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

Report on testbed replicability and performance

Deliverable: **D8.3**	Lead: UNIPD
Project month: M18	28 February 2021
Work package: WP8	Task: T8.3
Type: Report	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/.

Copyright Statement

Document Information

Author List

Organization	Name	E-mail
UNIPD	Francesco Vedovato	francesco.vedovato@dei.unipd.it
UNIPD	Paolo Villoresi	paolo.villoresi@dei.unipd.it
UNIPD	Giuseppe Vallone	giuseppe.vallone@dei.unipd.it
AIT	Florian Kutschera	florian.kutschera@ait.ac.at
TID	Victor Lopez	victor.lopezalvarez@telefonica.com
UPM	Vicente Martin	vicente@fi.upm.es
UPM	Jose Luis Rosales Bejarano	jose.rosales@fi.upm.es
PSNC	Rydlichowski Piotr	prydlich@man.poznan.pl
DTAG	Marc Geitz	marc.geitz@telekom.de

Reviewer List

Organization	Name	E-mail
RSCS	Stefan Röhrich	stefan.roehrich@rohde-schwarz.com
TPT	Romain Alléaume	romain.alleaume@telecom-paris.fr

Version History

Version	Date	Reason/Change	Editor/s
0.1	12. 10. 2020	Initial version	Francesco Vedovato
0.2	16. 11. 2020	First iteration, with inputs from partners of T8.3	Francesco Vedovato
0.3	08. 02. 2021	Second iteration, with inputs from partners of T8.3	Francesco Vedovato
0.4	23. 02. 2021	Third iteration, after inputs from PI	Francesco Vedovato
1.0	01. 03. 2021	Submitted version, after reviewers' comments	Francesco Vedovato

Executive Summary

This report presents to the general public what OPENQKD aims to realize and demonstrate in its four main testbeds, which are located in Berlin, Madrid, Poznam and Vienna. For each testbed, a formal description with targeted use-cases is presented. This document represents the starting point and the key ingredients for the implementation of the testbeds, whose actual development and results will be detailed in following deliverables.

Table of Contents

Executive Summary 4

1. Introduction 7

1.1. Purpose and scope of the document 7

1.2. Target Audience 7

1.3. Relation to other project work 7

1.4. Structure of the document 8

2. Berlin testbed 9

2.1. Formal description 9

2.2. Use-cases involved 10

3. Madrid testbed 14

3.1. Formal description 14

3.2. Use-cases involved 16

4. Poznam testbed 25

4.1. Formal description 25

4.2. Use-cases involved 26

5. Vienna testbed 37

5.1. Formal description 37

5.2. Use-cases involved 38

6. Remarks and conclusions 42

List of Figures

Figure 1: Map of Berlin testbed 9
Figure 2: UC-27 schematic. 11
Figure 3: UC-28 schematic. 13
Figure 4: Map of Madrid testbed 14
Figure 5: UC-15 schematic. 17
Figure 6: UC-16 schematic. 18
Figure 7: UC-17 schematic. 19
Figure 8: UC-18 schematic. 21
Figure 9: UC-25 schematic. 23
Figure 10: UC-26 schematic. 24
Figure 11: Map of Poznam testbed 25
Figure 12 : UC-01 schematic. 27
Figure 13: UC-06 schematic. 28
Figure 14: UC-07 schematic. 30
Figure 15: UC-08 schematic. 31
Figure 16: UC-09 schematic. 33
Figure 17: UC-10 schematic. 34
Figure 18: UC-11 schematic. 36
Figure 19: Map of Vienna testbed 37
Figure 20: UC-05 schematic. 39
Figure 21: UC-19 schematic. 40
Figure 22: UC-20 schematic. 41

Abbreviations and Acronyms

KPI	Key Performance Indicator
UC	Use Case
TBD	To Be Defined
QKD	Quantum Key Distribution
WP	Work Package

1. Introduction

1.1. Purpose and scope of the document

OPENQKD aims at bringing together a multidisciplinary team of the leading European telecommunication equipment manufacturers, end-users and critical infrastructure providers, network operators, QKD equipment providers, digital security professionals and scientists from 13 countries to reinforce Europe's position at the forefront of quantum communication capabilities globally. The project will create an open QKD testbed to promote network functionality and use-cases to potential end-users and relevant stakeholders from research and industry. Over 25 use-case trials have already been determined and will be complimented by open calls for funding third parties.

OPENQKD also aims at developing an innovation ecosystem and training ground, as well as helping to grow the technology and solution supply chains for quantum communication technologies and services. The OPENQKD network will be used to demonstrate the transparent integration of quantum-safe technologies and solutions broadly across the European digital landscape as well as advancing initiatives for the standardization and certification of QKD-enabled technologies.

The work in the OPENQKD testbed should lay the foundations for rolling out a pan-European quantum-safe digital infrastructure, with a solid basis to educate and lead a quantum-aware workforce and with European industry leaders already engaged.

The four OPENQKD main testbeds will be located in Berlin, Madrid, Poznam and Vienna. The purpose of Deliverable D8.3, entitled *Report on testbed replicability and performance*, is to publicly present the core ideas underlying each OPENQKD testbed and the use-cases involved, in order to have a synthetic but global overview of the project cornerstones.

1.2. Target Audience

This deliverable is *public,* and it will be made accessible via the OPENQKD website (https://openqkd.eu/). D8.3 is meant to give an overview of the OPENQKD testbeds: each testbed will provide its formal description, with the specification of involved OPENQKD partners, the targeted applications, the description of active use-cases, and the network. The target audience of this deliverable comprises not only the project partners, but also all the subjects that are interested in knowing the state-of-the-art of QKD technologies in Europe. We hope that such an audience will include the scientific community at large, the industry not participating in the project, policy and decision makers and the general public aware of European research and innovation in quantum technologies and quantum communication.

1.3. Relation to other project work

D8.3 is an outcome of Task 8.3, which builds on outputs of WP6 (*Quantum Network Functionality*), WP7 (*Deployment and Operation of QKD Testbeds*) - in particular T6.5 (*Support for Performance Evaluation and Metrics*) T7.2 (*Integration in classical network, co-existence of quantum and classical channels, network functionality*) and T7.3 (*Interoperability and benchmarking*) - and task T8.1 (Definition of network evaluation and performance) of WP8 (*Evaluation of Network Functionality and Performance*). Task 8.3 is an iterative task, repeated before each one of the field trial campaign and so it will interact with T8.4 (*Field trial execution and repeatability*).

1.4. Structure of the document

This report is structured as follows:

- Section 2 to 5 provide the formal description of each testbed, with a presentation of the planned use-cases (only the ones that will be implemented in the testbeds);
- Section 6 provides some concluding remarks.

2. Berlin testbed

2.1. Formal description

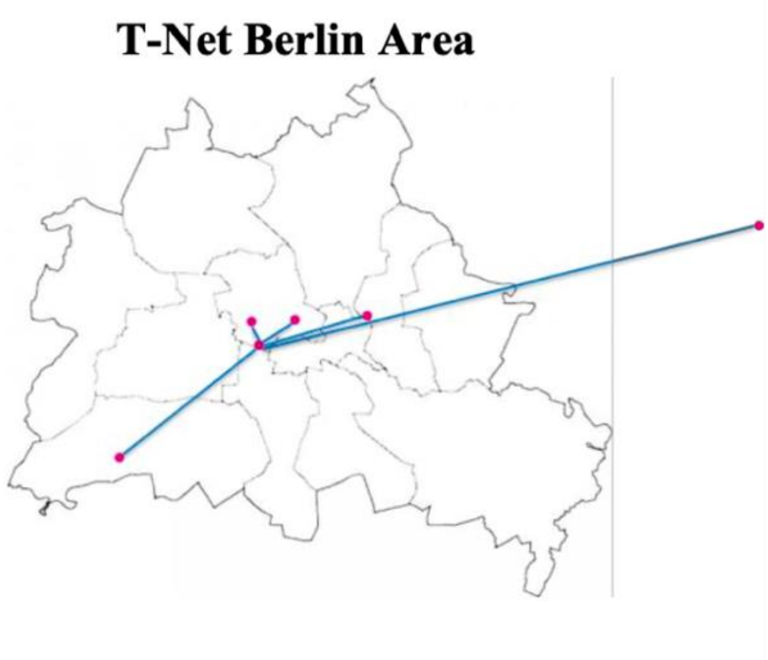


Figure 1: Map of Berlin testbed

The OpenQKD Testbed Berlin is focused on building the target architecture for Deutsche Telekom to support upcoming introductory QKD projects.

The testbed is located in an integration lab site at Winterfeldstrasse in Berlin, sharing site with 5G, fiber and ORAN laboratories. The laboratory is connected to a great number of different fiber lines, which can be used and configured on demand. Various network topologies for quantum and classical channels can be realized. Each network node of the laboratory consists of a dedicated 19” cabinet housing the quantum optical equipment, firewalls, encryptors, virtualized servers and a Hardware Security Module (HSM) for key storage. The networks between the cabinets are well separated and can be seen as unsecure network connections. Internet access and remote access is possible for each partner, based on an authentication and authorization concept.

Following the goals of the use cases, the lab consists of

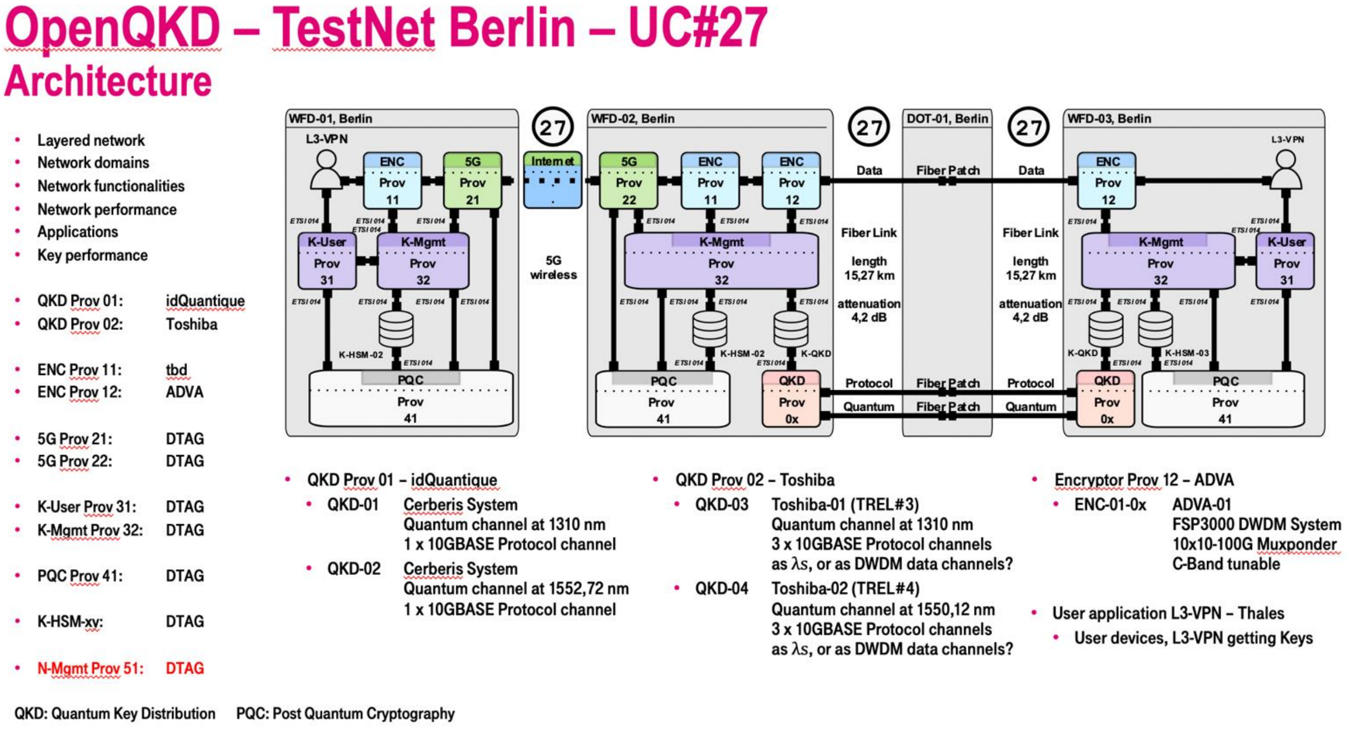
1. Full virtualized server infrastructure that allows flexible assignment of resources for the use case execution
2. Dynamic assignment of network resources
3. 5G connection to demonstrate the integration of mobile networks in a QKD setup

