Digital Europe Programme Project **QCI-CAT**
QCI: Proof of Concept – Secure Connectivity Austria
Digital Europe Work Programme 2021-2022
EU Secure Quantum Communication Infrastructure (DIGITAL-2021-QCI-01)
Project number: 101091642

Project starting date: fixed date: 1 January 2023
Project end date: 31 December 2025
Project duration: 36 months

Document:	**Deliverable**
Type:	Report
Dissemination Level:	Public
Title:	**Intermediary Report on the Status of the Medical Use Case**
Work-Package	WP7
Document number:	**D7.2**
Document Owner:	fragmentiX / Philipp Stanzer
Contributors:	FRX, AIT, MUG
Abstract:	The medical use case of QCI-CAT is designed to connect a data center in Vienna with the BLS4 Lab at Medical University of Graz, using QKD protected fiber connections in order to provide a quantum safe data repository using fragmentiX Secret Sharing for storing pathogen information.
Key words:	QKD, Secret sharing, medical data
Pages	31

Delivery Date Planned	2024-10-31 (M22)

Revision History

Version	Revision Points	Author(s) & Organization	Date
V 0.1	Initial version	P. Stanzer (FRX)	2024-09-11
V 0.2	Update Introduction	P. Stanzer (FRX)	2024-10-03
V 1.0	Update and formatting	P. Stanzer (FRX)	2024-10-17
V 2.0	Include feedback from review	P. Stanzer (FRX)	2024-10-29

Author List

Organization	Name	E-Mail address
FRX	P. Stanzer	Philipp.stanzer@fragmentix.com
AIT	F. Kutschera	Florian.kutschera@ait.ac.at
AIT	F. Prawits	florian.prawits@ait.ac.at
MUG	K. Zatloukal	kurt.zatloukal@medunigraz.at
AIT	S. Ramacher	sebastian.ramacher@ait.ac.at

Reviewer List

Organization	Name	E-Mail address
qtlabs	Sebastian Ecker	sebastian.ecker@qtlabs.at

Copyright Statement

Funding Acknowledgement:

This project has received funding from the European Union‘s Digital Europe Work Programme 2021-2022 under Project number: 101091642.

Table of content

Revision History 3
Author List 3
Reviewer List 3
Copyright Statement 3
Funding Acknowledgement: 3
List of Figures 6
Executive Summary 7
1. Introduction 8
1.1. Purpose and scope of the document 8
1.2. Target Audience 8
1.3. Relation to other project work 8
1.4. Structure of the document 8
2. Changes in the use case from Human Genome to Pathogen 9
2.1. Explanation 9
2.2. Impact 10
2.2.1. On the use case 10
2.2.2. On the whole project 10
3. Planning and design 11
3.1. Architecture and Network Design 11
3.2. Rollout plan 12
3.3. Adaptation to the new Pathogen use case 12
4. Hardware and Infrastructure 13
4.1. Fiber links and network equipment 13
4.2. Trusted repeater nodes 14
4.3. QKD devices and encryptors 15
4.4. Secret Sharing appliances and storage server 15
4.4.1. Secret Sharing appliances 15
4.4.2. Storage systems 18
4.5. Prototype testing 19
5. Setup, Integration and Demonstration 27
5.1. Connection infrastructure 27
5.2. Application layer 27
6. Next Steps 28
Summary 29

Appendix A - List of Acronyms.....30

Appendix B – Bibliography 31

List of Figures

Figure 1: Use case overview of involved sites 11
Figure 2: Overview of necessary equipment and connections 11
Figure 3: Rack plan for roll out coordination with frX and MUG 12
Figure 4: Network plan with all devices and fiber links 13
Figure 5: Setup and testing of network equipment (DWDM, switch, encryptor) 14
Figure 6: fragmentiX configuration interface with newly implemented features: WebDAV 16
Figure 7: fragmentiX configuration interface with newly implemented features: object locking 17
Figure 8: fragmentiX CLUSTER Node A and storage controller server in preparation for deployment at fragmentiX' offices 17
Figure 9: Storage extensions for two storage systems in preparation for deployment at fragmentiX' offices 18
Figure 10: Encoding scheme of the COW protocol 19
Figure 11: Block diagram COW transmitter (Tx) module. Optical paths are colored for easier distinguishability. The pulse train generated by and exiting the Tx is shown left-to-right. Acronyms: temperature controller (TEC), laser diode driver (LD), continuous wave (cw), intensity modulator (IM), attenuator (att.), optical (opt.), classical (cl.), electrical connection (el. conn.), wavelength division multiplex (WDM), small form factor pluggable (SFP), single mode fiber (SMF) 19
Figure 12: block diagram COW receiver (Rx) module. Optical paths have been colored for easier distinguishability. The incoming pulse train from the Tx is shown to the left. Used acronyms: band-pass filter (BPF), single photon avalanche detector (SPAD) 20
Figure 13: COW QKD system, Tx and Rx modules are connected by 25km fiber coil and the KMS dashboard for live monitoring key generation statistics. 20
Figure 14: Internal arrangement of components in COW QKD system: Tx (left) and Rx (right). The components still under development for continuous 24/7 operation concern the LD driver (left, Tx) and the polarization controller (right, Rx) 21
Figure 15: Post-processing pipeline QKD-R10 and ETSI014-compliant KMS, both compatible with COW QKD system 21
Figure 16: Secure key generation rates of the COW QKD system, comparison between operating the Rx module with SNSPDs vs InGaAs SPADs. 22
Figure 17: QKD system architecture of a QKD node with the KMS as central link between the Application and the QKD modules. (from [JLRT23]) 23
Figure 18: Decentralized key forwarding with keys S sent encrypted between using the QKD links to encrypt the key between Nodes S and D (from [JLRT23]) 23
Figure 19: Setup the demonstration at ECOC 2024 of three national domains (Spain, Germany, Austria) with the hardware and software components provided by different vendors. 25

Executive Summary

The medical use case of QCI-CAT is designed to connect a data center in Vienna with the BLS4 Lab at Medical University of Graz, using QKD protected fiber connections in order to provide a quantum safe data repository using fragmentiX Secret Sharing for storing pathogen information.

