT: Ordered Proof of Transit	

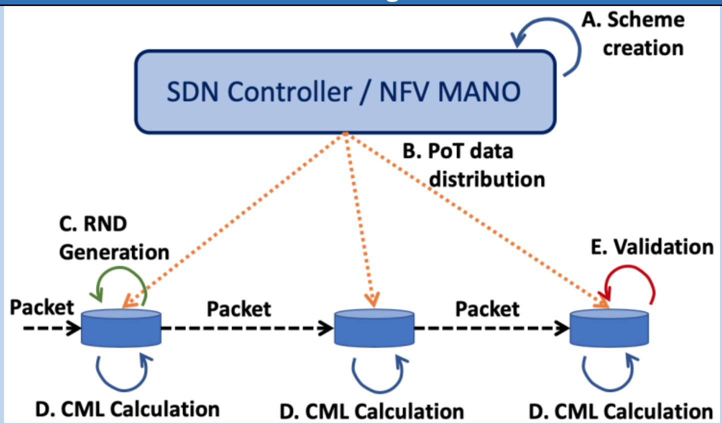
Partner	Role/Function
idQ	QKD System provider
TREL	QKD System provider
TID	Testbed and use case provider (End user: Telefónica Spain)
UPM	SW provider
RM	Testbed provider
Other	QKD experimental System provider

Impact	
Target sector planned impact: Securing the telecommunication infrastructure, especially the virtualized ones by making sure that service function chains are executed in the proper order and without skipping crucial steps (e.g. passing through a firewall) **Companies attracted through use case:** - Telefónica de España - BT - DT - Accenture, Upandrunning have demonstrated interest.	**Planned KPI demonstrations:** - Key indicators: number of OPoT marked packets per second compared to the average network packets processed in the network without OPoT. - (Late test) Inter-provider security - Increased latency (ms).

Implementation
Work plan/TODO list:

1. Define Service Function Chains according to available connection topology, systems and capabilities
2. Prepare QKD systems and SW deployment
3. Schedule exact date for deployment with hardware and personnel
4. Perform deployment
5. Adjust deployment
6. Finalize deployment and retrieve devices
7. Evaluate findings
8. Write Report

Block diagram



Site access

Note: Seven possible places can be used for this test, four 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 much more restricted access. Ideally, all the seven sites (with a topology that imply seven links -three of them in a star with a central node (UPM-RMCIEMAT, RMCIEMAT-UAM, RMCIEMAT-CSIC), three of them in a ring (Telefonica production network, ALMAGRO-NORTE, ALMAGRO-CONCEPCION, CONCEPCION-NORTE) and another link connecting both (ring and star) could be used. The RM Network and the Telefonica Network have different access requirements. An initial early deployment (three months) is planned for the demonstration and either network (ring or star) could be selected. If a longer time is afforded and movement of the equipment allowed, both networks can be used. In a late test, planned by the end of the project, since the fiber link connecting both topologies (and providers) is still being commissioned, both networks can be used jointly, demonstrating inter-provider capabilities for the use case. 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?

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

Internet connection
- **Site1** Yes ☒ No ☐ - **Site2** Yes ☒ No ☐ - **Site3** Yes ☒ No ☐
Existing equipment
What else is available and can be used? **Site1** - **Site2** - **Site3** -
Encryptors
Manufacturers and Devices ○ Encryptors would be wellcome, but not strictly necessary since the required encryption can be done in SW.
QKD Systems
Manufacturers and Devices - 3 Links in first phase - 7 links in second phase
Link details
Please fill out the following list for each link (physical connection between two nodes): (all currently available links are listed, the detailed links/topologies are commented in the “Site Access” section) **Link1: UPM – RMCIEMAT** - Number of parallel fibers:2 (moderately shared, several lambdas, backup line) - 24 Km, 6 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link2: RMCIEMAT-UAM** - Number of parallel fibers:2 (moderately shared, several lambdas, backup line) - 24 Km, 8 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link3: RMCIEMAT- RMCSIC** - Number of parallel fibers:2 (non-shared) - 6.5 Km, 3.5 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link4: RMCSIC-IMDEA NW** (shared, several lambdas)

- Number of parallel fibers:2
- 33 Km, 10 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link5: IMDEANW- URJC

- Number of parallel fibers:2 (shared, several lambdas)
- 22.5 Km, 6 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link6: URJC-RMCIEMAT

- Number of parallel fibers:2 (shared, several lambdas)
- 40 Km, 12 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link7: ALMAGRO-NORTE

- Number of parallel fibers:2 (non-shared)
- 3.9 Km, 8.5 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)
-

Link8: ALMAGRO-CONCEPCION

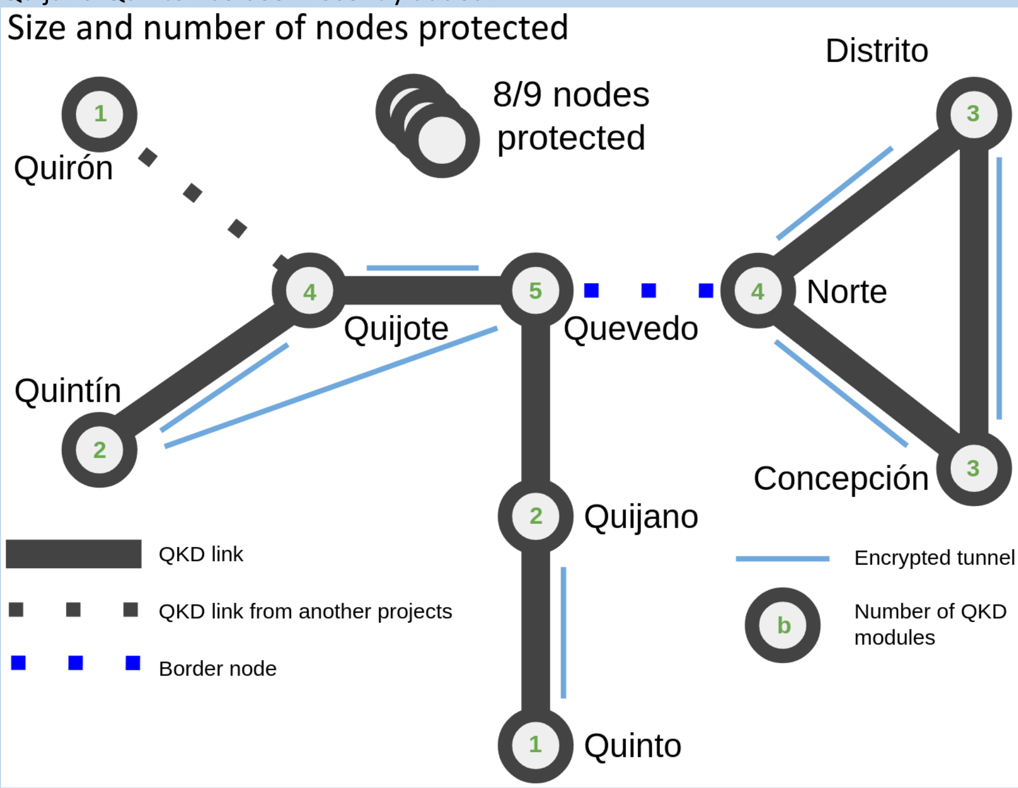
- Number of parallel fibers:2 (non-shared)
- 6.4 Km, 8 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

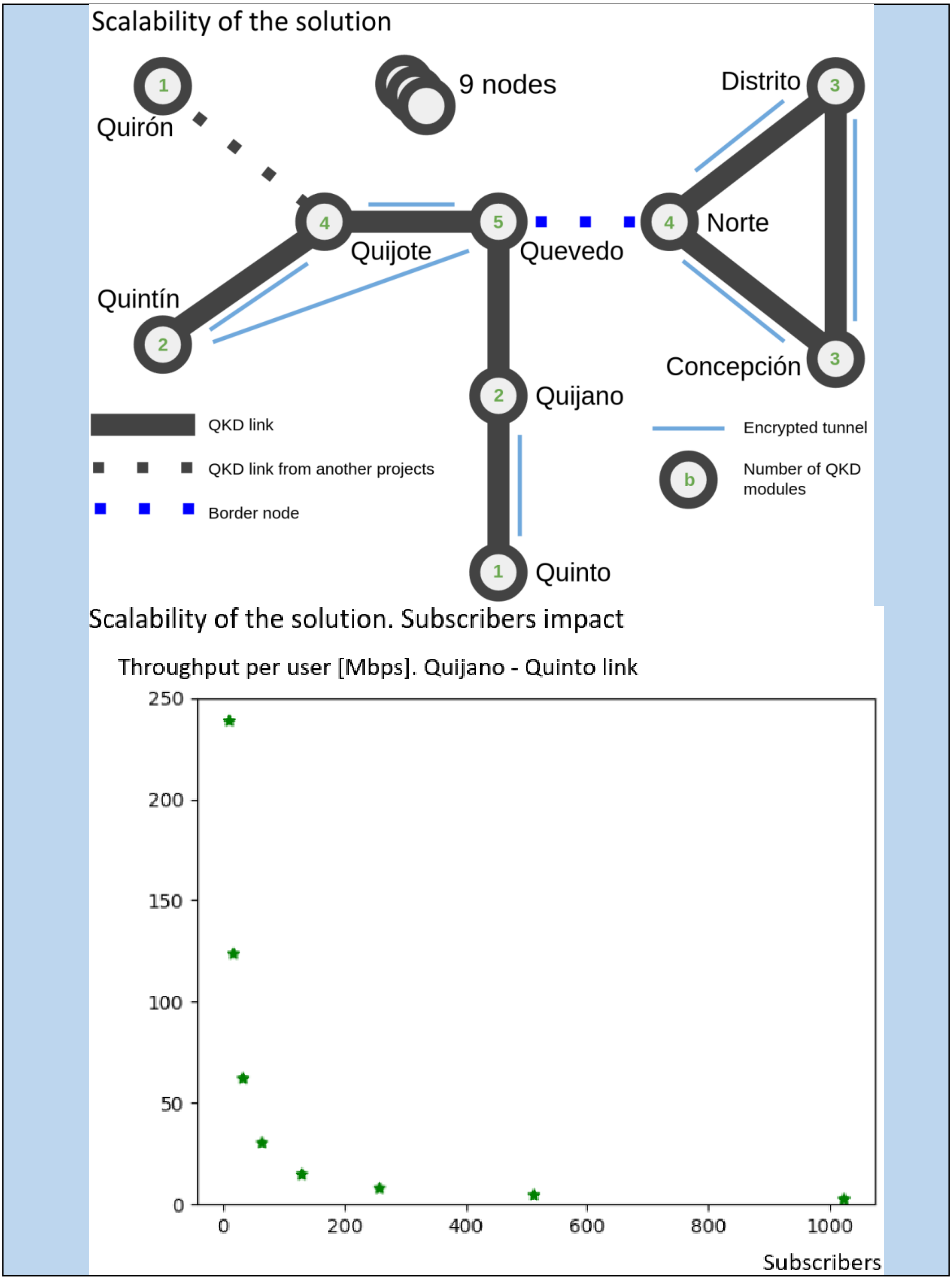
Link9: CONCEPCION- NORTE

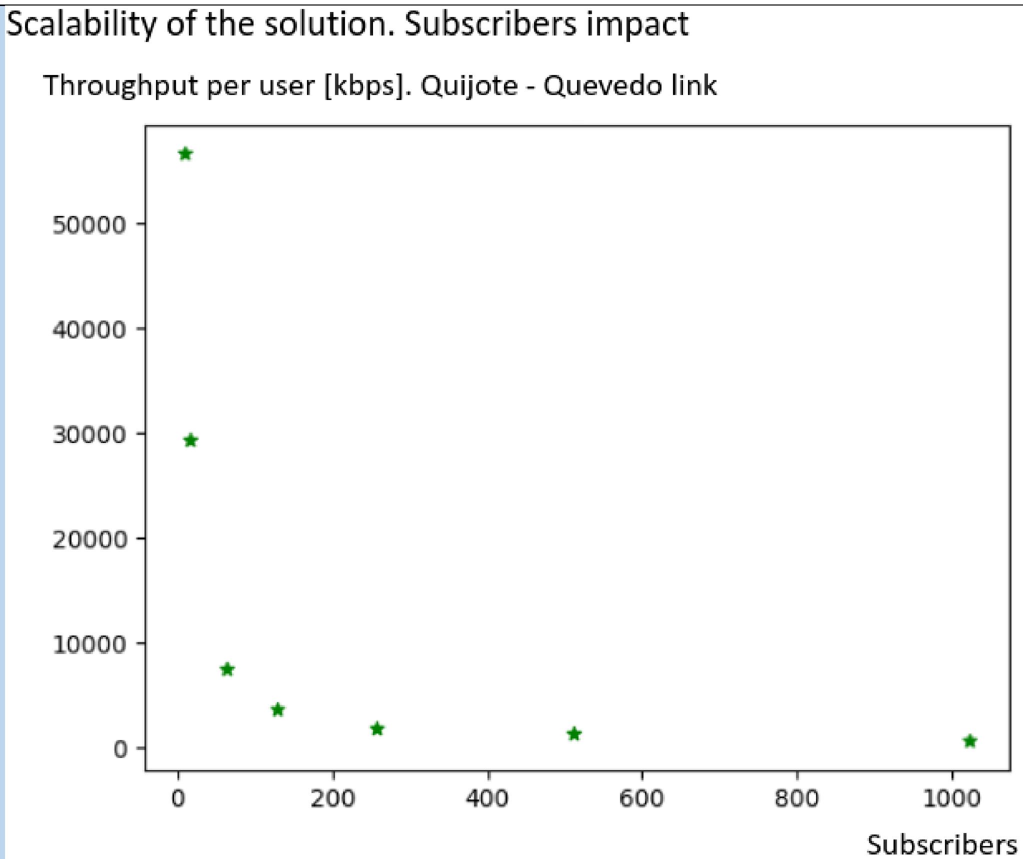
- Number of parallel fibers:2 (non-shared)
- 5 Km, 7 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths

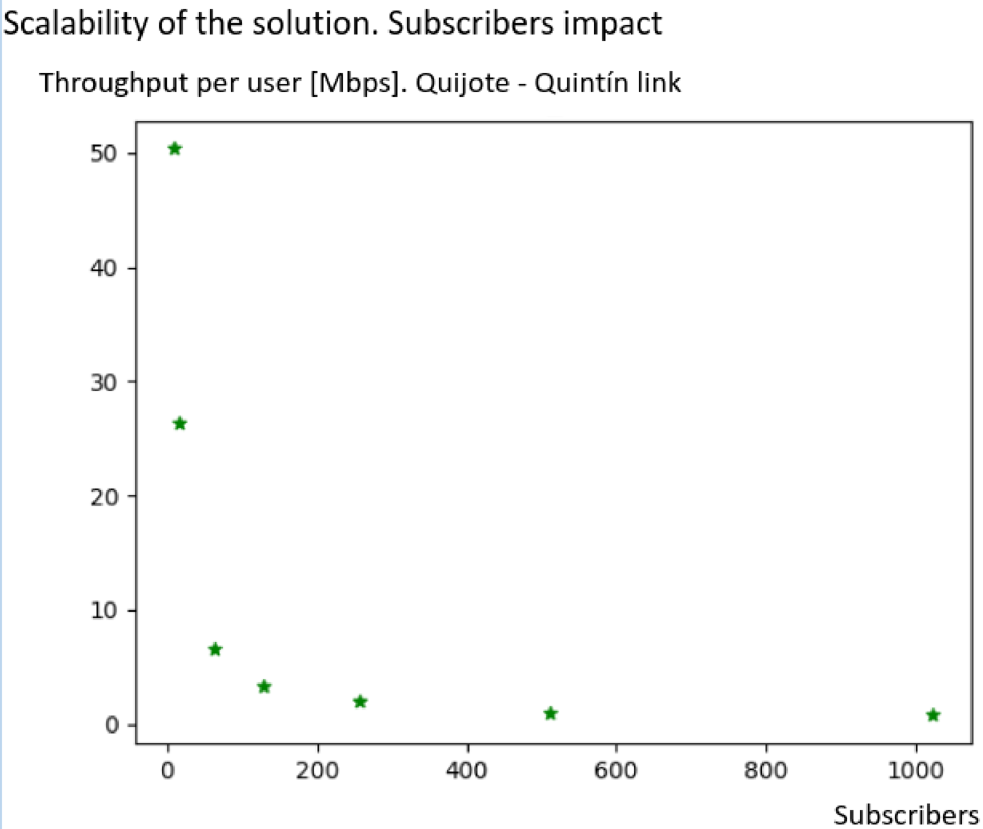
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)
Planned deployments
First phase deployment: three Links, May-Jul 2020 - Link1, QKDSystem1, May 2020 - Jul 2020 - Link2, QKDSystem2, May 2020 - Jul 2020 - Link3, QKDSystem3, May 2020 - Jul 2020 Second phase deployment (with inter-provider demonstrations): Seven links, May-Aug 2022.
Interfaces between layers: - Preferable 004 (because of QoS and expected latencies) 014 if 004 is not implemented.

Impact	
Target sector planned impact: - Any critical infrastructure: communications, water, electricity, etc. **Companies attracted through use case:** - Telefónica de España - BT - DT - Accenture - UpAndRunning	**Achieved KPI demonstrations:** - KPI 53: Size and number of nodes protected. - KPI 54: Scalability of the solution. All the KPIs designed for this UC have been fully achieved.
Time of demonstration	
Deployment: - Initial development and adaptation of the Madrid Network: 14 months. - The deployment is based on IPSec suite, which requires: ○ Around 10 minutes per tunnel link between a pair of trusted nodes. - Note that this deployment assumes that all the SDN stack of the Madrid Quantum Network is fully deployed and operative. - All the necessary infrastructure for this UC is ready and fully working, but the current traffic is not real industrial traffic, it is generic bulk traffic. In the following months, it is planned the integration of real industrial traffic, for example SCADA traffic.	
Time of demonstration: - The first version of the CIP UC based on the IPSec suite was developed on 04/2021. However, several improvements have been made since them. - This demonstrator is running on the Madrid Network since its first development and it is run periodically, daily or weekly, to measure the network performance. - This demonstrator can be executed on any set of links of the network with QKD systems available.	
Results	
Lessons learned: - QKD services can be used to provide protection to critical infrastructures. - Using a general-purpose technology, such as the IPSec suite, enables tunnelling techniques that transparently transport any type of IP communication based on QKD ITS security. - Using a software-defined technology, as this specific IPSec suite is, enables a seamless integration with the software-defined QKD nodes of the Madrid network.	

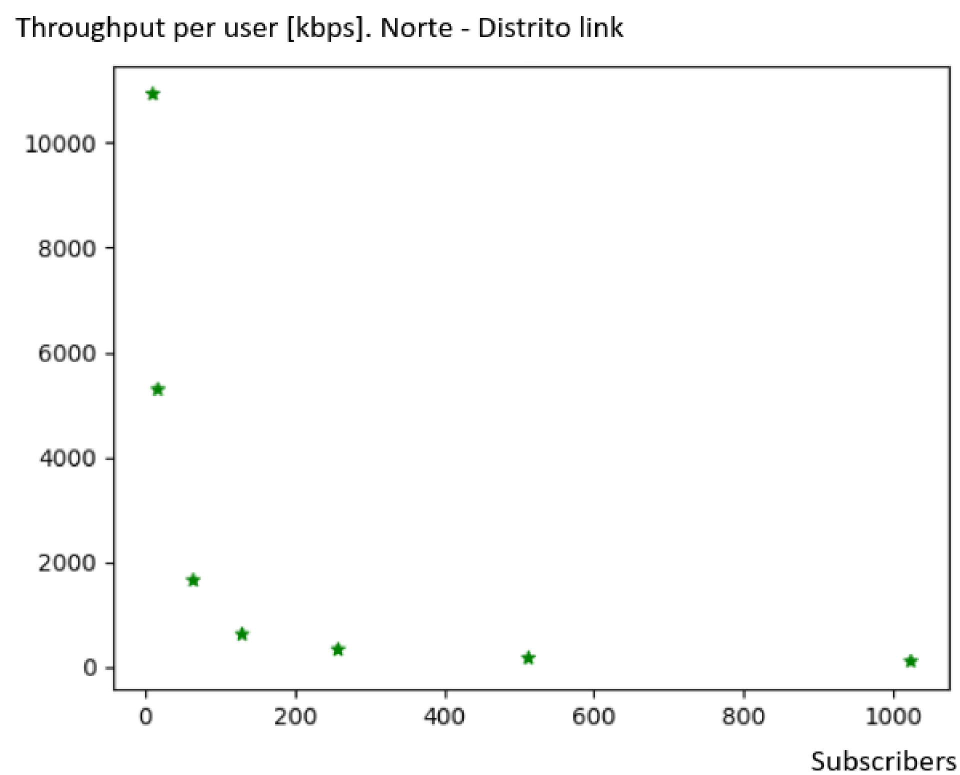
- As the IPSec suite is a software program, it needs enough computational power to perform the encryption of the communications relayed.
Changes necessary to already deployed infrastructure: - The current version of the CIP use case runs on top of the Madrid's SDN stack, which delivers QKD services using the ETSI ISG QKD 004 standard access point. - Additional computation power was needed in some IT systems deployed.
Target sector demonstrated impact: - Securing of telecommunication network providers' transmissions.
Estimated cost of implementation: - QKD system: 150k€ (2 DVs modules) - Personnel for installation and maintenance: 20k€ - Other equipment used: 10k€ - Desired airport cost for all of this: 10k€ - Software Development: Using as base the Madrid SDN Stack infrastructure, the implementation of the IPSec infrastructure requires 1PM during 14 months approximately. = 70K€ - Total cost: 260k€ UC working on one link.
Further comments: - The following figure shows the progress of the use case deployment depending on the availability of the QKD systems, which is the KPI 53. The links Quevedo-Quijano and Quijano-Quinto has been recently added.  - The following figures shows the KPI 54, which measures the scalability of the solution depending on the number of subscribers. The links Quevedo-Quijano and Quijano-Quinto has been recently added.


Scalability of the solution
9 nodes
Quirón
Distrito
Quintín
Quijote
Quevedo
Norte
Concepción
Quijano
Quinto
QKD link
QKD link from another projects
Border node
Encrypted tunnel
Number of QKD modules
Scalability of the solution. Subscribers impact
Throughput per user [Mbps]. Quijano - Quinto link
250
200
150
100
50
0
0
200
400
600
800
1000
Subscribers


Scalability of the solution. Subscribers impact
Throughput per user [kbps]. Quijote - Quevedo link
50000
40000
30000
20000
10000
0
0
200
400
600
800
1000
Subscribers


Scalability of the solution. Subscribers impact
Throughput per user [Mbps]. Quijote - Quintín link
50
40
30
20
10
0
0
200
400
600
800
1000
Subscribers

Scalability of the solution. Subscribers impact



- A video of the use case can be seen here: https://drive.upm.es/s/fed4HkCf5ePlhpS
- Name of the Video: UC16_Madrid_ CriticalInfrastructureProtection.mkv

3.6 Use Case 16

<table>
<tr><td colspan="2">ID: 16
Critical Infrastructure Protection</td><td rowspan="4"></td></tr>
<tr><td colspan="2">Target sector: Critical Infrastructure protection</td></tr>
<tr><td>Country: SP</td><td>Main site: Madrid</td></tr>
<tr><td colspan="2">Description from Proposal:
Nowadays, many industrial infrastructures are monitored and managed remotely through the network. These – typically SCADA (Supervisory Control and Data Acquisition) networks – are responsible for infrastructures that control systems ranging from the water supply to the electrical grid and are, thus, critical to our society. This use case intends to demonstrate the securing of this type of networks through QKD</td></tr>
</table>

Partner	Role/Function
idQ	QKD System provider
TREL	QKD System provider
TID	Testbed and use case provider (Enduser: Telefónica Spain)
UPM	SW provider
RM	Testbed provider
Other	QKD experimental System provider

<table>
<tr><th colspan="2">Impact</th></tr>
<tr><td>Target sector planned impact:
Securing critical infrastructures has a large impact in many sectors: water, electricity, etc…
Companies attracted through use case:
- Telefónica de España
- BT
- DT
- Accenture, UpAndRunning</td><td>Planned KPI demonstrations:
- Size and number of nodes protected,
- Scalability of the solution</td></tr>
<tr><th colspan="2">Implementation</th></tr>
<tr><td colspan="2">Work plan/TODO list:
9. Define control structure according to available connection topology, systems and capabilities
10. Prepare QKD systems and SW deployment
11. Schedule exact date for deployment with hardware and personnel
12. Perform deployment
13. Adjust deployment
14. Finalize deployment and retrieve devices
15. Evaluate findings
16. Write Report</td></tr>
<tr><th colspan="2">Block diagram</th></tr>
<tr><td colspan="2"></td></tr>
<tr><th colspan="2">Site access</th></tr>
</table>

Note: Nine possible places can be used for this test, six 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 much more restricted access. Ideally, all the sites (with a topology that imply seven links -three of them in a star with a central node and several hops in one of the branches(UPM-RMCIEMAT, RMCIEMAT-UAM, RMCIEMAT-CSIC, CSIC-IMDEANW, IMDEANW-URJC), three of them in a ring (Telefonica production network, ALMAGRO-NORTE, ALMAGRO-CONCEPCION, CONCEPCION-NORTE) and another link connecting both (ring and star) could be used. An initial early deployment (three months) is planned for the demonstration and either network (ring or star) could be selected. If a longer time is afforded and movement of the equipment allowed, both networks can be used. In a late test, planned by the end of the project, since the fiber link connecting both topologies (and providers) is still being commissioned, both networks can be used jointly, demonstrating inter-provider capabilities for the use case. 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?