<table>
<tr><td>Testbed name:</td><td>OpenQKD Testbed Berlin</td></tr>
<tr><td>Location:</td><td>Berlin, Germany</td></tr>
<tr><td>Partner responsible / Host:</td><td>Deutsche Telekom AG (DTAG)</td></tr>
<tr><td>Partner(s) involved:</td><td>IDQuantique, Toshiba
Adva Optical, Rohde & Schwarz, Thales</td></tr>
<tr><td>Applications / Collector for:</td><td>1. Integration of QKD into telecommunication networks and early realization of a target architecture.</td></tr>
<tr><td>Use cases involved:</td><td>UC27, UC28</td></tr>
<tr><td>Network topology:</td><td>The network topology is use-case dependent</td></tr>
<tr><td>Nodes:</td><td>3 nodes, labelled Lab1, Lab2, Lab3</td></tr>
<tr><td>Links:</td><td><table>
<tr><th>Link</th><th>Length [km]</th><th>Loss [dB]</th></tr>
<tr><td>1 Lab1 – Lab2</td><td>TBD</td><td>TBD</td></tr>
<tr><td>2 Lab2 – Lab3</td><td>TBD</td><td>TBD</td></tr>
<tr><td>3 Lab1 – Lab2 (5G mobile network lni)</td><td>-</td><td>-</td></tr>
</table></td></tr>
<tr><td>Network functions:</td><td>• Network key distribution and management
• Data Center Infrastructure
• Multiple layer interworking
• Multiple vendor interoperability
• Dark fibers and DWDM systems
• Modular MAN and WAN network architecture and systems</td></tr>
</table>

2.2. Use-cases involved

Identifier Number:	UC-27
Name:	Using post-quantum cryptography (PQC) / quantum-resistant-algorithms (QRA) to additionally secure the QKD Key Management Layer, the transport layer and to extend the network to a 5G radio cell
Partner(s) involved:	Deutsche Telekom, Adva Optical, Rohde & Schwarz, Thales IDQuantique, Toshiba
Starting/End date:	01.07.2020/30.06.2021
QKD equipment used:	IDQ-12 (C-Band), IDQ-14(O-Band) TRELQKD-LD (C-Band), TRELQKD-MU (O-Band)
Encryptors used:	Thales, 4x Mistral Network Security (VPN) 4x Adva SFP3000 10TCE

Link(s) of the testbed network used:	Lab1 – Lab2, Lab2 – Lab3, 5G radio link
Brief description of UC purpose/scope:	While the combination of QKD and symmetric encryption is used to secure the communication among applications along the core fiber networks, the communication across future 5G wireless networks is unique within this project. This use case proposes an integration of core fiber and 5G access networks, where the fiber sections are secured by QKD and the 5G services are secured by post-quantum cryptography (PQC). As a result, telecommunication services (voice, video, data or chat) will be secured by both quantum secure encryption method to allow telco operators to make use of the optimum security level to secure their confidentiality asset.



OpenQKD – TestNet Berlin – UC#27

Architecture

- Layered network
- Network domains
- Network functionalities
- Network performance
- Applications
- Key performance

QKD Prov 01:	idQuantique
QKD Prov 02:	Toshiba
ENC Prov 11:	tbd
ENC Prov 12:	ADVA
5G Prov 21:	DTAG
5G Prov 22:	DTAG
K-User Prov 31:	DTAG
K-Mgmt Prov 32:	DTAG
PQC Prov 41:	DTAG
K-HSM-xy:	DTAG
N-Mgmt Prov 51:	DTAG

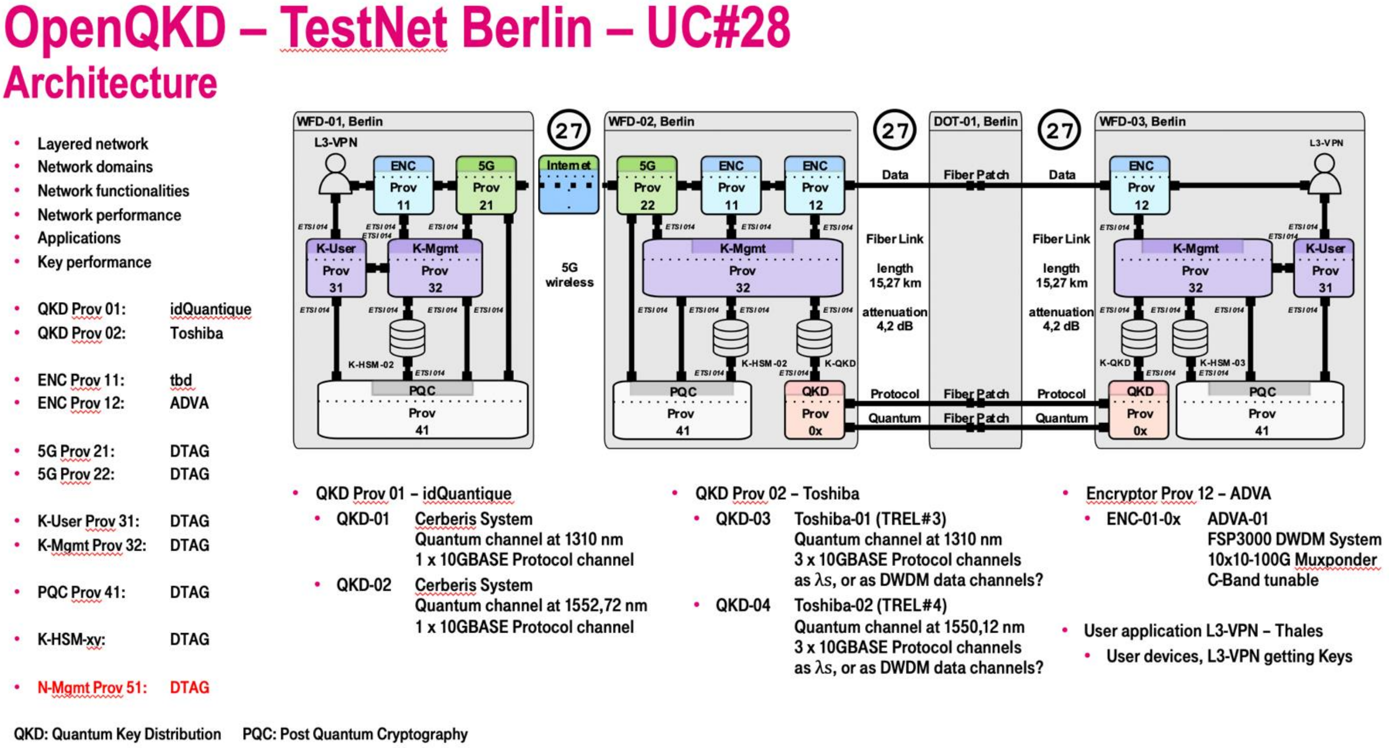
- QKD Prov 01 – idQuantique
  - QKD-01 Cerberis System
Quantum channel at 1310 nm
1 x 10GBASE Protocol channel
  - QKD-02 Cerberis System
Quantum channel at 1552,72 nm
1 x 10GBASE Protocol channel
- QKD Prov 02 – Toshiba
  - QKD-03 Toshiba-01 (TREL#3)
Quantum channel at 1310 nm
3 x 10GBASE Protocol channels
as λs, or as DWDM data channels?
  - QKD-04 Toshiba-02 (TREL#4)
Quantum channel at 1550,12 nm
3 x 10GBASE Protocol channels
as λs, or as DWDM data channels?
- Encryptor Prov 12 – ADVA
  - ENC-01-0x ADVA-01
FSP3000 DWDM System
10x10-100G Muxponder
C-Band tunable
- User application L3-VPN – Thales
  - User devices, L3-VPN getting Keys

QKD: Quantum Key Distribution PQC: Post Quantum Cryptography

Figure 2: UC-27 schematic.

Identifier Number:	UC-28
Name:	Integration of QKD to telecoms core network architecture
Partner(s) involved:	*tbd*
Starting/End date:	*07.2021 / 01.2022*
QKD equipment used:	*tbd*

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



OpenQKD – TestNet Berlin – UC#28

Architecture

- Layered network
- Network domains
- Network functionalities
- Network performance
- Applications
- Key performance

QKD Prov 01:	idQuantique
QKD Prov 02:	Toshiba
ENC Prov 11:	tbd
ENC Prov 12:	ADVA
5G Prov 21:	DTAG
5G Prov 22:	DTAG
K-User Prov 31:	DTAG
K-Mgmt Prov 32:	DTAG
PQC Prov 41:	DTAG
K-HSM-xy:	DTAG
N-Mgmt Prov 51:	DTAG

QKD: Quantum Key Distribution PQC: Post Quantum Cryptography

- QKD Prov 01 – idQuantique
  - QKD-01 Cerberis System
    Quantum channel at 1310 nm
    1 x 10GBASE Protocol channel
  - QKD-02 Cerberis System
    Quantum channel at 1552,72 nm
    1 x 10GBASE Protocol channel
- QKD Prov 02 – Toshiba
  - QKD-03 Toshiba-01 (TREL#3)
    Quantum channel at 1310 nm
    3 x 10GBASE Protocol channels
    as λs, or as DWDM data channels?
  - QKD-04 Toshiba-02 (TREL#4)
    Quantum channel at 1550,12 nm
    3 x 10GBASE Protocol channels
    as λs, or as DWDM data channels?
- Encryptor Prov 12 – ADVA
  - ENC-01-0x ADVA-01
    FSP3000 DWDM System
    10x10-100G Muxponder
    C-Band tunable
- User application L3-VPN – Thales
  - User devices, L3-VPN getting Keys

Figure 3: UC-28 schematic.

