Final report of operation of testbeds and local sites

Deliverable D7.5

Final report of operation of testbeds and local sites	
Deliverable: **D7.5**	Lead: UNIGE
Project month: 41	1.03.2023
Work package: WP6	Task: T7.1
Type: Demonstrator	Version: 1.0
Dissemination level: public	

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

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

Document Information

Author List

Organization	Name	E-mail
UNIGE	Hugo Zbinden	hugo.zbinden@unige.ch
DTTG	Marc Geitz	marc.geitz@telekom.de
UPM	Juan P. Brito	juanpedro.brito@upm.es
PSNC	Piotr Rydlichowski	prydlich@man.poznan.pl
AIT	Florian Kutschera	Florian.Kutschera@ait.ac.at
	Giannis Patronas	giannisp@nvidia.com
CAM	Adrian Wonfor	aw300@cam.ac.uk
ICFO	Daniel Tiemann	Daniel.Tiemann@icfo.eu
TU	Rebecca Mayrhofer	R.Mayrhofer@tudelft.nl
SIG	Olivana Palivan	oriana.palivan@sig-ge.ch
UNIPD	Francesco Vedovato	francesco.vedovato@unipd.it
CNRS	Eleni Diamanti	eleni.diamanti@lip6.fr

Reviewer List:

Organization	Name	E-mail
TSIX	Gonzague Reydet	gonzague.reydet@thalesgroup.com
DTU	Tobias Gehring	tobias.gehring@fysik.dtu.dk

Version History:

Version	Date	Reason/Change	Editor
1	20.12.2023	Templates for Input Request	Hugo Zbinden
2	02.02.2023	First draft	Hugo Zbinden with many inputs from the testbed coordinators
3	14.02.2023	All but one inputs received	Hugo Zbinden
4	24.02.2023	Final version after review	Hugo Zbinden
5	01.03.2023	Ready to submit	Cristina Tamas

Executive Summary

This deliverable demonstrates the activities in the different test-beds and local sites over the whole duration of OPENQKD. It shows the big variety of sites, fiber-links, QKD-devices, encryptors and use-cases etc.

Table of Contents

1. Introduction

1.1. Purpose and scope of the document

The purpose of this deliverable is to demonstrate the variety of installations that have been implemented and tested. We illustrate this by maps of networks, a brief description of highlights and use-cases, table with the specifications of all links, and finally a couple of nice pictures. It is not supposed to be a comprehensive report about all activities undertaken during projects at the different sites. For this please refer to many other specialized reports elaborated in this and all other work-packages.

1.2. Target audience

European Commission, interested scientists.

1.3. Relation to other project work

This report gathers inputs from the use case WP 2. Demonstrated use cases illustrate the outcome of all other OpenQKD WPs.

2. Summary and main results of the major testbeds

2.1. Berlin

The OpenQKD Testbed Berlin is situated in the Berlin metropolitan area and connects several Deutsche Telekom AG (DTAG) office buildings, university institutes and network operation centers. All sites are connected by dark single mode fibers, allowing for connection length between 2km up to 100km. The network is a star-shaped architecture, with the location of Winterfeldtstr. 21 at the center, as shown by Figure 2.1.1.

Figure 2.1.1: The star-shaped fiber network of the OpenQKD testbed in the Berlin metropolitan area.

DTAG decided for a layered QKD architecture, composed of a quantum layer, a key management layer and an application layer. Three QKD nodes are deployed at the central location of Winterfeldtstrasse, and the connecting fiber links are looped via the remote locations. Figure 2.1.2 shows the three-layer QKD stack architecture.

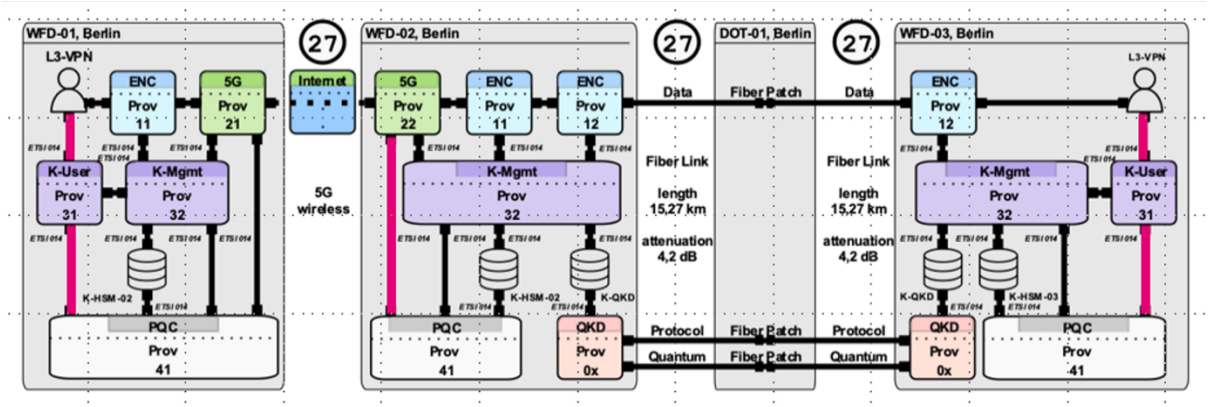


Figure 2.1.2: Three architecture layers (quantum, key management and application) deployed in the OpenQKD testbed Berlin.

Figure 2.1.3 and 2.1.4 show the physical set-up of the Berlin testbed, including the QKD systems by IDQuantique and Toshiba, Encryptors by Adva Optical and Thales, the Hardware Security modules by Gemalto, Firewalls, Switches, Quantum Number Generators by IDQuantique and a 5G access point. The servers host the key management systems and applications in a virtual environment.

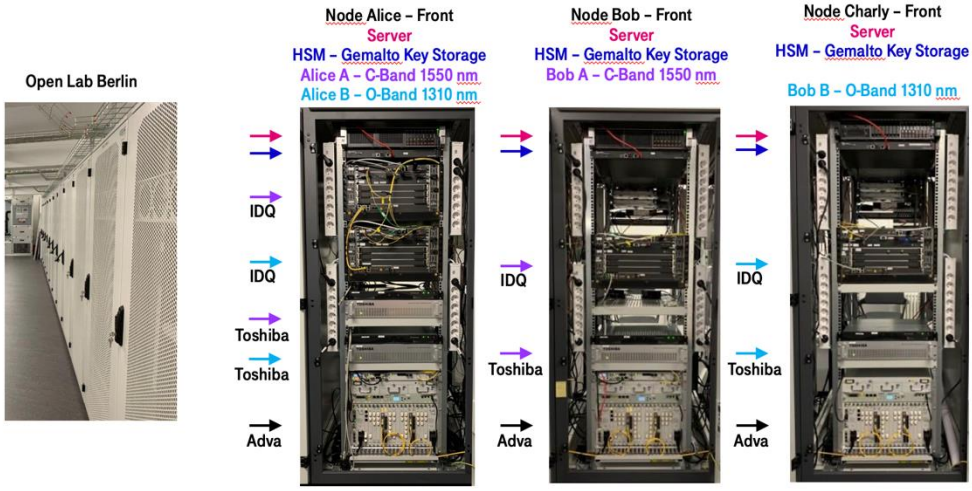


Figure 2.1.3: Three nodes of the OpenQKD testbed Berlin. (From top down): the front side of the rack hosting a server for the key management system (red arrow), a Gemalto HSM (blue arrow), IDQ systems from IDQuantique and Toshiba operating at 1310 and 1550nm wavelength and optical DWDM line terminations with AES encryption by Adva.

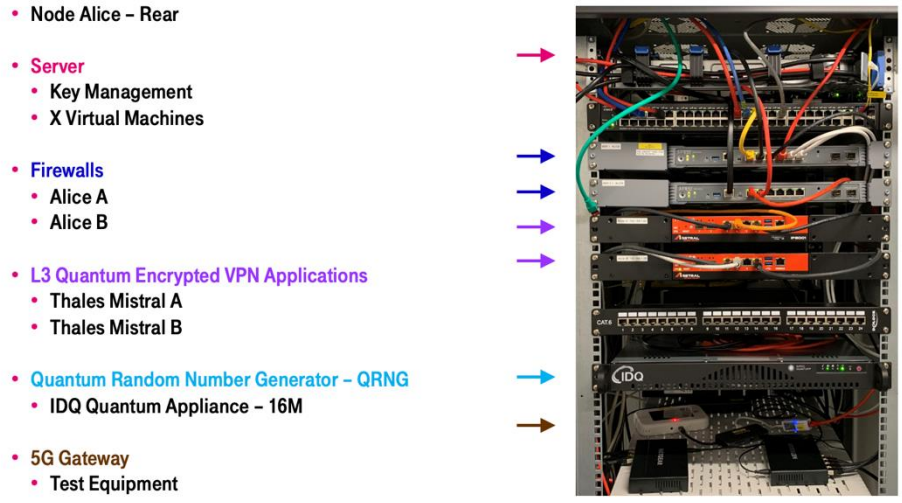


Figure 2.1.4: The back side of the Alice rack. (From top down): the backside of the server hosting the key management system, firewalls, two L3 Mistral encryptors by Thales, an IDQ QRNG appliance and a 5G access point.

Highlights of the Berlin testbed are based on the implemented use cases:

Use Case 28: Integration of QKD into a telecom provider infrastructure.

This use case has been fully implemented.

- QKD systems by IDQ and Toshiba installed, linked by dark and classical fiber lines and the QKD exchange has been proved.
- Integration of the QKD systems to a Key Management System (KMS). An ETSI-QKD014 API has been deployed to extract the keys to a local key store.
- A hardware security module (Gemalto KeyStore 250) has been deployed to store encryption keys (as a single point of truth). No other place in the QKD system stack is to store encryption artifacts.
- The hardware security modules deployed a classical trust chain, so that the web service application clients and servers of the KMS could authenticate themselves (in accordance to the ETSI-QKD014 standard).
- A User Key Management system using the ETSI-QKD014 API has been deployed to extract encryption keys from the local key store and hand them over to the consuming applications.
- Applications are: Adva L1 Encryptors with AES cards, Thales Mistal L3 encryptors, applications and software encryptors (Voice, Video, Chat, File Transfer and Stream service).
- A Provider Key Management running the encryption key forwarding process via an intermediate QKD node.
- A monitoring system to monitor the health of the QKD stack and to store the KPI data. The KPI data has also been exported to the central storage system operated by AIT.

An end-to-end monitoring system to prove the operation of the platform within regular time intervals.

Use Case 27: Integration of QKD and PQC

This use case has been fully implemented.

- A PQC key exchange system mimicking a QKD system has been implemented and deployed.
- PQC keys secured by PQC KEM (Key Encapsulation Mechanism) and authenticated by PQC SIG (Signatures) were exchanged between all QKD nodes.
- PQC keys were exported to the local key store / hardware security module. PQC and QKD keys were differentiated by meta data only.
- Due to the network agnosticm of PQC, we could demonstrate a key exchange via 5G mobile networks integrated to the QKD testbed.
- Mobile clients exchanged keys with the testbed's KMS and payload data encryption was demonstrated.
- Applications could query keys originated form QKD or PQC. The keys could optionally be combined by a KDF or XOR operation to produce hybrid keys. Hybrid

keys are better encryption keys, because they build on multiple security factors, i.e. quantum physics and complexity theory.