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

Internet connection

- **Site1** Yes ☐ No ☐
- **Site2** Yes ☐ No ☐
- **Site3** Yes ☐ No ☐

Existing equipment

What else is available and can be used?

Site1

-

Site2

-

Site3

-

Encryptors

Manufacturers and Devices

- Encryptors would be welcome, but not strictly necessary since the required encryption can be done in SW.

QKD Systems

Manufacturers and Devices

- 3 Links first phase
- 7 links second phase

Link details

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

(all currently available links are listed, the detailed links/topologies are commented in the "Site Access" section)

Link1: UPM – RMCIEMAT

- Number of parallel fibers:2 (moderately shared, several lambdas, backup line)
- 24 Km, 6 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link2: RMCIEMAT-UAM

- Number of parallel fibers:2 (moderately shared, several lambdas, backup line)
- 24 Km, 8 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link3: RMCIEMAT- RMCSIC

- Number of parallel fibers:2 (non-shared)
- 6.5 Km, 3.5 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link4: RMCSIC-IMDEA NW (shared, several lambdas)

- Number of parallel fibers:2
- 33 Km, 10 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link5: IMDEANW- URJC

- Number of parallel fibers:2 (shared, several lambdas)
- 22.5 Km, 6 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link6: URJC-RMCIEMAT - Number of parallel fibers:2 (shared, several lambdas) - 40 Km, 12 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link7: ALMAGRO-NORTE** - Number of parallel fibers:2 (non-shared) - 3.9 Km, 8.5 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) - **Link8: ALMAGRO-CONCEPCION** - Number of parallel fibers:2 (non-shared) - 6.4 Km, 8 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link9: CONCEPCION- NORTE** - Number of parallel fibers:2 (non-shared) - 5 Km, 7 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)
Planned deployments
First phase deployment: three Links, May-Jul 2020 - Link1, QKDSystem1, May 2020 - Jul 2020 - Link2, QKDSystem2, May 2020 - Jul 2020 - Link3, QKDSystem3, May 2020 - Jul 2020 Second phase deployment (with inter-provider demonstrations): Seven links, May-Aug 2022. -
Interfaces between layers: - Preferable 004 (because of QoS and expected latencies) 014 if 004 is not implemented.

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

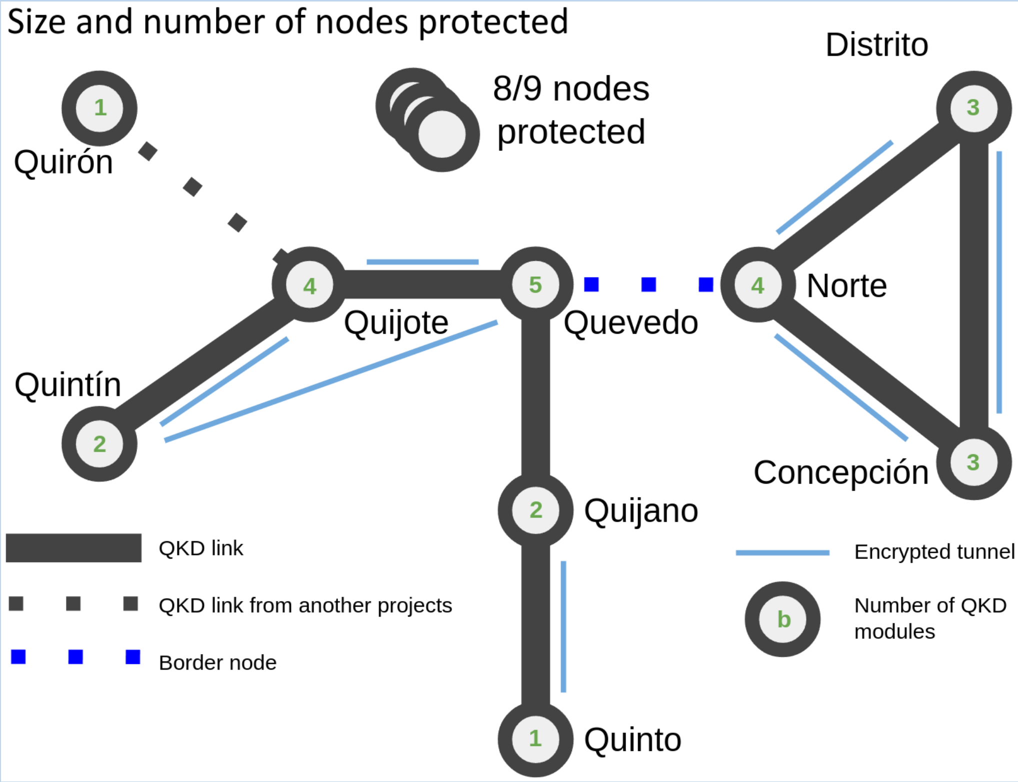
- Any critical infrastructure: communications, water, electricity, etc. **Companies attracted through use case:** - Telefónica de España - BT - DT - Accenture - UpAndRunning	- KPI 53: Size and number of nodes protected. - KPI 54: Scalability of the solution. All the KPIs designed for this UC have been fully achieved.

Time of demonstration
Deployment: - Initial development and adaptation of the Madrid Network: 14 months. - The deployment is based on IPSec suite, which requires: o Around 10 minutes per tunnel link between a pair of trusted nodes. - Note that this deployment assumes that all the SDN stack of the Madrid Quantum Network is fully deployed and operative. - All the necessary infrastructure for this UC is ready and fully working, but the current traffic is not real industrial traffic, it is generic bulk traffic. In the following months, it is planned the integration of real industrial traffic, for example SCADA traffic.
Time of demonstration: - The first version of the CIP UC based on the IPSec suite was developed on 04/2021. However, several improvements have been made since them. - This demonstrator is running on the Madrid Network since its first development and it is run periodically, daily or weekly, to measure the network performance. - This demonstrator can be executed on any set of links of the network with QKD systems available.
Results
Lessons learned: - QKD services can be used to provide protection to critical infrastructures. - Using a general-purpose technology, such as the IPSec suite, enables tunnelling techniques that transparently transport any type of IP communication based on QKD ITS security. - Using a software-defined technology, as this specific IPSec suite is, enables a seamless integration with the software-defined QKD nodes of the Madrid network. - As the IPSec suite is a software program, it needs enough computational power to perform the encryption of the communications relayed.
Changes necessary to already deployed infrastructure: - The current version of the CIP use case runs on top of the Madrid's SDN stack, which delivers QKD services using the ETSI ISG QKD 004 standard access point. - Additional computation power was needed in some IT systems deployed.
Target sector demonstrated impact: - Securing of telecommunication network providers' transmissions.
Estimated cost of implementation: - QKD system: 150k€ (2 DVs modules) - Personnel for installation and maintenance: 20k€ - Other equipment used: 10k€ - Desired airport cost for all of this: 10k€

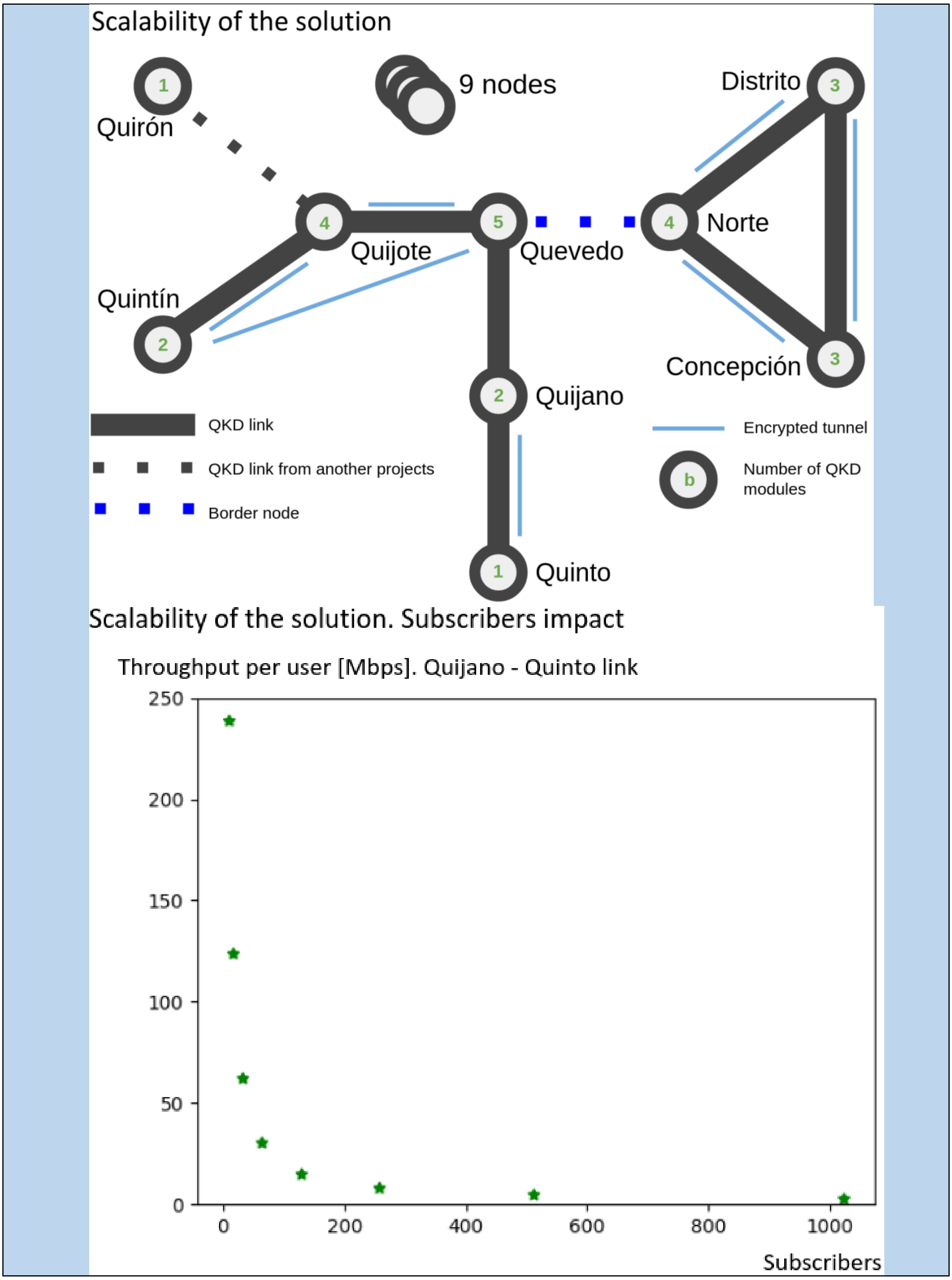
- Software Development: Using as base the Madrid SDN Stack infrastructure, the implementation of the IPSec infrastructure requires 1PM during 14 months approximately. = 70K€
- Total cost: 260k€ UC working on one link.

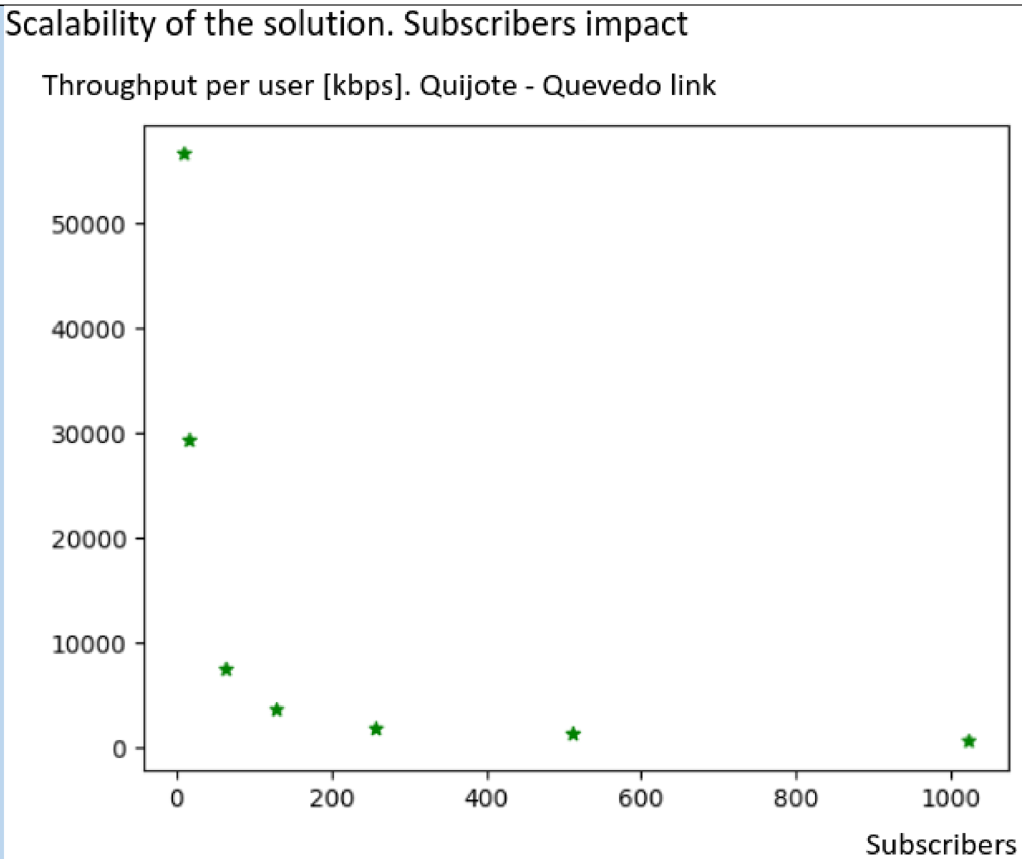
Further comments:

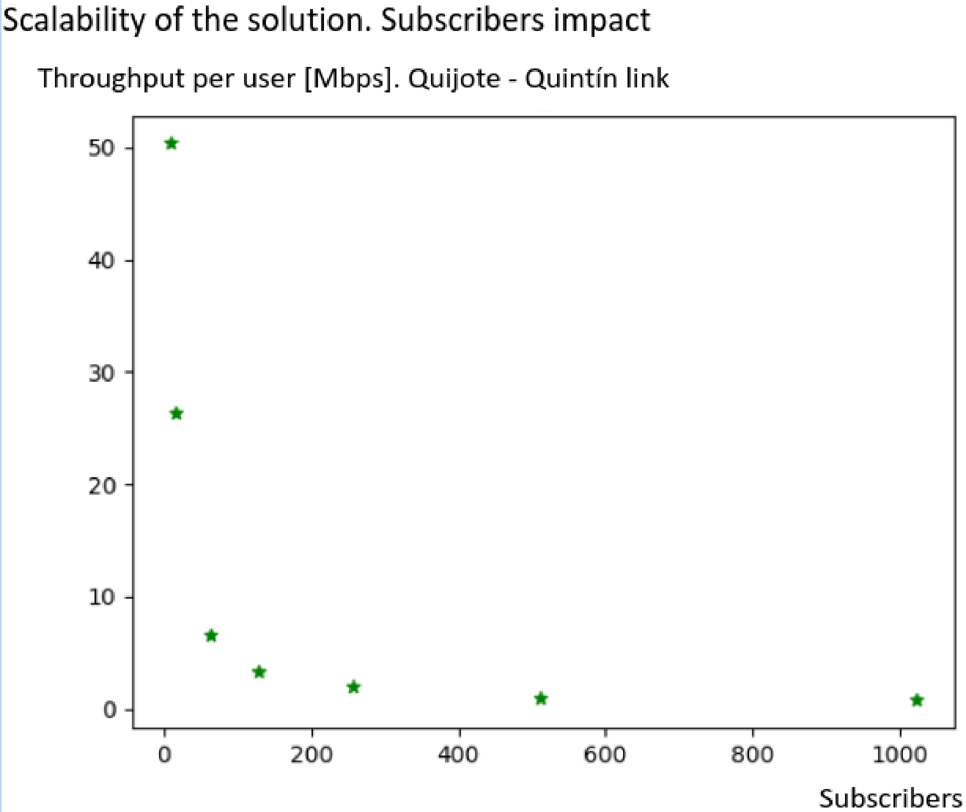
- The following figure shows the progress of the use case deployment depending on the availability of the QKD systems, which is the KPI 53. The links Quevedo-Quijano and Quijano-Quinto has been recently added.

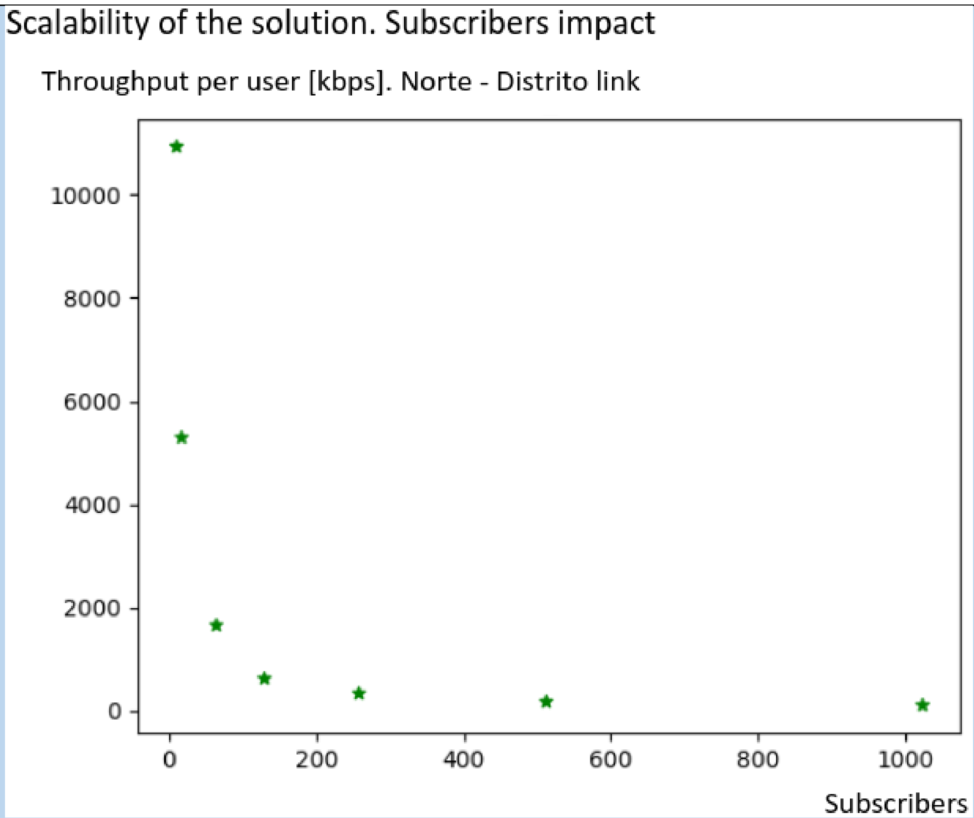


- The following figures shows the KPI 54, which measures the scalability of the solution depending on the number of subscribers. The links Quevedo-Quijano and Quijano-Quinto has been recently added.


Scalability of the solution
9 nodes
Quirón
1
Distrito
3
4
5
4
Quijote
Quevedo
Norte
Quintín
2
Concepción
3
2
Quijano
QKD link
QKD link from another projects
Border node
Encrypted tunnel
b
Number of QKD modules
1
Quinto
Scalability of the solution. Subscribers impact
Throughput per user [Mbps]. Quijano - Quinto link
250
200
150
100
50
0
0
200
400
600
800
1000
Subscribers


Scalability of the solution. Subscribers impact
Throughput per user [kbps]. Quijote - Quevedo link
50000
40000
30000
20000
10000
0
0
200
400
600
800
1000
Subscribers


Scalability of the solution. Subscribers impact
Throughput per user [Mbps]. Quijote - Quintín link
50
40
30
20
10
0
0
200
400
600
800
1000
Subscribers



- A video of the use case can be seen here: https://drive.upm.es/s/fed4HkCf5ePIhpS
- Name of the Video: UC16_Madrid_ CriticalInfrastructureProtection.mkv

3.7 Use Case 17

ID: 17

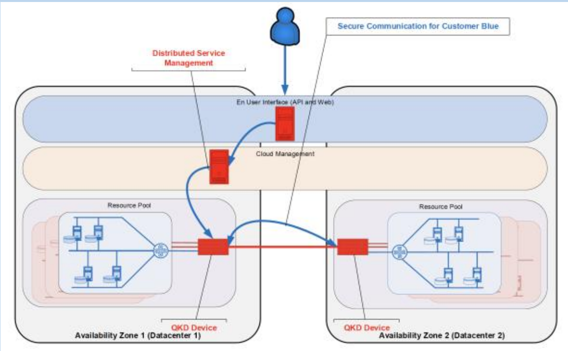
QKD as a Cloud Service

Target sector: *Secure cloud services*

Country: SP | **Main site: Madrid**

Description from Proposal:

Several cloud datacenters will be linked using QKD. Instead of using directly the link to encrypt all the traffic, as has been done in other use cases, here the QKD systems will be integrated in the cloud infrastructure to provide secret keys as a service. In this way, client applications can request keys to encrypt only the data that needs it, thus optimizing the infrastructure and making QKD available to all users of the cloud. Since many business, including banks, are migrating all their IT services to cloud providers, this is a significant application. As a starting point an implementation using two OpenStack deployments in two nodes of the network will be used, extending it later to more places to study the scalability and performance of the network.



Partner	Role/Function
idQ	QKD System provider
TREL	QKD System provider
TID	Testbed and SW provider
UPM	SW provider
RM	Testbed provider

Impact

Target sector planned impact:	Planned KPI demonstrations:
Secure cloud services **Companies attracted through use case:** - Telefónica de España - BT - DT	- number of requests served per unit time. - Number of users that the infrastructure can serve. - Scalability of the solution.

Implementation

Work plan/TODO list:

17. Define parameters for the test.
18. Prepare QKD systems and SW deployment
19. Schedule exact date for deployment with hardware and personnel
20. Perform deployment

21. Adjust deployment
22. Finalize deployment and retrieve devices
23. Evaluate findings
24. Write Report

Block diagram

Site access

Note: Nine possible places can be used for this test, six 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 much more restricted access. Ideally, all the sites (with a topology that imply seven links -three of them in a star with a central node and several hops in one of the branches(UPM-RMCIEMAT, RMCIEMAT-UAM, RMCIEMAT-CSIC, CSIC-IMDEANW, IMDEANW-URJC), three of them in a ring (Telefonica production network, ALMAGRO-NORTE, ALMAGRO-CONCEPCION, CONCEPCION-NORTE) and another link connecting both (ring and star) could be used. An initial early deployment (three months) is planned for the demonstration and either network (ring or star) could be selected. For this use-case, since Telefónica Cloud services were the main proposers, we would prefer an installation in the Telefónica Ring with just three links. 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?

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

Internet connection

- **Site1** Yes ☐ No ☐
- **Site2** Yes ☐ No ☐
- **Site3** Yes ☐ No ☐

Existing equipment

What else is available and can be used?