3. Madrid testbed

3.1. Formal description

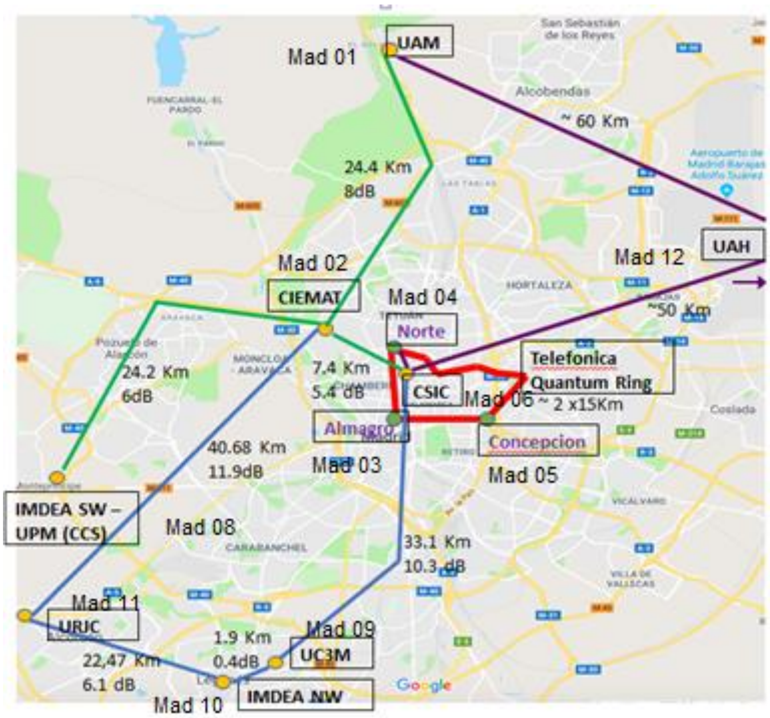


Figure 4: Map of Madrid testbed

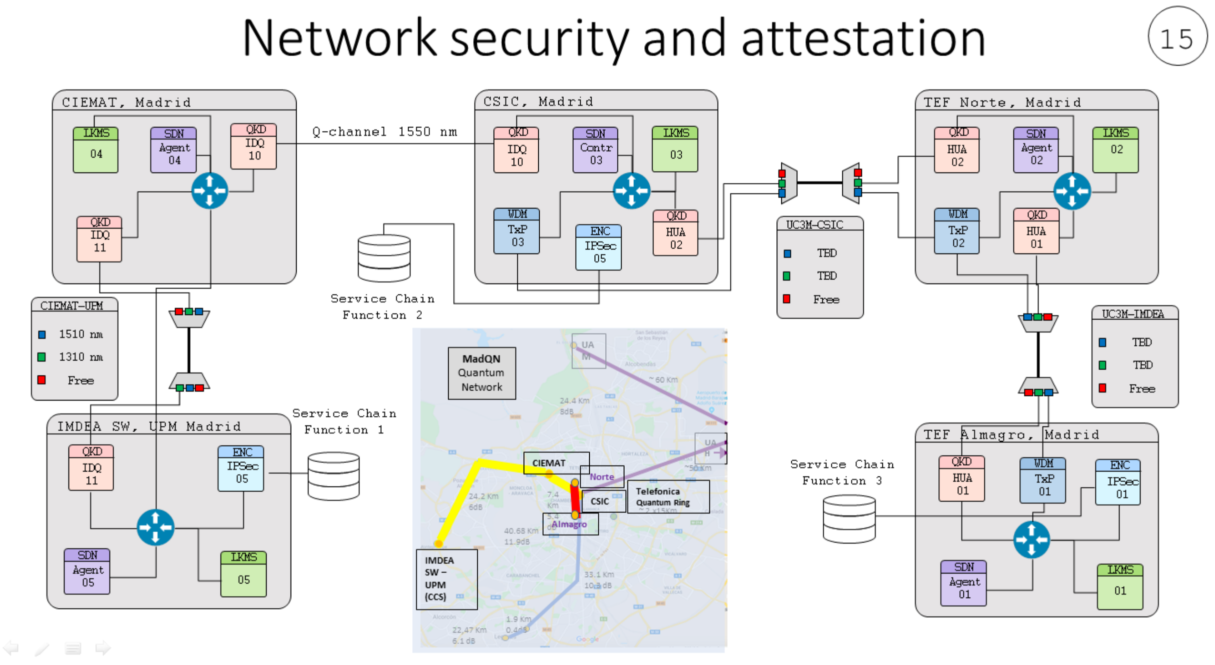
The Madrid QKD Testbed has two components, one is a ring of about 15 km installed in the Telefónica Spain production network (in red) and the other is part of the Madrid Research Network. The Points of Presence (PoPs) are shown as yellow circles. The part in the production network is ideal to test high TRL devices, since the systems installed there must follow the standard procedures for telco equipment and comply with operators' constraints. On the other hand, the ring is of exclusive use for the quantum testbed and the fibres are not lit, which makes it ideal for testing new services. The rest of the network (blue, green and yellow lines) is part of the Madrid Research network (REDIMadrid). The PoPs in this network are more open to experimentation and are adequate for devices with lower TRL. The fibres must be shared with classical channels, which can be used to demonstrate quantum/classical channel co-propagation. The green lines denote fibres that are very sparsely populated (less than three classical channels) and have backup lines, so that special tests can be done on these lines. The blue lines are slightly more populated (4-5 channels) and have no backup link, so the installation of QKD equipment must be done carefully and in windows of time outside the critical service times for the academic and research communities. The dark fibre link shown in yellow is under deployment. The current number of PoPs is 9 although in the production ring more (3-4 more) can be easily added. The network connects several campuses with the National Research and Education Network (RedIris Neutral point) where it is connected with the European network Géant.

<table>
<tr><td>Testbed name:</td><td>Madrid ES</td></tr>
<tr><td>Location:</td><td>Madris, Spain</td></tr>
<tr><td>Partner responsible / Host:</td><td>Partner responsible TID
Host: Telefonica & REDIMadrid (Madrid Research Network)</td></tr>
<tr><td>Partner(s) involved:</td><td>Telefonica Investigacion Y Desarrollo Sa (TID), Fundacion Imdea Software (RM), Universidad Politécnica De Madrid (UPM)</td></tr>
<tr><td>Applications / Collector for:</td><td>1. Secure critical infrastructure
2. 5G testbed connection
3. eHealth
4. Metro-SDQN
5. Network Function Virtualization securing and deployment
6. Cloud datacentre infrastructure (simulated, but full stack although no real production data centres)</td></tr>
<tr><td>Use cases involved:</td><td>UC 15, UC 16, UC 17, UC 18, UC 25, UC 26</td></tr>
<tr><td>Network topology:</td><td>Metro mesh + Ring</td></tr>
<tr><td>Nodes:</td><td>1 UAM (Mad 01)
2 CIEMAT (Mad 02)
3 ALMAGRO (Mad03)
4 NORTE (Mad 04)
5 CONCEPCIÓN (Mad 05)
6 CSIC (Mad 06)
7 UPM(CCS)-IMDEA-SW (Mad 08)
8 UC3M (Mad 09)
9 IMDEA-NW (Mad 10)
10 URJC (Mad 11)
11 UAH (Mad 12)</td></tr>
<tr><td>Links:</td><td>
<table>
<tr><th>Link Number</th><th>Length [km]</th><th>Loss [dB]</th></tr>
<tr><td>1 Almagro-Norte</td><td>3.9</td><td>6</td></tr>
<tr><td>2 Norte-Concepción</td><td>5.5</td><td>7</td></tr>
<tr><td>3Concepción- Almagro</td><td>6.4</td><td>7</td></tr>
<tr><td>4 CIEMAT-UAM</td><td>24.5</td><td>8</td></tr>
<tr><td>5 CIEMAT-IMDEA SW</td><td>24.2</td><td>6</td></tr>
<tr><td>6 CIEMAT-CSIC</td><td>7.42</td><td>5.4</td></tr>
<tr><td>7 CSIC- UC3M</td><td>33.1</td><td>10.3</td></tr>
<tr><td>8 UC3M-IMDEA-NW</td><td>1.91</td><td>0.4</td></tr>
<tr><td>9 CIEMAT-URJC</td><td>40.68</td><td>11.93</td></tr>
<tr><td>10 URJC – IMDEA NW</td><td>22.47</td><td>6.1</td></tr>
<tr><td>11 NORTE-CSIC (in construction)</td><td>2 (approx.)</td><td>-</td></tr>
<tr><td>12 CSIC-UAH (pending)</td><td>50 (approx.)</td><td>-</td></tr>
<tr><td>13 UAH-UAM (pending)</td><td>60 (approx.)</td><td>-</td></tr>
</table>
</td></tr>
</table>

Network functions:	1. SDN: SDN control (components network) but a more standard (layered network) is also possible. 2. Co-Existence: 22% dark fiber, 78% lit fiber (DWDM. 37% less than 3 channels, 31% 4-5 channels) 3. Interoperability: full
Brief formal description	

3.2. Use-cases involved

Identifier Number:	UC-15
Name:	Network security and attestation
Partner(s) involved:	UPM (Software provider), TID (Testbed and use case provider -Enduser: Telefónica Spain) RM (Testbed provider).
Starting/End date:	1-12-2020/30-04-2021
QKD equipment used:	TREL, IDQ
Encryptors used:	Not essential, software encryption is done.
Link(s) of the testbed network used:	Mad 08-Mad 02-Mad 06-Mad 04-Mad 03
Brief description of UC purpose/scope:	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 behaviour 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



Network security and attestation

15

Figure 5: UC-15 schematic.

Identifier Number:	UC-16
Name:	Critical Infrastructure protection (Telco)
Partner(s) involved:	UPM (Software provider), TID (Testbed and use case provider –End user: Telefónica Spain) RM (Testbed provider).
Starting/End date:	1-07-2020/31-11-2020 phase (a), 1-12-2020/30-04-2021 phase (b) 1-10-2022/28-02/2023 phase (c)
QKD equipment used:	TREL, IDQ
Encryptors used:	Not essential, software encryption is done.
Link(s) of the testbed network used:	Phase (a): Mad 08-Mad 02-Mad 06-Mad 09-Mad 10; Phase (b): Mad 08-Mad 02-Mad-06-Mad 04- Mad 03 Phase (c): Mad 01-Mad 02-Mad-08 +Mad 02-Mad 06-Mad 09- Mad-10-Mad-11 (Mesh) + Mad 06- Mad 04 (bridge RM to TID) + Mad 04-Mad-05-Mad 03- Mad 04 (Ring)

Brief description of UC purpose/scope:	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.

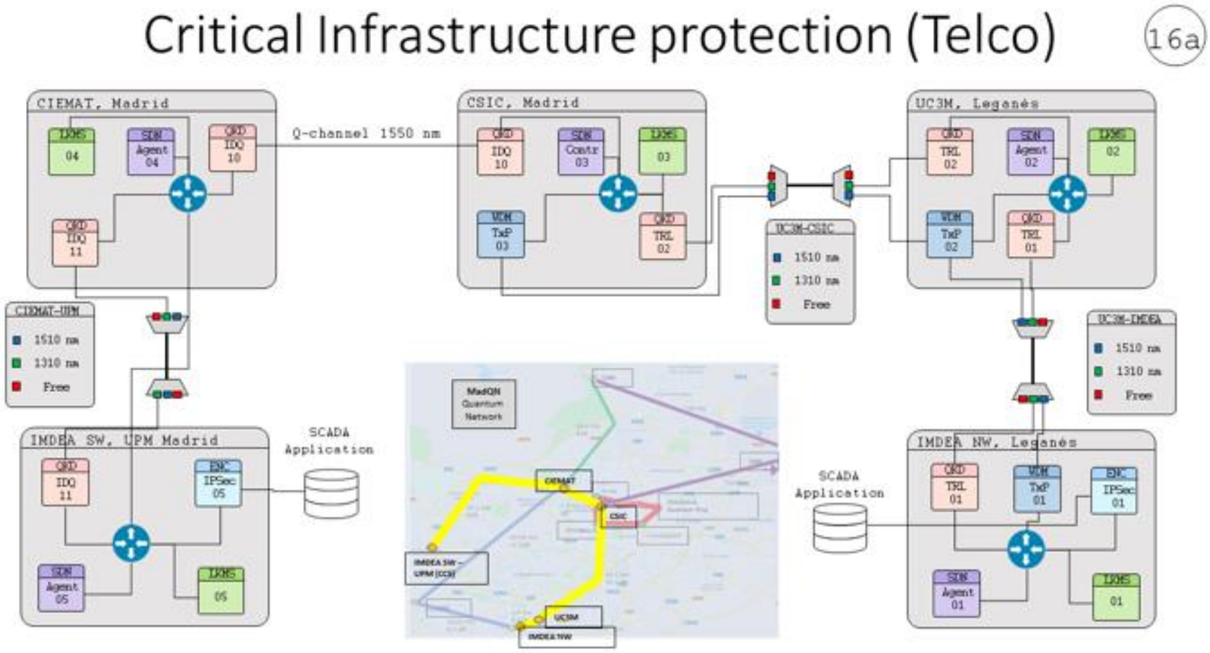


Figure 6: UC-16 schematic.

Identifier Number:	UC-17
Name:	QKD as a Cloud Service
Partner(s) involved:	UPM (Software provider), TID (Testbed and use case provider –End user: Telefónica Spain) RM (Testbed provider).
Starting/End date:	1-12-2020/30-04-2021 phase (a) 1-10-2022/28-02/2023 phase (b)
QKD equipment used:	TREL, IDQ
Encryptors used:	3 link encryptors

Link(s) of the testbed network used:	Phase (a):
	Mad 05-Mad 04-Mad 03-Mad 05
	Phase (b):
	Mad 08-Mad 02-Mad-06-Mad 04- Mad 03

	Phase (c): Mad 01-Mad 02-Mad-08 +Mad 02-Mad 06-Mad 09- Mad-10-Mad-11 (Mesh) + Mad 06- Mad 04 (bridge RM to TID) + Mad 04-Mad-05-Mad 03- Mad 04 (Ring)
Brief description of UC purpose/scope:	Several cloud data centres 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.