- The key forwarding process has been secured by an additional end-to-end PQC layer, preventing unencrypted key material on intermediate nodes.
- The internal, vertical APIs within a QKD system stack were hardened by PQC authentication and encryption. This was not possible for every API, because most hardware systems did not yet support PQC. The software applications and the user key management, however, were using a PQC encryption and authentication. An additional PQC trust chain to authenticate the web servers has been deployed.
- As an add-on, a "multi-PQC algorithm / multi network path solution" has been implemented and deployed to integrate the OpenQKD testbeds of Madrid, Poznan and Berlin. Random numbers secured by different PQC KEM and SIG algorithms were exchanged over disjoint network paths, i.e. a ground path via the internet and a space path via the commercial Iridium network. On both end points, the encryption keys were combined using a KDF or XOR operation.
- The latter solution has been applied to mobile clients, using disjoint networks (via the T-Mobile and Vodafone mobile networks) to connect to the Berlin OpenQKD testbed. Clients exchange keys with the testbed, which were forwarding the key to an IT application. Mobile client and the IT application could then use the encryption keys to generate an AES-secured channel.

OpenCall: VeriQloud / Qline:

The QLine by VeriQloud has been integrated to the OpenQKD testbed Berlin.

- Deployment of five QLine nodes into the OpenQKD testbed, as documented in D3.2. Dark fiber links and classical fiber links are connecting the nodes. The setup was arranged as two QLines integrated over an AWG (Arayed Wavelenght Grating) with a single photon detector.
- Demonstration of QKD between all nodes.
  Demonstration of two QLines operating time multiplexed sharing a single detector. Each QLine was operated at a different light frequency.

Integration of the QLine nodes to the KMS of the testbed. Encyption keys are imported to the local key store, where they are persisted with accompanying meta data. This enabled the consumption of QLine encryption keys for any connected application northbound to the KMS.

The Use Cases have been operated on the fiber links shown by Table 2.1.1.

Testbed location:	**Berlin**	**Responsible Partner**	**Deutsche Telekom**
Number of nodes	3	Number of links	4
Link Number	Length [km]	Loss [dB]	Dark/shared
1 WFD – DOT	15,3	4,2	Dark
2 WFD – HSR	10,6	3,2	Dark
3 WFD - ERP	8,5	3,7	Dark
4 WFD - KST	2,3	2,0	Dark
Use case number	**#27**	**Name**	**5G Networks**
Partners involved:	DTAG		
Starting date	07.2020	End date	12.2022
No of used fibers (quantum/classical channel:	Only classical links (fiber, 5G, Satellite) have been used. For the hybrid PQC / QKD solution, the links established for UC28 have been reused.		
QKD equipment used:	IDQ, Toshiba	Encryptors used:	ADVA
Comments:	The use case was not limited to QKD nodes. Mobile devices and IoT devices have been integrated to the testbed.		
Use case number	**#28**	**Name**	**QKD Network**
Partners involved:	DTAG, ADVA, Idquantique, Toshiba, Thales		
Starting date	01.2021	End date	03.2022
No of used fibers (quantum/classical channel:	1-4		
QKD equipment used:	IDQ, Toshiba	Encryptors used:	ADVA
Comments:	Three nodes situated at Winterfeldtstrasse, looped fiber links were applied for the quantum channel.		

Table 2.1.1: Fiber links, deployed systems and partner involvement in the Berlin testbed.

2.2. **Madrid**

The Madrid SD-QKD network has successfully deployed 8 use cases based on delivering QKD services, besides 3 more use cases from open calls. This test bed is based in an SDN approach to quantum communications and implements several ETSI GS QKD standard specifications. Is composed by 9 nodes and 9 links that sum more than 120 km. Figure 2.2.1 shows the network scheme.

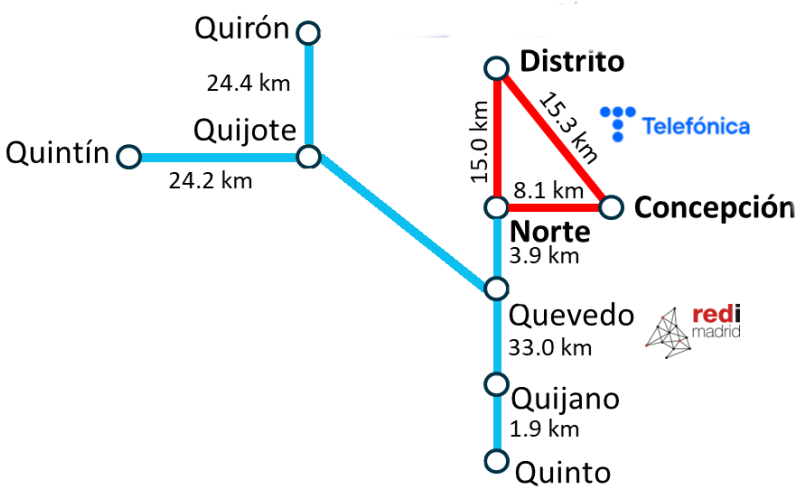


Figure 2.2.1: Final deployment of the Madrid Quantum Network.

There are two domains in the Madrid test bed: first the institutional and academical network provider RediMadrid (RM) and second the Research & Innovation branch of the incumbent network operator Telefónica I+D, (TID), so a border link is needed. The management and control system, both the central SDN controller and its agents, is developed by UPM, as well as the local KMS (LKMS) in each trusted node. There are three vendors of QKD systems deployed in the network, IDQ, TREL and HUDU (the latest from an open call) and the key is consumed by several hardware and software secure applications (e.g., ADVA encryptors). This makes the Madrid Quantum Network a multi-vendor and multi-tenant QKD network. The figure 2.2.2 depicts an example of the deployed infrastructure working with the use cases.

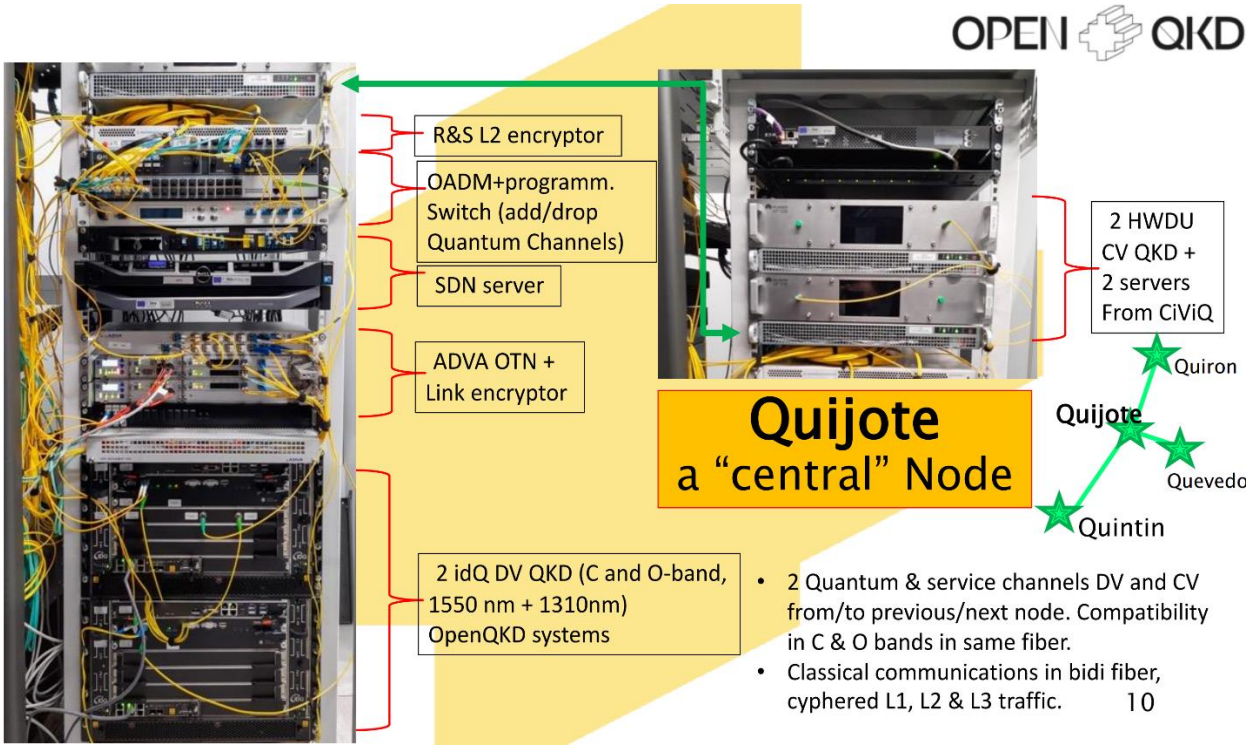


Figure 2.2.2: The Quijote Node on the Madrid Quantum Network. This central node allocates 2 DV QKD devices from IdQ, 2 CV QKD devices from Huawei, 1 encryptor (and OTN) from ADVA, 1 encryptor from Rohde & Swatch, classical optical infrastructure and a set of servers to control all the devices and services on the network.

Testbed location:	**Madrid**	**Responsible Partner**	**UPM**
Number of nodes	9	Number of links	9
Link Number	Length[km]	Loss [dB]	Dark/shared
1 Quintín-Quijote	24.2	5.97	Classical: shared. Quantum: dark
2 Quijote-Quirón	24,4	7.22	Classical: shared. Quantum: dark
3 Quijote-Quevedo	7.4	4	Classical: shared. Quantum: shared
4 Quevedo-Quijano	33	10.30	Classical: shared. Quantum: shared
5 Quijano-Quinto	1.9	0.4	Classical: shared. Quantum: shared
6 Distrito-Norte	10	7.7	Classical: shared. Quantum: dark
7 Distrito-Concepción	12	6.67	Classical: shared. Quantum: dark
8 Concepción-Norte	6.4	6.8	Classical: shared. Quantum: dark
9 Quevedo-Norte (border)	1	0.2	Classical: shared. Quantum: shared
Use case number	**15**	**Name**	**Network security and attestation**
Partners involved:	IDQ, TREL, TID, UPM, RM, other		
Starting date	05.2020	End date	12.2022
No of used fibers (q/c):	1/1 per link		
QKD equipment used:	IDQ, TREL	Encryptors used:	-
Comments:	- Use case tested in both network domains (TID and RM, 2 scenarios). - Technology deployed: SDN-like ordered proof of transit (OPoT) by UPM.		
Use case number	**16**	**Name**	**Critical Infrastructure Protection**