Site1

-

Site2

-

Site3

-

Encryptors

Manufacturers and Devices

- 3 link encryptors

QKD Systems

Manufacturers and Devices

- 3 links

Link details

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

Link1: UPM – RMCIEMAT

- Number of parallel fibers:2 (moderately shared, several lambdas, backup line)
- 24 Km, 6 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)
-

Link2: RMCIEMAT-UAM

- Number of parallel fibers:2 (moderately shared, several lambdas, backup line)
- 24 Km, 8 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link3: RMCIEMAT- RMCSIC

- Number of parallel fibers:2 (non-shared)
- 6.5 Km, 3.5 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link4: RMCSIC-IMDEA NW (shared, several lambdas)

- Number of parallel fibers:2
- 33 Km, 10 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link5: IMDEANW- URJC

- Number of parallel fibers:2 (shared, several lambdas)
- 22.5 Km, 6 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

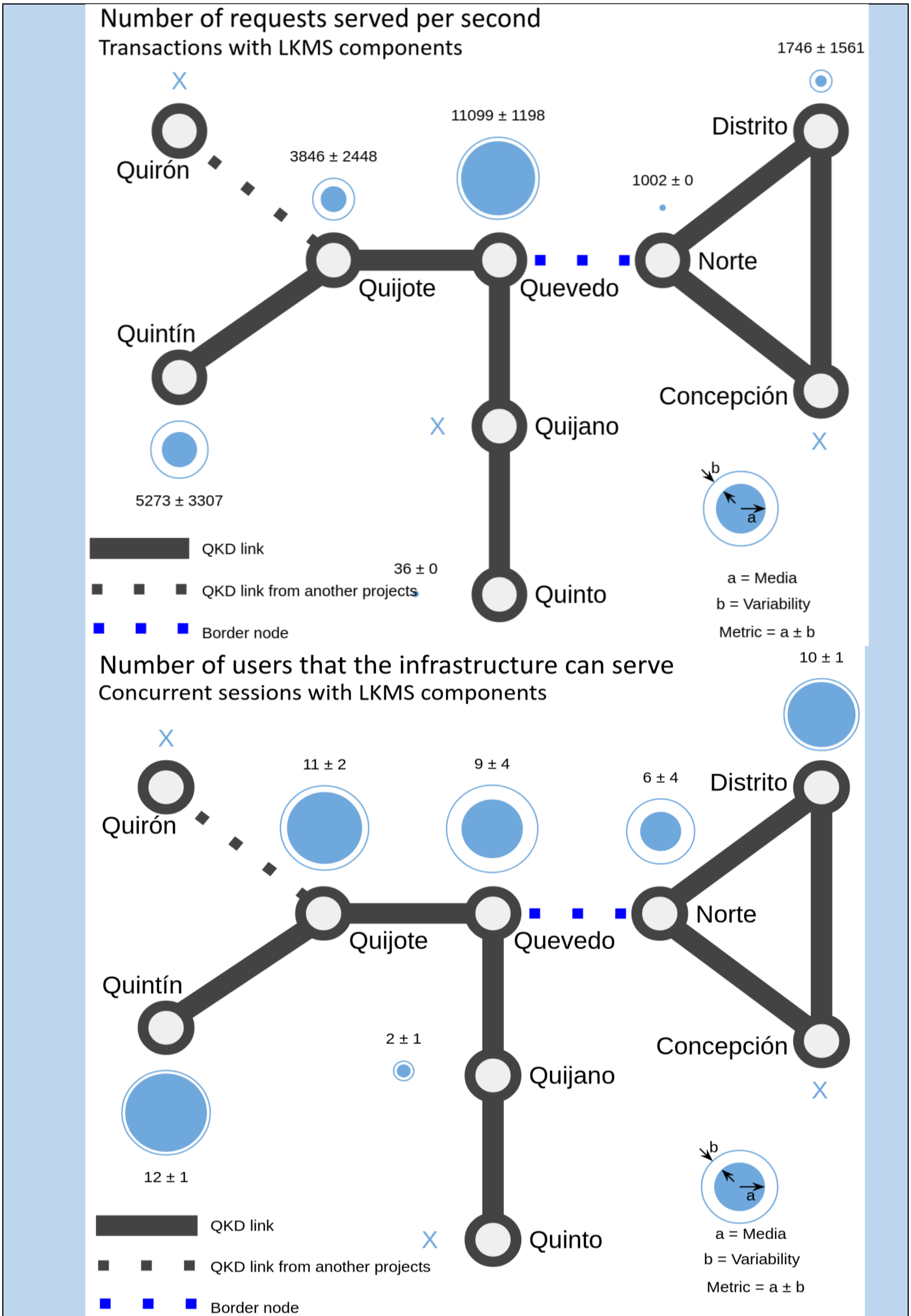
Link6: URJC-RMCIEMAT

- Number of parallel fibers:2 (shared, several lambdas)
- 40 Km, 12 dB losses, SMF

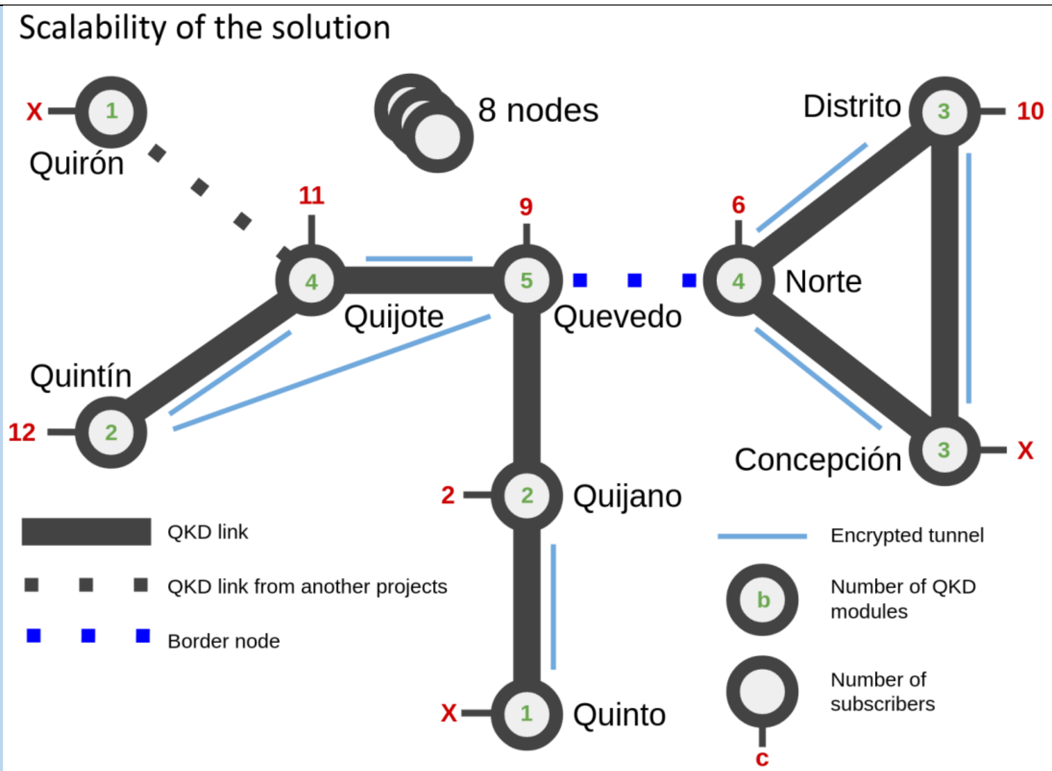
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link7: ALMAGRO-NORTE** - Number of parallel fibers:2 (non-shared) - 3.9 Km, 8.5 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link8: ALMAGRO-CONCEPCION** - Number of parallel fibers:2 (non-shared) - 6.4 Km, 8 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link9: CONCEPCION- NORTE** - Number of parallel fibers:2 (non-shared) - 5 Km, 7 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)
Planned deployments
- We have planned a late deployment in the Telefonica production ring: Dec. 2021-Mar. 2022
Interfaces between layers: - Preferable 004 (because of QoS and expected latencies) 014 if 004 is not implemented.

Impact	
Target sector planned impact: - Digital services providers. - Other infrastructure based on data centres, such as HPC clusters, network operators… **Companies attracted through use case:** - Telefónica de España - BT - DT	**Achieved KPI demonstrations:** - KPI 17: Number of requests served per unit time. - KPI 52: Number of users that the infrastructure can serve. - KPI 55: Scalability of the solution. All the KPIs designed for this UC have been fully achieved.

Time of demonstration
Deployment: - Initial development and adaptation of the Madrid Network: 7 months. - The deployment simulates QKD a cloud technology, which requires: ○ Around 10 minutes per deployment in each trusted node involved. - Note that this deployment assumes that all the SDN stack of the Madrid Quantum Network is fully deployed and operative.
Time of demonstration: - The first version of the QKD as a cloud service based on a cloud technology was developed on 05/2020. However, several improvements have been made since them. - This demonstrator was run on the Madrid Network at the month 8.
Results
Lessons learned: - QKD services can be delivered in a cloud infrastructure as a service to all the hosted application programs running over it. - As the cloud technology is a software program, it needs enough computational power to perform the encryption of the communications relayed.
Changes necessary to already deployed infrastructure: - The current version of the QKD as a cloud service use case runs on top of the Madrid's SDN stack, which delivers QKD services using the ETSI ISG QKD 004 standard access point. - Additional computation power was needed in some IT systems deployed.
Target sector demonstrated impact: - Securing the communications of application programs hosted in a cloud infrastructure.
Estimated cost of implementation: - QKD system: 150k€ (2 DVs modules) - Personnel for installation and maintenance: 20k€ - Other equipment used: 10k€ - Desired airport cost for all of this: 10k€ - Software Development: Using as base the Madrid SDN Stack infrastructure, the implementation of the IPsec infrastructure requires 1PM during 14 months approximately. = 35K€ - Total cost: 225k€ UC working on one link.
Further comments: - The following figures show the availability of the network to support this use case, known as KPI 17, 52 and 55:



- The following figure shows the KPI 55, which measures the scalability of the solution:



- A video of the use case can be seen here: https://drive.upm.es/s/fed4HkCf5ePIhpS
- Name of the Video: UC17_Madrid_QKDAsACloudService.mkv

3.8 Use Case 18

ID: 18 e-Health services		
Target sector: *Health*		
Country: **SP**	**Main site: Madrid**	
Description from Proposal: Securing the access to health data and services is an application where security is mandatory. In this use case we intend to demonstrate how to secure health related data and services. The use case that we are envisioning with a network of hospitals in Madrid is actually double. On one side it is about the secure transfer of patients' data and also accessing health databases for research purposes (data mining). These databases can be very large in the case of personalized medicine, where also genomic data has to be transferred in many cases. However, there is another application that we envision will also have a large impact and it is related to the raise of technologies like virtual or augmented reality made possible also by technologies like 5G networks. The usage of these technologies in hospitals will imply applications ranging from simple remote medical assistance to remote surgical operations, where securing the communications line and low latency will be crucial. In this use case we will also have the 5G networks lab of Telefonica and the IMDEA Networks institute. To connect one of the hospitals to the fiber infrastructure 1-2 free space link(s) will be used, for this a system from Padova could be used (initial talks with P. Villoresi) and another being also developed in Madrid (CSIC). It is possible that the Open Calls could be useful in this use case, since hospital personnel would also be involved and for the external Free space link.		

Partner	Role/Function
idQ	QKD System provider
TREL	QKD System provider
TID	Testbed and SW provider
UPM	SW provider
RM	Testbed provider
Other	QKD Free Space System provider

<table>
<tr><th colspan="2">Impact</th></tr>
<tr><td>Target sector planned impact:
Secure and privacy in e-health
Companies attracted through use case:
- Telefónica de España
- HM Hospitals (a network of 17 hospitals, the second largest private group in Spain)</td><td>Planned KPI demonstrations:
- Latency in serving a request.
- Encrypted data throughput
- Scalability of the solution.</td></tr>
<tr><th colspan="2">Implementation</th></tr>
<tr><td colspan="2">Work plan/TODO list:
25. Define parameters for the test.
26. Prepare QKD systems and SW deployment
27. Schedule exact date for deployment with hardware and personnel
28. Perform deployment
29. Adjust deployment
30. Finalize deployment and retrieve devices
31. Evaluate findings
32. Write Report</td></tr>
<tr><th colspan="2">Block diagram</th></tr>
<tr><td colspan="2"></td></tr>
</table>

Site access
Note: Nine possible places (fiber) can be used for this test, plus 1-2 free space links. Six of them (fiber) are in the RM network and they can be accessed with less restrictions and the other three are within the Telefonica production network, with much more restricted access. Ideally, all the sites (with a topology that imply seven links -three of them in a star with a central node and several hops in one of the branches (UPM-RMCIEMAT, RMCIEMAT-UAM, RMCIEMAT-CSIC, CSIC-IMDEANW, IMDEANW-URJC), three of them in a ring (Telefonica production network, ALMAGRO-NORTE, ALMAGRO-CONCEPCION, CONCEPCION-NORTE) and another link connecting both (ring and star) could be used. The RM Network and the Telefonica Network have different access requirements. An initial early deployment (three months) is planned for the demonstration and either network (ring or star) could be selected. If a longer time is afforded and movement of the equipment allowed, both networks can be used. In a late test, planned by the end of the project, since the fiber link connecting both topologies (and providers) is still being commissioned, both networks can be used jointly, demonstrating inter-provider capabilities for the use case. For this use case we envision mainly the RM network because of its easier connection with one of the HM hospitals, this link will be made using a free space link with the UPM node. Other could be also possible and also the use of the Telefonica production ring (later, when the RM-Telefónica link would be available, since a Free space link with these is not considered) 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? - **Site1** AC 230 ☐ DC 48 ☐ - **Site2** AC 230 ☐ DC 48 ☐ - **Site3** AC 230 ☐ DC 48 ☐
Internet connection
- **Site1** Yes ☐ No ☐ - **Site2** Yes ☐ No ☐ - **Site3** Yes ☐ No ☐
Existing equipment
What else is available and can be used?

Site1 - **Site2** - **Site3** -
Encryptors
Manufacturers and Devices ○ 3 link encryptors would be needed.
QKD Systems
Manufacturers and Devices ○ 3 links
Link details
Please fill out the following list for each link (physical connection between two nodes): (all currently available links are listed, the detailed links/topologies are commented in the "Site Access" section) **Link1: UPM – RMCIEMAT** - Number of parallel fibers:2 (moderately shared, several lambdas, backup line) - 24 Km, 6 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link2: RMCIEMAT-UAM** - Number of parallel fibers:2 (moderately shared, several lambdas, backup line) - 24 Km, 8 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link3: RMCIEMAT- RMCSIC** - Number of parallel fibers:2 (non-shared) - 6.5 Km, 3.5 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link4: RMCSIC-IMDEA NW (shared, several lambdas)

- Number of parallel fibers:2
- 33 Km, 10 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link5: IMDEANW- URJC

- Number of parallel fibers:2 (shared, several lambdas)
- 22.5 Km, 6 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link6: URJC-RMCIEMAT

- Number of parallel fibers:2 (shared, several lambdas)
- 40 Km, 12 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link7: ALMAGRO-NORTE

- Number of parallel fibers:2 (non-shared)
- 3.9 Km, 8.5 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link8: ALMAGRO-CONCEPCION

- Number of parallel fibers:2 (non-shared)
- 6.4 Km, 8 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link9: CONCEPCION- NORTE

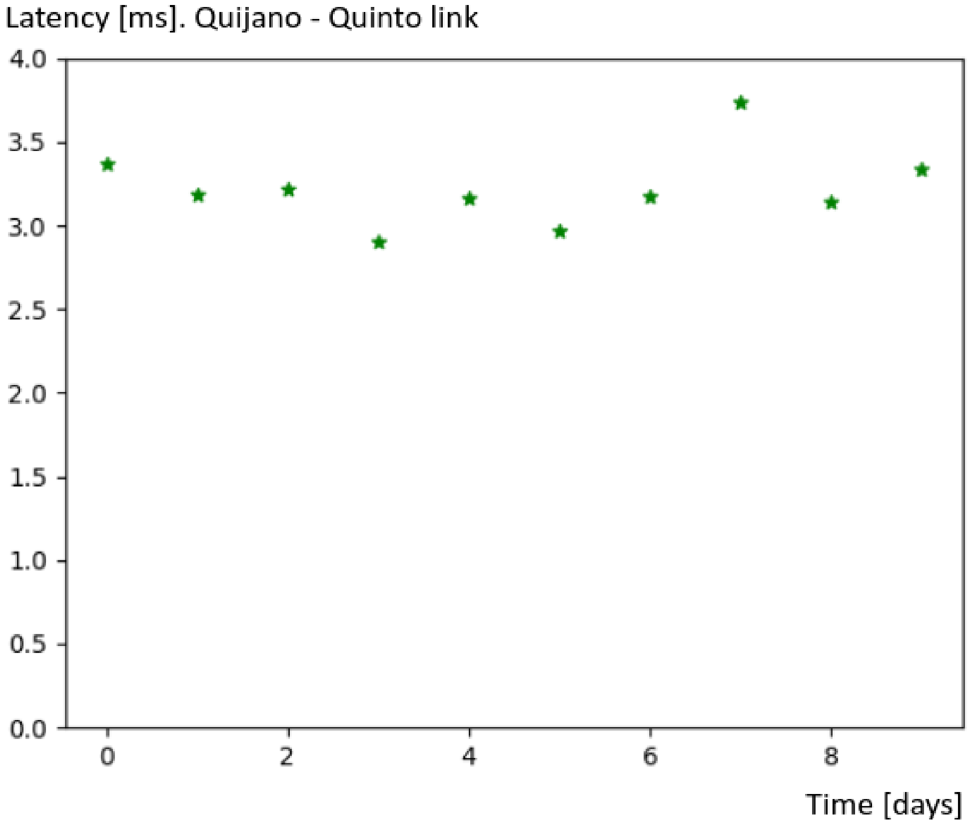
- Number of parallel fibers:2 (non-shared)
- 5 Km, 7 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths

- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link10-11: Free space links:** Up to two free space links are considered, one would be from U. Padova (initial talks with P. Villoresi) and other from Madrid (CSIC, V. Fernández). These links might need some additional funding from the Open Calls.
Planned deployments
This deployment might need to be coordinated with the Open Calls. Two time slots are considered an early one May-Sept 2020 and a later one Sept. 2021-Jan 2022 or even later (May 2022-Aug 2022). 3-4 Link encryptors would be needed. -
Interfaces between layers: - Preferable 004 (because of QoS and expected latencies) 014 if 004 is not implemented.

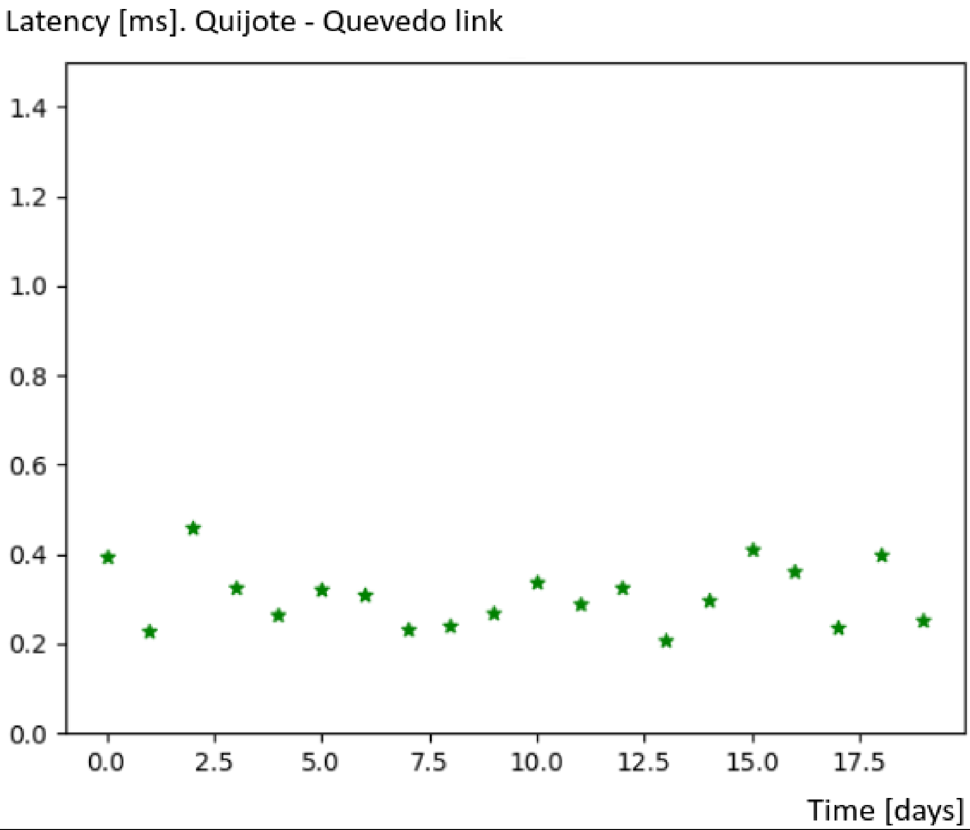
Impact	
Target sector planned impact: - Secure and privacy in e-health. - Secure access to medical data by researchers. **Companies attracted through use case:** - Telefónica de España - HM Hospitals (a network of 17 hospitals, the second largest private group in Spain)	**Achieved KPI demonstrations:** - KPI 30: Latency in serving a request. - KPI 18: Encrypted data throughput. - KPI 56: Scalability of the solution. All the KPIs designed for this UC have been fully achieved.
Time of demonstration	
Deployment: - Initial development and adaptation of the Madrid Network: 14 months. - The deployment is based on IPSec suite, which requires: ○ Around 10 minutes per tunnel link between a pair of trusted nodes. - Note that this deployment assumes that all the SDN stack of the Madrid Quantum Network is fully deployed and operative. - The QKD secure transfer proposed on this UC will protect a set of sensitive medical data.	
Time of demonstration: - The first version of the e-Health UC based on the IPSec suite was developed on 04/2021. However, several improvements have been made since them. - This demonstrator is being run on the Madrid Network since its first development and it is run periodically to measure the network performance, daily or weekly. - This demonstrator can be executed on any set of links of the network with QKD systems available.	

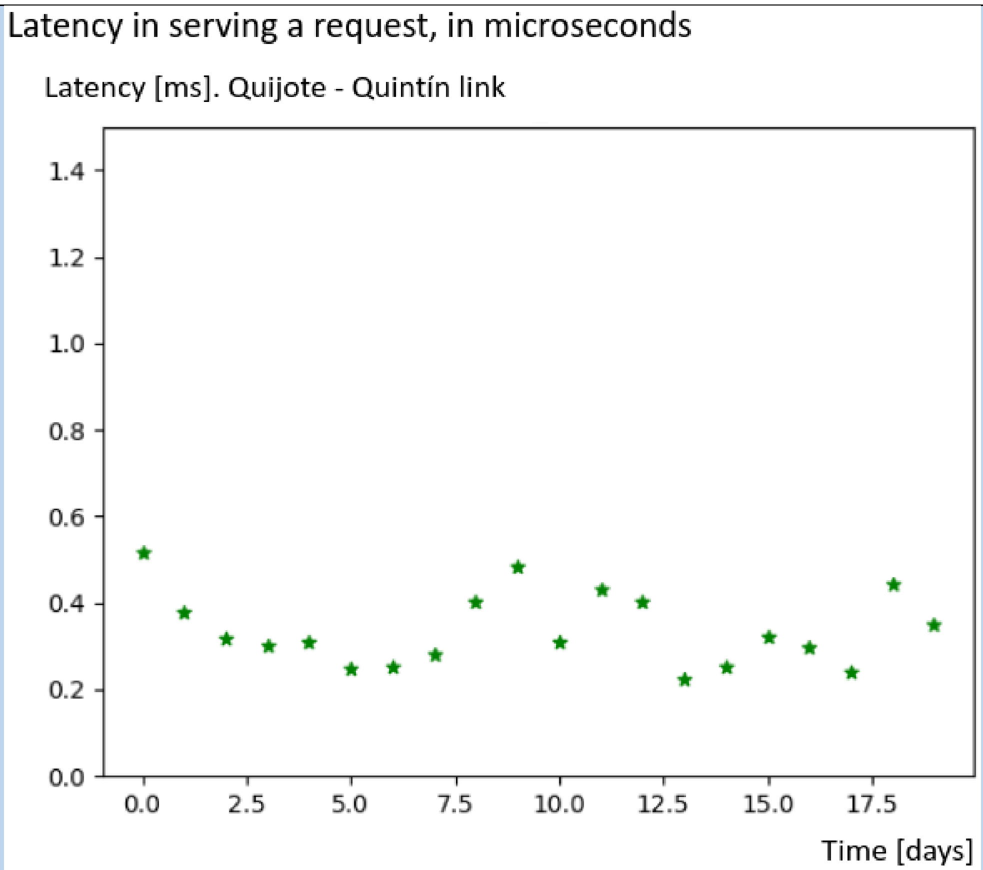
Results
Lessons learned: - QKD services can be used to provide quantum-safe communications for e-Health services. - Using a general-purpose technology, such as the IPSec suite, enables tunnelling techniques that transparently transport any type of IP communication based on QKD ITS security. - Using a software-defined technology, as this specific IPSec suite, enables a seamless integration with the software-defined QKD nodes of the Madrid network. - As the IPSec suite is a software program, it needs enough computational power to perform the encryption of the communications relayed.
Changes necessary to already deployed infrastructure: - The current version of the e-Health services use case runs on top of the Madrid's SDN stack, which delivers QKD services using the ETSI ISG QKD 004 standard access point. - Additional computation power was needed in some IT systems deployed.
Target sector demonstrated impact: - Securing of health institutions' transmissions.
Estimated cost of implementation: - QKD system: 150k€ (2 DVs modules) - Personnel for installation and maintenance: 20k€ - Other equipment used: 10k€ - Desired airport cost for all of this: 10k€ - Software Development: Using as base the Madrid SDN Stack infrastructure, the implementation of the IPsec infrastructure requires 1PM during 14 months approximately. = 70K€ - Total cost: 260k€ UC working on one link.
Further comments: - The following figures show the performance of the solution in terms of latency for serving a request, which is the KPI 30. This use case can be tested on any available link on the network, nevertheless, the Quijano-Quinto link is the unique one that operates over the simulated 5G infrastructure.