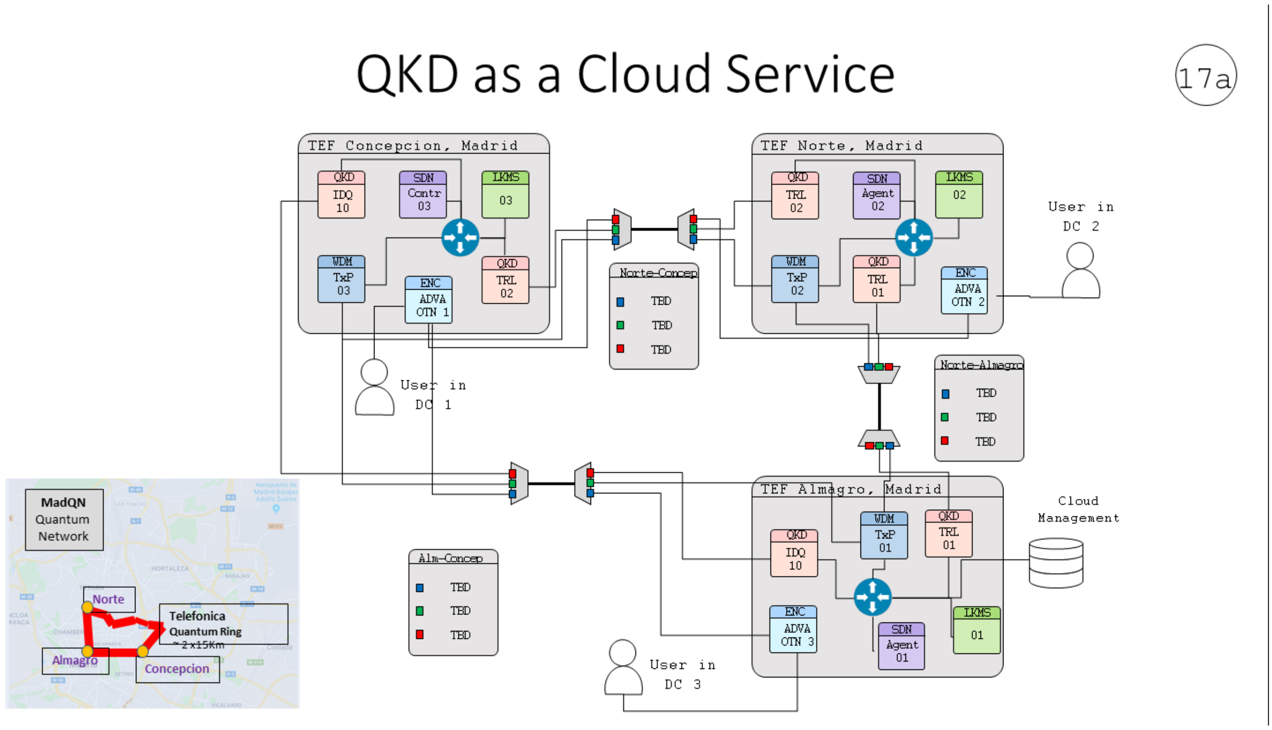


Figure 7: UC-17 schematic.

Identifier Number:	UC-18
Name:	e-Health services
Partner(s) involved:	UPM (Software provider), TID (Testbed and use case provider) RM (Testbed provider).
Starting/End date:	1-05-2021/30-09-2021
QKD equipment used:	TREL, IDQ
Encryptors used:	3 link encryptors
Link(s) of the testbed network used:	Mad 01-Mad 02-Mad 06-Mad 09 + Mad 02-Mad 08
Brief description of UC purpose/scope:	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 personalised medicine, where also genomic data has to be transferred in many cases. However, there is another family of applications that we envision will also have a large impact. 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 (intial talks with P. Viloresi) 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.

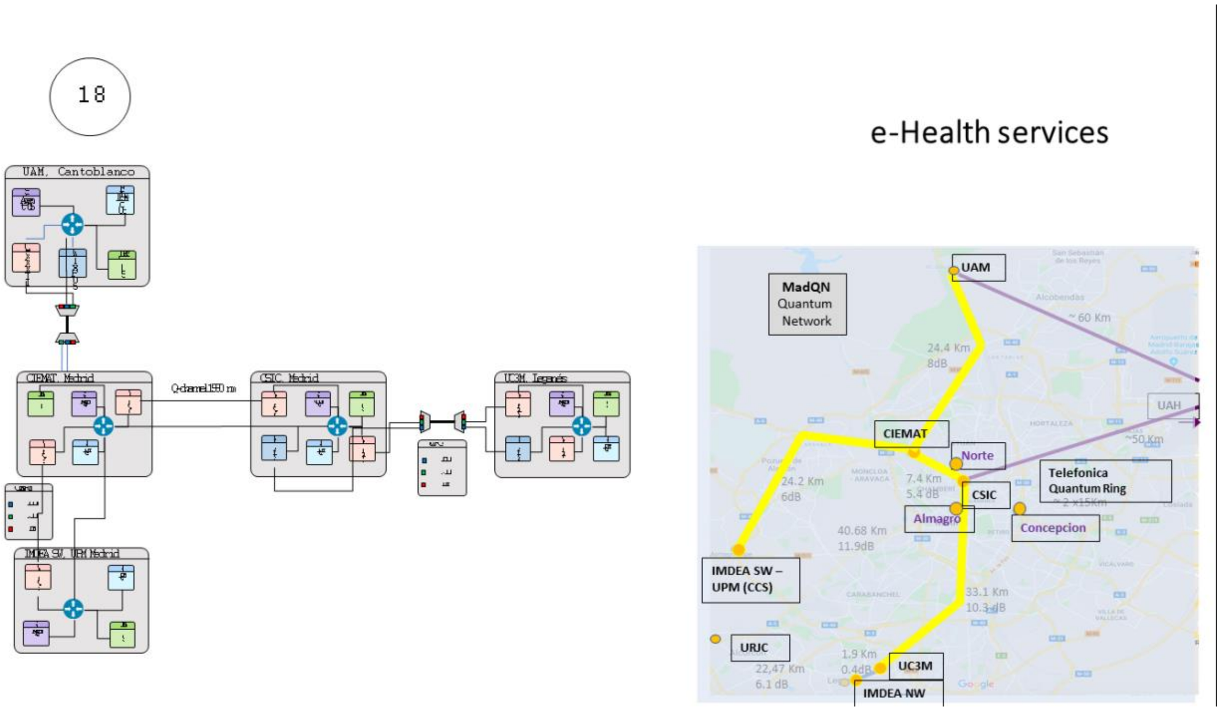


Figure 8: UC-18 schematic.

Identifier Number:	UC-25
Name:	Quantum Cryptography for B2B and 5G networks
Partner(s) involved:	UPM (Software provider), TID (Testbed and use case provider) RM (Testbed provider).
Starting/End date:	1-07-2020/30-11-2020 Phase (a) 1-12-2020/30-04-2021 Phase (b) 1-10-2022/28-02-2023 Phase (c)
QKD equipment used:	TREL, IDQ
Encryptors used:	Encryption can be done in SW for the first phase (HW encryptors are welcome, but, given the difficulty of the links (shared fibre, amplifier bypassing, additional OTN equipment), the effort was put first in agreeing the QKD systems and making sure that they work.

	6 encryptors in the second phase (If level 1 encryption: 3 links in the Telefónica Quantum Ring, plus CSIC-Norte, CSIC-UC3M and UC3M-IMDEA NW) If level 2 or 3 this can be reduced to 4 links (3 in Telefónica Quantum ring and other in Norte-IMDEA NW) As a extreme case with just one Level 2/3 in Norte-IMDEA NW.
Link(s) of the testbed network used:	Phase (a) Mad 06 –Mad09- Mad 10 Phase (b) Mad 08- Mad 02 –Mad 06 –Mad 09- Mad 10 Phase (c): Mad 01-Mad 02-Mad-08 +Mad 02-Mad 06-Mad 09- Mad-10-Mad-11 (Mesh) + Mad 06- Mad 04 (bridge RM to TID) + Mad 04-Mad-05-Mad 03- Mad 04 (Ring)
Brief description of UC purpose/scope:	As the network is evolving towards flexible and scalable architectures, it enables 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. Among 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 centre premises (e.g. for 5G), to incorporate quantum-safe security for end users communications.

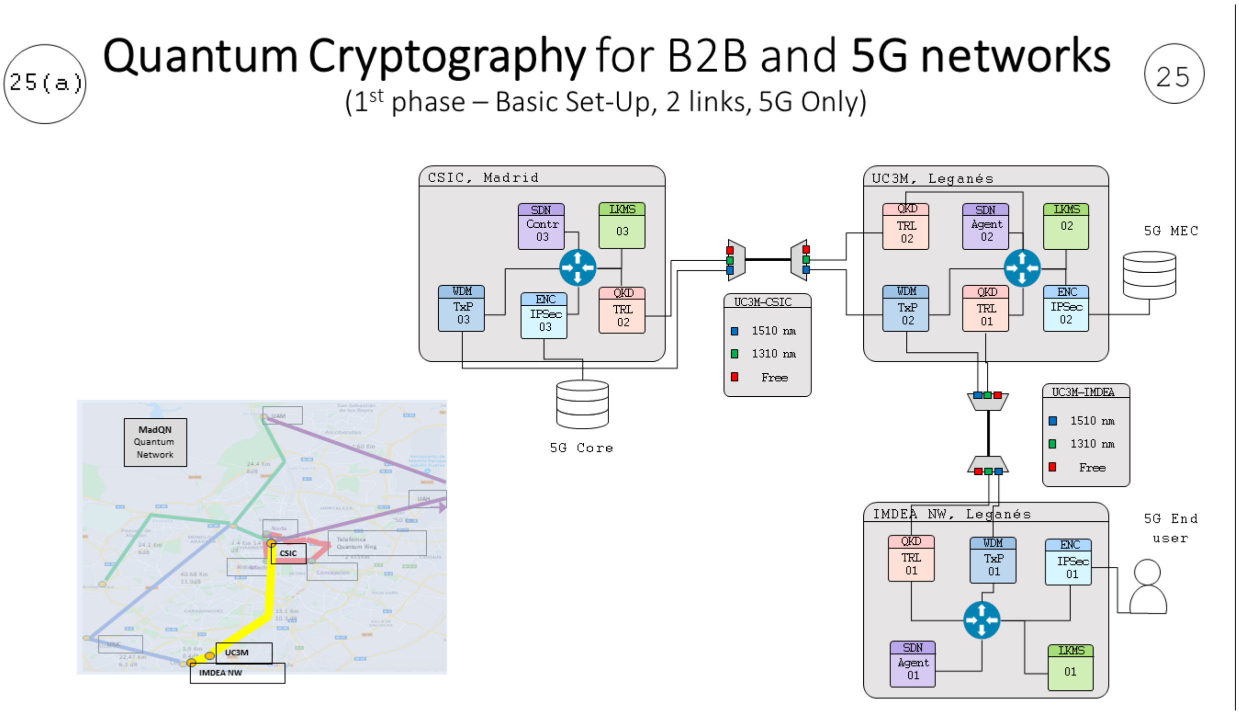
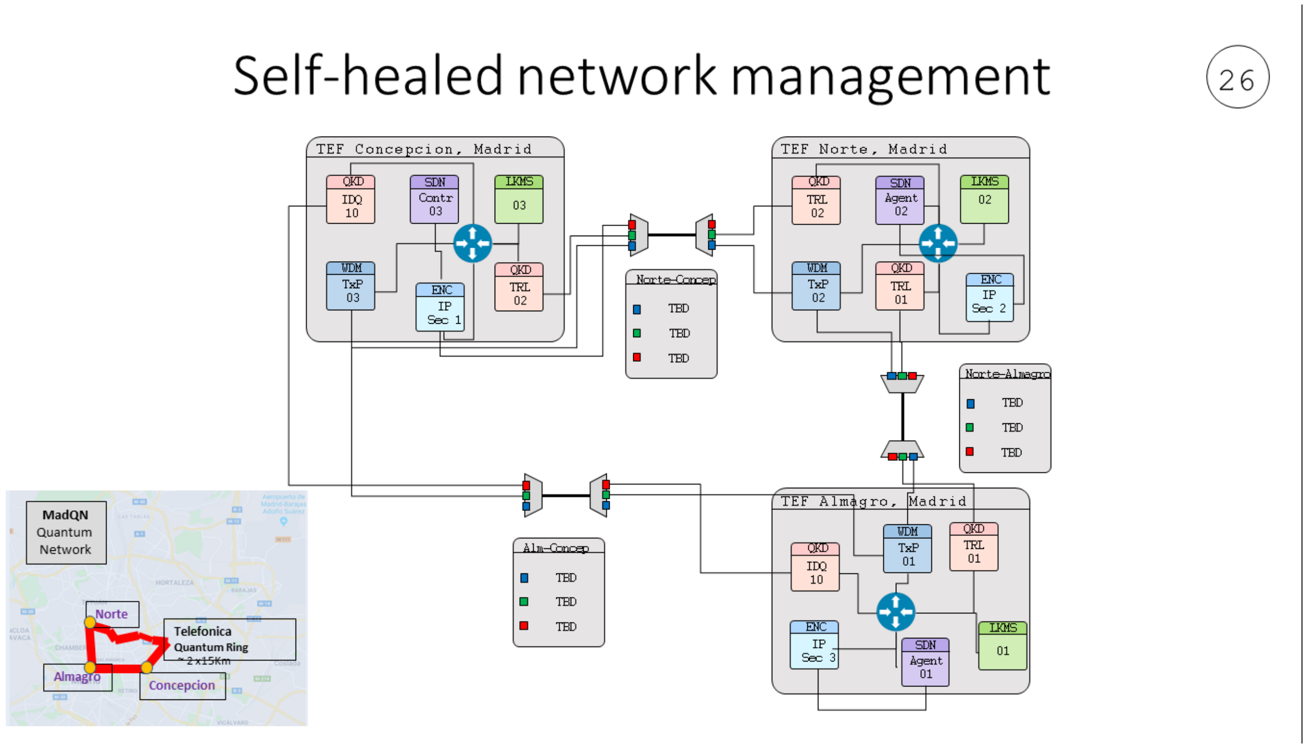