Partners involved:	IDQ, TREL, TID, UPM, RM, other		
Starting date	05.2021	End date	12.2022
No of used fibers (quantum/classical channel:	1/1 per link		
QKD equipment used:	IDQ, TREL	Encryptors used:	Software
Comments:	- Use case tested among all network links (TID and RM, 8 link). - Technology deployed: SDN-aware IPSec software encryption by UPM. - Traffic delivered: SCADA frames for industrial purposes.		
Use case number	**17**	**Name**	**QKD as a Cloud Service**
Partners involved:	IDQ, TREL, TID, UPM, RM, other		
Starting date	05.2021	End date	07.2022
No of used fibers (q/c):	1/1 per link		
QKD equipment used:	IDQ, TREL	Encryptors used:	-
Comments:	- Use case availability tested among all network nodes (TID+RM, 8 nodes). - Technology deployed: key management system by UPM. - Traffic delivered: Simulated requests from hosted VM.		
Use case number	**18**	**Name**	**e-Health services**
Partners involved:	IDQ, TREL, TID, UPM, RM, other		
Starting date	05.2021	End date	11.2022
No of used fibers (q/c):	1/1 per link		
QKD equipment used:	IDQ, TREL	Encryptors used:	-
Comments:	- Use case tested among all network links (TID and RM, 8 link). - Technology deployed: SDN-aware IPSec software encryption by UPM. - Traffic delivered: Simulated medical information.		
Use case number	**25**	**Name**	**Quantum Cryptography for B2B and 5G networks**
Partners involved:	IDQ, TREL, TID, UPM, RM, other		
Starting date	05.2021	End date	11.2022
No of used fibers (q/c):	1/1 per link		
QKD equipment used:	IDQ, TREL	Encryptors used:	-
Comments:	- Use case tested among all network links (TID and RM, 8 link). - Technology deployed: SDN-aware IPSec software encryption by UPM and simulated 5G core network by TID. - Traffic delivered: Simulated B2B transaction.		
Use case number	**26**	**Name**	**Self-healed network management**
Partners involved:	IDQ, TREL, TID, UPM, RM, other		
Starting date	09.2021	End date	11.2022
No of used fibers (q/c):	1/1 per link		
QKD equipment used:	IDQ, TREL	Encryptors used:	-
Comments:	- Use case tested in both network domains (TID and RM, 2 scenarios). - Technology deployed: custom software encryption by UPM and OpenStack as the target software for virtual image deployment. - Traffic delivered: NVF-ready virtual images.		
Use case number	**33**	**Name**	**Quantum Cryptography with minimal amount of QKD devices allowing independent protection of users in collocated computing centers**

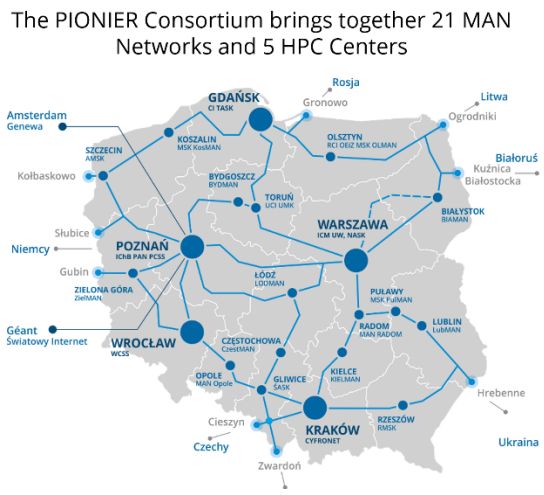
Partners involved:	TID, RM, UPM, HWDU		
Starting date	09.2020	End date	07.2022
No of used fibers (q/c):	1/0 per link		
QKD equipment used:	HWDU	Encryptors used:	-
Comments:	- Use case tested in both network domains (TID and RM, 9 links). - Technology deployed: SDN controlling by UPM for configuring optical capabilities of CV-QKD and optical network domain by HWDU.		
Use case number	**34**	**Name**	**Security independence of a network provider from QKD device manufacturers**
Partners involved:	TID, RM, UPM, IDQ, HWDU		
Starting date	09.2020	End date	07.2022
No of used fibers (q/c):	1/1 per link		
QKD equipment used:	IDQ, HWDU	Encryptors used:	-
Comments:	- Use case tested only in TID network domain, 1 link. - Technology deployed: SDN controlling and key managing by UPM for extracting key from multi-vendor sources (CV-QKD by HWDU and DV-QKD by IDQ) and combining them.		
Use case number (open call)	**40**	**Name**	**QuGENOME: Quantum Enabled Private Recognition of Composite Signals in Genome**
Partners involved:	RM, UPM, IT, CBRA, HWDU		
Starting date	12.2020	End date	02.2022
No of used fibers (q/c):	1/1 per link		
QKD equipment used:	IDQ, HWDU	Encryptors used:	-
Comments:	- Use case tested only in RM network domain, 2 link. - Technology deployed: Multi-party computation capabilities based on oblivious transfer by IT, SDN controlling and key managing by UPM for delivering symmetric and raw key from multi-vendor sources (CV-QKD by HWDU and DV-QKD by IDQ). - Delivered traffic: Genomic data.		
Use case number (open call)	**41**	**Name**	**KaaS: Key as a Service**
Partners involved:	RM, UPM, UAR, IDQ		
Starting date	12.2020	End date	02.2022
No of used fibers (q/c):	1/1 per link		
QKD equipment used:	IDQ	Encryptors used:	-
Comments:	- Use case tested only in RM network domain, 1 link. - Technology deployed: multi-technology access network to QKD with path diversity by UAR and UPM. - Delivered traffic: quantum-distributed keys to final users.		
Use case number (open call)		**Name**	**QGeKO: Quantum secure distribution of precise GNSS Keys and Orders**
Partners involved:	RM, UPM, GMV, IDQ		

Starting date	7.2022	End date	12.2022
No of used fibers (q/c):	1/1 per link		
QKD equipment used:	IDQ	Encryptors used:	-
Comments:	- Use case tested only in RM network domain, 1 link. - Technology deployed: quality of service for GNSS access software. - Delivered traffic: Global navigation satellite system (Galileo) ephemerides data.		

2.3. Poznan

OPENQKD testbed in Poznań was installed, implemented and managed by PSNC. PSNC is owner and operator of the metro area network in Poznań – POZMAN and Polish Research and Education Network – PIONIER. Both networks are part of national and European research network infrastructures, both in terms of networking and computing.

The majority of PSNC OPENQKD use cases were implemented in POZMAN network. PSNC used both IDQ and TOSHIBA QKD devices. For the encryptors PSNC used SENATAS/THALES and ADVA devices.



Type of connected unit	Number of units
Research institutions	221
Universities	196
Post-secondary schools	21
High schools, secondary schools, primary schools and vocational schools	234
Healthcare	59
Public safety	27
Goverment administration	27
Provincial administration	59
District, municipality and city administration	73
Other administration	9
Court and public prosecutor's office	26
Cultural institutions	104
Other educational	27

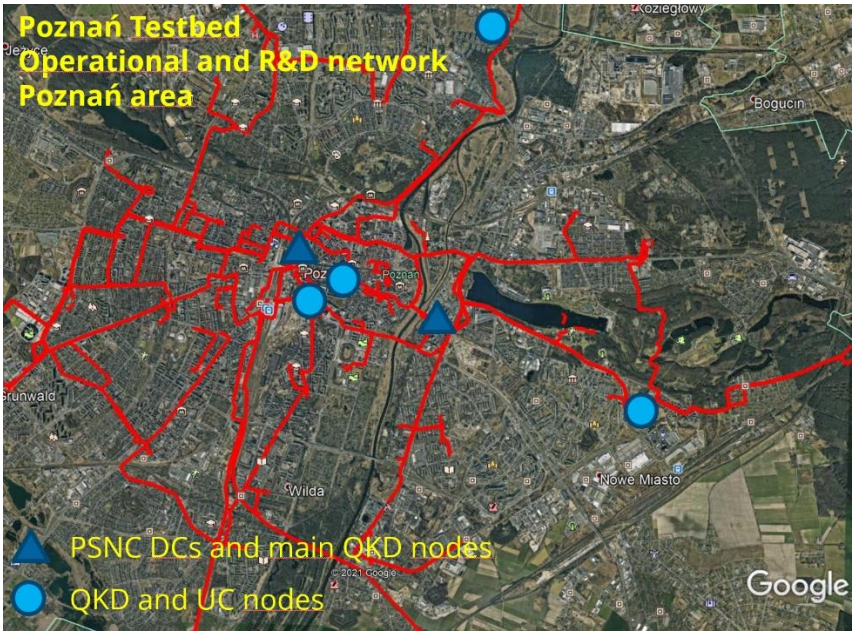


Fig. 2.3.1 PSNC POZMAN and PIONIER networks – base for OPENQKD testbed.

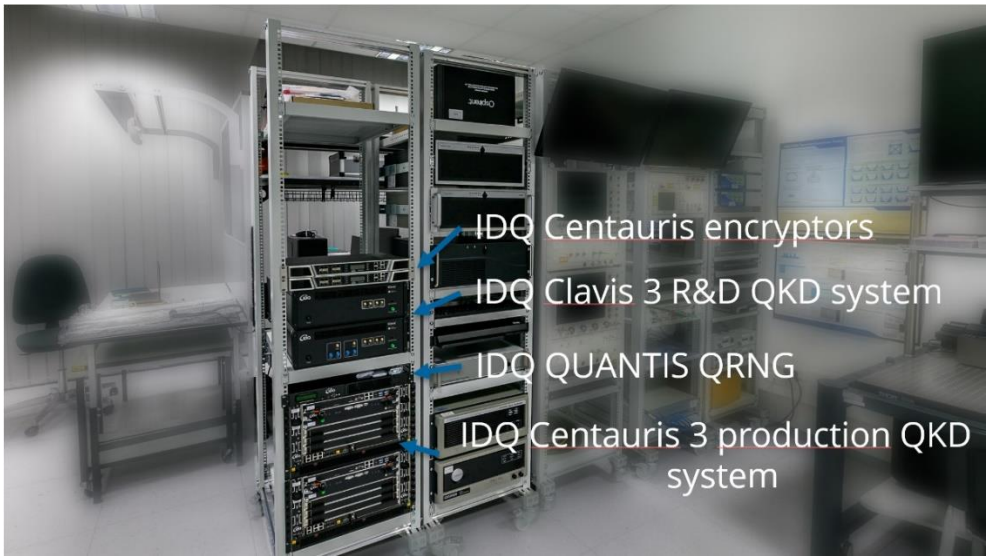


Fig. 2.3.2 PSNC QKD equipment in use cases.

All QKD system were monitored by PSNC Network Operation Center.

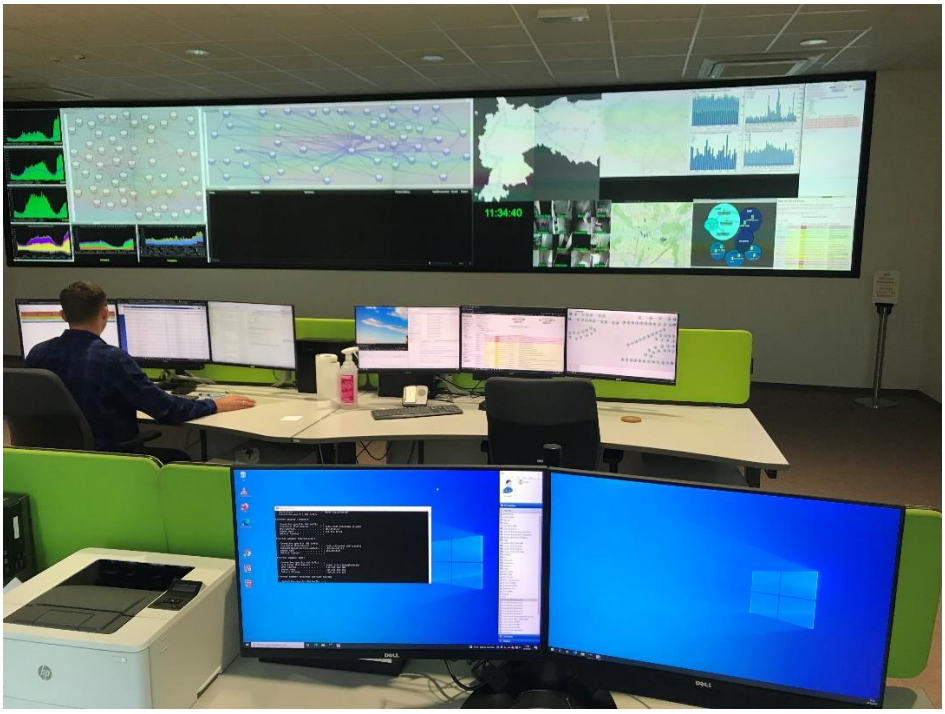


Fig 2.3.3: PSNC NOC.