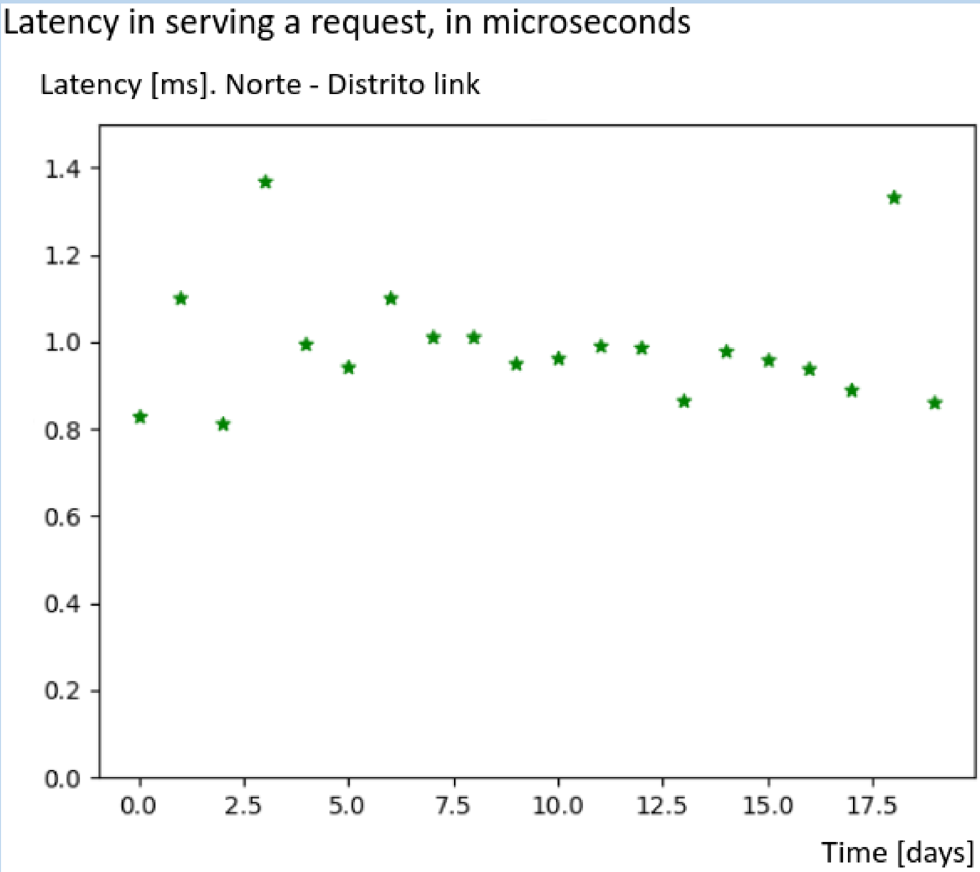
Latency in serving a request, in microseconds



Latency in serving a request, in microseconds

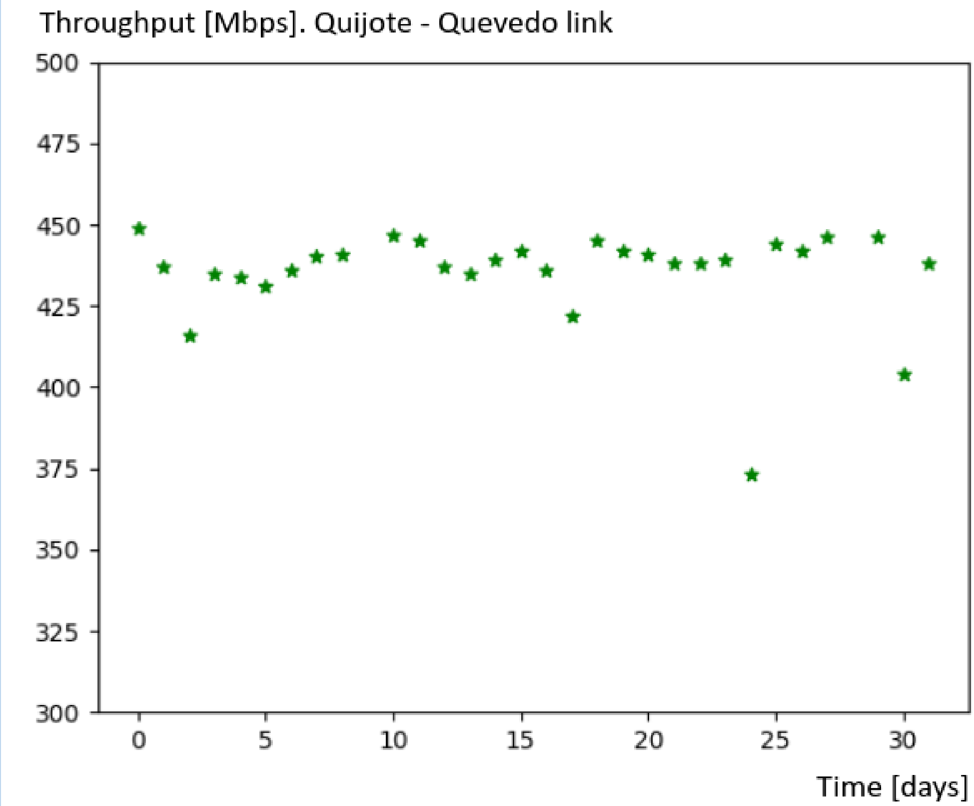



Latency in serving a request, in microseconds
Latency [ms]. Quijote - Quintín link
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0.0
0.0
2.5
5.0
7.5
10.0
12.5
15.0
17.5
Time [days]


Latency in serving a request, in microseconds
Latency [ms]. Norte - Distrito link
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0.0
0.0
2.5
5.0
7.5
10.0
12.5
15.0
17.5
Time [days]

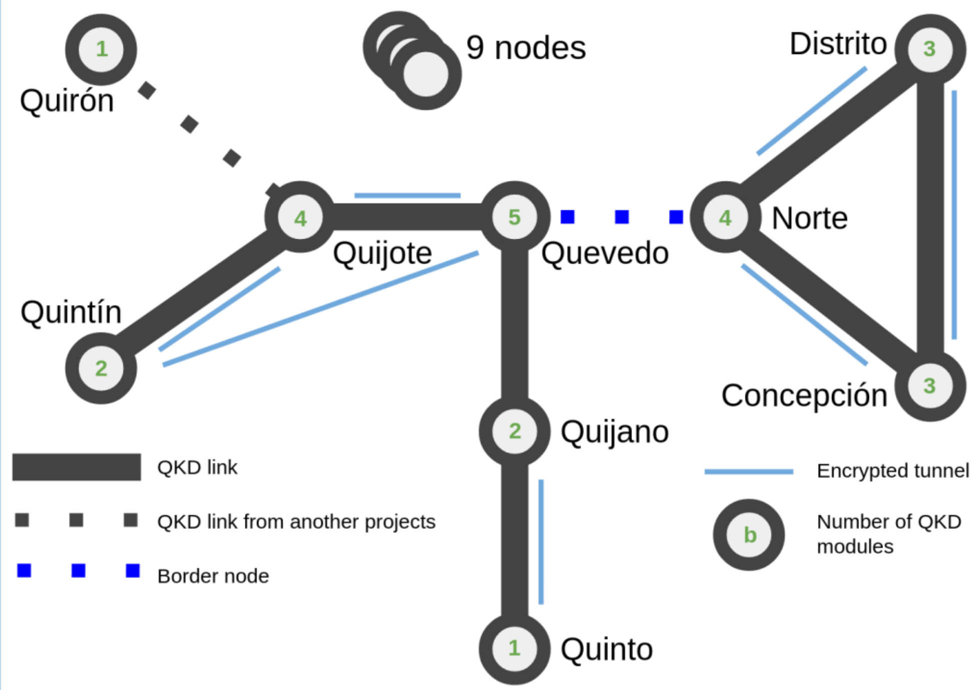
- The following figure shows the KPI 18, which depicts the performance of the network in terms of throughput.

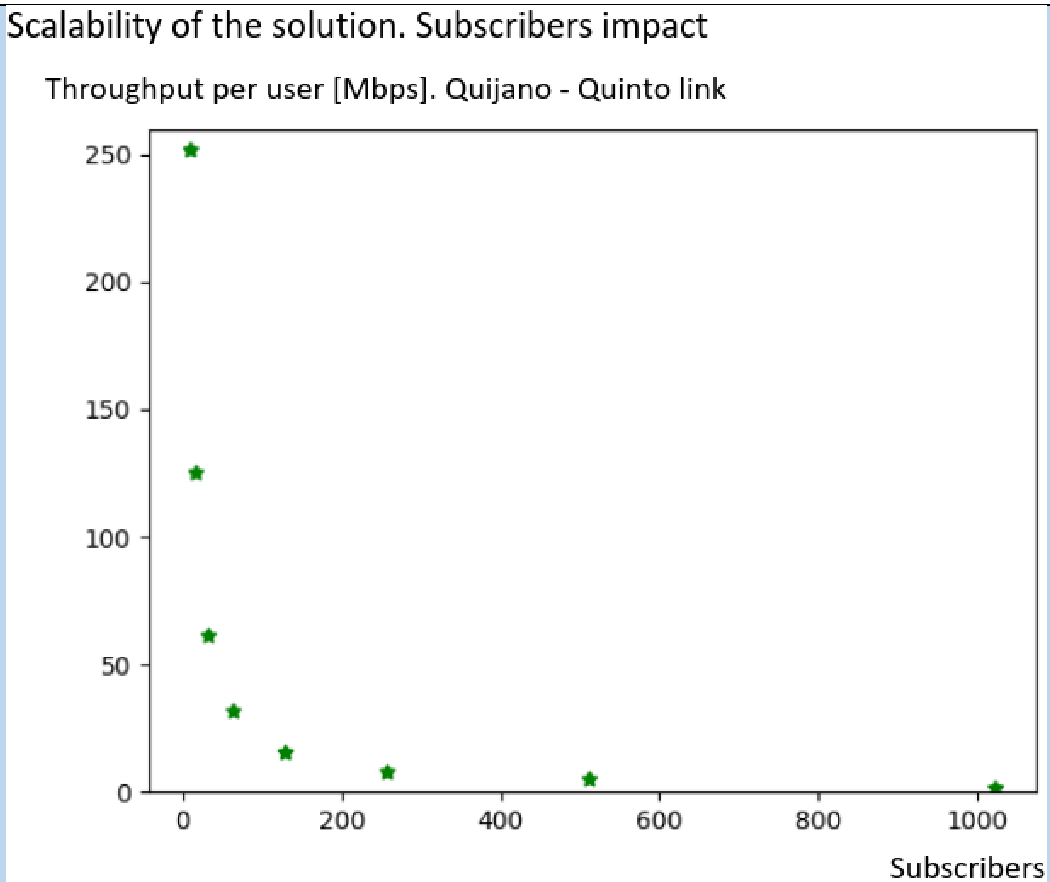
Encrypted data throughput

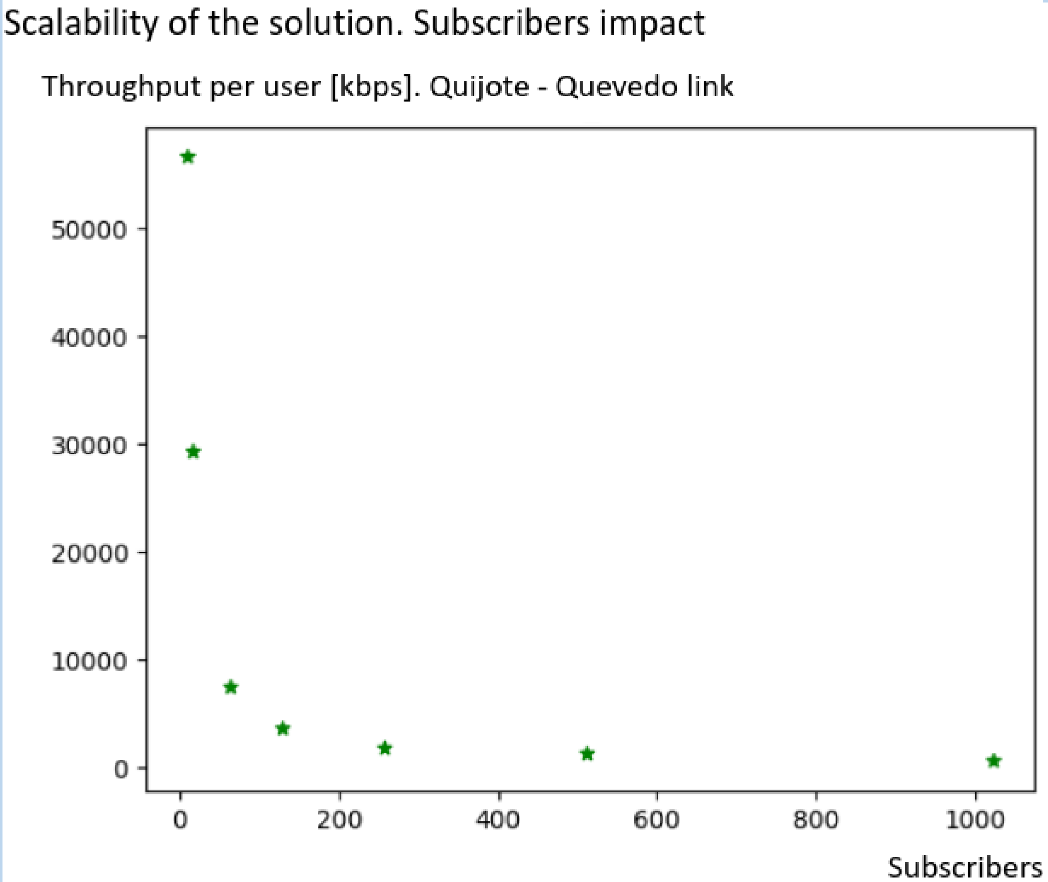


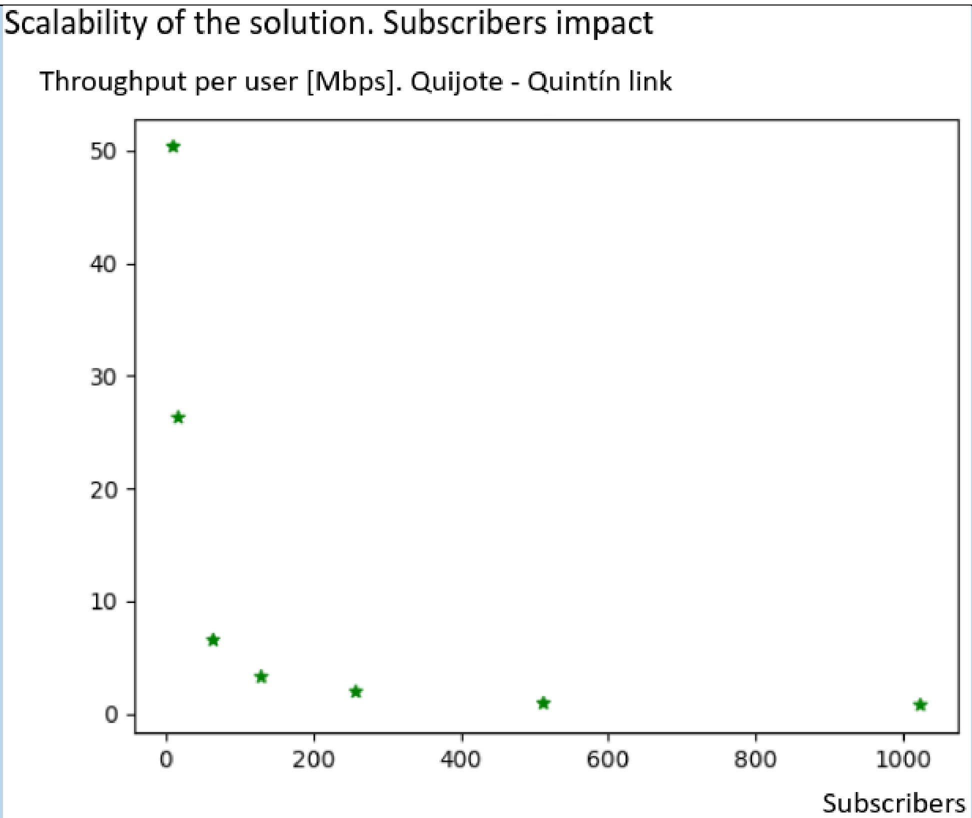
- Finally, the KPI 56, shown in the following figures, measures the scalability of the solution depending on the number of subscribers:

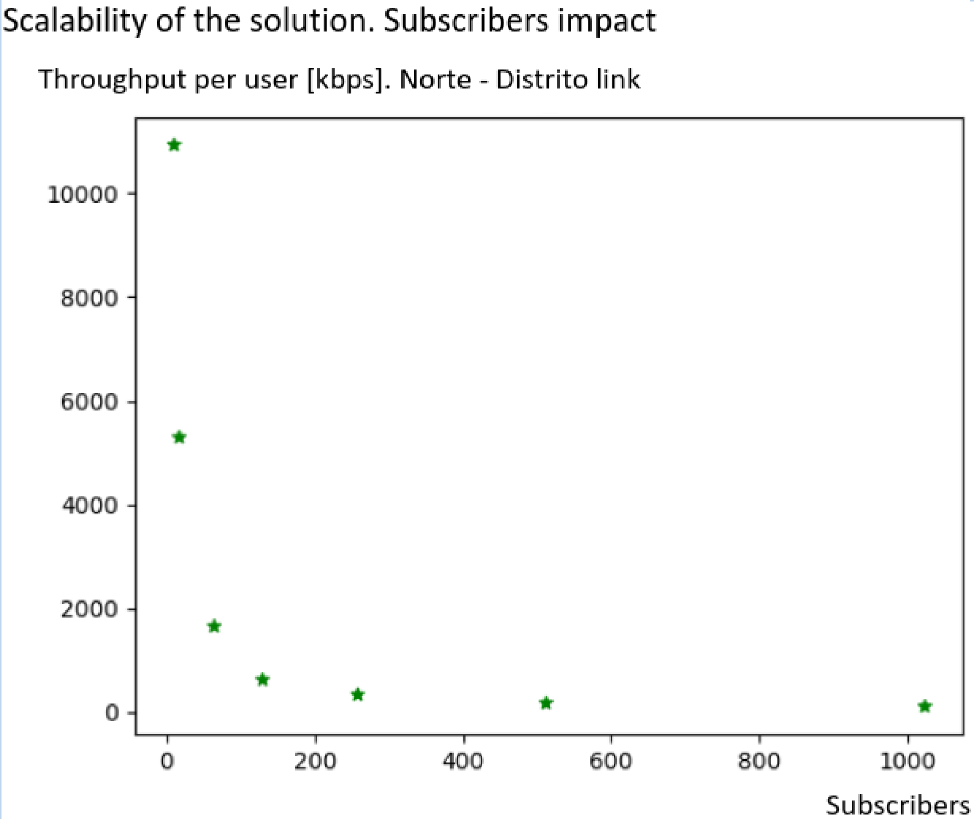
Scalability of the solution




Scalability of the solution. Subscribers impact
Throughput per user [Mbps]. Quijano - Quinto link
250
200
150
100
50
0
0
200
400
600
800
1000
Subscribers

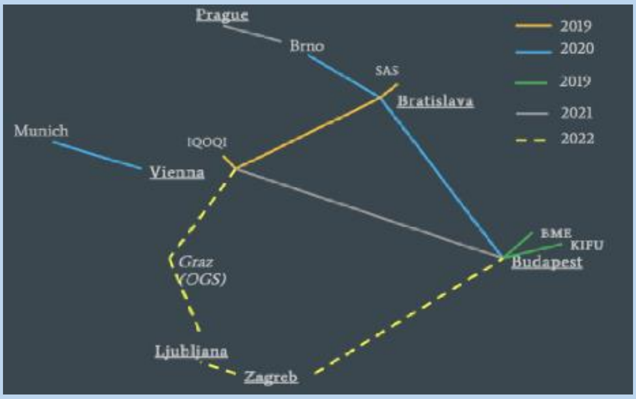

Scalability of the solution. Subscribers impact
Throughput per user [kbps]. Quijote - Quevedo link
50000
40000
30000
20000
10000
0
0
200
400
600
800
1000
Subscribers





- A video of this use case can be found here: https://drive.upm.es/s/fed4HkCf5ePIhpS
- Name of the Video: UC18_Madrid_e-Health.mkv

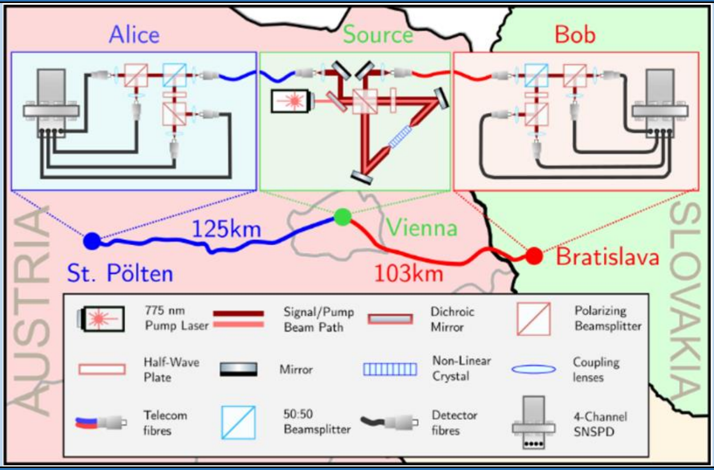
3.9 Use Case 19

<table>
<tr><td colspan="2">ID: 19 Building a European quantum internet</td><td rowspan="4">
</td></tr>
<tr><td colspan="2">Target sector: Research & Education</td></tr>
<tr><td>Country: AT</td><td>Main site: IQOQI Vienna</td></tr>
<tr><td colspan="2">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.</td></tr>
</table>

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

<table>
<tr><th colspan="2">Impact</th></tr>
<tr><td>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.</td><td>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</td></tr>
<tr><th colspan="2">Implementation</th></tr>
<tr><td colspan="2">Work plan/TODO list:
15. Generating a secure key with the use of SNSPDs
16. Optimize key rate by dispersion compensation
17. Implementing automated and efficient real-time data analysis
18. Evaluate findings
19. Implement encryptor and interfaces to the network and the partner from academia</td></tr>
</table>

Block diagram



Site access

- **St. Pölten:** Unrestricted ☐ Restricted ☒
  If restricted how: restricted to trained persons only
- **Vienna:** Unrestricted ☐ Restricted ☒
  If restricted how: restricted to trained persons only
- **Bratislava:** 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?