Figure 9: UC-25 schematic.

Identifier Number:	UC-26
Name:	Self-healed network management
Partner(s) involved:	UPM (Software provider), TID (Testbed and use case provider) RM (Testbed provider).
Starting/End date:	1-12-2020/30-04-2021
QKD equipment used:	TREL, IDQ
Encryptors used:	not strictly necessary since the required encryption can be done in SW.
Link(s) of the testbed network used:	Mad 05-Mad 04-Mad 03 –Mad 05
Brief description of UC purpose/scope:	Novel network paradigms can play a very important role for the integration of QKD in the operator’s networks. But it is not wise to look at the beneficial arrangement in only one direction. Within the operator’s network, QKD is a technology to be deployed only in secure areas or PoPs, where the rest of the network elements (NEs) are also deployed. This situation allows such NEs to make use of the QKD-derived keys to secure its own communications towards network management systems or SDN controllers. Therefore, upon installation we can

	simultaneously control the QKD elements, while securing any control plane channel between the PoPs and data centers. Examples of these channels are the communications between a SDN controller and a NE, or the communication between NFV architectures (e.g. OpenSource MANO-OSM) and remote virtual infrastructure managers (VIMs).



Self-healed network management

26

Figure 10: UC-26 schematic.

4. Poznam testbed

4.1. Formal description

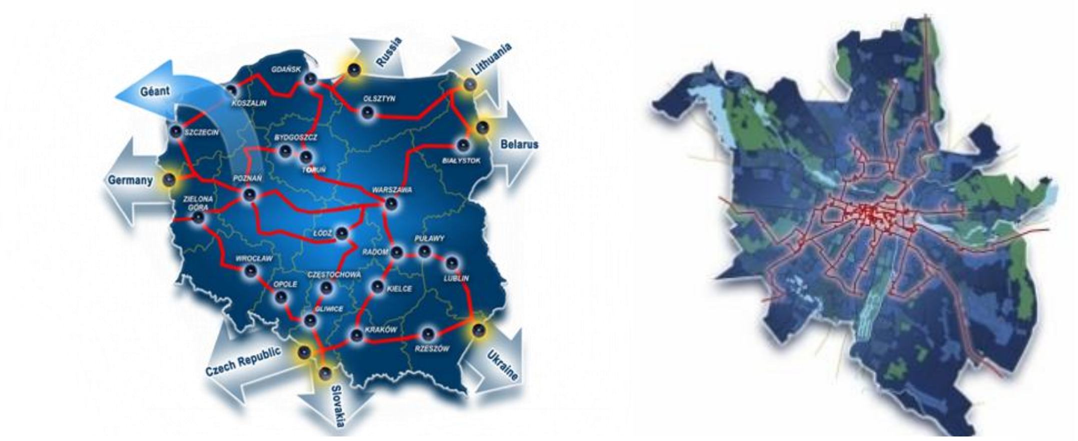


Figure 11: Map of Poznam testbed

PSNC QKD testbed will be based on POZMAN and PIONIER network infrastructure and services. Testbed network will include local partners (such as hospitals, city hall, government institutions etc.) that collaborate with PSNC and develop, operate number of critical services. These services will benefit from QKD technologies and OPENQKD project and using it these services can be further enhanced to provide new functionalities and performance.

Testbed name:	Poznan
Location:	Poznan, Poland
Partner responsible / Host:	PSNC
Partner(s) involved:	Toshiba, IDQuantique, ADVA, VSB
Applications / Collector for:	1. Healthcare 2. e-Government 3. ICT Networks 4. Inter/Intra-Datacenter 5. High Performance Computing 6. Long distance link
Use cases involved:	UC01, UC06, UC07, UC08, UC09, UC10, UC11
Network topology:	Metro mesh network with spurs
Nodes:	1. PSNC-01 2. PSNC-02 3. PSNC-03 4. PSNC-04 5. PSNC-05 6. PSNC-07 7. VSB

<table>
<tr><td>Links:</td><td><table>
<tr><th>Link</th><th>Length [km]</th><th>Loss [dB]</th></tr>
<tr><td>1 PSNC01 – PSNC04</td><td>8</td><td>2</td></tr>
<tr><td>2 PSNC01 – PSNC05</td><td>4</td><td>2</td></tr>
<tr><td>3 PSNC01 – PSNC03</td><td>9</td><td>2.5</td></tr>
<tr><td>4 PSNC01 – VSB</td><td>71</td><td>TBD</td></tr>
<tr><td>5 PSNC01 – PSNC02</td><td>6.1</td><td>1.5</td></tr>
<tr><td>6 PSNC01 – PSNC07</td><td>5</td><td>2</td></tr>
</table></td></tr>
<tr><td>Network functions:</td><td>• SDN: Capable
• Co-Existence: available separate dark fibers on all links, optical transmission system on different fiber pair.
• Interoperability: Yes</td></tr>
</table>

4.2. Use-cases involved

Identifier Number:	UC-01
Name:	High Performance Computing
Partner(s) involved:	PSNC, ADVA
Starting/End date:	2022-01-01 2022-03-31
QKD equipment used:	TREL
Encryptors used:	ADVA
Link(s) of the testbed network used:	PSNC01-PSNC02
Brief description of UC purpose/scope:	With use case #01 we intend to connect the PSNC data centres (primary and backup) in Poznań. These sites are also main Point Of Presence of PIONIER network (Polish National Research and Education Network), GEANT network and other international PSNC and PIONIER partners. Due to resilience and Service Level Agreement requirements these data centres are connected using two independent optical cables, different cable route and cable pipes. The two routes have 4 and 10 km in distance. A QKD system will be installed along with an encryptor to ensure that network traffic, backup services, data from HPC machines may relay on secure connection and critical messages forwarded to the PIONIER Network Operator Center.

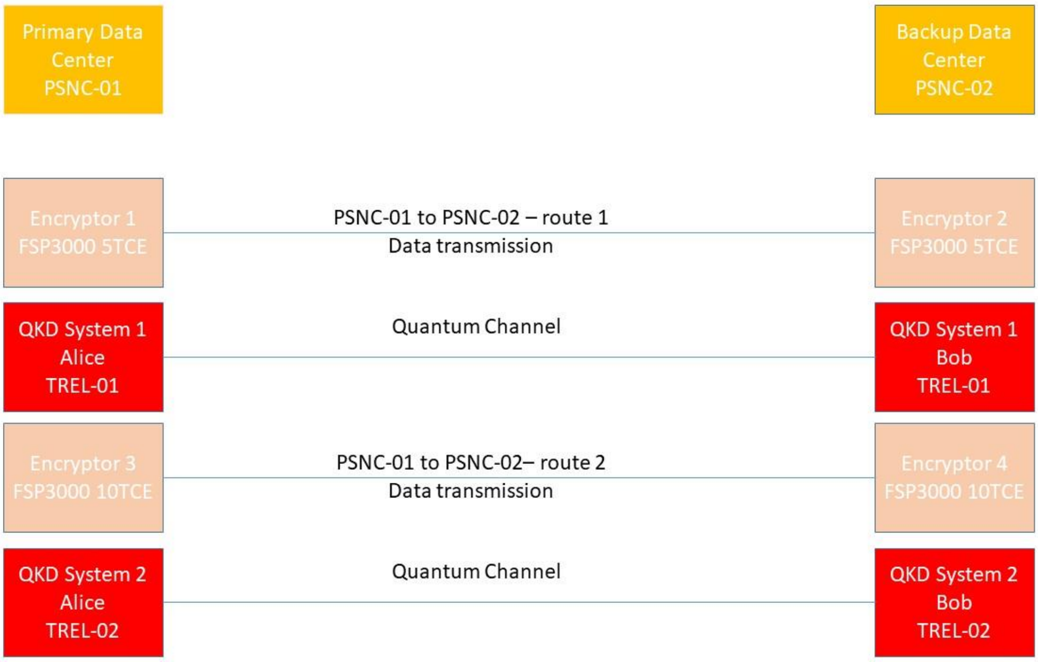

Primary Data Center PSNC-01
Backup Data Center PSNC-02
Encryptor 1 FSP3000 5TCE
PSNC-01 to PSNC-02 – route 1
Data transmission
Encryptor 2 FSP3000 5TCE
QKD System 1 Alice TREL-01
Quantum Channel
QKD System 1 Bob TREL-01
Encryptor 3 FSP3000 10TCE
PSNC-01 to PSNC-02– route 2
Data transmission
Encryptor 4 FSP3000 10TCE
QKD System 2 Alice TREL-02
Quantum Channel
QKD System 2 Bob TREL-02

Figure 12 : UC-01 schematic.

Identifier Number:	UC-06
Name:	High Performance Computing
Partner(s) involved:	PSNC, ADVA, VSB
Starting/End date:	2022-02-01 2022-04-30
QKD equipment used:	TREL
Encryptors used:	ADVA
Link(s) of the testbed network used:	PSNC01-VSB
Brief description of UC purpose/scope:	With use case #06 we intend to connect the VSB and PSNC data centres in Ostrava and Poznań. These sites are also Point Of Presence of HPC infrastructures and National Research and Education Network infrastructures, GEANT network and other international VSB, PSNC partners. Load balancing of work schedule of supercomputers or parallel processing of “big data” within a network of supercomputers involves the transport of virtual machines, which is to be secured through QKD layer equipment. Compression techniques of virtual machines will be evaluated for fast data exchange optimized for QKD technology. Two nodes will be deployed at

	the Cieszyn and Ostrava supercomputing centers and the impact of QKD on HPC traffic pattern and services will be investigated. QKD link is planned to be implemented with one trusted relay along the route and key rate in the rage of 1 Mbps. The HPC traffic from Cieszyn – remote HPC site will be forwarded using PSNC PIONIER network to PSNC datacenter in Poznań. Due to segment lengths and required number of QKD trusted nodes it is not possible to connect directly by QKD PSNC and VSB datacenters in Ostrava and Poznan. A QKD system will be installed along with an encryptor to ensure that network traffic, backup services, data from HPC machines may relay on secure connection and critical messages forwarded to the PIONIER Network Operator Center.