PSNC OPENQKD use cases included both metro and backbone scenarios. The main applications were inter-datacentre connectivity, cross-border and intercity connectivity scenarios (also with reference Time and Frequency infrastructure).

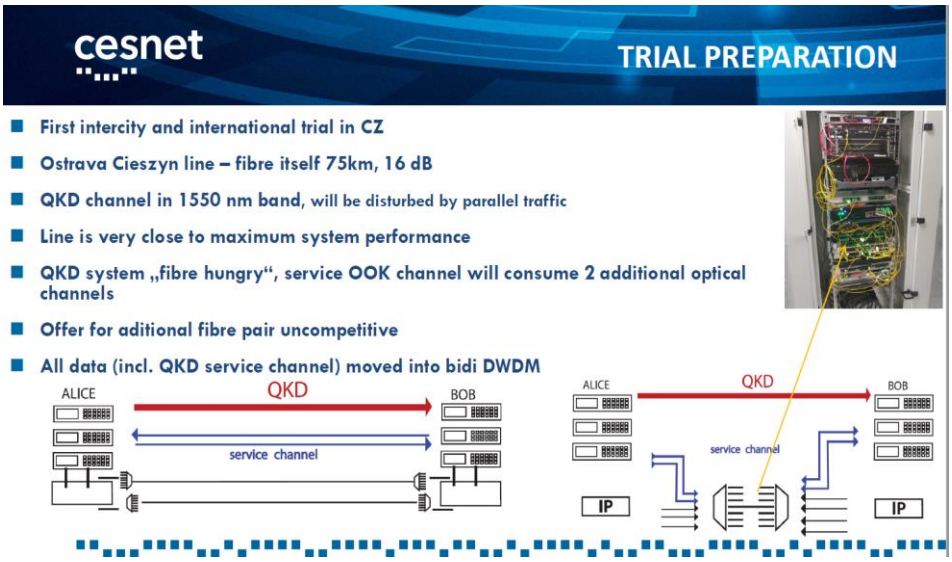


Fig.2.3.4: PSNC QKD cross border link use case.

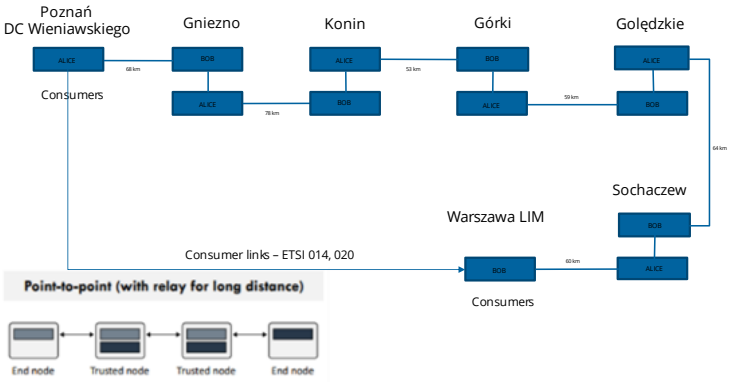


Fig. 2.3.5: PSNC intercity QKD link use case.

Testbed location:	**Poznań**	**Responsible Partner**	**PSNC**
Number of nodes	10	Number of links	5
Link Number	Length [km]	Loss [dB]	Dark/shared
1 POZ - WAR	380 km	84,56 (over 6 spans)	Dark
2 CIE - OST	75	16	Dark
3 PSNC 01 – PSNC 02	4	2	Dark
4 PSNC 01 – PSNC 02	4	2	Dark
5 PSNC 01 – PSNC 02	4	2	Dark
Use case number	**#06**	**Name**	**HPC - VSB**
Partners involved:	PSNC, VSB, THALES, ADVA		
Starting date	07.2021	End date	04.2022
No of used fibers (quantum/classical channel:	1/0 (service channel multiplexed with DWDM)		
QKD equipment used:	IDQ,	Encryptors used:	SENATAS/THALES
Comments:	Cross border QKD link operation and maintenance.		
Use case number	**#01**	**Name**	**HPC - PSNC**
Partners involved:	PSNC, IDQ, TOSHIBA, SENATAS/THALES, ADVA		
Starting date	01.2021	End date	01.2023
No of used fibers (quantum/classical channel:	1/2		
QKD equipment used:	IDQ, Toshiba	Encryptors used:	ADVA, SENATAS/THALES
Comments:	Metro inter data center link.		
Use case number	**#11**	**Name**	**Time and Frequency**
Partners involved:	PSNC, IDQ		
Starting date	06.2022	End date	01.2023
No of used fibers (quantum/classical channel:	1/2		
QKD equipment used:	IDQ	Encryptors used:	-
Comments:	Intercity backbone link with trusted node configuration.		
Use case number	**#08**	**Name**	**e-Governmnt**
Partners involved:	PSNC, TOSHIBA, ADVA		
Starting date	11.2022	End date	02.2023
No of used fibers (quantum/classical channel:	1/2		
QKD equipment used:	TOSHIBA	Encryptors used:	ADVA
Comments:	City Hall QKD link.		

2.4. **Vienna**

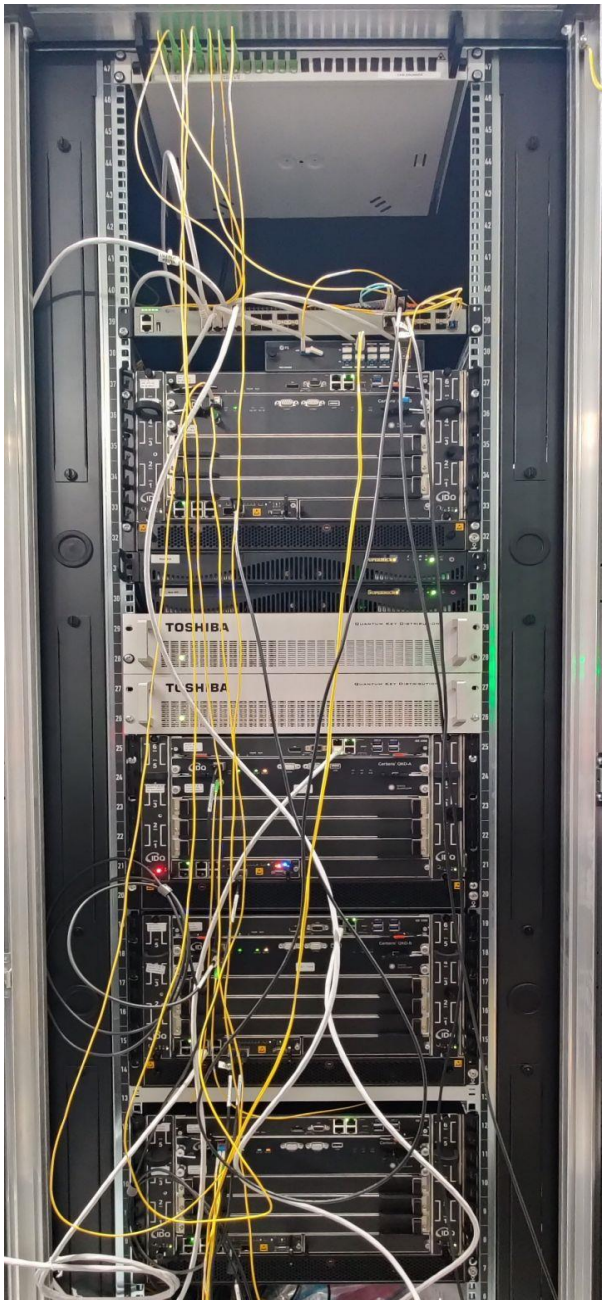


Figure 2.4.1: QKD Setup at AIT (2 systems locally and 2 Links to external locations)

The Vienna test bed has a total of 12 links that are connected using 24 pairs of fiber and a free space link. The free space link was provided by ThinkQuantum and connected a total of three locations: Alice was located at Siemens, which sent the photons over free space to AIT,

where they were converted from free space to fiber and transmitted to the VIX2 where Bob was located.

The use case “Distributed cloud storage secured by ITS QKD” connected two ministries and a data center besides the QKD Systems from IDQuantique a link from ThinkQuantum was also used, all of them together with encryptors from ADVA. At each of the ministries a fragmentiX Cluster was used to split up the data to store it at the three locations and to put then back together at a later point in time to read the files again.