- **St. Pölten:** AC 230 ☒ DC 48 ☐
- **Vienna:** AC 230 ☒ DC 48 ☐
- **Bratislava:** AC 230 ☒ DC 48 ☐

Internet connection

- **St. Pölten:** Yes ☒ No ☐
- **Vienna:** Yes ☒ No ☐
- **Bratislava:** Yes ☒ No ☐

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
    o For classical communication LTE will be used
    o 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
    o **Dark Fiber**
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)
    o **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

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:

- 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

Estimated cost of implementation:

- Cost of QKD system: 7.000,00€
- Cost of the encryptor: 15.000,00€
- Cost for other equipment: 120.000,00€

<table>
<tr><th colspan="2">Impact</th></tr>
<tr><td>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)</td><td>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</td></tr>
<tr><th colspan="2">Time of demonstration</th></tr>
<tr><td colspan="2">Deployment:
- Start of deployment: June 2019, ready for experiments: July 2021</td></tr>
<tr><td colspan="2">Time of demonstration:
- July 2021 – December 2021, QKD-runs starting in September, 3 successful runs of 3 days, 8 days, 4 days</td></tr>
<tr><th colspan="2">Results</th></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">Estimated cost of implementation:
- Cost of QKD system: 7.000,00€
- Cost of the encryptor: 15.000,00€
- Cost for other equipment: 120.000,00€</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">Further comments:
n.a.</td></tr>
</table>

KPI Groups (Unique and Sorted)	KPI name	
Rates	Key creation rates	1.4 Hz
	Key consumption rates	n.a.
	Key transmission rate	1.0 Hz
	QBER / excess noise	7.0%
Throughput	Data Transactions	n.a.
	Data Throughput	10 Mbit on average for g(2)-correlation
Latency	Quantum network latency	Not measured (research project)
	classical network latency	Not measured (research project)
Compatibility with existing Infrastructure	Modularity	Research project → most of equipment built by hand on optical tables, repeated alignment required Receiver: can be operated in standard 19-inch-rack + helium compressor & hoses Source: optical table, consists of readily bought laser and dispersion compensation, entanglement creation stag self-built
	Equipment Size	Both receiver stations: 19-inch-rack of 160cm height + helium compressor (50x44x43cm HxDxW) and helium hoses Sender station: Optical table incl. source, laser, isolator stage, dispersion compensation + laminar airflow: 200x100x150cm HxDxW
	Deployment (Size & Automation)	Once started, ran for up to 8 days
	Scalability	n.a.
Security & certification	Security & certification	n.a. (research, quantum optics layer)
Resistance to Failure & Link stability	Resistance to Failure	Main problem: overhead; quantum optical equipment (laser, source, detectors) ran stable with no reported failure
	Link stability	8 days max., main problem: stability of internet connection
Use Case or Testbed specific features	Use Case or Testbed specific features	Connection of research facilities Vienna-Bratislava

Non-technical KPIs	number	Examples (references, links)
Number of publications	4	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
Number of public relation communications	3	Via social media. For final (summarizing) publication, press statements and interviews in newspapers are planned, needs to be published first
Number of videos or newsletters	0	
Number of web site visits and visit duration		www.quapital.eu

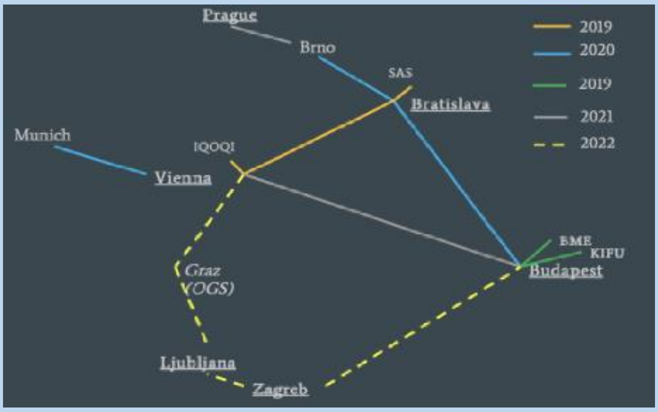
3.10 Use Case 20

ID: 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.

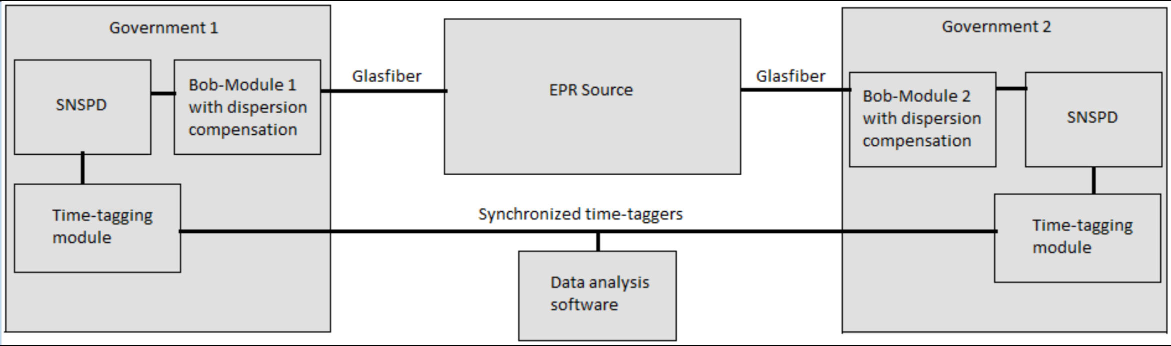
Planned KPI demonstrations:
- Entanglement based 24/7 operation of QKD-secured long-distance links over several months without readjusting the setup
- Low bandwidth polarization compensation
- QKD-secured and stable communication between European embassies and governments

Implementation

Work plan/TODO list:

20. Generating a secure key with the use of SNSPDs
21. Optimize key rate by dispersion compensation
22. Implementing automated and efficient real-time data analysis
23. Evaluate findings
24. Write Report

Block diagram



Site access

- **St. Pölten:** Unrestricted ☐ Restricted ☒
  If restricted how: restricted to trained persons only
- **Vienna:** Unrestricted ☐ Restricted ☒
  If restricted how: restricted to trained persons only
- **Bratislava:** 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?

- **St. Pölten:** AC 230 ☒ DC 48 ☐
- **Vienna:** AC 230 ☒ DC 48 ☐
- **Bratislava:** AC 230 ☒ DC 48 ☐

Internet connection

- **St. Pölten:** Yes ☒ No ☐
- **Vienna:** Yes ☒ No ☐
- **Bratislava:** Yes ☒ No ☐

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

- 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
Estimated cost of implementation: - Cost of QKD system: 7.000,00€ - Cost of the encryptor: 15.000,00€ - Cost for other equipment: 120.000,00€

<table>
<tr><th colspan="2">Impact</th></tr>
<tr><td>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)</td><td>Achieved KPI demonstrations:
- 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</td></tr>
<tr><th colspan="2">Time of demonstration</th></tr>
<tr><td colspan="2">Deployment:
- Start of deployment: June 2019, ready for experiments: July 2021</td></tr>
<tr><td colspan="2">Time of demonstration:
- July 2021 – December 2021, QKD-runs starting in September, 3 successful runs of 3 days, 8 days, 4 days</td></tr>
<tr><th colspan="2">Results</th></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">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
- 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</td></tr>
<tr><td colspan="2">Estimated cost of implementation:
- Cost of QKD system: 7.000,00€
- Cost of the encryptor: 15.000,00€
- Cost for other equipment: 120.000,00€</td></tr>
<tr><td colspan="2"></td></tr>
</table>

KPI Groups (Unique and Sorted)	KPI name	
Rates	Key creation rates	1.4 Hz
	Key consumption rates	n.a.
	Key transmission rate	1.0 Hz
	QBER / excess noise	7.0%
Throughput	Data Transactions	n.a.
	Data Throughput	10 Mbit on average for g(2)-correlation
Latency	Quantum network latency	Not measured (research project)
	classical network latency	Not measured (research project)
Compatibility with existing Infrastructure	Modularity	Research project → most of equipment built by hand on optical tables, repeated alignment required Receiver: can be operated in standard 19-inch-rack + helium compressor & hoses Source: optical table, consists of readily bought laser and dispersion compensation, entanglement creation stag self-built
	Equipment Size	Both receiver stations: 19-inch-rack of 160cm height + helium compressor (50x44x43cm HxDxW) and helium hoses Sender station: Optical table incl. source, laser, isolator stage, dispersion compensation + laminar airflow: 200x100x150cm HxDxW
	Deployment (Size & Automation)	Once started, ran for up to 8 days
	Scalability	n.a.
Security & certification	Security & certification	n.a. (research, quantum optics layer)
Resistance to Failure & Link stability	Resistance to Failure	Main problem: overhead; quantum optical equipment (laser, source, detectors) ran stable with no reported failure
	Link stability	8 days max., main problem: stability of internet connection
Use Case or Testbed specific features	Use Case or Testbed specific features	Connection of European Union members Austria & Slovakia

Non technical KPIs	number	Examples (references, links)
Number of publications	4	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
Number of public relation communications	3	Via social media. For final (summarizing) publication, press statements and interviews in newspapers are planned, needs to be published first
Number of videos or newsletters	0	
Number of web site visits and visit duration		www.quapital.eu

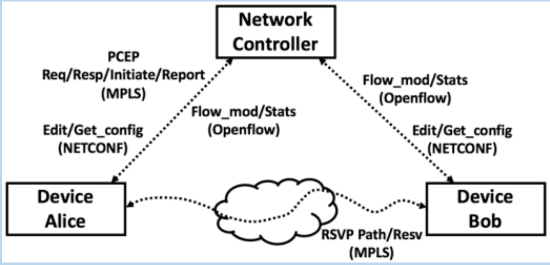
3.11 Use Case 25

ID: 24

Quantum Cryptography for B2B and 5G networks

Target sector: *Commercial and infrastructure*

Country: SP | **Main site: Madrid**



Description from Proposal:
As the network is evolving towards flexible and scalable architectures, it enables for a higher granularity when managing network services. This means that new technologies and services can be seamlessly integrated in the network within very few days, while networks can be sliced and their management left for the end users be changed on demand. One of the most desired and demanded capabilities is to have an enhanced layer for securing the transport segment, traditionally seen as a "black box" from the end user perspective. QKD will play an important role when securing the network, as traditional transport services (e.g. virtual private networks-VPNs, label switched paths-LSPs or tunnels) can additionally integrate QKD for securing end-to-end communications. This will allow services on top of the transport network, such as VPNs for business to business (B2B) or connectivity from base stations to core or data center premises (e.g. for 5G), to incorporate quantum-safe security for end users communications.

Partner	Role/Function
idQ	QKD System provider
TREL	QKD System provider
TID	Testbed and SW provider
UPM	SW provider
RM	Testbed provider
Other	QKD experimental System provider

Impact

Target sector planned impact:
Secure and privacy in e-health

Companies attracted through use case:
- Telefónica de España
- BT
- DT

Planned KPI demonstrations:
- Connection latencies
- Transactions per unit time
- Data throughput

Implementation

Work plan/TODO list:

33. Define parameters for the test.
34. Prepare QKD systems and SW deployment

35. Schedule exact date for deployment with hardware and personnel
36. Perform deployment
37. Adjust deployment
38. Finalize deployment and retrieve devices
39. Evaluate findings
40. Write Report

Block diagram

Site access

Note: Nine possible places can be used for this test, six 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 much more restricted access. Ideally, all the sites (with a topology that imply seven links -three of them in a star with a central node and several hops in one of the branches(UPM-RMCIEMAT, RMCIEMAT-UAM, RMCIEMAT-CSIC, CSIC-IMDEANW, IMDEANW-URJC), three of them in a ring (Telefonica production network, ALMAGRO-NORTE, ALMAGRO-CONCEPCION, CONCEP-CION-NORTE) and another link connecting both (ring and star) could be used.

An initial early deployment (three months) is planned for the first demonstration, which is smaller but important since it will connect with 5G lab from Telefonica which is located at IMDEA Net-works. This link is the most difficult in the Madrid network since it will be shared with several lambdas, does not have a backup line with similar capacity that would allow for a temporary re-routing of the classical traffic while work is done. It also has amplifiers that need to be by-passed. This line will be in trial mode till May 2020 and this will allow us to do many tests, so a first deploy-ment is scheduled for Feb-Apr. 2020 using the CSIC-IMDEANW, IMDEANW-URJC links. A later test, including more nodes is scheduled for Dec. 2021-March 2022, mixing topologies and network pro-viders.

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?

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

Internet connection

- **Site1** Yes ☐ No ☐
- **Site2** Yes ☐ No ☐
- **Site3** Yes ☐ No ☐

Existing equipment

What else is available and can be used?

Site1

-
Site2
-
Site3
-

Encryptors

Manufacturers and Devices

- 2 first phase
- 4 second phase

QKD Systems

Manufacturers and Devices

- 2 first phase
- 6 second phase

Link details

Please fill out the following list for each link (physical connection between two nodes):
(all currently available links are listed, the detailed links/topologies are commented in the "Site Access" section)

Link1: UPM – RMCIEMAT
- Number of parallel fibers:2 (moderately shared, several lambdas, backup line)
- 24 Km, 6 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link2: RMCIEMAT-UAM
- Number of parallel fibers:2 (moderately shared, several lambdas, backup line)
- 24 Km, 8 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

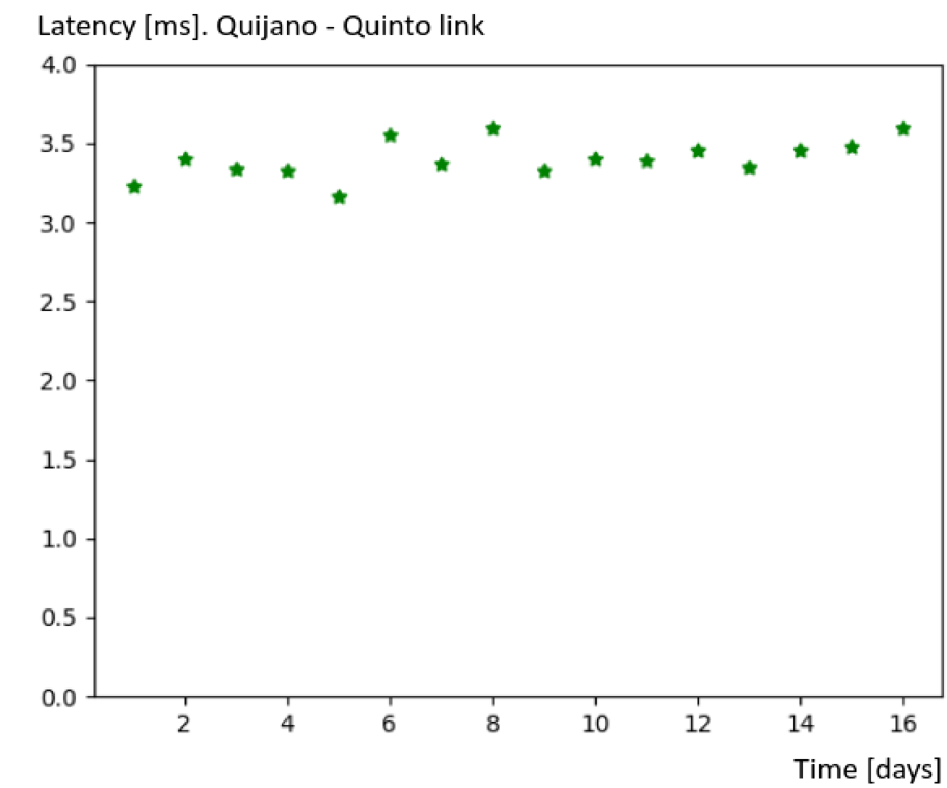
Link3: RMCIEMAT- RMCSIC
- Number of parallel fibers:2 (non-shared)
- 6.5 Km, 3.5 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

Link4: RMCSIC-IMDEA NW (shared, several lambdas)
- Number of parallel fibers:2
- 33 Km, 10 dB losses, SMF
- Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths
- Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed
- Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

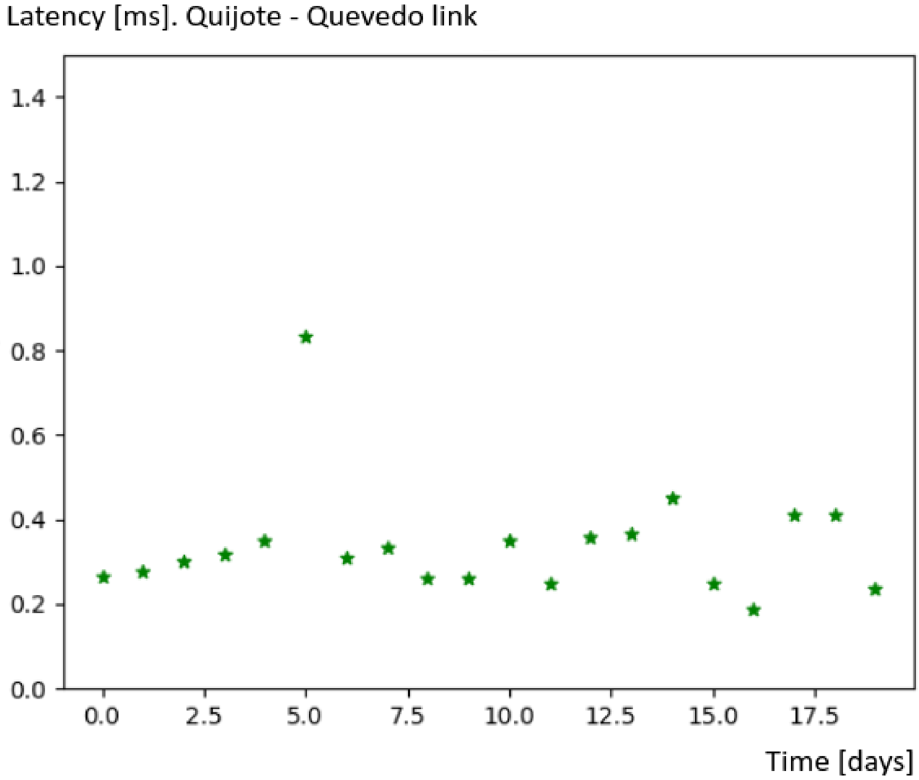
Link5: IMDEANW- URJC - Number of parallel fibers:2 (shared, several lambdas) - 22.5 Km, 6 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link6: URJC-RMCIEMAT** - Number of parallel fibers:2 (shared, several lambdas) - 40 Km, 12 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link7: ALMAGRO-NORTE** - Number of parallel fibers:2 (non-shared) - 3.9 Km, 8.5 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link8: ALMAGRO-CONCEPCION** - Number of parallel fibers:2 (non-shared) - 6.4 Km, 8 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link9: CONCEPCION- NORTE** - Number of parallel fibers:2 (non-shared) - 5 Km, 7 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)
Planned deployments
- First phase: 2 links. Feb 2020 - April 2020 - Second phase: 6 links. Dec. 2021 - March 2022
Interfaces between layers: - Preferable 004 (because of QoS and expected latencies) 014 if 004 is not implemented.

<table>
<tr><th colspan="2">Impact</th></tr>
<tr><td>Target sector planned impact:
- Commercial.
- Infrastructure features as in 5G.
Companies attracted through use case:
- Telefónica de España
- BT
- DT</td><td>Achieved KPI demonstrations:
- KPI 21: Transactions per unit time
- KPI 22: Data throughput
- KPI 31: Connection latencies

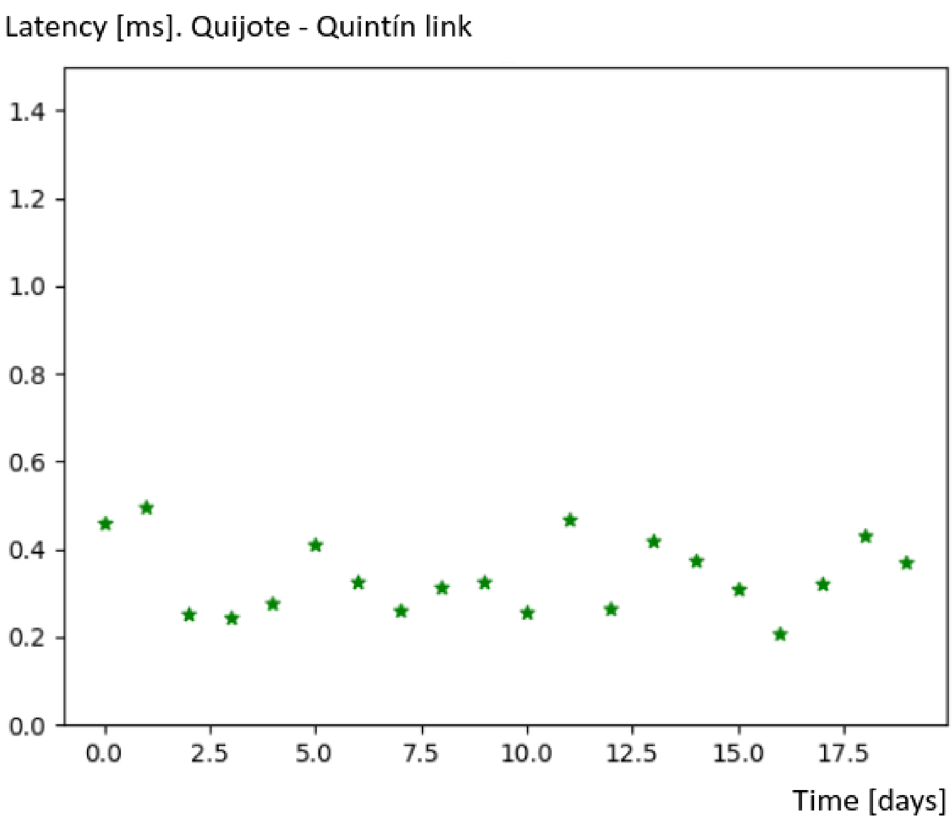
All the KPIs designed for this UC have been fully achieved.</td></tr>
<tr><th colspan="2">Time of demonstration</th></tr>
<tr><td colspan="2">Deployment:
- Initial development and adaptation of the Madrid Network: 14 months.
- The deployment of the infrastructure based on 5G requires:
  o Around 25 days to install and properly configure and launch the 5G network simulator.
- The deployment is based on IPSec suite, which requires:
  o Around 10 minutes per tunnel link between a pair of trusted nodes.
- Note that this deployment assumes that all the SDN stack of the Madrid Quantum Network is fully deployed and operative.
- The QKD devices planned to perform this use case arrived in Madrid a few months ago, so it has only been possible to implement them a few weeks ago.
- The QKD secure transfer proposed on this UC will protect a set of sensitive corporative data.</td></tr>
<tr><td colspan="2">Time of demonstration:
- The first version of the QC for B2B over 5G UC based on the IPSec suite was developed on 04/2021. However, several improvements have been made since them.
- This demonstrator is running on the Madrid Network since its first development and it runs periodically, daily or weekly, to measure the network performance.
- This demonstrator can be executed on any set of links of the network with QKD systems available.</td></tr>
<tr><th colspan="2">Results</th></tr>
<tr><td colspan="2">Lessons learned:
- QKD services can be used to deliver quantum-safe communications to B2B and 5G services.
- Using a general-purpose technology, such as the IPSec suite, enables tunnelling techniques that transparently transport any type of IP communication based on QKD ITS security.
- Using a software-defined technology, as this specific IPSec suite, enables a seamless integration with the software-defined QKD nodes of the Madrid network.
- As the IPSec suite is a software program, it needs of enough computational power to perform the encryption of the communications relayed.</td></tr>
<tr><td colspan="2">Changes necessary to already deployed infrastructure:
- The current version of the B2B and 5G services use case runs on top of the Madrid's SDN stack, which delivers QKD services using the ETSI ISG QKD 004 standard access point.
- The 5G network was simulated using Free5GC.
- Additional computation power was needed in some IT systems deployed.</td></tr>
<tr><td colspan="2">Target sector demonstrated impact:
- Securing of B2B communications through 5G</td></tr>
<tr><td colspan="2">Estimated cost of implementation:
- QKD system: 150k€ (2 DVs modules)</td></tr>
</table>

- Personnel for installation and maintenance: 20k€ - Other equipment used: 10k€ - Desired airport cost for all of this: 10k€ - Software Development: Using as base the Madrid SDN Stack infrastructure, the implementation of the IPSec infrastructure requires 1PM during 14 months approximately. = 70K€ - The 5G simulation = 0K€ - Total cost: 260k€ UC working on one link.
Further comments: - The following figure shows the performance of the solution in terms of latency for serving a request, which is the KPI 31. Note that the Quijano-Quinto link operates over the simulated 5G infrastructure. Latency in serving a request, in microseconds 