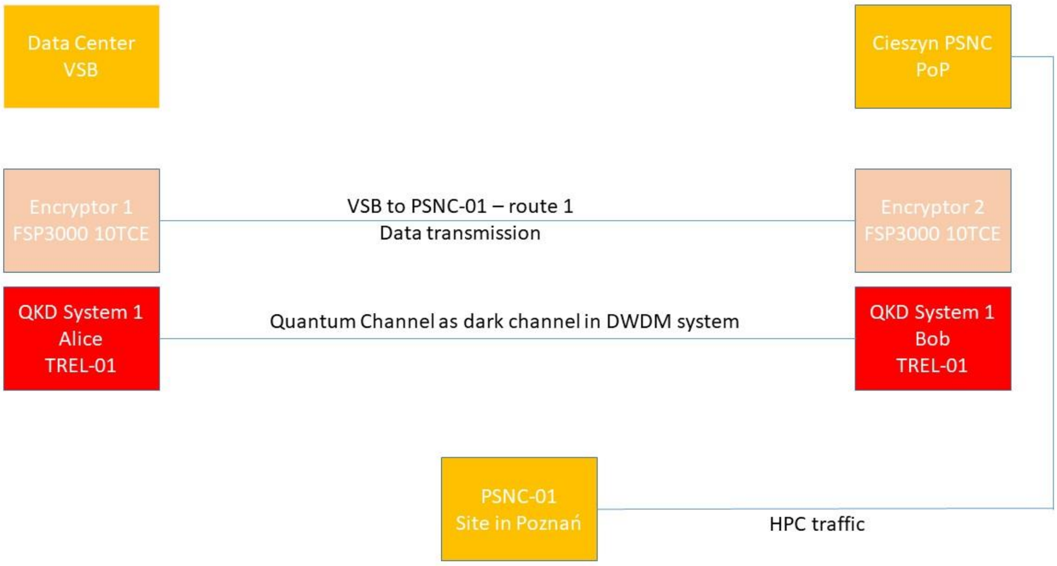


Figure 13: UC-06 schematic.

Identifier Number:	UC-07
Name:	Healthcare
Partner(s) involved:	PSNC, ADVA
Starting/End date:	2022-01-01 2022-03-31
QKD equipment used:	TREL
Encryptors used:	ADVA
Link(s) of the testbed network used:	PSNC01-PSNC03
Brief description of UC purpose/scope:	With use case #07 we intend to connect the PSNC datacenter in Poznań and hospital where PSNC delivers a number of IT services. PSNC site is also main Point Of Presence of PIONIER network (Polish National Research and Education Network), GEANT network and other international PSNC and PIONIER partners. Hospital site is one of the main PSNC metro area POZMAN sites. Existing medical infrastructure and its modern services rely heavily on storing of digital medical data, results and its frequent exchange between hospitals, medical institutions, and medical staff (using remote and mobile services, devices). It applies for both the medical test results and its interpretation documentation. One of the important aspects in this context is also telemedicine and remote live transmission, participation in medical surgeries, activities and consulting. Due to inherent personal and confidential data, these services are planned to be secured and integrated with QKD layer network and services. This requirement is strengthened by the increasing amount of medical services that store, analyze and sent entire human genome data that should be protected particularly well. These use cases introduce specific requirements for the data security and potential QKD integration. The QKD network services must run on various hardware and software platforms. The nodes will be deployed in Poznan between hospitals and PSNC data centers. Impact on services and infrastructure will be investigated. The route have 9 km in distance. A QKD system will be installed along with an encryptor to ensure that network traffic, services, may rely on secure connection and critical messages forwarded to the PIONIER and POZMAN Network Operator Center.

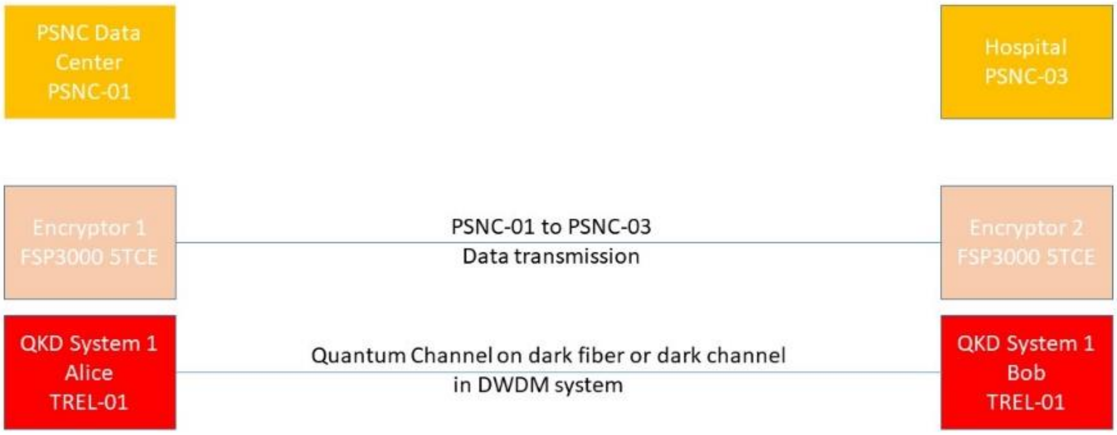

PSNC Data Center PSNC-01
Hospital PSNC-03
Encryptor 1 FSP3000 5TCE
PSNC-01 to PSNC-03 Data transmission
Encryptor 2 FSP3000 5TCE
QKD System 1 Alice TREL-01
Quantum Channel on dark fiber or dark channel in DWDM system
QKD System 1 Bob TREL-01

Figure 14: UC-07 schematic.

Identifier Number:	UC-08
Name:	e-Government
Partner(s) involved:	PSNC, ADVA
Starting/End date:	2022-04-01 2022-06-30
QKD equipment used:	TREL
Encryptors used:	ADVA
Link(s) of the testbed network used:	PSNC01-PSNC05
Brief description of UC purpose/scope:	With use case #08 we intend to connect the PSNC datacenter in Poznań and Poznan city hall branches that provide critical IT services for citizens. PSNC site is also main Point Of Presence of PIONIER network (Polish National Research and Education Network), GEANT network and other international PSNC and PIONIER partners. City hall site is one of the main PSNC metro area POZMAN sites. Currently more and more local and central government institutions—in particular city halls—provide a large number of services for citizens using digital platforms. Large numbers of confidential, private and state documents are being digitized, confirmed and sent between various institutions that generally use different

	software and hardware platforms for each specific service. Most of these services were and are developed independently and use different technologies, software solutions, architecture and hardware solutions. An important element of such platforms is user authentication (trusted profiles etc.). Apart from the documents aspect, local state institutions provide different services like registration to schools, exam evaluations, digital libraries etc. All these services are to be secured and further enhanced with QKD network layer infrastructure and its impact is to be evaluated. The nodes will be deployed in Poznan between PSNC data centers and Poznan city hall branches. These use cases introduce specific requirements for the data security and potential QKD integration. The QKD network services must run on various hardware and software platforms. The nodes will be deployed in Poznan between city hall branches and PSNC data centers. Impact on services and infrastructure will be investigated. The route have 4 km in distance. A QKD system will be installed along with an encryptor to ensure that network traffic, services, may rely on secure connection and critical messages forwarded to the PIONIER and POZMAN Network Operator Center.

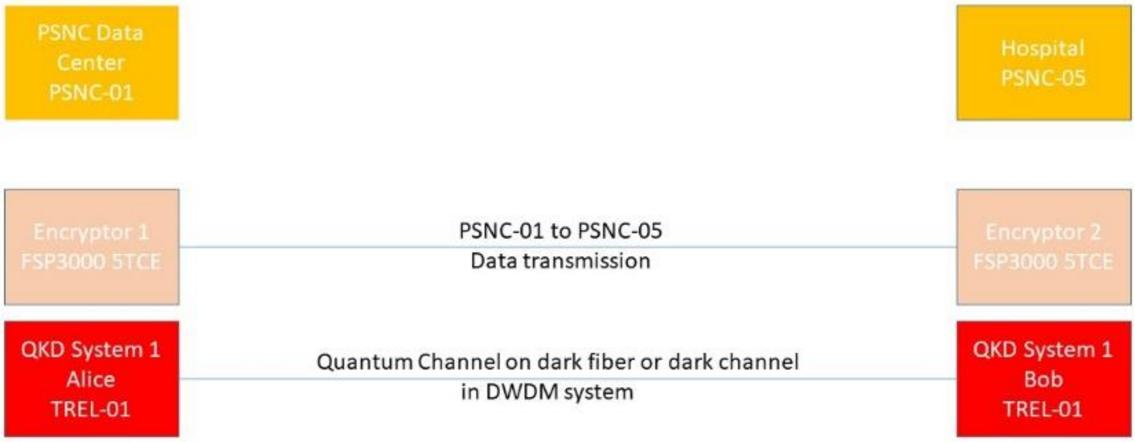

PSNC Data Center PSNC-01
Hospital PSNC-05
Encryptor 1 FSP3000 5TCE
PSNC-01 to PSNC-05 Data transmission
Encryptor 2 FSP3000 5TCE
QKD System 1 Alice TREL-01
Quantum Channel on dark fiber or dark channel in DWDM system
QKD System 1 Bob TREL-01

Figure 15: UC-08 schematic.

Identifier Number:	UC-09
Name:	Banking
Partner(s) involved:	PSNC, ADVA
Starting/End date:	2022-07-01 2022-08-30
QKD equipment used:	TREL
Encryptors used:	ADVA
Link(s) of the testbed network used:	PSNC01-PSNC04
Brief description of UC purpose/scope:	With use case #09 we intend to connect the PSNC datacenter in Poznań and banking datacenter that provide critical digital banking services for citizens. PSNC site is also main Point Of Presence of PIONIER network (Polish National Research and Education Network), GEANT network and other international PSNC and PIONIER partners. Banking datacenter site is one of the PSNC metro area POZMAN sites. The banking sector relies heavily on advanced, fast digital services delivered to end users and between the bank data centers themselves. Large amounts of confidential data is being sent, backed up and synchronized between various banking institutions and divisions. Digital trading platforms are delay and speed sensitive. The services and communication channels between banking institutions are to be secured with advanced QKD network layer infrastructure. The nodes will be deployed in Poznan between PSNC data centers and data centers that host services for the banking sector. The investigated impact will include maximum possible key exchange rate, delay introduced for the services and management overhead of QKD network layer, number of interconnected, synchronized and secured by QKD network layer systems/platforms, distance vs key rate vs optical power. It is proposed to investigate also concept of “quantum money” and possible implementation in exemplary transactions. All these services are to be secured and further enhanced with QKD network layer infrastructure and its impact is to be evaluated. The nodes will be deployed in Poznan between PSNC data centers and banking data centers. These use cases introduce specific requirements for the data security and potential QKD integration. The QKD network services must run on various hardware and software platforms. Impact on services and infrastructure will be investigated. The route have 8 km in distance. A QKD system will be installed along with an encryptor to ensure that network

	traffic, services, may rel y on secure connection and critical messages forwarded to the PIONIER and POZMAN Network Operator Center.