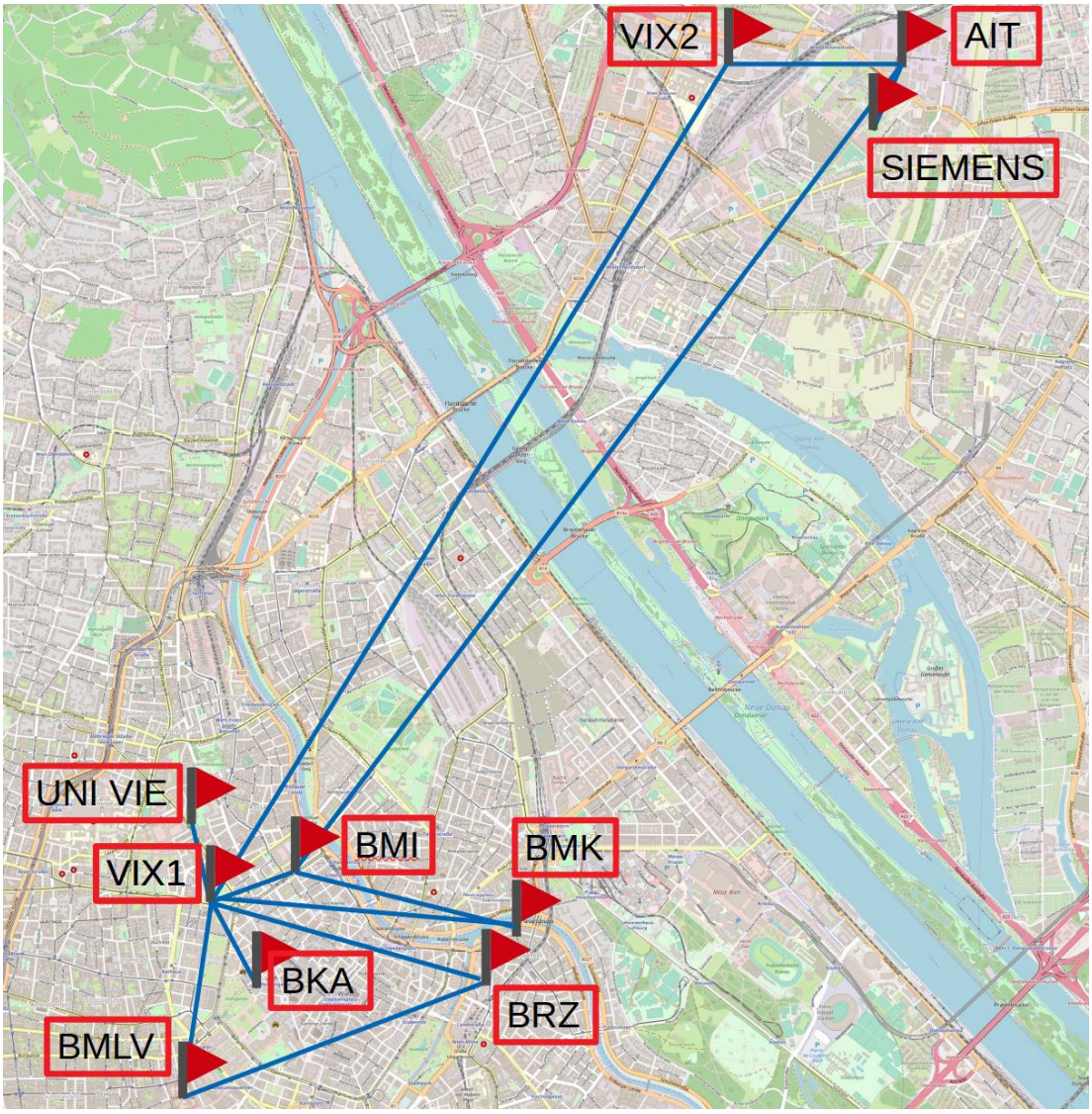


Fig. 2.4.2: Map of the Vienna network

Testbed location:	**Vienna**	**Responsible Partner**	**AIT**
Number of nodes	10	Number of links	12
Link Number	Length [km]	Loss [dB] in C-Band	Dark/shared
1 AIT – VIX2	4	1,2	Dark
2 AIT – SIEMENS	0,2	8	Freespace
3 AIT – BMI	22,3	6,6	Dark
4 VIX1 – VIX2	28	8	Dark
5 VIX1 – BKA	2,2	0,5	Dark
6 VIX1 – BMI	2,2	0,4	Dark
7 VIX1 – BMK	4,6	1,3	Dark
8 VIX1 – BMLV	5,5	2,5	Dark
9 VIX1 – BRZ	5,1	1,5	Dark
10 VIX1 – UNI VIE	4,1	1,4	Dark
11 BMI – BMK	4,1	1,2	Dark
12 BMLV – BRZ	15,4	4,3	Dark
Use case number	**#05**	**Name**	**Data encryption between governmental agencies**
Partners involved:	AIT, ADVA, Idquantique		
Starting date	05.2022	End date	11.2022
No of used fibers (quantum/classical channel:	2 1/3		
QKD equipment used:	IDQ	Encryptors used:	ADVA
Comments:	A link between BMLV and BRZ was established and govermental data was encrypted		
Use case number	**#29**	**Name**	**Distributed cloud storage secured by ITS QKD**
Partners involved:	AIT, ADVA, frX, Idquantique		
Starting date	07.2021	End date	09.2022
No of used fibers (quantum/classical channel:	6 3/9		
QKD equipment used:	IDQ, ThinkQuantum	Encryptors used:	ADVA
Comments:	Additional to the IDQ systems, a system from ThinkQuantum was used		
Use case number	**#56**	**Name**	**evolutionQ**
Partners involved:	AIT, evolutionQ, Idquantique, TEUR		
Starting date	10.2022	End date	02.2023
No of used fibers (quantum/classical channel:	Local Setup		

QKD equipment used:	IDQ, Toshiba	Encryptors used:	
Comments:	All systems are set up at AIT and the key interfaces are being accessed by evolutionQ over a VPN connection		

3. Summary and main results of the local sites

3.1. Athens

The MLNX Athens testbed consists of a set of IDQ Cerberis-3 devices connected with a 2km fiber. The QKD devices are integrated with 2x MLNX Bluefield-2 encryptors. The MLNX testbed introduces high-end datacenter nodes with state-of-the art SmartNICS that feature various accelerators for encryption and offloading support. In the next-generation datacenters the SmartNICS aim to play the important role of isolating the network from the soft-ware running on servers which further enhances security. In this context, SmartNICS can also act as the local root-of-trust devices that can authenticate and secure all local server application interactions with the datacenter network. Quantum key distribution plays an important role in this testbed, as it provides a perfectly secure out-of-band channel for key exchange, thus extending the local SmartNIC root-of-trust role, which can now deliver keys for symmetric encryption and authentication to local offloading accelerators on behalf of cryptography applications that run on the server. The testbed is shown in Figure 3.1.2 and the functional description of the system is shown in Figure 3.1.3.

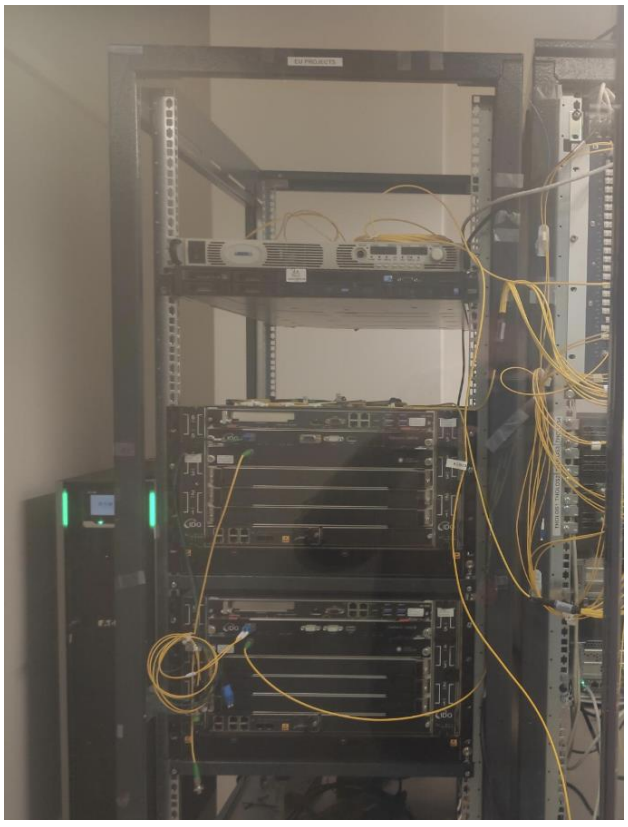


Figure 3.1.2: Athens testbed

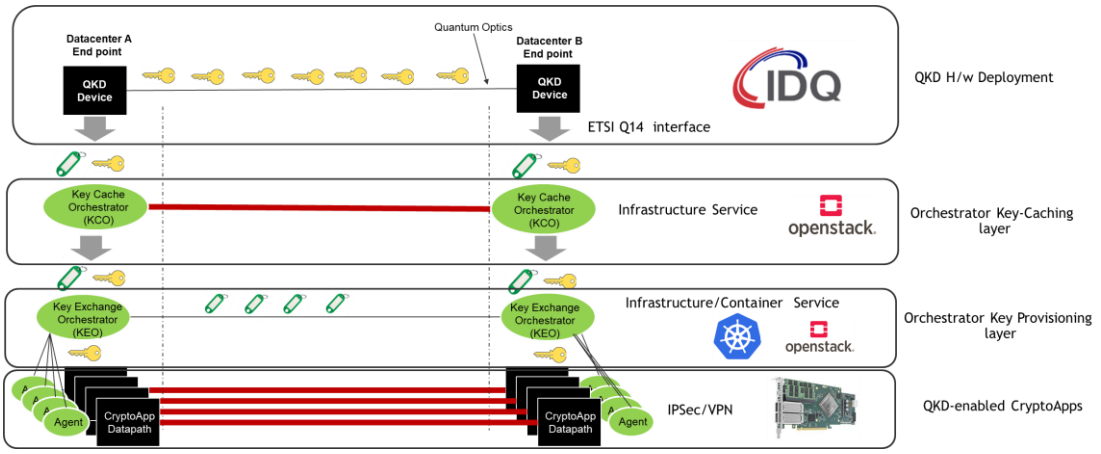


Figure 3.1.3: Functional description of the Athens testbed

Testbed location:	**Athens**	**Responsible Partner**	**Mellanox**
Number of nodes	2	Number of links	1
Link Number	Length [km]	Loss [dB]	Dark/shared
1 Bluefield A – Bluefield B	2	3,4	Dark
Use case number	**#12**	**Name**	**QKD in Cloud Datacenters**
Partners involved:	Mellanox		
Starting date	04.2021	End date	09.2021
No of used fibers (quantum/classical channel):	2/2		
QKD equipment used:	IDQ	Encryptors used:	Mellanox
Comments:			

3.2. **Barcelona**

A CV-QKD system for continuous operation, which has been developed at ICFO as part of the CiViQ project of the EU quantum flagship, was combined with high-speed QRNG technology in form of a commercial module made by Quside. Subsequently, the CV-QKD system was deployed in a field tests across a 25km fibre link between two locations in the Barcelona metropolitan area: the laboratory at ICFO and the data centre at CTTI (Center for Telecommunications and Information Technology). The field test demonstrated that the system is able to generate secret keys between both locations, and thus ready for performing the use-case demonstration. The use-case consisted of the demonstration of a secure video-conference between the two locations. A software was developed to request the keys from the QKD; the obtained keys are used with AES to encrypt the video-conference.

With use-case #32, the application of a secured video transmission across the link using the CV-QKD system of ICFO was successfully demonstrated.

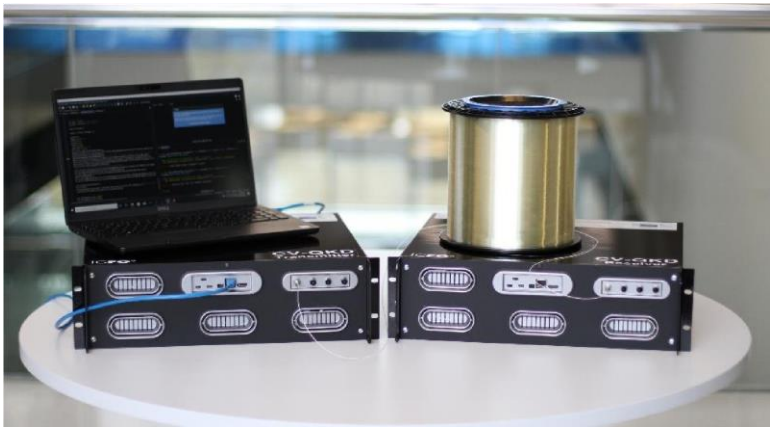


Fig. 3.2.1: Transmitter (Alice) and Receiver (Bob) with fibre spool at ICFO

Fig. 3.2.2: Transmitter installed at CTTI datacentre

Fig. 3.2.3: Map of testbed, shows locations of ICFO and CTTI in the Barcelona metropolitan area

(Images credit: ICFO)

Press release:

https://www.icfo.eu/news/2067/catalonia-pioneer-in-the-implementation-of-quantum-security-on-the-internet/

Testbed location	Barcelona
Responsible partner	ICFO
Number of nodes	2
Number of links	1

Link Number	Length [km]	Loss [dB]	Dark/shared
1 ICFO-CTTI	25	5.5	dark

Use case number:	#32
Name:	Secured video transmission
Partners involved	ICFO
Start date	03/01/2021
End date	10/09/2022
No of used fibers (quantum/classical channel	Only 1 fiber, classical channel done by TCP/IP and VPN
QKD equipment used	ICFO
Encryptors used	Software
Comments	For this demo, the video-conference software requests keys from the QKD using ETSI004 interface and encrypts the data in the application layer.