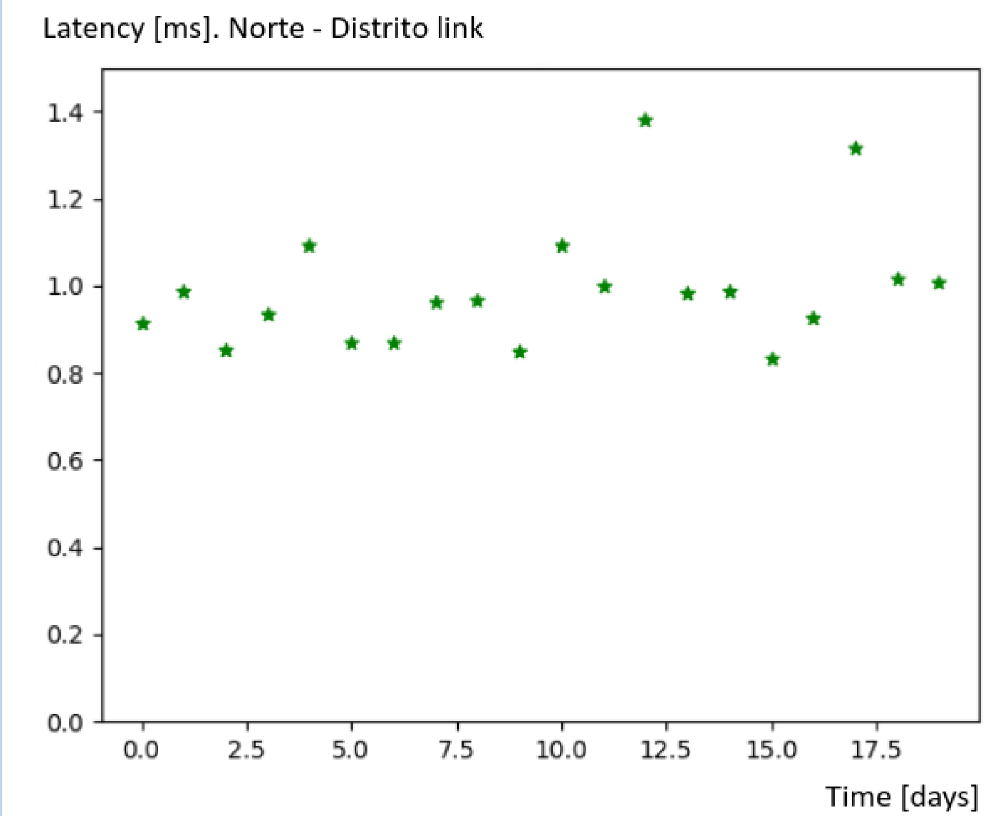
Latency in serving a request, in microseconds



Latency in serving a request, in microseconds

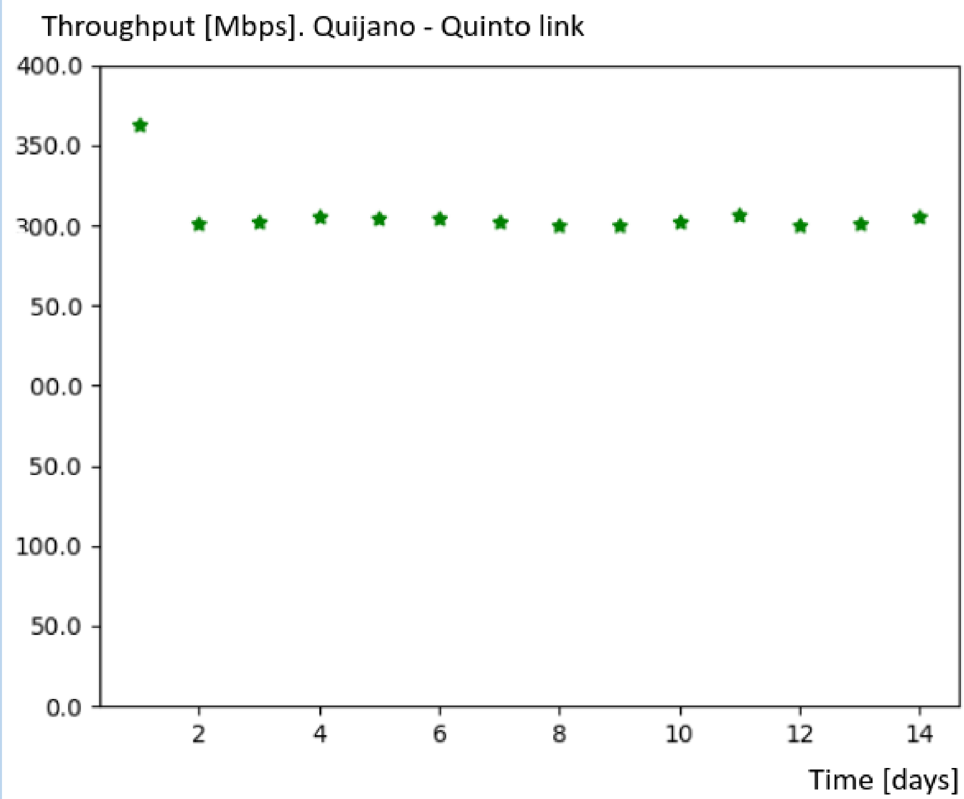


Latency in serving a request, in microseconds

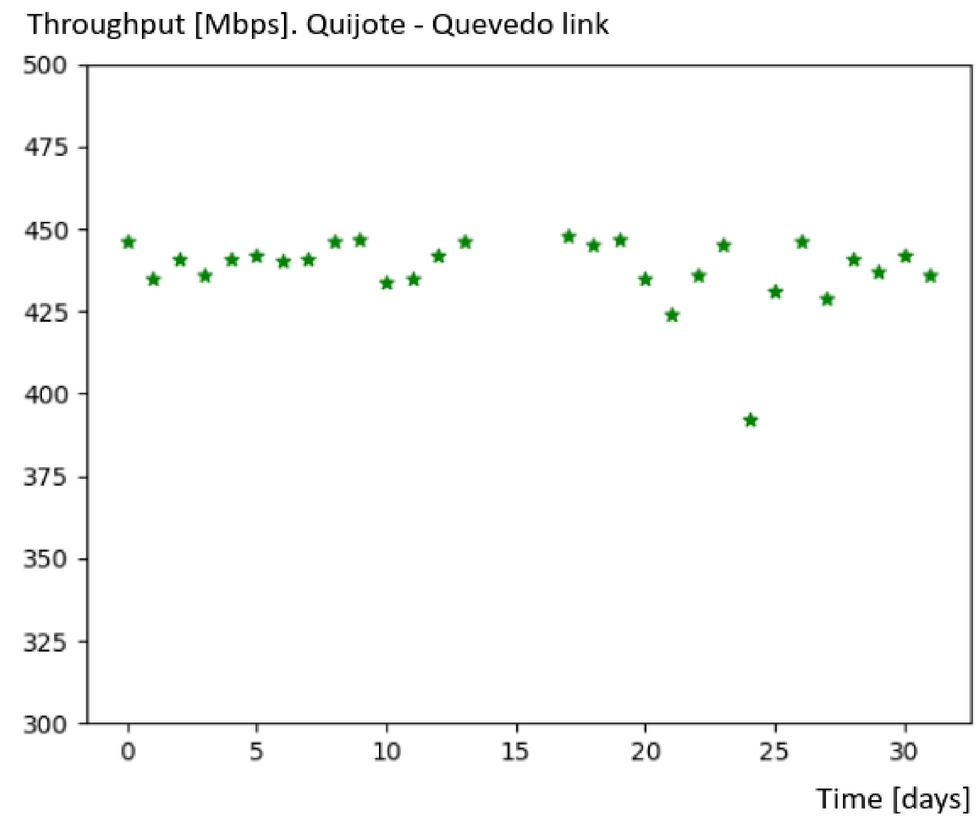


- The following figure shows the KPI 22, which depicts the performance of the solution evaluated in terms of throughput.

Encrypted data throughput

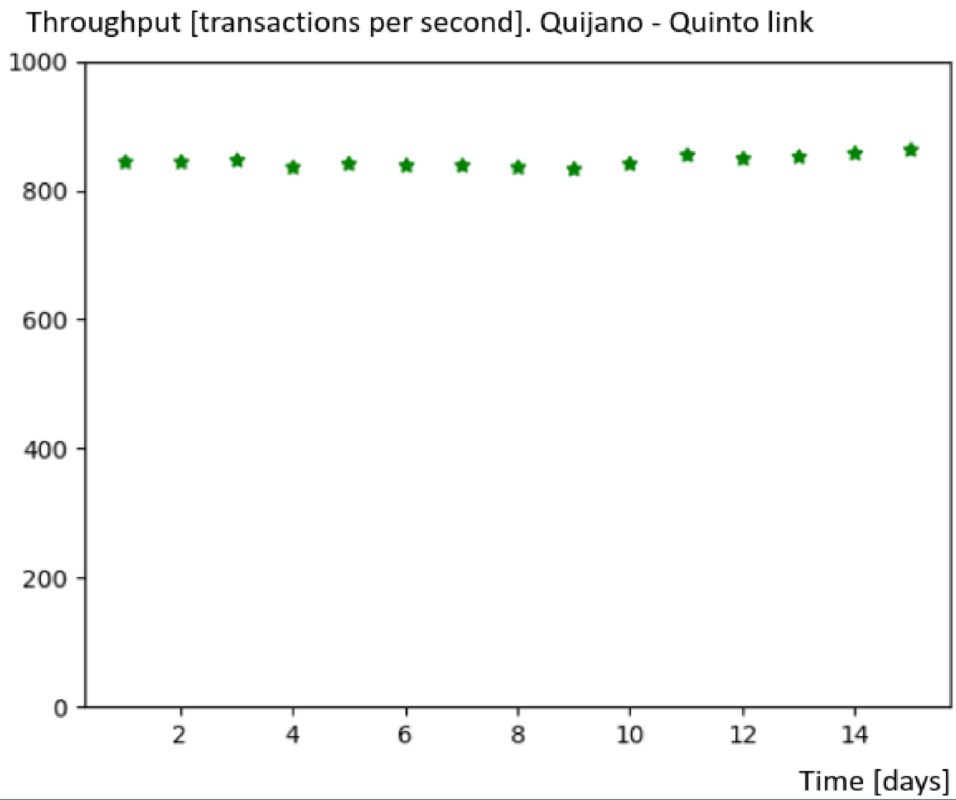


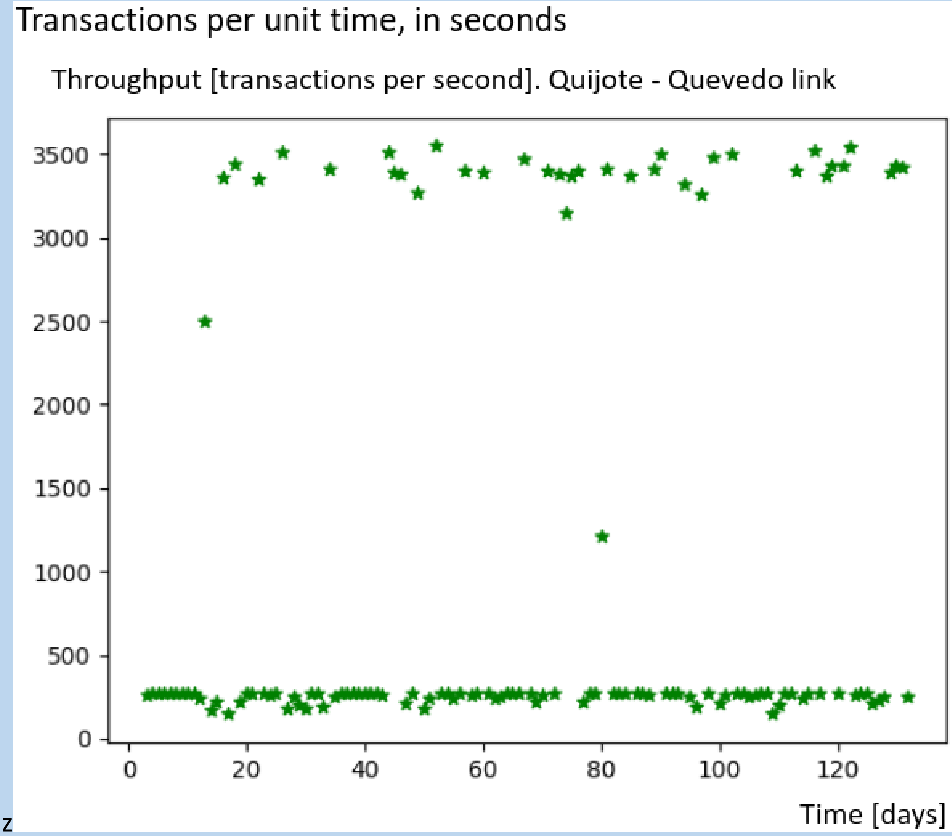
Encrypted data throughput



- Finally, the KPI 21, shown in the following figures, measures the number of transactions per unit time able to handle the use case evaluator:

Transactions per unit time, in seconds





z

- A set of videos of this use case can be found here: https://drive.upm.es/s/fed4HkCf5ePIhpS
- Name of the Videos:
  - UC25_Madrid_ B2B5G.mkv
  - UC25_Madrid_ B2B5G_Core.mkv

3.12 Use Case 26

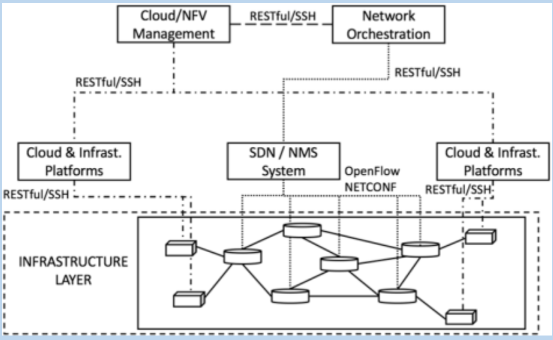
ID: 25

Self-healed network management

Target sector: *Commercial and infrastructure*

Country: SP | **Main site: Madrid**

Description from Proposal:
As the network is evolving towards flexible and scalable architectures, it enables for a higher granularity when managing network services. This means that new technologies and services can be seamlessly integrated in the network within very few days, while networks can be sliced and their management left for the end users be changed on demand. One of the most desired and demanded capabilities is to have an enhanced layer for securing the transport segment, traditionally seen as a "black box" from the end user perspective. QKD will play an important role when securing the network, as traditional transport services (e.g. virtual private networks-VPNs, label switched paths-LSPs or tunnels) can additionally integrate QKD for securing end-to-end communications. This will allow services on top of the transport network, such as VPNs for business to business (B2B) or connectivity from base stations to core or data center premises (e.g. for 5G), to incorporate quantum-safe security for end users communications.



Partner	Role/Function
idQ	QKD System provider
TREL	QKD System provider
TID	Testbed and SW provider
UPM	SW provider
RM	Testbed provider
Other	QKD experimental System provider

Impact

Target sector planned impact:
Secure and privacy in e-health

Companies attracted through use case:
- Telefónica de España
- BT
- DT

Planned KPI demonstrations:
- Latencies for control commands
- Deployment time of SW images.
- Integration capability with 5G

Implementation

Work plan/TODO list:
41. Define parameters for the test.
42. Prepare QKD systems and SW deployment
43. Schedule exact date for deployment with hardware and personnel

44. Perform deployment
45. Adjust deployment
46. Finalize deployment and retrieve devices
47. Evaluate findings
48. Write Report

Block diagram

Site access

Note: Nine possible places can be used for this test, six 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 much more restricted access. Ideally, all the sites (with a topology that imply seven links -three of them in a star with a central node and several hops in one of the branches (UPM-RMCIEMAT, RMCIEMAT-UAM, RMCIEMAT-CSIC, CSIC-IMDEANW, IMDEANW-URJC), three of them in a ring (Telefonica production network, ALMAGRO-NORTE, ALMAGRO-CONCEPCION, CONCEPCION-NORTE) and another link connecting both (ring and star) could be used.

A relatively late deployment is planned (four months, Sept-Dic. 2021) for the demonstration and both network topologies (ring or star) can be used. 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?
- **Site1** AC 230 ☐ DC 48 ☐
- **Site2** AC 230 ☐ DC 48 ☐
- **Site3** AC 230 ☐ DC 48 ☐

Internet connection

- **Site1** Yes ☐ No ☐
- **Site2** Yes ☐ No ☐
- **Site3** Yes ☐ No ☐

Existing equipment

What else is available and can be used?
Site1
-
Site2
-
Site3
-

Encryptors

Manufacturers and Devices
- Encryptors would be welcome, but not strictly necessary since the required encryption can be done in SW.

QKD Systems
Manufacturers and Devices o 6 links
Link details
Please fill out the following list for each link (physical connection between two nodes): (all currently available links are listed, the detailed links/topologies are commented in the "Site Access" section) **Link1: UPM – RMCIEMAT** - Number of parallel fibers:2 (moderately shared, several lambdas, backup line) - 24 Km, 6 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link2: RMCIEMAT-UAM** - Number of parallel fibers:2 (moderately shared, several lambdas, backup line) - 24 Km, 8 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link3: RMCIEMAT- RMCSIC** - Number of parallel fibers:2 (non-shared) - 6.5 Km, 3.5 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link4: RMCSIC-IMDEA NW** (shared, several lambdas) - Number of parallel fibers:2 - 33 Km, 10 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link5: IMDEANW- URJC** - Number of parallel fibers:2 (shared, several lambdas) - 22.5 Km, 6 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)

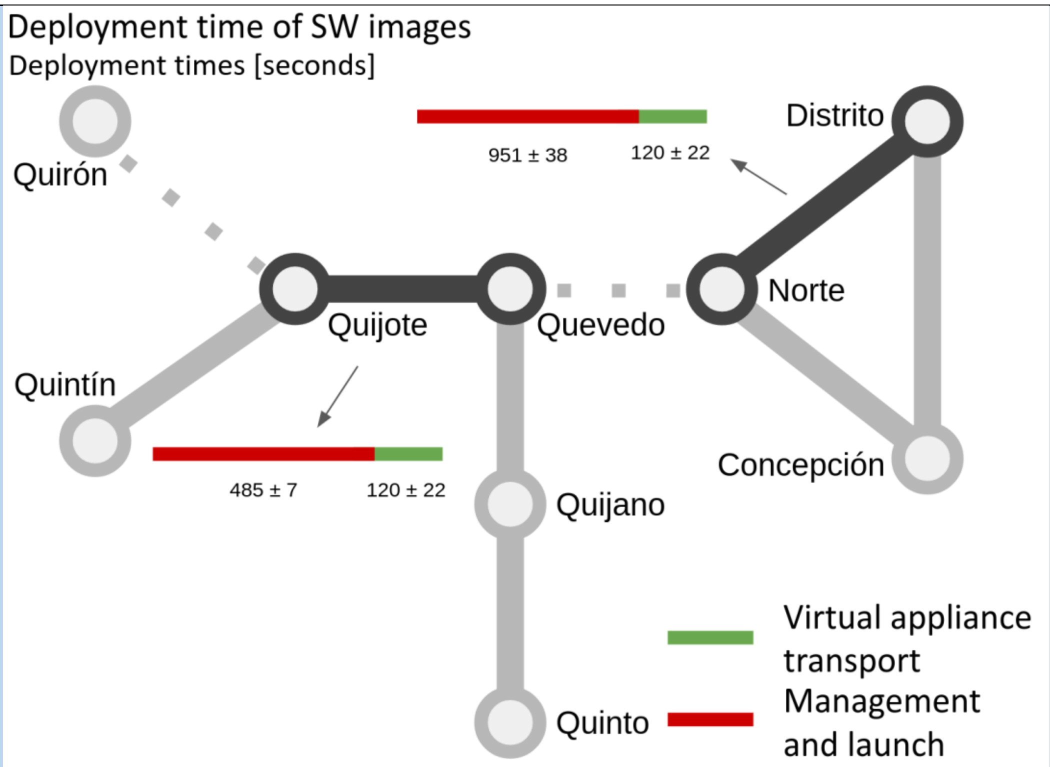
Link6: URJC-RMCIEMAT - Number of parallel fibers:2 (shared, several lambdas) - 40 Km, 12 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link7: ALMAGRO-NORTE** - Number of parallel fibers:2 (non-shared) - 3.9 Km, 8.5 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link8: ALMAGRO-CONCEPCION** - Number of parallel fibers:2 (non-shared) - 6.4 Km, 8 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range) **Link9: CONCEPCION- NORTE** - Number of parallel fibers:2 (non-shared) - 5 Km, 7 dB losses, SMF - Telecom connection: Client data rates (1/10/100GB) and format (Ethernet, OTN, Fiber Channel) and occupied wavelengths - Quantum link: Fiber for QKD system (dark/shared); if shared -> wavelength and launch power of telecom channel needed - Other wavelength restrictions of QKD and auxiliary channel (none / wavelength range)
Planned deployments
- 6 links September 2021 - Dec 2021
Interfaces between layers: - Preferable 004 (because of QoS and expected latencies) 014 if 004 is not implemented.

Impact	
Target sector planned impact: - Network operators' management systems. - Digital services providers' management systems. **Companies attracted through use case:** - Telefónica de España - BT - DT	**Achieved KPI demonstrations:** - KPI 15: Deployment time of SW images (fully achieved). - KPI 32: Latencies for control commands (ongoing)

Time of demonstration

Deployment:
- Initial development and adaptation of the Madrid Network: 10 months.
- The deployment is based on a NFV management technology, OpenStack, and a secure transportation tool developed by Madrid team, DAAP. To deploy the use case is required:
    o Around 3 days to install and configure OpenStack in the trusted node. This step is required only once.
    o Around 5 and 10 minutes to deploy Trusted Node images to manage the QKD infrastructure. This time depends on the size of the image. Currently is around 9GB.
- Note that this deployment assumes that all the SDN stack of the Madrid Quantum Network is fully deployed and operative.

Time of demonstration: - The first version of the self-healed network management based on OpenStack was developed on 9/2021. However, several improvements have been made since them. - The first version of the self-healed network management based on DAAP was developed on 11/2021. - This demonstrator can be executed on the nodes running the mentioned technology, namely Quijote and Norte.
Results
Lessons learned: - QKD services can enhance the network management by feeding self-healed solutions. - As OpenStack and DAAP are software programs, they need enough computational power to perform the encryption of the communications relayed.
Changes necessary to already deployed infrastructure: - The current version of the QKD as a cloud service use case runs on top of the Madrid's SDN stack, which delivers QKD services using the ETSI ISG QKD 004 standard access point. - Additional computation power was needed in some IT systems deployed.
Target sector demonstrated impact: - Securing the communications of the network management in NFV operations.
Estimated cost of implementation: - QKD system: 150k€ (2 DVs modules) - Personnel for installation and maintenance: 20k€ - Other equipment used: 10k€ - Desired airport cost for all of this: 10k€ - Software Development: Using as base the Madrid SDN Stack infrastructure, the implementation of the IPSec infrastructure requires 1PM during 10 months approximately. = 50K€ - The 5G software simulator = 0K€ - Total cost: 240k€ UC working on one link.
Further comments: - The following figure show the deployment time of software images for NFV in two different scenarios in the network, known as KPI 15.



- A set of videos of the use case can be seen here: https://drive.upm.es/s/fed4HkCf5ePIhpS
- Name of the Videos:
  - UC26_Madrid_Self-healedNetworkManagement_Part1.mkv
  - UC26_Madrid_Self-healedNetworkManagement_Part2.mkv

3.13 Use Case 33

ID: 33

Quantum Cryptography with minimal amount of QKD devices allowing independent protection of users in collocated computing centers

Target sector: *Commercial and infrastructure*

Country: SP | **Main site: Madrid**

Description from Proposal:

This use case aims at demonstrating the feasibility of interconnecting independent users, operating at collocated computing centers, who utilize independent QKD devices. Simultaneously the number of devices and quantum+ classical channels should not increase as $N*(N-1)*M$ (devices) and $N+N*(N-1)/2 = M*N*(N+1)/2$ (quantum + classical channels) but much more moderately, the optimum being: $M*N$ devices and just N links. The economic approach is feasible by directional and possibly wavelength switching of quantum channels that are multiplexed with the classical ones in order to allow sharing of communication media. The discussed reduction would allow practically feasible utilization of the technology for such realistic user requirements (security independent utilization of public infrastructures).

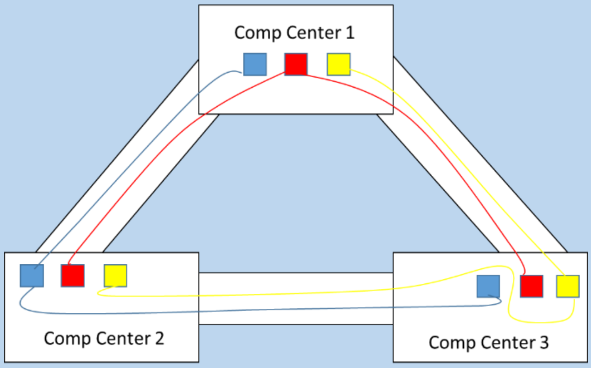
In practice this would require flexible technology, allowing rapid realignment adaptation, with respect to directional and wavelength switching. Additionally, an SDN class (QKD) network architecture would be essential to realize an implementation of this type.