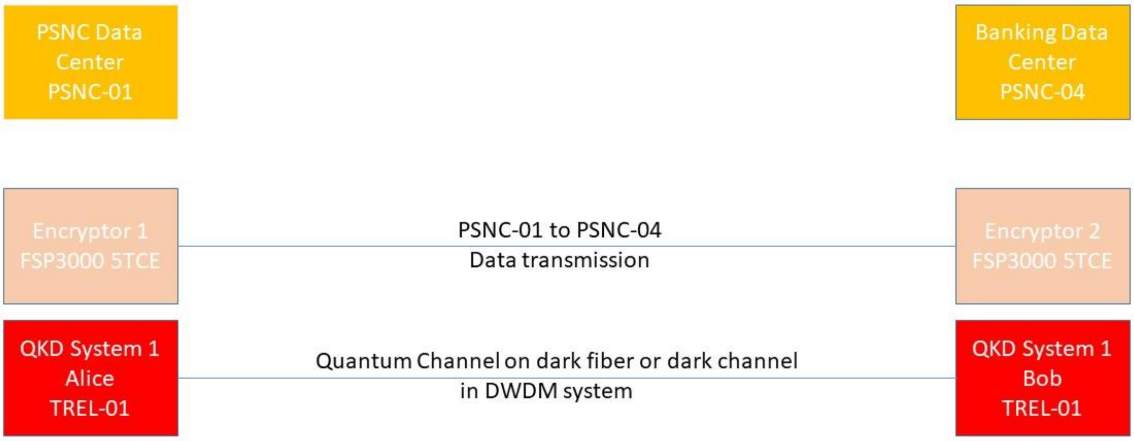

PSNC Data Center PSNC-01
Banking Data Center PSNC-04
Encryptor 1 FSP3000 5TCE
PSNC-01 to PSNC-04 Data transmission
Encryptor 2 FSP3000 5TCE
QKD System 1 Alice TREL-01
Quantum Channel on dark fiber or dark channel in DWDM system
QKD System 1 Bob TREL-01

Figure 16: UC-09 schematic.

Identifier Number:	UC-10
Name:	Police
Partner(s) involved:	PSNC, ADVA
Starting/End date:	2022-05-01 2022-08-30
QKD equipment used:	TREL
Encryptors used:	ADVA
Link(s) of the testbed network used:	PSNC01-PSNC07
Brief description of UC purpose/scope:	With use case #10 we intend to connect the PSNC datacenter in Poznań and local police datacenter that provide critical services for police infrastructure. PSNC site is also main Point Of Presence of PIONIER network (Polish National Research and Education Network), GEANT network and other international PSNC and PIONIER partners. Police datacenter site is one of the PSNC metro area POZMAN sites. Police currently uses different advanced digital tools in its operational activities. Such tools frequently use large amount of confidential, operational data, big

	data analytics and deep learning techniques. Data is being collected and stored from large number of different digital sources and its integrity and security is essential. Such services are planned to be secured and enhanced with QKD network layer equipment. The nodes will be deployed in Poznan between PSNC data centers, City Hall divisions and local Police departments. Investigated aspects will include: speed and key exchange rate, management overhead, delay connected with QKD network layer integration with various operational software tools, distance vs key speed vs optical power dependency. All these services are to be secured and further enhanced with QKD network layer infrastructure and its impact is to be evaluated. These use cases introduce specific requirements for the data security and potential QKD integration. The QKD network services must run on various hardware and software platforms. Impact on services and infrastructure will be investigated. The route have 5 km in distance. A QKD system will be installed along with an encryptor to ensure that network traffic, services, may relay on secure connection and critical messages forwarded to the PIONIER and POZMAN Network Operator Center.

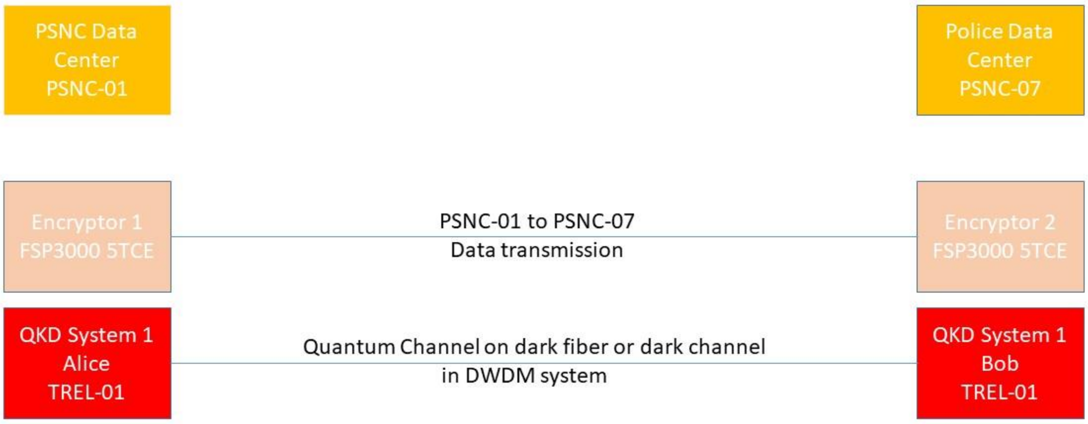

PSNC Data Center PSNC-01
Police Data Center PSNC-07
Encryptor 1 FSP3000 5TCE
PSNC-01 to PSNC-07 Data transmission
Encryptor 2 FSP3000 5TCE
QKD System 1 Alice TREL-01
Quantum Channel on dark fiber or dark channel in DWDM system
QKD System 1 Bob TREL-01

Figure 17: UC-10 schematic.

Identifier Number:	UC-11
Name:	High Performance Computing
Partner(s) involved:	PSNC, ADVA
Starting/End date:	2022-09-01 2023-02-28
QKD equipment used:	TREL
Encryptors used:	ADVA
Link(s) of the testbed network used:	PSNC01-PSNC02
Brief description of UC purpose/scope:	With use case #11 we intend to connect one of the PSNC nodes and PoPs that include devices and infrastructure for the distribution of the reference time and frequency signals. PSNC takes part in national and international projects that are focused on establishing reference time and frequency signals distribution system. The signals are transmitted either on separate dark fibers (with specially designed transmission system) or within the spectrum of existing optical data transmission system. The latest project involves transmission of reference optical carrier that can be used in various metrological systems using optical combs at the transmission terminals. Already established reference T&F transmission system use PIONIER (Polish National Research and Education Network) and POZMAN, GEANT network and other international PSNC and PIONIER partners network nodes and infrastructure. The links require also special monitoring and maintenance procedures due to calibration requirements. A QKD system will be installed along and together with reference T&F links with an encryptor. Performance and influence of both systems will be analyzed and performance evaluated, In order to ensure that network traffic, and services are properly analyzed, critical messages will be forwarded and analyzed in the PIONIER Network Operator Center. The system and use case has the capability to be extended on cross-border international links.

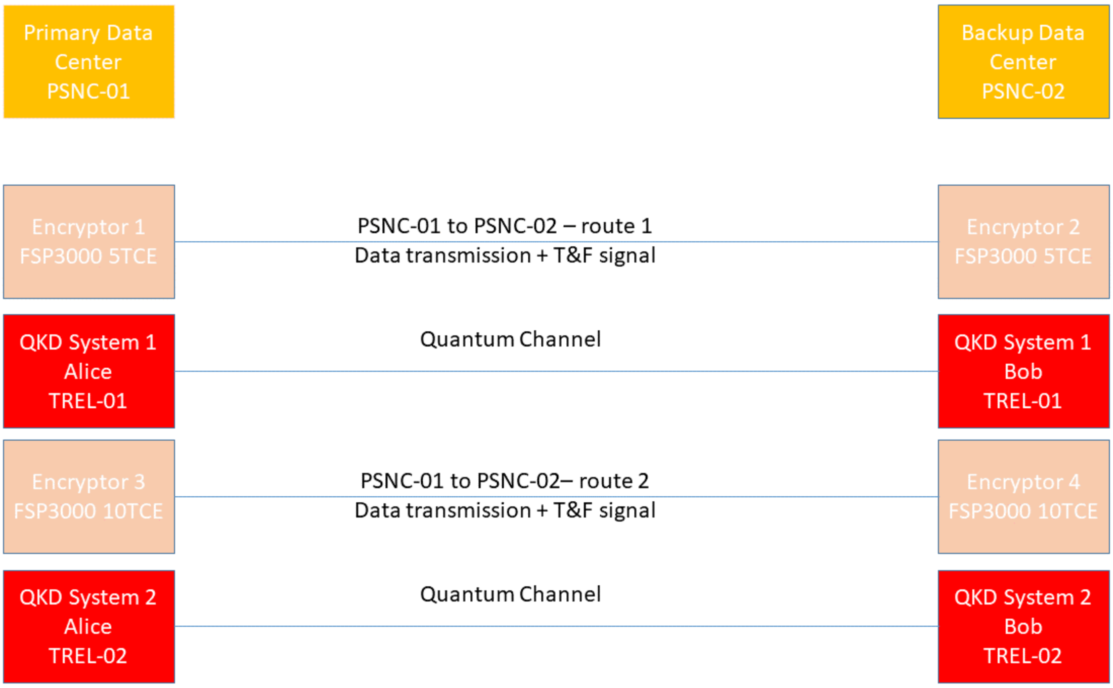

Primary Data Center PSNC-01
Backup Data Center PSNC-02
Encryptor 1 FSP3000 5TCE
PSNC-01 to PSNC-02 – route 1
Data transmission + T&F signal
Encryptor 2 FSP3000 5TCE
QKD System 1 Alice TREL-01
Quantum Channel
QKD System 1 Bob TREL-01
Encryptor 3 FSP3000 10TCE
PSNC-01 to PSNC-02– route 2
Data transmission + T&F signal
Encryptor 4 FSP3000 10TCE
QKD System 2 Alice TREL-02
Quantum Channel
QKD System 2 Bob TREL-02

Figure 18: UC-11 schematic.

5. Vienna testbed

5.1. Formal description

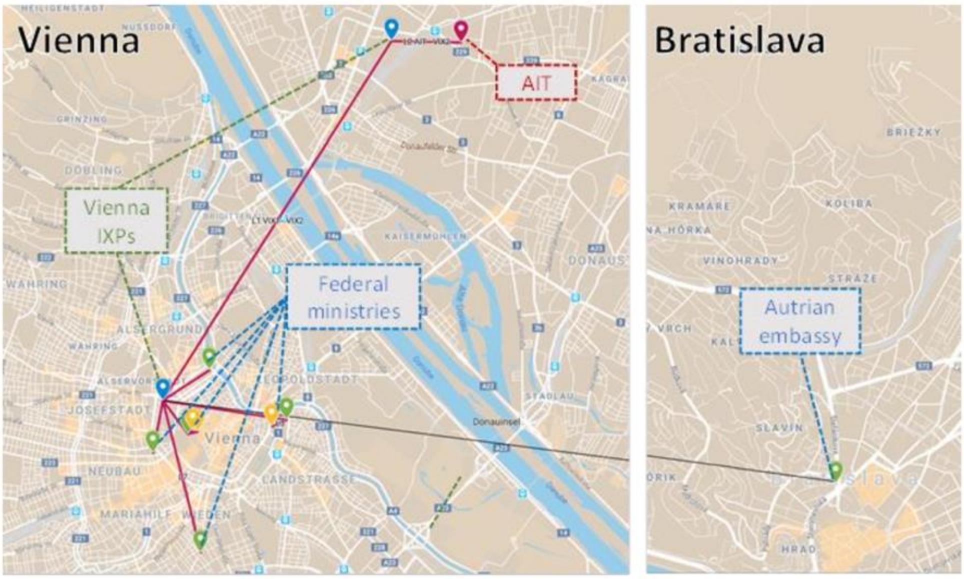


Figure 19: Map of Vienna testbed

The Vienna testbed operated by IQOQI consists of two long-distance telecom fiber links connecting the metropolitan areas of Vienna and Bratislava as well as St. Pölten. The QKD scheme deploys the BBM92-protocol, i.e., it is based on polarization-entanglement between single photon pairs transmitted over these links. The photons are produced by a state-of-the-art source of photonic entanglement utilizing a nonlinear optical process. They are coupled into single-mode fibers which are patched to the network displayed above. Compensation equipment for drifts in polarization, chromatic dispersion and polarization mode dispersion along the fibers are applied and monitored electronically. At the receiver stations in St. Pölten and Bratislava, an unconditionally secure key can be created from measuring the respective photon's polarization state with different randomly chosen polarizer settings. Classical communication via Ethernet is conducted to compare a subset of the measurement results. This allows for definite exclusion of any adversary trying to eavesdrop the quantum channel. One can therefore create a physically secure one-time pad usable to encrypt a message which can then be sent via any arbitrary channel without compromising the message's cryptographic security.