3.3. Cambridge

The Cambridge testbed has two major constituents, a long-haul fibre pair between Cambridge and London and a metropolitan fibre network within Cambridge.

The Long-haul testbed is part of our UK Quantum network connecting Cambridge with Bristol and BT Labs at Adastral Park. The section used within OpenQKD is 128 km long with 28dB of loss at 1550nm.

The Cambridge Metropolitan network comprises over 20 fibre pairs within the Cambridge area, provided by the University's own Granta Backbone fibre network, lengths vary between 2 – 20 km. Cambridge runs 4 links with Toshiba metropolitan QKD systems supporting ADVA FSP3000 based 100 Gb/s and 10 Gb/s AES encrypted classical services with QKD provided keys. There is also a key management service layer around the network.

Use case 31 Long distance QKD secured data transmission

Within the use case we implement QKD using our own Toshiba long distance QKD systems. When operating with QKD alone the link supports a secure key rate of 3.6kb/s with a QBER of 4.7%. In addition we co-propagate 100Gb/s QKD traffic along the link using our ADVA FSP3000 equipment, which ingests QKD keys from the Toshiba QKD system using an ETSI 014 standard compliant key management layer. When both QKD and 100Gb/s classical traffic are in operation we still achieve a secure key rate of 2.1kb/s with a QBER of 5.7%. Results from 120 days of operation with and without classical traffic are shown in figure 3.3.1.

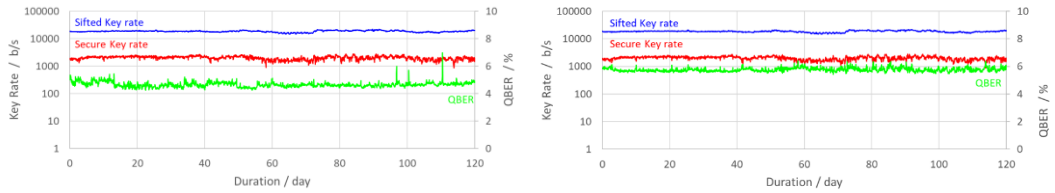


Figure 3.3.1: 120 day operation of the 128km 28dB loss Cambridge to London link, left: QKD alone, right: QKD with 100Gb/s data traffic.

We use this system to enable remote back up of research date and magnetic resonance images provided by the University of Cambridge medical school. Images are securely transmitted from our West Cambridge Data Centre to the Telehouse North datacentre in London Docklands. Figure 3.3.2 shows a schematic of the Use case 31 within the Cambridge network

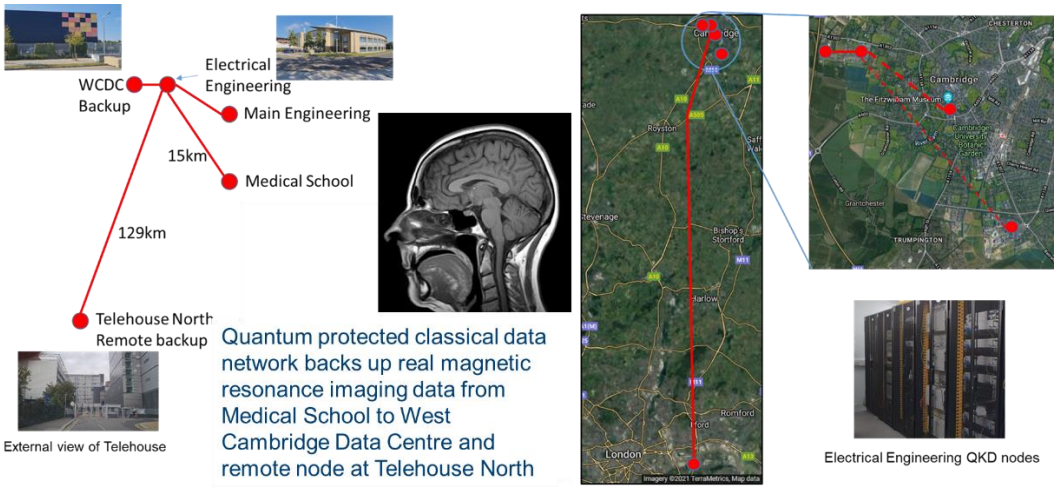


Figure 3.3.2: Schematic of the Cambridge to London network for Use Case 31

Use Case 30 - Demonstrate protection of medical data in transit (QKD) and at rest (Shamir secret sharing) within metro network

This use case uses the Cambridge metropolitan network with fibre routes of 5-20km to facilitate the protection of medical data from the Cambridge Biomedical Campus while in transit to the Cambridge Science Park and the West Cambridge Data Centre. This is achieved by the use of QKD from Toshiba with ADVA 10Gb/s encrypted classical data transport. While at rest it is secured by Shamir secret sharing systems from Fragmentix. Figure 1 shows a schematic layout of the use case

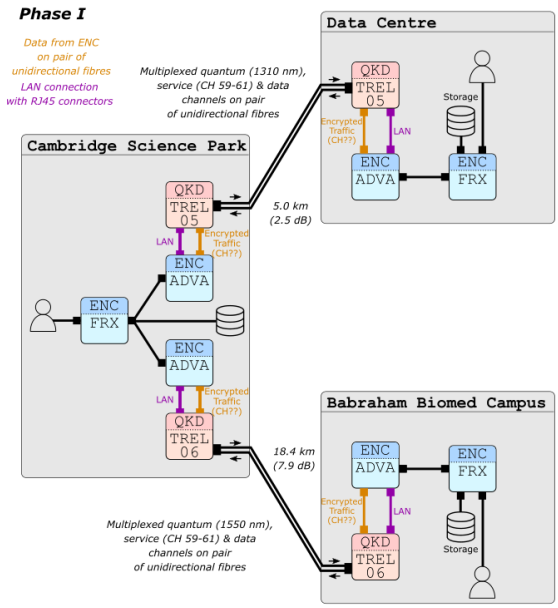
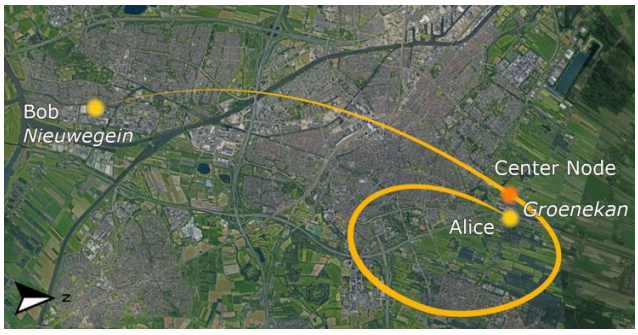


Figure 3.3.3: Schematic of the 3 nodes of Use case 30, deployed on the Cambridge metropolitan network.

Toshiba will provide the equipment for this use case by mid February and it will run until the end of OpenQKD and as long beyond as possible.

3.4. **Delft**



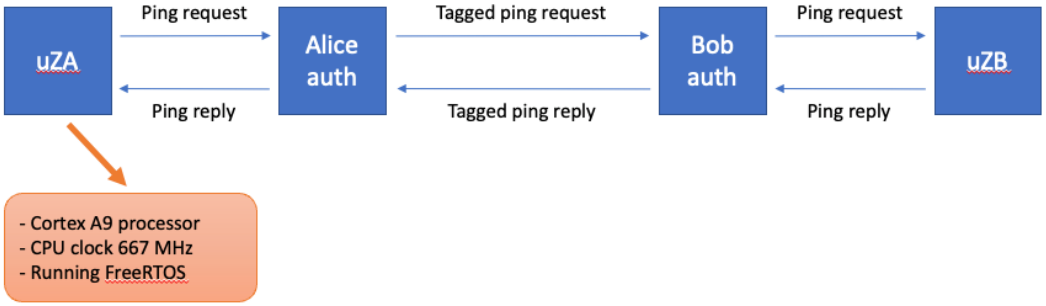
We let MicroZed-Alice (uZA) send ping requests to MicroZed-Bob (uZB) for a longer period of time to test the reliability of the authentication proxy.

We measured round-trip time (RTT) statistics by collecting timestamps of ping requests and ping replies on uZA.

Key Points :

- Total duration of the experiment: 7 full days
- Interval between two consecutive ping requests: 12 seconds (5 messages per minute)

- Total number of ping requests sent: 50400
- Total number of ping replies received: 50395 (only 5 ping requests did not receive a reply)
- Raw size of a ping request message: 45 bytes (16 bytes of Ethernet header + 20 bytes of IP header + 8 bytes of ICMP header + 1 byte of payload data)
- Raw size of a ping reply message: 45 bytes (same as for ping request)
- MAC used: VMAC with 21-bit tags



Mark-3 QKD System : 4,470,321 bits (1766 kB) of key were generated in total during the experiment. Total Time for the run was exactly 1 week. For key material in store, 21 bits consumed when sending, another 21 bits when replying. Key store contents calculated based on measured amount of key created, minus 42 bits subtracted at every ping request

3.5. **Geneva**

Fig. 3.5.1: QKD device and encryptors installed at SIG Headquarter

3 Use cases ran in Geneva with different applications:

- Datacenter 10G Ethernet point-to-point link with production data. It proved the feasibility of having standard Datacenter link encrypted and running stable. The link ran successfully without any impact on real data, during 2 months. No particular challenge for this use case. It highlighted nevertheless the importance of training before operations since the NMS Key values are not the standard on the telecom market.
- Quantum Vault : This use case demonstrated the use of QKD for securing sensitive data (Private Keys) at rest by combining Shamir Secret Sharing with One Time Pad and QKD for the communication between the 6 storage nodes located in Geneva Datacenters. Standard telecom fibers have been provided by SIG. The network was setup in one week with the great support of the optical engineer of SIG. Mt pelerin specialized in digital asset management was able to implement the Quantum Vault software prototype over Raspberry Pie interfacing and requesting keys to the QKD nodes using the ETSI REST API QKD014.
- Customer point to point (initial Smartgrid): 1G ethernet point to point link for business customer. It prooved the importance of physical environment: temperature, rack space, cleanliness of the space. It also proved the need of encrypting only dedicated links, not mutualized networks, such as MPLS point to point link. The initial use case was planned for Smartgrid. Yet, 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. Therefore, the use changed 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.