In the implementation illustration, presented below we depict a network connecting four collocated centers, whereby it is assumed that the network provider allocates 4 communication channels for 4 computing centers, each of the latter hosting 2 or 3 independent users, and that the network provider has reserved 2 wavelengths for QKD purposes in one of the communication channels and one wavelength in each of the other.

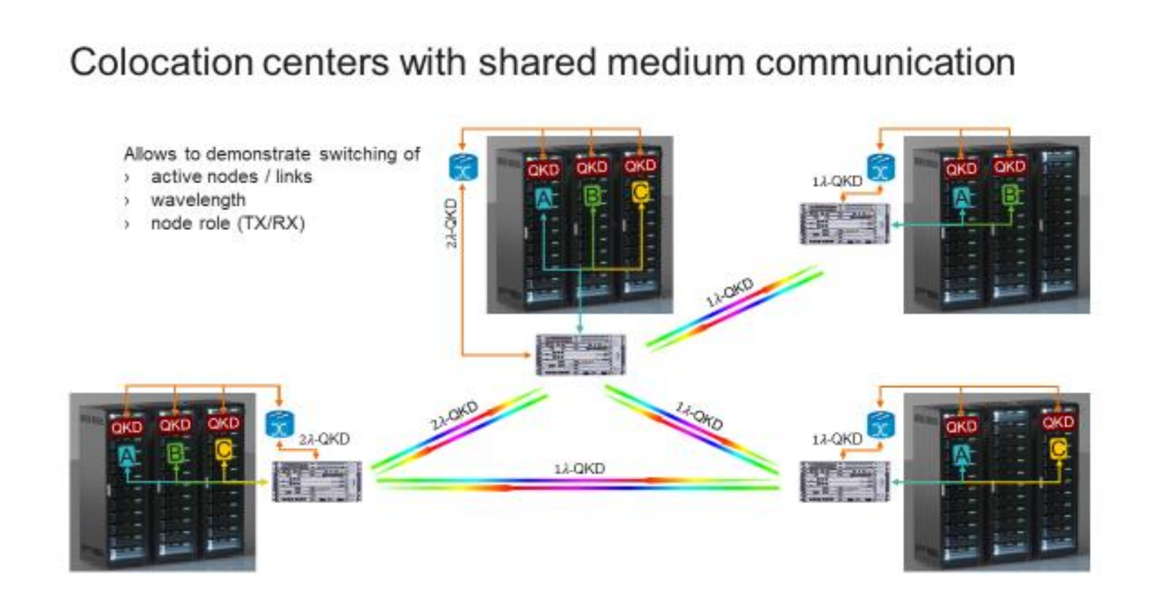
SDN control operation is then responsible for switching while rapid realignment will be guaranteed by the quick adaptivity of QKD devices.

This use case supports Use Case 17 – QKD as a

Abstract scheme



cloud service and Use Case 25 – Quantum Cryptography for B2B networks (5G is not relevant here). HWDU plans to install 10 QKD devices in 7 locations to this end.	
Partner	**Role/Function**
TID	Testbed and SW provider
RM	Testbed provider
UPM	SW provider
HWDU	QKD System provider
Other	
Impact	
Target sector planned impact: Security and privacy in distributed computing centers **Companies attracted through use case:** - Telefónica - BT - DT	**Planned KPI demonstrations:** - Connection latencies - Key rates - Data throughput
Implementation	
Work plan/TODO list: 49. Select locations for the test and verify feasibility based on network parameters (local tests if necessary) 50. Prepare QKD systems and interfaces (fall of 2020) 51. Organize necessary OTN equipment wherever necessary (free of charge) 52. Schedule delivery and deployment with all involved partners 53. Deploy and carry out an initial test phase 54. Full scale operation, data collection 55. Analysis of results and publication	
Block diagram	
Illustration of a feasible imlementation	



A provider offers the possibility to rent server racks distributed over multiple data centers. This allows clients to run their services and storage in a geolocation-redundant fashion, which is safe against most failures, even most natural disasters. For economic reasons, shared building/cooling/maintenance, the data-center service is provided to multiple clients in the same data center, a colocation center.

The colocation-center provider adds the feature of QKD-secured connections between the data centers, e.g., for data synchronization and backups. This gives maximum control to the customer, the key generation and distribution is carried out in the domain of the customer. The QKD devices/links/networks for each customer might be by different QKD providers, respectively.

Only a limited amount of fiber connections is available between the data centers and multiple customers have to share the same fiber for individual data traffic and QKD, respectively. The requirements for key generation are assumed to be moderate, different QKD links should be operate in a time and/or wavelength multiplexed fashion to limit the required channel count for the QKD links.

The network of the data centers might be a star or ring topology, the channel allocation for the QKD links should be centrally controlled by SDN. An example: Customer A might have rented racks in four different locations as shown in the picture, customer B and C only have rented 3 racks, respectively. Three data centers are connected in a ring, while one of the data centers is only attached to one of the ring nodes. For most of the connections only one wavelength (e.g. ITU34) is available, for one of the connection two wavelengths (e.g. ITU33 & ITU34) are available. All customers want to generate keys between all their racks, respectively. So not all QKD connections can be active at the same time. To avoid exclusive QKD network utilization, the QKD devices will operate on different wavelengths depending on their peer. So if C and A want to perform QKD on the bottom link, they need to time multiplex on ITU34. When they both want to perform QKD on the left link, A could switch to ITU33 and C could stay on ITU34.

Multiple requirements for the QKD devices can be derived:

* The QKD devices need to be able to be operate on the same fiber as QKD devices from other providers, time or wavelength multiplexed.
* The QKD channel allocation should be implemented dynamically with SDN, which controls the time and wavelength multiplexing.
* The QKD devices need to support the channel and link switching driven by SDN.
* The inclusion of the QKD devices in the racks need to be tamper proof.

This defines a very modular and flexible SDN based QKD scenario with the need of path and wavelength switching.

Site access
Note: With previous tests in Telefonica production environment HWDU devices are ready for a very broad variety site access conditions
Available power
From Previous experience with the Telefonica production environment, necessary power is available.
Internet connection
We need at least one internet connection. One was (is) available at the Almagro site of Telefonica.
Existing equipment
We shall bring necessary telecommunication equipment if such is not provided by the network itself
Encryptors
Manufacturers and Devices To be provided as necessary by the network. Huawei encryptors will not be used.
QKD Systems
Manufacturers and Devices o 5 CV QKD Links – all switchable (directional, wavelength), and controllable by Madrid SDN controllers. The devices (depending on distance and attenuation) can c-propagate with up to 20 downstream 1dBm channels

Impact	
Target sector planned impact: - Commercial - Infrastructure features **Companies attracted through use case:** -	**Achieved KPI demonstrations:** - 36 different loop-free links could be realized with only 5 transmitters and 5 receivers. - Four different QKD links are connected simultaneously over the same fiber pair to demonstrate shared-medium QKD.
Time of demonstration	
Deployment: - Initial coordination and adaptation of the Madrid Network: 14 months. - The deployment is based on the management of different QKD links connected simultaneously over the same fiber to demonstrate shared-medium QKD ○ Around 40 seconds to configure each new Quantum link. - Note that this deployment is managed by the SDN stack of the Madrid Quantum Network, that has been improved to be operative with these new features. - The optical switching is done through the Madrid SDN Stack. - The deployment of the SDN stack takes into account this new QKD switching feature.	
Time of demonstration: - The first version of the QKD optical switching was ready on 10/2021 and continuous improvements are being made.	

- This demonstrator can be executed on all the nodes running the QKD switching technology (see further comments).

Results

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.

Changes necessary to already deployed infrastructure:

- The QKD hardware has been improved to offer this new feature, making the devices wavelength tuneable and exposing this feature through a simple interface to be managed through the SDN Stack.
- The control of the Optical Switching is done through the use of QuAM/QuAI interfaces. These interfaces need to be upgraded on the Madrid Quantum Network Stack

Target sector demonstrated impact:

- Security and privacy in distributed computing centres.

Estimated cost of implementation:

- QKD systems: 120k€ (3 CV modules)
- Personnel for installation and maintenance: 20k€
- Other equipment used: 10k€
- Desired airport cost for all of this: 10k€
- Software Development: Using as base the Madrid SDN Stack infrastructure, the implementation of this infrastructure requires 1PM during 10 months approximately. = 50K€
- Total cost: 200k€ UC working on two links.

Further comments:

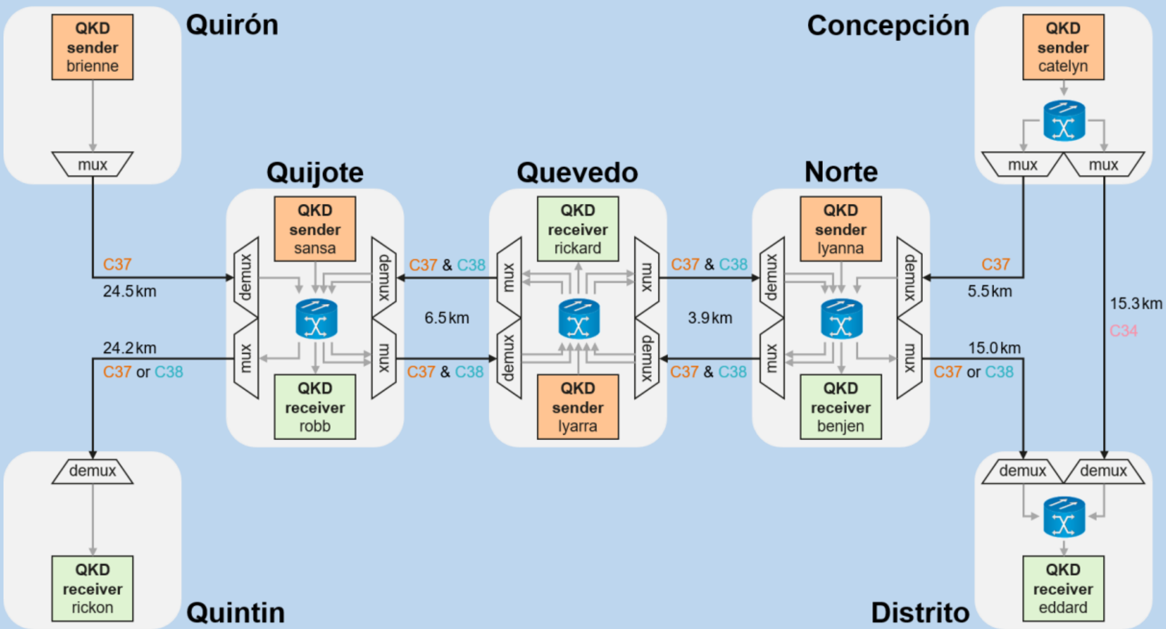


Figure 1: Abstract hardware installation overview. Five HWDU QKD sender and five HWDU QKD receiver have been deployed in seven different locations. Through light-path switches (blue

cylinders) any sender can reach any receiver, although the total link loss is too high for the most distant links. The light-path switches have been combined with optical multiplexers and demultiplexers to allow different wavelengths to be used for QKD. The multiplexing hardware is also used for copropagating classical channels and/or QKD signals of IDQ or Toshiba devices. The HWDU QKD sender and receiver can be tuned to any wavelength in the C-band. The multiplexing setup limits the wavelengths as indicated in the figure to channel C37 (193.7 THz / 1548 nm) in most connections. Many connections also support C38 (193.8 THz / 1547 nm), one connection only supports C34 (193.4 THz / 1550 nm). The distances between the different locations are given as reported by OTDR measurements.

Figure 1 gives a rough overview of the QKD device, switching, and multiplexing hardware installation for this demonstration. Figures 2 – 6 show possible scenarios with different light-path switch and wavelength settings. All links in the same scenario are active at the same time. The different settings can be configured in a time division multiplexed manner according to quality of service requirements.

In each Figure and the table below the figures, the link losses and key rates are measured by the QKD devices and are depicted for each link, respectively. Since links can go through multiple switching and multiplexing stages, the link loss of a multi-hop link is not necessarily equal to the sum of the link losses of the single hop links.

The HWDU QKD devices support link losses between 0 and 23dB. The C38 link between Norte and Quintin as shown in Figure 5 scratches with 22.8dB at the maximum supported reach.

The HWDU QKD devices allow customers to configure trusted loss for a trusted transmit perimeter. All presented links in Figures 2-6 utilize this feature and the loss introduced by the first switching and multiplexing stage is trusted for each link, respectively. E.g. the trusted loss in the Norte – Quintin link is 1.4dB (switch + mux as shown in Figure 1). The total loss in the Norte – Quintin link including the trusted transmit loss is 24.2dB. The HWDU devices support a total link loss of up to 28dB, with at least 5dB of this loss configured as trusted transmit loss. The configured trusted losses can be found in the table below the figures.

The given key rates are only preliminary indications. No long-term measurements have been performed so far, finite-size effects are therefore not considered. This will be addressed in the following period. The key rate depends on many factors, not only on the loss. E.g. the Raman noise on each link, respectively. System instabilities also reduce the key rate at the moment, which will be addressed in the following period. Because of the different influences, key rates for links with higher loss can be higher as for links with lower loss.

The scenarios in Figures 5 and 6 utilize the multi-wavelength capabilities. Respectively, four different QKD links are connected simultaneously over the same fiber pair Norte-Quevedo in Figure 5 and Quevedo-Quijote in Figure 6 to demonstrate shared-medium QKD.

Many switching and wavelength configurations beyond the shown scenarios are possible depending on the requirements. The extensive switching capabilities and flexibility demonstrate the reduction of QKD device hardware. 36 different, loop-free links can be realized with only five transmitters and five receivers.

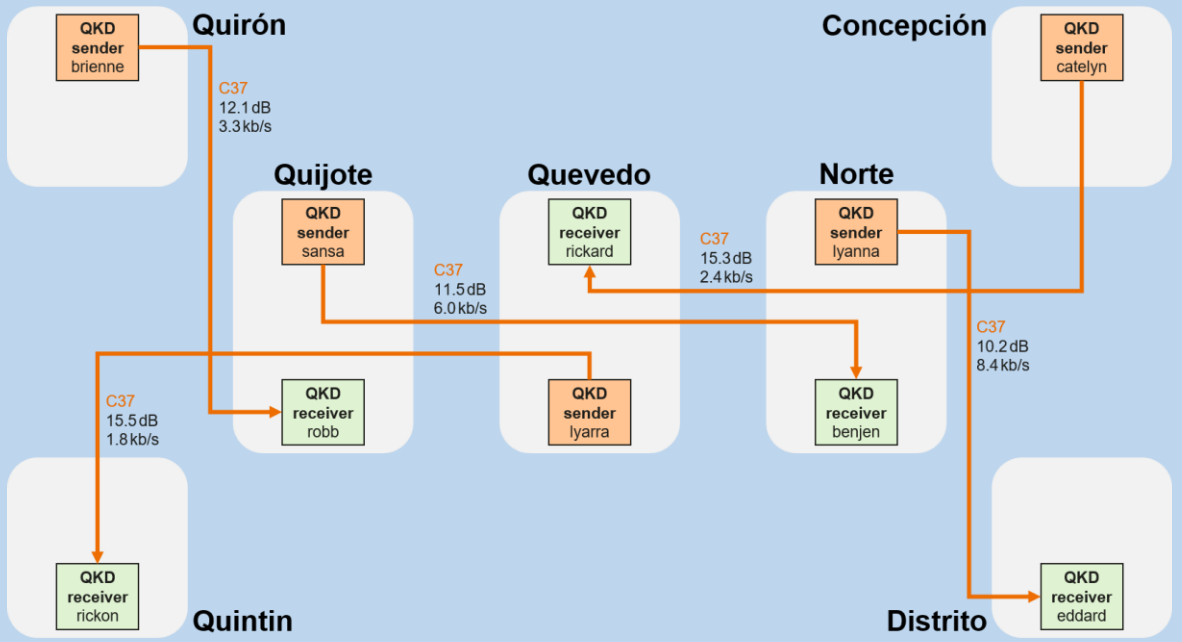


Figure 2: Scenario 1 with simultaneous connections on C37.

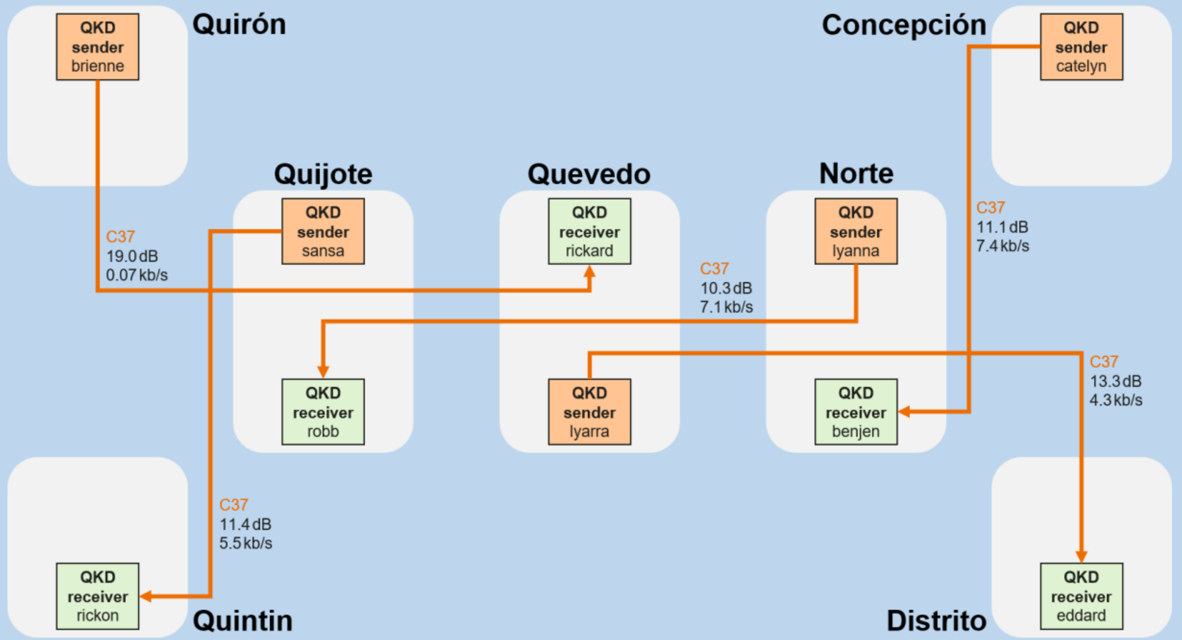


Figure 3: Scenario 2 with simultaneous connections on C37.

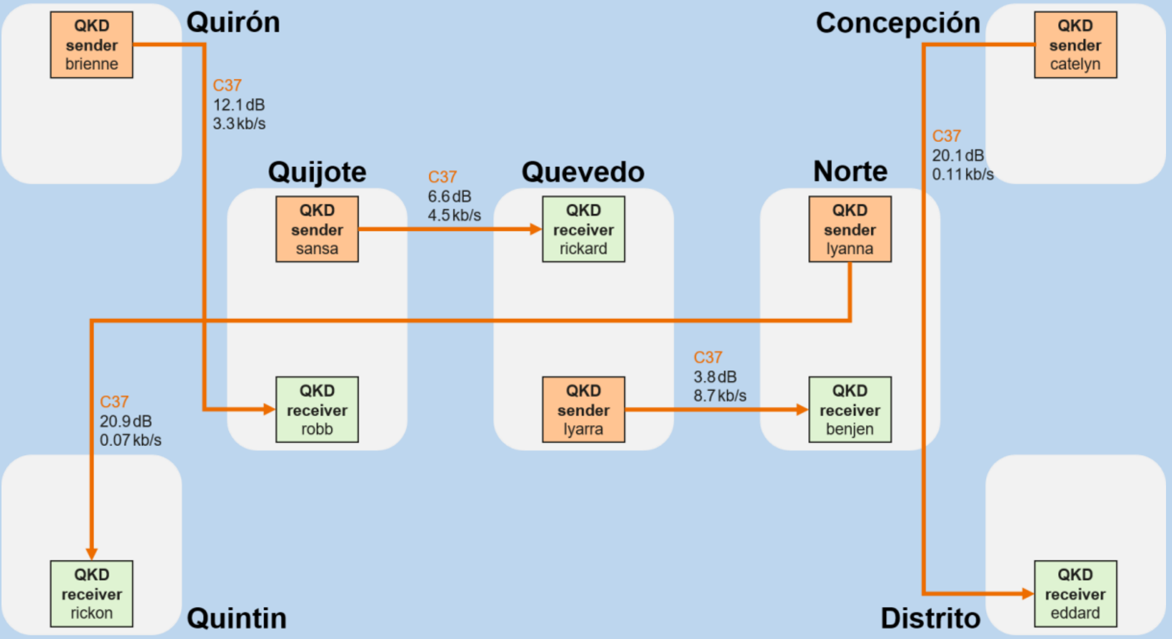


Figure 4: Scenario 3 with simultaneous connections on C37.

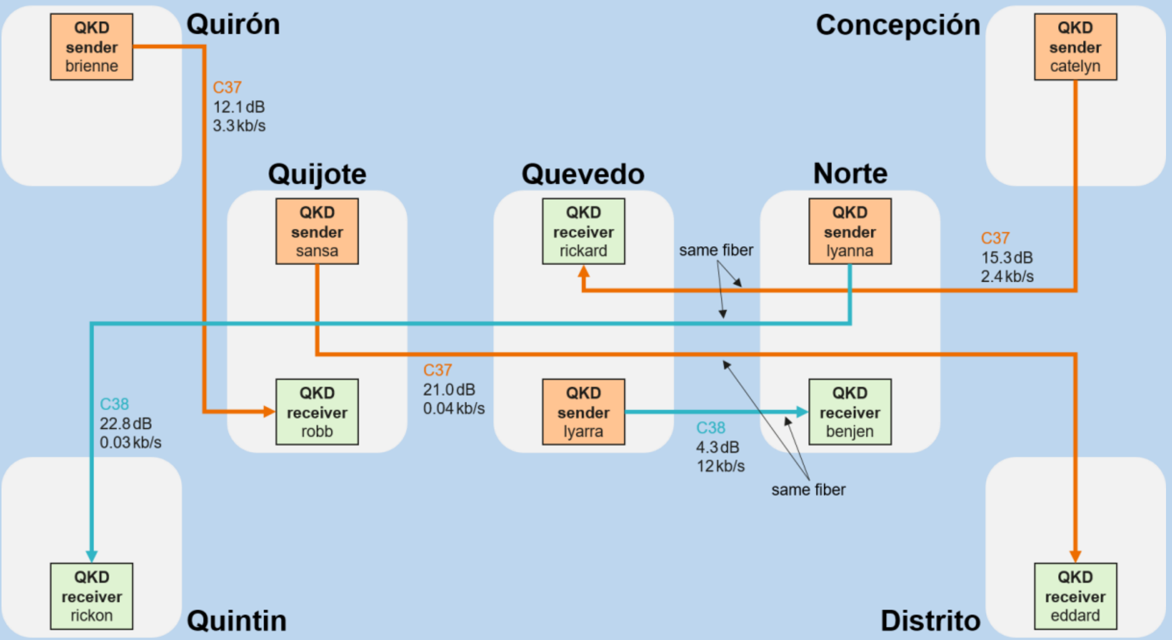


Figure 5: Scenario 4 with simultaneous connections on C37 & C38. Four different QKD links are connected simultaneously over the same fiber pair Norte-Quevedo as shared-medium demonstration.