Testbed name:	Vienna
Location:	Vienna, Austria
Partner responsible / Host:	OEAW
Partner(s) involved:	AIT, IDQ, TREL, MPL, ADVA, RSCS Other partners (external to OPENQKD): • Slovak Academy of Sciences (Partner in Bratislava) • Ruder Boskovic Institute (Partner in Zagreb)

<table>
<tr><td></td><td>
<ul>
<li>Department of Telecommunication and Media Informatics (Partner in Budapest)</li>
<li>Cesnet (Technical Support)</li>
<li>Türk Telekom International AT AG (Fiber Provider)</li>
</ul>
</td></tr>
<tr><td>Applications / Collector for:</td><td>1) Government communication
2) establishment of QKD network connection</td></tr>
<tr><td>Use cases involved:</td><td>UC05, UC19, UC20, UC29</td></tr>
<tr><td>Network topology:</td><td>point-to-point connection with source in the middle</td></tr>
<tr><td>Nodes:</td><td>1) Vienna
2) St. Pölten
3) Bratislava</td></tr>
<tr><td>Links:</td><td>
<table>
<tr><th>Link</th><th>Length [km]</th><th>Loss [dB]</th></tr>
<tr><td>• Link1: Vienna – St. Pölten</td><td>129.4</td><td>31.87</td></tr>
<tr><td>• Link2: Vienna – Bratislava</td><td>119.2</td><td>32.62</td></tr>
<tr><td>• Link3: AIT - VIX1</td><td>1.5</td><td>0.345</td></tr>
<tr><td>• Link4: VIX1 – VIX2</td><td>9.7</td><td>2,231</td></tr>
<tr><td>• Link5: VIX2 – BMLV</td><td>3.1</td><td>0.713</td></tr>
<tr><td>• Link6: BMLV – BRZ</td><td>3.7</td><td>0.851</td></tr>
</table>
</td></tr>
<tr><td>Network functions:</td><td>• Distributed-storage capability (FRX)
• Co-Existence: mainly dark fibre, co-existence on selected links
• Interoperability: full</td></tr>
</table>

5.2. Use-cases involved

Identifier Number:	UC-05
Name:	Data encryption between governmental agencies
Partner(s) involved:	AIT, MPL, IDQ, TEUR, ADVA, FRX
Starting/End date:	11.2021
QKD equipment used:	IDQ, MPL, TEUR
Encryptors used:	ADVA
Link(s) of the testbed network used:	Link 3 to Link 6
Brief description of UC purpose/scope:	Data security and privacy are among the top concerns of the European Union as well as of the member states. The national governments have large amounts of confidential data which must be shared between different ministries and other government agencies. Highly sensitive data are being sent, backed up and synchronized between various stakeholders. Therefore, a first initial QKD network is initiated and implemented between different ministries in Vienna (AT) to secure data in transit.

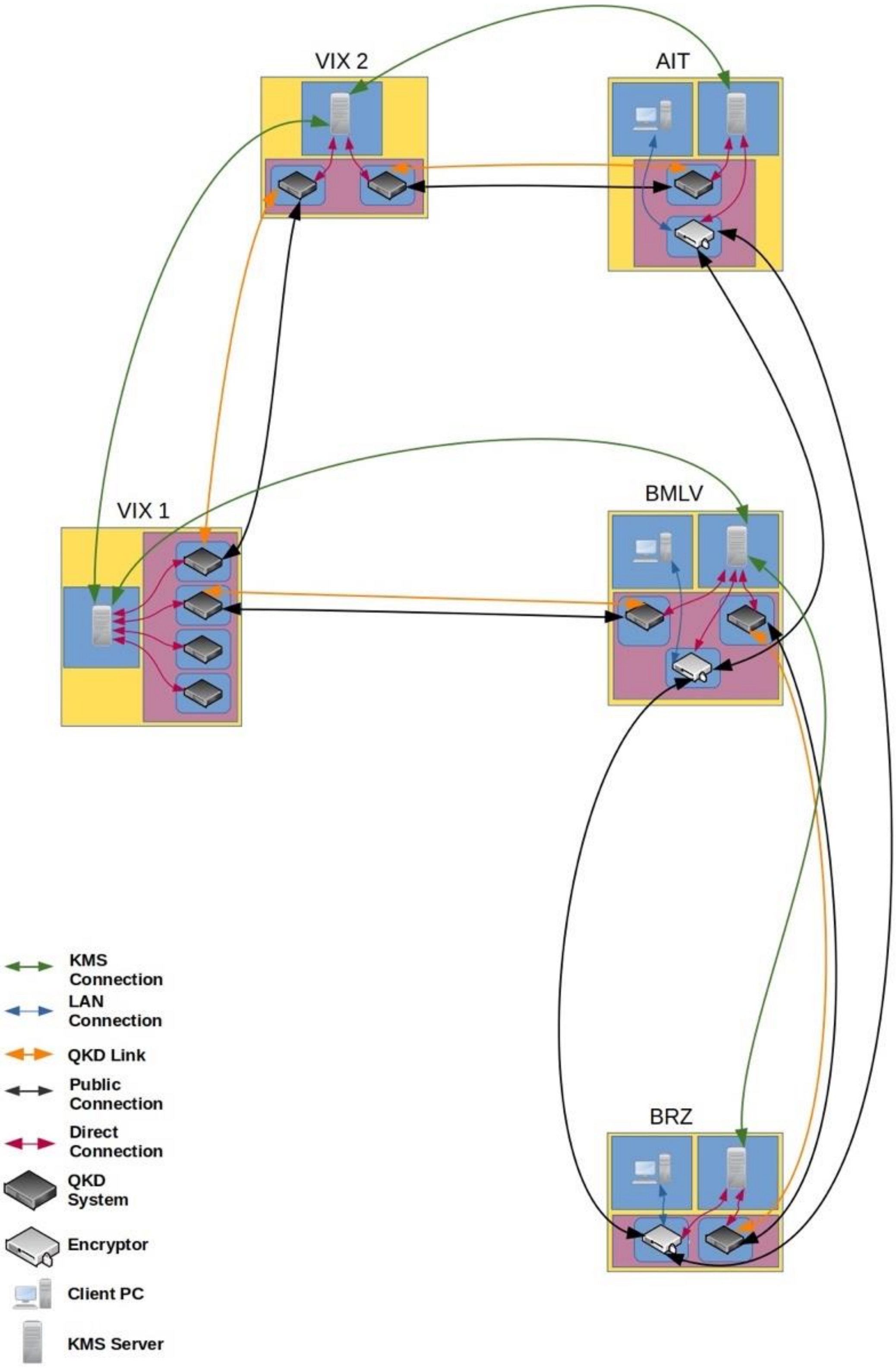


Figure 20: UC-05 schematic.

Identifier Number:	UC-19
Name:	Academic Network Backbone
Partner(s) involved:	OEAW, Slovak Academy of Sciences, Türk Telekom
Starting/End date:	TBD
QKD equipment used:	Source of polarization-entangled photon pairs, Bob-Modules
Encryptors used:	Self-built receiver modules
Link(s) of the testbed network used:	Link 1 and Link 2
Brief description of UC purpose/scope:	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.

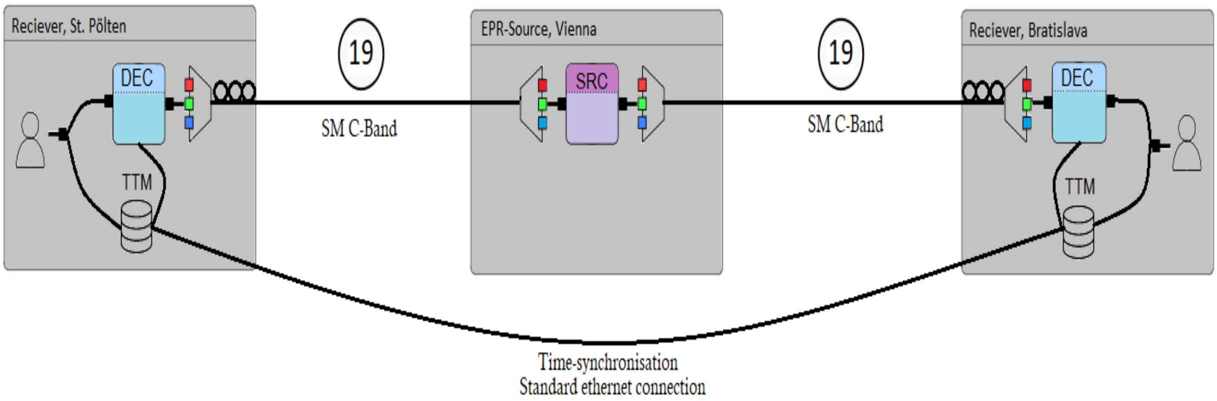


Figure 21: UC-19 schematic.

Identifier Number:	UC-20
Name:	Inter-government cross-border link
Partner(s) involved:	OEAW, Slovak Academy of Sciences, Ruder Boskovic Institute, Department of Telecommunication and Media Informatics (Budapest), Cesnet, Türk Telekom
Starting/End date:	TBD
QKD equipment used:	Source of polarization-entangled photon pairs, Bob-Modules
Encryptors used:	Self-built receiver modules

Link(s) of the testbed network used:	Link 1 and Link 2
Brief description of UC purpose/scope:	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.

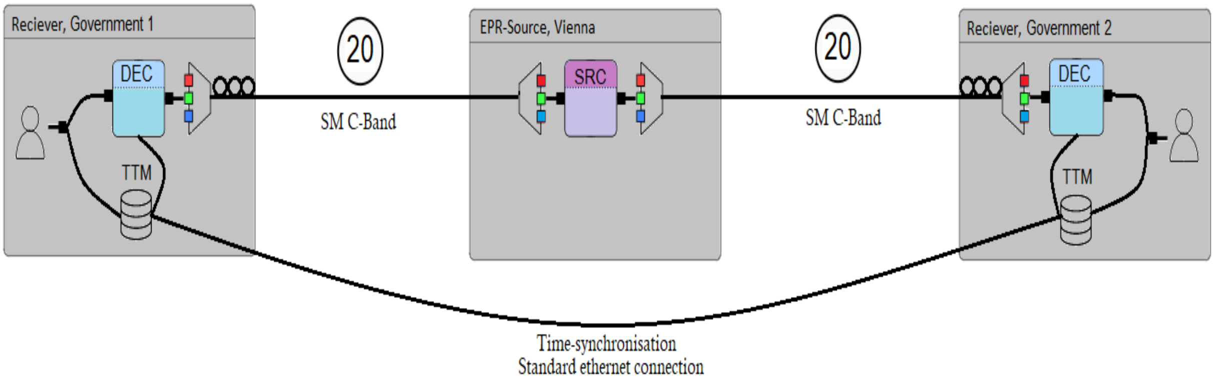


Figure 22: UC-20 schematic.

Identifier Number:	UC-29
Name:	Distributed cloud storage secured by ITS QKD
Partner(s) involved:	AIT, MPL, IDQ, TEUR, ADVA, FRX
Starting/End date:	01.2022
QKD equipment used:	IDQ, MPL, TEUR
Encryptors used:	ADVA
Link(s) of the testbed network used:	Link 3 to Link 6
Brief description of UC purpose/scope:	Encryption is very relevant for securing government data at rest. Based on the QKD infrastructure of use-case 29 in connection with a secure cloud solution based on secret sharing, a completely information-theoretic secure storage solution for government data will be initiated and implemented.

Schematic of UC-29 is similar to the one of UC-05.

6. Remarks and conclusions

We presented in this document the description of the four main testbeds of OPENQKD, by collecting the information regarding the testbed locations, partners involved, applications targeted, network topology, nodes, and functions.

Additionally, for each testbed a list of the involved use-cases is presented, with some details (where available) on the QKD equipment and encryptors used, and a short description of the use-case scope. The actual development and deployment of the testbeds will be presented in a separated deliverable.