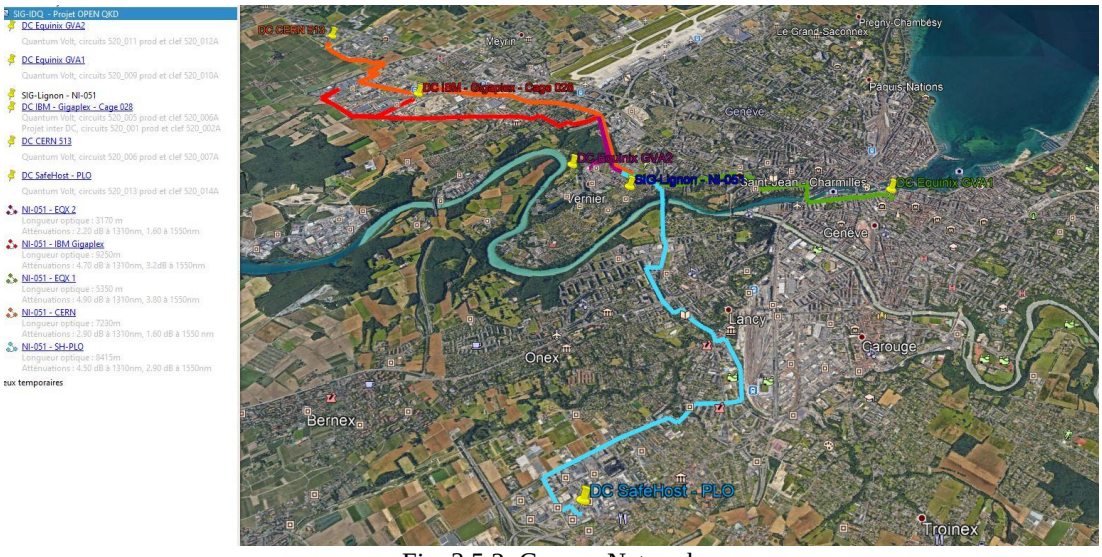


Fig. 3.5.2: Geneva Network

Testbed location:	**Geneva**	**Responsible Partner**	**SIG**	
Number of nodes	6	Number of links	14	
Links PFO: pair of fibres SC: Service Channel QC: Quantic Channel	Length [km]	Loss [dB]	Dark/shared	
Ni51–Gigaplex, 4 PFO: 1 PFO for SC, 1 PFO for MUX, 2 PFO for QC	9.250	4.70 dB at 1310 3.20 dB at 1550	Dark	
Ni51–Safehost, 2 PFO: 1 PFO for SC1, PFO for QC	8.415	4.50 dB at 1310 2.90 dB at 1550	Dark	
Ni51–Equinix 1, 2 PFO: 1 PFO for SC , 1 PFO for QC	5.350	4.90 dB at 1310 3.80 dB at 1550	Dark	
Ni51–Equinix 2, 2 PFO: 1 PFO for SC, 1 PFO for QC	3.170	2.20 dB at 1310 1.60 dB at 1550	Dark	
Ni51 – CERN, 2 PFO: 1 PFO for SC, 1 PFO for QC	7.203	2.90 dB at 1310 1.60 dB at 1550	Dark	
Ni51 – Business Customer site, 2 PFO: 1 PFO for SC, 1 PFO for QC	13.800	6.90 dB at 1310 6.2 dB at 1550	Dark	

Use case number	**14**	**Name**	**SIG Datacentre**	
Partners involved:	IDQuantique, SIG			
Starting date	01.2020	End date	12.2020	
No of used fibers (quantum/classical channel:	2 PFO (1 PFO and 1 single fibre effectively used)			
QKD equipment used:	IDQ01	Encryptors used:	Adva FSP3000 10G	
Comments:	Quantum and production channels up and running with real data during 2 months (10-12.2020)			

Use case number	**3**	**Name**	**Quantum Vault**	
Partners involved:	Mt-Pelerin	IDQuantique	SIG	
Starting date	03.2020	End date	12.2020	

No of used fibers (quantum/classical channel:	10 PFO (5 PFO and 5 single fibres effectively used)		
QKD equipment used:	IDQ02, IDQ03, IDQ04, IDQ05, IDQ06	Encryptors used:	
Comments:	Quantum and production channels are up and running. Key distribution (splitting) is working with success.		

Use case number	**02**	**Name**	**Business customer point to point (initial SmartGrid)**	
Partners involved:	ID Quantique, SIG			
Starting date	11.2021	End date	01.2022	
No of used fibers (quantum/classical channel:	2 PFO (1 PFO and 1 single fibre effectively used)			
QKD equipment used:	IDQ02 – IDQ03	Encryptors used:	Cisco 4451-X hardware running IOS- XE >= 17.2	
Comments:	Business customer point to point link encrypted up and running.			

3.6. **Graz**

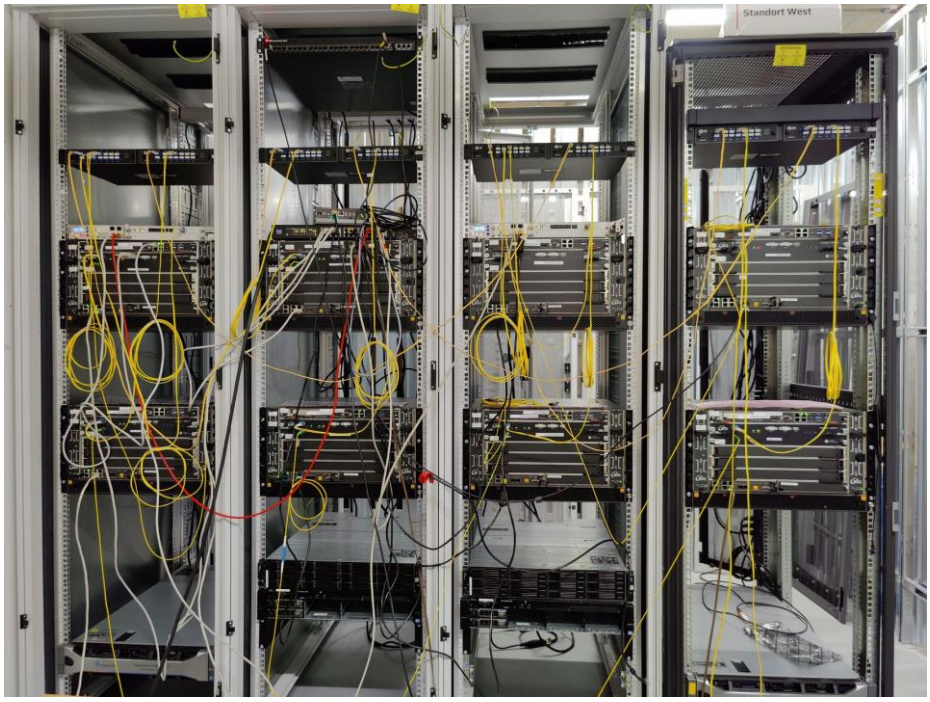


Figure 3.6.1: Configuration Setup at fragmentiX headquarter

In the OpenQKD demonstration, Whole Slide Imaging data from digital pathology together with genome data have been split into three fragments with the requirement to combine two fragments to retrieve full information. Each of the three single fragments alone do not contain enough information to access the original data. These three fragments have been stored at different locations, whereby two have been stored outside of the Medical University in data centers protected with access control and video surveillance methods. This method outperforms nowadays disaster recovery or protection against single-point failures like fire and unforeseeable events in datacenters because no complete copy of all sensitive data is stored at a single cloud storage believed to be secure.

Testbed location:	**Graz**	**Responsible Partner**	**AIT**
Number of nodes	4	Number of links	4
Link Number	Length [km]	Loss [dB] in C-Band	Dark/shared
1 MUG – DCN	9	4,2	Dark
2 MUG – DCS	8,9	3,3	Dark
3 LKH – DCN	19,9	6,8	Dark
4 LKH – DCS	11,8	4,4	Dark

Use case number	**#21**	**Name**	**ITS securing sensitive medical data at rest and in transit**
Partners involved:	AIT, ADVA, Idquantique, Toshiba		
Starting date	06.2021	End date	01.2022
No of used fibers (quantum/classical channel:	8 4/12		
QKD equipment used:	IDQ, TEUR	Encryptors used:	ADVA
Comments:	Data was split into 3 parts with 2 of those packages being secured in transport using QKD		

3.7. **Oberpfaffenhofen / Matera**

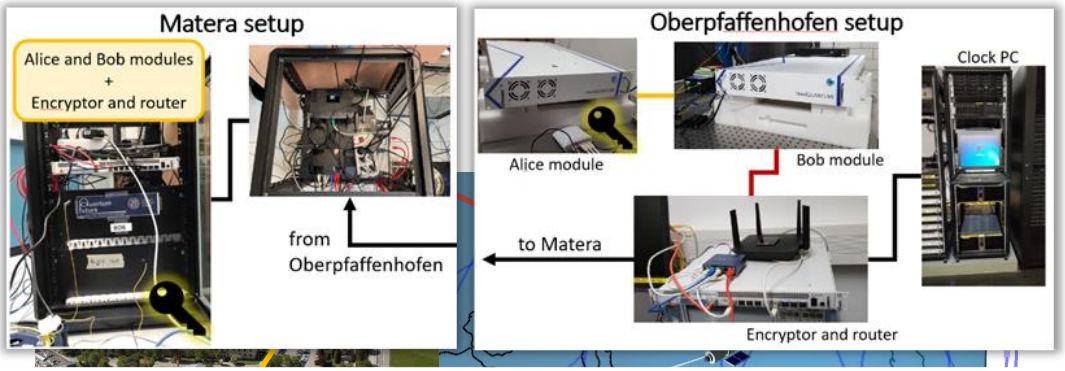
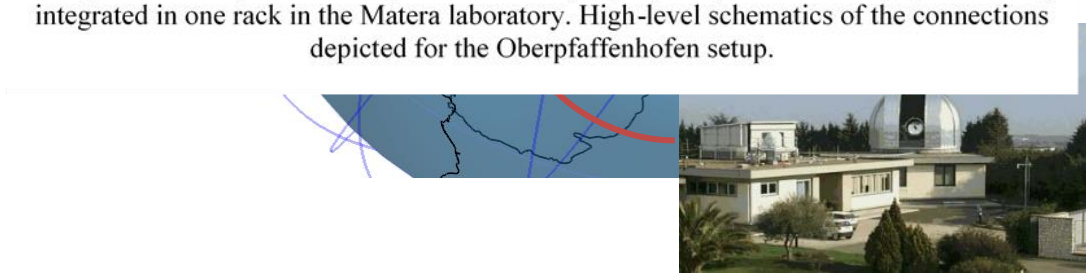


Figure 1: Equipment employed in the demonstration of OPENKD use-case #23. On the left, the setup for the last-mile QKD link in Matera, on the right the setup for the link in Oberpfaffenhofen; the two setups are essentially equal, except for all the equipment being integrated in one rack in the Matera laboratory. High-level schematics of the connections depicted for the Oberpfaffenhofen setup.



The OPENQKD use-case 23 has showcased long-distance QKD-secured transfer of clock synchronization data. The data was generated by simultaneously measuring time differences between the clocks present at in the laboratories in Matera and in Oberpfaffenhofen and the time signal received from Galileo, the European Global Navigation Satellite System. The data was collected at the two locations, encrypted with quantum generated keys and transferred over the internet by creating a virtual local subnet. The long-haul connection between the two labs (which are located more then 900km apart) has not been directly implemented, but we have shown that employing upcoming QKD satellites and the currently existing optical ground stations (OGS) in Matera and Oberpfaffenhofen it will be possible to establish such a link. The experimental QKD demonstration involved two last-mile connections at the two sites, as required to bridge the distance between the OGS and the time laboratories.