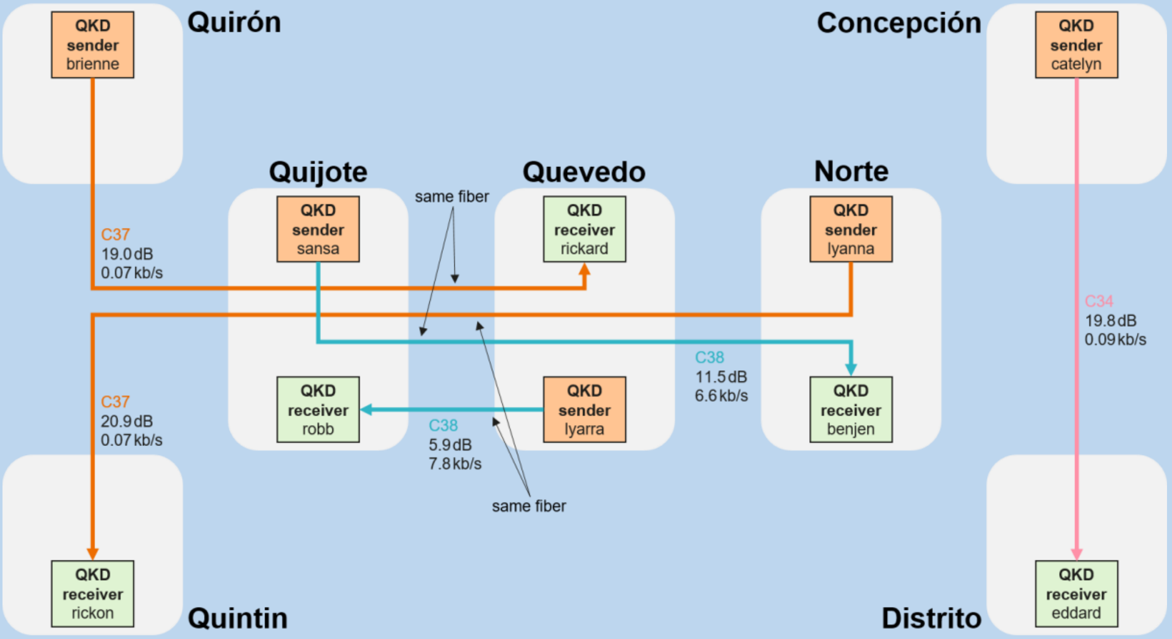


Figure 6: Scenario 5 with simultaneous connections on C34, C37 & C38. Four different QKD links are connected simultaneously over the same fiber pair Quevedo-Quijote as shared-medium demonstration.

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
catelyn (Concepción)	eddard (Distrito)	193,4	3,3	19,8	9,0E+01
	(- via Norte -)	193,7	5,3	20,1	1,1E+02
	benjen (Norte)	193,7	5,3	11,1	7,4E+03
	rickard (Quevedo)	193,7	5,3	15,3	2,4E+03
	robb (Quijote)	193,7		too high	no key
	rickon (Quintin)	193,7		too high	no key
lyanna (Norte)	eddard (Distrito)	193,7	1,1	10,2	8,4E+03
		193,8	1,1	10,5	8,1E+03
	benjen (Norte)	193,7	0,5	1,6	1,7E+04
		193,8	0,5	1,7	1,7E+04
	rickard (Quevedo)	193,7	1,4	5,1	9,0E+03
		193,8	1,4	5,2	3,2E+03
	robb (Quijote)	193,7	1,4	10,3	7,1E+03
		193,8	1,4	12,1	5,2E+03
	rickon (Quintin)	193,7	1,4	20,9	7,2E+01
		193,8	1,4	22,8	3,6E+01
lyarra (Quevedo)	eddard (Distrito)	193,7	1,4	13,3	4,3E+03
		193,8	1,4	13,3	4,3E+03
	benjen (Norte)	193,7	1,4	3,8	8,7E+03

		193,8	1,4	4,3	1,2E+04
	rickard (Quevedo)	193,7	0,5	0,1	1,4E+04
		193,8	0,5	0,2	1,4E+04
	robb (Quijote)	193,7	1,4	4,8	1,1E+04
		193,8	1,4	5,9	7,8E+03
	rickon (Quintin)	193,7	1,4	15,5	1,8E+03
		193,8	1,4	17,3	7,0E+02
sansa (Quijote)	eddard (Distrito)	193,7	1,4	21,0	4,1E+01
		139,8	1,4	20,9	4,1E+01
	benjen (Norte)	193,7	1,4	11,5	6,0E+03
		139,8	1,4	11,5	6,6E+03
	rickard (Quevedo)	193,7	1,4	6,6	4,5E+03
		139,8	1,4	6,9	1,0E+04
	robb (Quijote)	193,7	0,5	1,2	1,2E+04
		139,8	0,5	1,3	1,6E+04
	rickon (Quintin)	193,7	1,1	11,4	5,5E+03
		139,8	1,1	11,8	6,2E+03
brienne (Quirón)	eddard (Distrito)	193,7		too high	no key
	benjen (Norte)	193,7		too high	no key
	rickard (Quevedo)	193,7	3,3	19,0	7,3E+01
	robb (Quijote)	193,7	3,3	12,1	3,3E+03
	rickon (Quintin)	193,7		too high	no key

- A video of this use case can be found here: https://drive.upm.es/s/fed4HkCf5ePIhpS
- Name of the Video: UC33_Madrid_QKD_OpticalSwitching.mkv

3.14 Use Case 34

ID: 34

security independence of a network provider from QKD device manufacturers

Target sector: *Commercial and infrastructure*

Country: SP | **Main site: Madrid**

Abstract scheme

Description of Proposal:

This use case aims at demonstrating the possibility to security-wise decouple QKD-providers/manufacturers from secure infrastructure operators. The principle is simple and in theory well known since a long time. It is almost obvious that if two (or more) QKD providers deliver key between two identical end points then a combination of both keys (the simplest version being XORing) the resulting key is unrelated to any of the two original keys.

Even if each QKD provider is leaking her/his entire key to a third party then the combination remains secure for the user/operator if the mentioned third parties do not collude one with the other (a requirement that is imperative).

In this sense it is even better if the manufacturers are driven by incompatible interests and would not have any incentive for collaboration. Paradoxically the best security for the user can be achieved if mutual enemies are her/his key providers. In this case, however, all the security responsibility lies with the operator/designer of the embedding network.

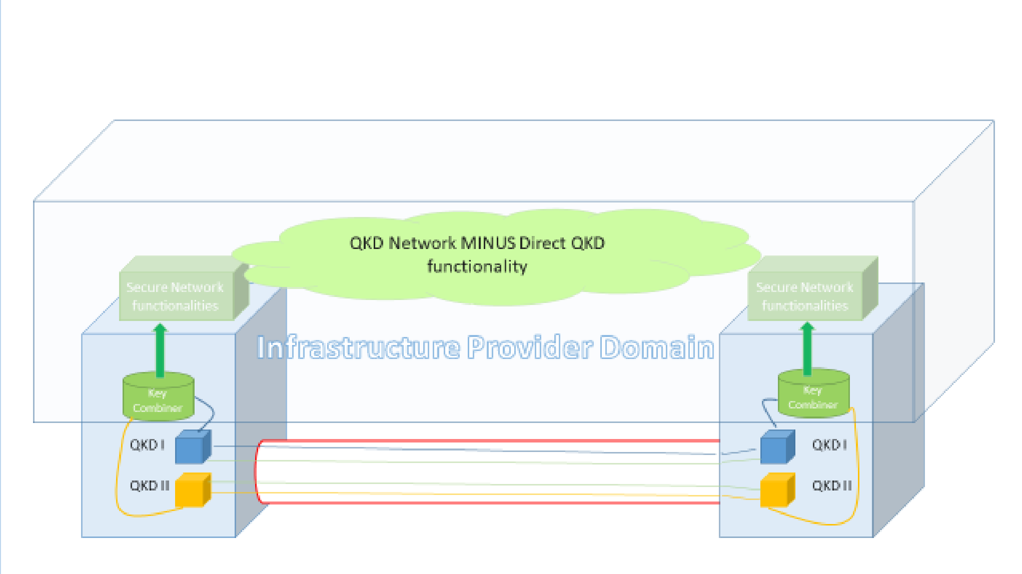
Alternatively, in a more lavish scenario, an end-user can utilize independent networks (a scenario that had been put forward back in SECOQC that is almost equivalent to finding non intersecting routing paths in the network). This idea is certainly intellectually appealing but more difficult to realize.

The combination can be extended to include Post Quantum Keys to further increase compatibility with emerging (NIST) standards and ensure a practically-water proof security against emerging realistic threats (as is a quantum computer that has been related to “quantum safety”)

The basic challenge of this use case is to be able to prototypically demonstrate in an OpenQKD test bed. In the Madrid testbed the conditions are in principle perfect as several QKD providers are active and the network layer design and implementation is in the responsibility of UPM.

This use case further requires test-bed level integration of at least two QKD manufactures –

something that obviously would demonstrate practicality and interoperability of QKD in general The use case is strongly related to Use –case 16 “Critical infrastructure Protection” and “Use case 15 “Network security and attestation”	
Partner	**Role/Function**
TID	Testbed and SW provider
RM	Testbed provider
UPM	SW provider
IdQuantique	QKD System provider
HWDU	QKD System provider
Other	
Impact	
Target sector planned impact: Security and privacy in QKD Networks with security independence from QKD providers **Companies attracted through use case:** - Telefónica - BT - DT	**Planned KPI demonstrations:** - Connection latencies - Final key-rate through the joint link - Data throughput
Implementation	
Work plan/TODO list: 56. Select locations for the test and verify feasibility based on network parameters (local tests if necessary) 57. Prepare QKD systems and interfaces (fall of 2020) 58. Organize necessary OTN equipment wherever necessary (free of charge) 59. Schedule delivery and deployment with all involved partners 60. Deploy and carry out an initial test phase 61. Full scale operation, data collection 62. Analysis of results and publication	
Block diagram	
Illustration of a feasible imlementation	

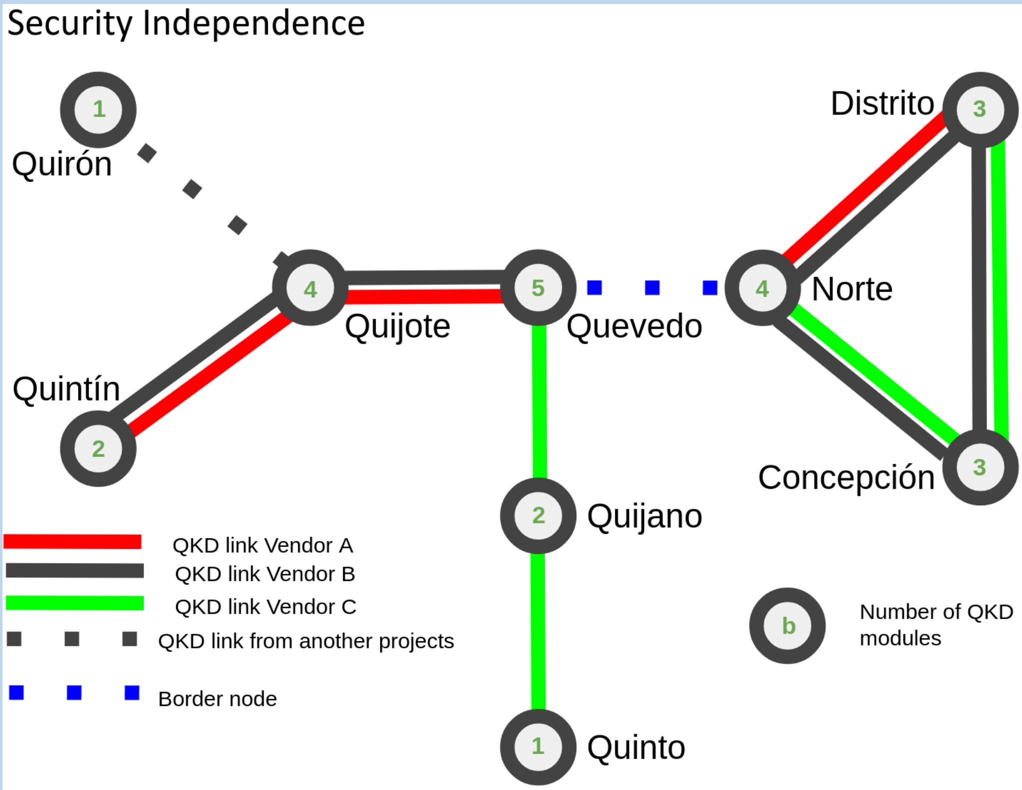


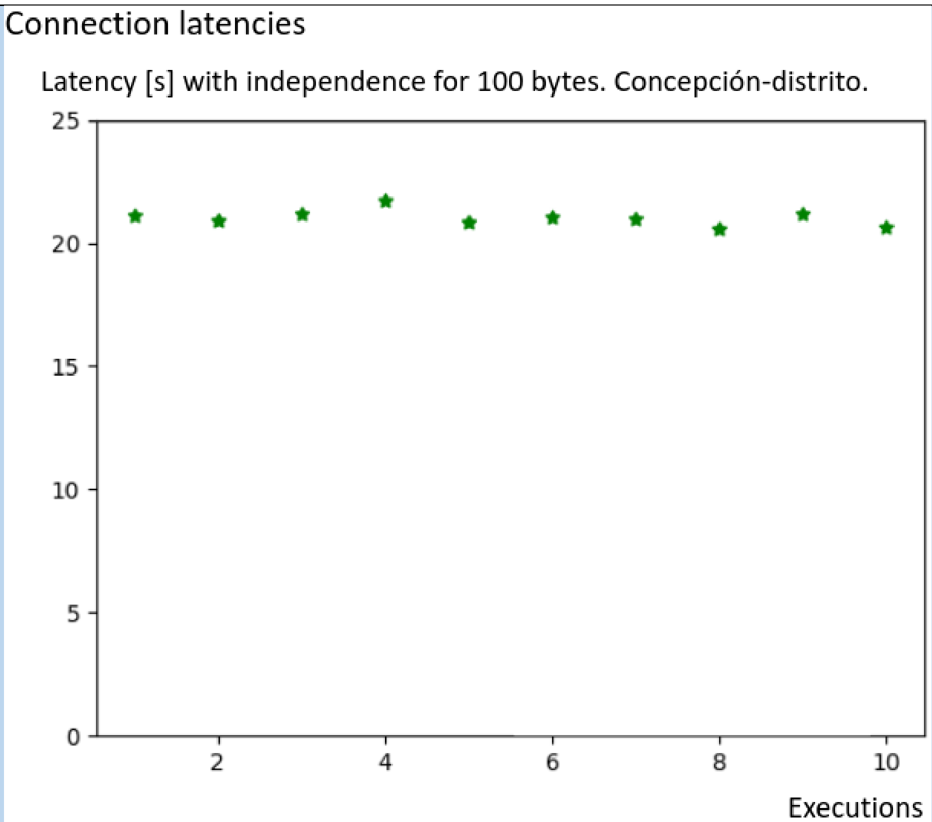
A provider of a network hires two QKD manufacturers to provide QKD systems. Here the systems are positioned in Nodes that are owned and managed by the Network operator. The QKD systems' signals can co propagate over the same quantum link, this being graphically represented here as the same fiber, in which all classical and quantum channels co-propagate jointly. In, practice, however, co-propagation of two (in principle also more) quantum channels co-propagate on the same fiber while classical post-processing can be outsourced elsewhere.
The outputs of the independent QKD devices (here I and II) needs to be combined appropriately in a functional element (Key Combiner), provided by the infrastructure designer/operator. Its output is then fed into higher network functional elements that are not considered here. This is also not necessary as the architectural design of the full network is completely independent from the "Combined QKD Layer" the output of which can be universally integrated in any network design.
A number of requirements for the QKD devices can be derived:
* The QKD devices need to be able to be operate on the same fiber as QKD devices from other providers, typically wavelength multiplexed.
* The inclusion of the QKD devices need to be tamper proof (something that does not need to be explicitly the case in a demonstration test bed).
This defines a highly secure design, in which the operator/user does nt need to trust manufacturer.

Site access
Note: With previous tests in Telefonica production environment HWDU devices are ready for a very broad variety site access conditions. AS in this case HWDU envisions co-propagation with IdQantique devices need to be suited to same environment for which the HWDU ones need to. HWDU guarantees for that.
Available power
From Previous experience with the Telefonica production environment, necessary power is available.
Internet connection
We need at least one internet connection. One was (is) available at the Almagro site of Telefonica.
Existing equipment
We shall bring necessary telecommunication equipment if such is not provided by the network itself

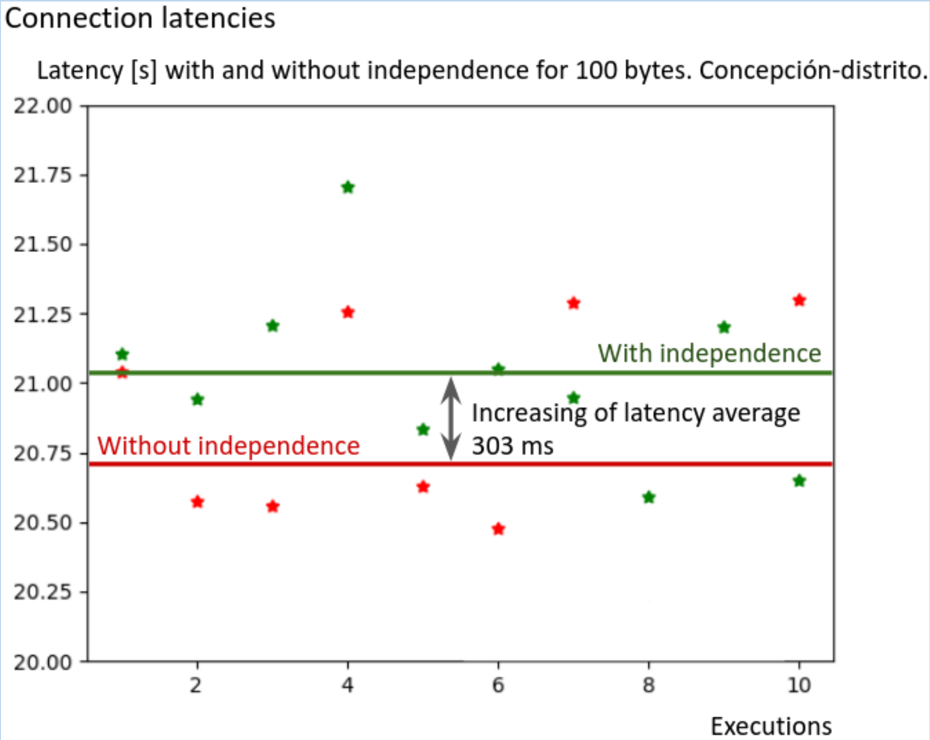
Encryptors
Manufacturers and Devices To be provided as necessary by the network. Huawei encryptors will not be used.
QKD Systems
Manufacturers and Devices o 5 CV QKD Links – all switchable (directional, wavelength), and controllable by Madrid SDN controllers. The devices (depending on distance and attenuation) can c-propagate with up to 20 downstream 1dBm channels o Two of these links can be used for the present use case, while this also operate in parallel in the x1 use case.

Impact	
Target sector planned impact: - Commercial. - Infrastructure features. **Companies attracted through use case:** - Telefónica de España - BT - DT - Huawei - IdQ - Toshiba	**Achieved KPI demonstrations:** - KPI UC34_1: Connection latencies (fully achieved) - KPI UC34_2: Final key-rate through the joint link (ongoing) - KPI UC34_3: Data throughput (ongoing)
Time of demonstration	
Deployment: - Initial development and adaptation of the Madrid Network: 10 months. - The deployment is based on two physical links consuming key through the Madrid's ETSI ISG QKD 004 standard access point. To deploy the use case is required: o Around 10 minutes to configure the application entities. o This UC additionally requires the use of several gateways connected to multiple VPNs where the different QKD devices are hosted (network segregation). - Note that this deployment assumes that the complete SDN stack of the Madrid Quantum Network is fully deployed and operational.	
Time of demonstration: - The first version of security independence use case based on SDN applications was developed on 02/2022 and continuous improvements are being made. - This demonstrator can be executed on the nodes running the mentioned technology, namely Concepción and Distrito.	
Results	
Lessons learned: - QKD key from several links can be efficiently combined to make security independent of the vendor in QKD networks. - 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.
Changes necessary to already deployed infrastructure: - The current version of this use case runs on top of the Madrid's SDN stack, which delivers QKD services using the ETSI ISG QKD 004 standard access point. - There are certain nodes that need to access simultaneously to different segregated networks. - Additional computation power was needed in some IT systems deployed.
Target sector demonstrated impact: - Delivered vendor-independent secure key in QKD networks.
Estimated cost of implementation: - QKD systems: 150k€ (2 DV modules) +80k€ (2 CV modules) - Personnel for installation and maintenance: 20k€ - Other equipment used: 10k€ - Desired airport cost for all of this: 10k€ - Software Development: Using as base the Madrid SDN Stack infrastructure, the implementation of this infrastructure requires 1PM during 10 months approximately. = 50K€ - Total cost: 320k€ UC working on one link.
Further comments: - The following figure shows a map of the networks where this metric has been evaluated  - The following figure show the connection time of applications that consume the vendor-independent QKD key, known as KPI UC34_1.



The following figure shows the detail of the impact of this KPI UC34_1 with respect the normal operation:



- A video of the use case can be seen here: https://drive.upm.es/s/fed4HkCf5ePIhpS
  Name of the Video:
  UC34_Madrid_SecurityIndependenceOfANetworkProviderFromQKDDeviceManufacturers.mkv

3.15 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.

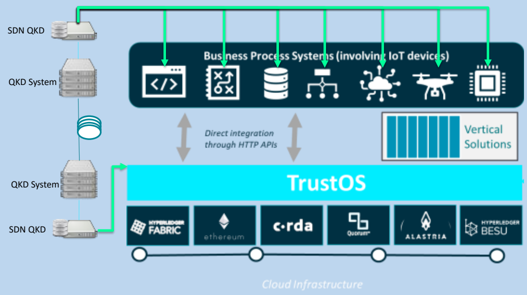
Blockchain adoption to deliver trust in corporate environments leverage in deploying private networks. Telefonica has developed **TrustOS (https://aiofthings.telefonicatech.com/en/technology-services/blockchain-services/trust-os)**, a kind of middleware that makes business applications and solutions 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:

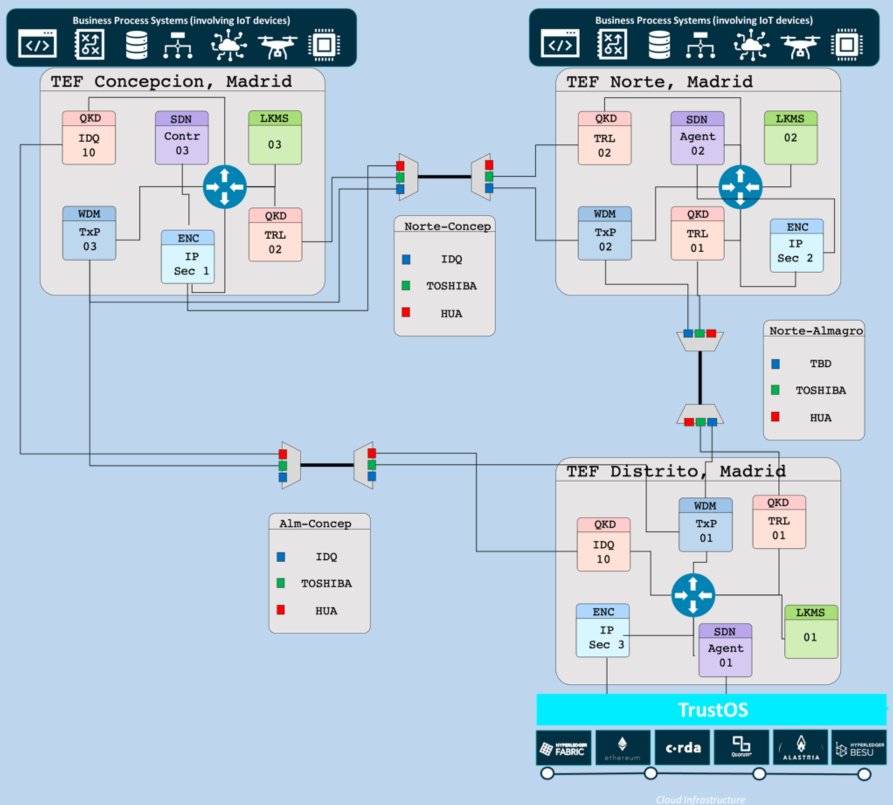
- -Telco: Audit data information for about infrastructure sites or devices, such as mobile communication towers or terminal logistic chain
- -E-health: IoT areas related with privacy and confidentiality of the information
- -Defense: Military IoT equipment with strong security demands.

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

TREL	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:

<u>Telefónica Quantum Ring (Distrito-Norte-Concepción)</u>

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.

Planned deployments
- 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
Lessons learned: -
Changes necessary to already deployed infrastructure: -
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.
Estimated cost of implementation: - QKD systems: 150k€ - Personnel for installation and maintenance: 20k€ - server equipment used: 15k€ - License from TrusOS: 0k€ (non-commercial solution available for testing) - Software Development: 1PM during 3 months approximately. = 23K€ Total cost: 200k€ UC working on one link.

KPIs	
Number of IoT devices connected simultaneosly	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

4 Remarks and Conclusions

Some use cases already 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 are currently catching up with many demos planned for summer 2022 and results by the end of the year. These achievements will be made available in a later deliverable.