Testbed location 1	**Matera**	**Responsible Partner**	**UNIPD**
Testbed location 2	**Oberpfaffenhofen**	**Responsible Partner**	**DLR**
Number of nodes	4	Number of links	2
Link Number	Length [km]	Loss [dB]	Dark/shared
1 Oberpfaffenhofen	0,5	1	Dark
2 Matera	10	8	Dark
Use case number	**#23**	**Name**	**Globally securing space and ground infrastructure**
Partners involved:	DLR, UNIPD, Rohde&Schwarz		
Starting date	7.11.2022	End date	11.11.2022
No of used fibers (quantum/classical channel:	(1/0 in Matera + 1/1 in Oberpfaffenhofen)		
QKD equipment used:	UNIPD/ThinkQuantum	Encryptors used:	Rohde&Schwarz
Comments:	Two independent last-mile connections implemented, long-haul connection emulated, transmission of encrypted data over the internet with IPv3 protocol for creation of a virtual local subnet. The last-mile connection in Matera has been implemented via a QKD system realized in-house by UNIPD. The last-mile connection in Oberpfaffenhofen has been implemented via a QUKY system lent by ThinkQuantum srl (UNIPD spin-off).		

3.8. **Ostrava**

PSNC and VSB in Ostrava implemented and tested the HPC use case UC06 using cross-border dark fiber connection between Poland and Czech Republic. The use case was implemented and running between July 2021 – April 2022 and involved two phases. In the first phase partners installed, integrated and verified operation of the QKD link between PSNC PIONIER network node in Cieszyn, Poland and VSB node in computer center in Ostrava, Czech Republic. QKD link was implemented using IDQ Cerberis 3 devices and IDQ CN6100 10G encryptors. Quantum channel was implemented using dedicated dark fiber between Cieszyn and Ostrava provided by CESNET – National Research and Education Network. The service channel between the QKD devices was running within CESENT DWDM system spectrum. The Figure 1, 2 and 3 present overall physical QKD link implementation.

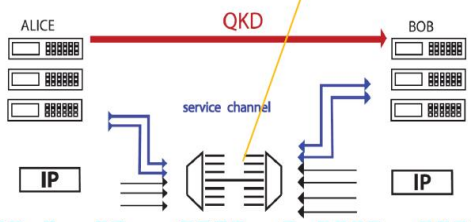
The final step for QKD link configuration was focused on the management software for both – encryptors and QKD devices. For this purpose, PSNC installed dedicated Virtual machine that was used for monitoring and maintenance of the encryptors and QKD devices. The virtual machine was installed in Poznań and used dedicated VLAN service in PIONIER network for connecting to the QKD device in Cieszyn and Ostrava. To achieve cross-border QKD management capability PSNC and CESNET set up a dedicated VLAN that was exchanged between the operators using own peering service and interface.

Fig. 3.8.1; The cross-border link between Ostrava (CZ) and Cieszyn (PL).

cesnet

TRIAL PREPARATION

- First intercity and international trial in CZ
- Ostrava Cieszyn line – fibre itself 75km, 16 dB
- QKD channel in 1550 nm band, will be disturbed by parallel traffic
- Line is very close to maximum system performance
- QKD system „fibre hungry“, service OOK channel will consume 2 additional optical channels
- Offer for aditional fibre pair uncompetitive
- All data (incl. QKD service channel) moved into bidi DWDM



Testbed location:	**Ostrava**	**Responsible Partner**	**VSB**
Number of nodes	2	Number of links	1
Link Number	Length [km]	Loss [dB]	Dark/shared
1 CIE - OST	75	16	Dark
Use case number	**#06**	**Name**	**HPC - VSB**
Partners involved:	PSNC, VSB, THALES, ADVA		
Starting date	07.2021	End date	04.2022
No of used fibers (quantum/classical channel:	1/0 (service channel multiplexed with DWDM)		
QKD equipment used:	IDQ,	Encryptors used:	SENATAS/THALES
Comments:	Cross border QKD link operation and maintenance.		

Using the installed infrastructure it was possible to perform additional activities in the testbed that were published under several publications: “Quantum Channel Characteristics from the Point of View of Stability” , “Measurements of Cross-Border Quantum Key Distribution Link” and “First cross border trial of quantum key distribution sharing fiber”.

3.9. **Padova**

For the field-trials realized in the Padova testbed UNIPD developed in-house 3 pairs of fiber-based QKD devices exploiting 3-state 1-decoy efficient BB84 protocol with polarization encoding, two systems working at 1550 nm and one system working at 1310 nm. UNIPD also developed a free-space system comprising a transmitter and a receiver with single-mode-fiber coupling capabilities for working in daylight. The developed systems are compatible with ETSI004 and ETSI014 standards, and have been tested with R&S and ADVA encryptors. By using the nodes reported in Table 3.9.1 UNIPD performed the following trials exploiting the QKD hardware realized in-house:

1. QKD test with quantum and classical signals into two separate dark fibers using the links 1 and 6
2. QKD test with coexistence of quantum and classical communication into the same fiber using the links 2 and 6. See Fig. 3.9.2.
3. QKD test with intermodal free-space/fiber channel using the combination of links 3 and 4 (Use-Case 24). See Fig. 3.9.2.

UNIPD also tested the ThinkQuantum (UNIPD spin-off) QUKY system adapted for being used with SNSPD detectors by exploiting the link 5 in a two-way (CNR-DEI-DFA-LNL-DFA-DEI-CNR). UNIPD also tested QUKY with R&S and ADVA encryptors in the DEI-CNR link.

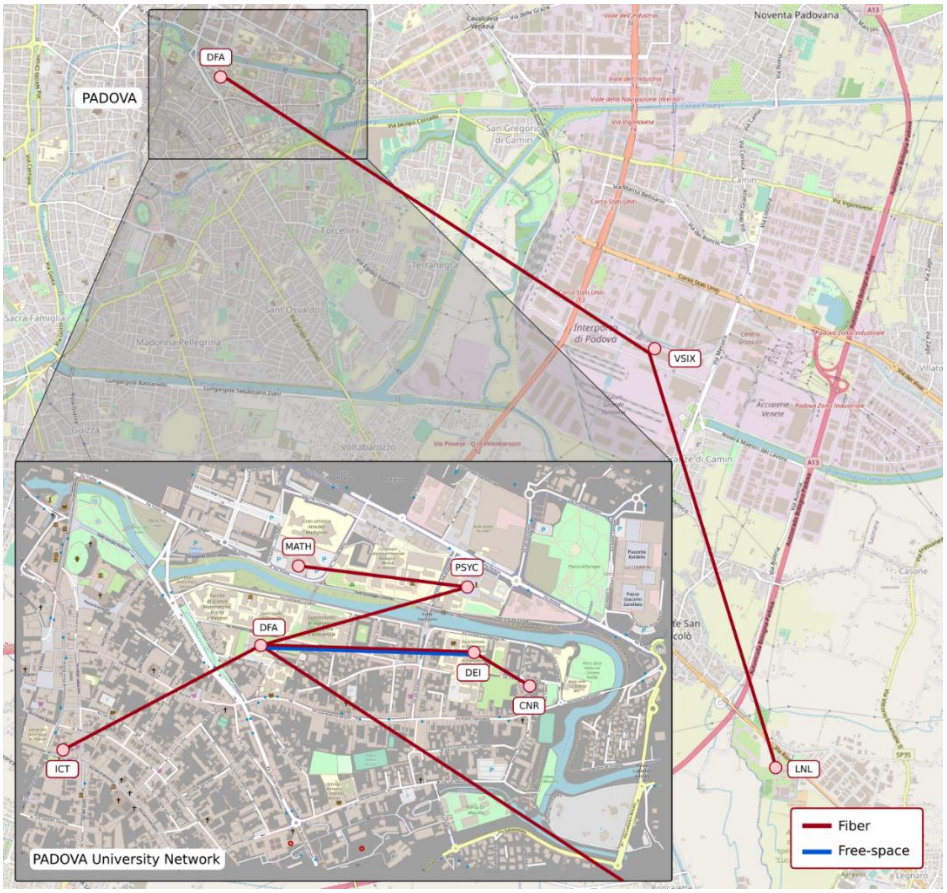


Figure 3.9.1: map of the Padova testbed

Figure 3.9.2: pictures of the QKD devices for fiber (left) and free-space (right) links used in Padova testbed.

Table 3.9.1 presents some data about the links of the Padova testbed shown in Fig. 3.9.1.

Testbed location:	**Padova**	**Responsible Partner**	**UNIPD**
Number of nodes	8	**Number of links**	6
Link Number	**Length [km]**	**Loss [dB]**	**Notes**
1 ICT-DFA-PSYC-MATH	3.4	9	2 dark fibers (1 quantum + 1 classical)
2 ICT-DFA-VSIX	13	6.7	1 dark fiber for both quantum and classical
3 DFA-DEI	0.660	~10	Free-space link
4 DEI-CNR	0.5	0.5	4 dark fibers
5 CNR-DEI-DFA-LNL	~18	11	2 dark fibers
6 ICT-VSIX	13	6	2 dark fibers
Use case number	**#24**	**Name**	**Interfacing satellite and terrestrial QKD**
Partners involved:	UNIPD		
Starting date	21/03/2022	End date	31/03/2022
No of used fibers	2		

QKD equipment used:	1 free-space QKD system realized in-house 1 QUKY system from ThinkQuantum srl	Encryptors used:	none
Comments:	We implemented 2 scenarios: 1) untrusted: intermodal link DFA-(DEI)-CNR, in which DFA-DEI in free-space and DEI-CNR in fiber with Alice at DFA and Bob at CNR 2) trusted: one free-space link DFA-DEI + one fiber link CNR-DEI with two Alices sharing the same Bob placed at DEI		

Table 3.9.1: Padova testbed data.

3.10. **Paris**

Fig. 3.10.1 QKD devices and fibres installed at the CNRS-Sorbonne Université LIP6 laboratory in Paris.

The Paris quantum communication testbed is composed of 4 nodes, two in Paris (located at University labs in the 5th and 13th districts of Paris, LIP6 and MPQ respectively), one at the location of Orange Innovation in Châtillon, at the outskirts of Paris, and one at the University lab of Télécom Paris in Palaiseau, in the Saclay area outside Paris. Several nodes will soon be added in the Paris-Saclay region (near Palaiseau). The links are composed of two low-loss dark fibres (except for the LIP6-MPQ link, which only has one fibre and where a second one will be added shortly). The infrastructure hence allows to test QKD devices requiring two fibre channels. A demonstration of an encrypted video exchange using QKD devices from IDQ and encryptors from Thales was realized during *Salon de l'Innovation* of Orange (internal exhibition of Orange's innovative work) in October 2022. Future demonstrations of use cases include CV-QKD, entanglement distribution and quantum memories. The demonstration was also supported by the Ile-de-France region project ParisRegionQCI.

Fig. 3.10.2 Map of the testbed:

Testbed location:	**Paris**	**Responsible Partner**	**CNRS**
Number of nodes	4	Number of links	5
Link Number	Length [km]	Loss [dB]	Dark/shared
1 LIP6 - OrangeInnovation	14	3,77	Dark
2 LIP6 - OrangeInnovation	14	3,82	Dark
3 OrangeInnovation - Telecom	43	10,4	Dark
4 OrangeInnovation - Telecom	43	10,4	Dark
5 LIP6 - MPQ	7,1	9,8	Dark
Use case number	**04**	**Name**	**Secure links between universities in greater Paris area**
Partners involved:	CNRS, Orange Innovation, IDQ, Thales SIX		
Starting date	05.2022	End date	02.2023
No of used fibers (quantum/classical channel:	Quantum channel: fiber #1 Classical channel: fiber #2		
QKD equipment used:	IDQ Cerberis	Encryptors used:	Thales Mistral
Comments:	Exchange of quantum encrypted video during Salon de l'innovation of Orange.		