Within this use case it is planned to install and test the Trusted Repeater Nodes (TRNs) developed by fragmentiX and the QKD system developed by AIT over the long distance from Vienna to Graz.

Due to the delayed national co-funding, the delayed procurement of the QKD devices and the unexpected changes (outlined in section 2) that lead to revising the use case completely, the deployment is not finished yet. The TRNs were shipped in October and testing of the QKD devices is ongoing until the end of October at AIT labs.

The remaining hardware (i.e., fragmentiX Secret Sharing appliances, storage systems and fiber connections) is already in place or ready for deployment together with the QKD devices. During the delay, improvements and updates were implemented.

Once, the demonstration is in place, an extension of the QKD network to St. Johann is planned together with the other use case.

1. Introduction

This document reports on the status of the Medical Use Case, connecting the BLS4 Lab at Medical University of Graz to datacenters and relevant organizations in and around Vienna, as well as to St. Johann i. P. using QKD protected fiber links.

1.1. Purpose and scope of the document

The purpose of the document is to provide a comprehensive overview of the progress made in WP7 from project start until end of month 22.

1.2. Target Audience

Anyone interested in the progress and the intermediary results of this demonstration. Especially members of the QCI-CAT consortium and distinct governmental officials and experts in the medical environment.

1.3. Relation to other project work

The knowledge and experience gathered, while planning and implementing the Medical Use Case are directly related and used as input for WP2 in Task 2.4 “Preparation of a Governance document for the access and work with sensitive medical data in the medical context”. This document will also provide the base for the final report on this use case and the respective section in the reporting of the whole project.

The progress of the use case depends on acquisition of the equipment in WP4.

The extension to St. Johann will be done in cooperation with Task T5.6 of WP5, Governmental Use Case.

The trusted repeater node (TRN) prototypes, needed in this use case are developed in WP8 of this project.

1.4. Structure of the document

The structure of this document is closely tied to the division of WP7 into its five tasks:

Section 2 explains the necessary changes within the use case, section 3 focuses on the planning and design in task T7.1, section 4 on the hardware and infrastructure prepared for this use case (T7.2., T7.3 and T7.5), section 5 describes the setup, integration and demonstration itself (T7.4) and section 6 gives an outlook at the next steps.

2. Changes in the use case from Human Genome to Pathogen

During the course of the project, unexpected events required substantial changes to the use case and its schedule.

2.1. Explanation

About eight months after project start, the situation for the medical use case has changed in two ways:

- Because of the sudden and unexpected death of a major stakeholder – Prof. Speicher – at Medical University Graz, the scope of the project that originally focused on securely exchanging human genome sequence data had to be changed.
- With the Medical University Vienna leaving the consortium, the second institution providing human genome data was removed from the use case as well.

The implementation of the medical use case was no longer possible as designed initially.

Lessons learned from the COVID-19 pandemic and the fact that new pandemics will challenge our society in the future makes the need for innovative solutions to securely handle medical data related to high-risk pathogens evident. This demand fits the objectives of QCI-CAT and uses the full potential of the desired solutions for a quantum safe communication network.

This lead to the idea for remodeling the medical use case as outlined below.

The revised use case focuses on secure transfer and storage of high risk pathogens and related data, while protecting all of the following:

- the genetic sequence of the pathogens
- data on their behavior
- other relevant properties
- information where these pathogens are stored
- how they are protected from unauthorized access

This information is highly sensitive (even more than human genetic data) due to the risk of misuse and weaponization of certain pathogens. Therefore, handling of this data has to meet highest-level bio-security and cybersecurity requirements.

It is planned that pathogen sequence data and related information generated in the high containment laboratory of the Medical University Graz (Group Dr. Zatloukal) is stored distributed across multiple physical locations by using the fragmentiX secret sharing technology. The secrecy and privacy of the transmission of the encrypted data fragments is guaranteed by QKD technology. The S3 data storages used, are located at different locations in Austria, thereby generating a distributed and secure data repository for these highly sensitive data.

The original geographic challenge of securing the data transmission over long distances (i.e., between Vienna and Graz) has not changed. It will be solved by using the original design of deploying trusted repeater nodes (TRNs; developed in WP8 of this project) in between the endpoints at the involved institutions and organizations.

2.2. Impact

Due to the changes explained above, the following impacts on the use case and the whole project were identified.

2.2.1. On the use case

On the one hand, the focus of the demonstration shifted a bit toward secure storage (and restricted access) of highly sensitive and potentially dangerous data and away from data exchange and collaboration between researchers at different institutions.

On the other hand, the redesign caused additional work in adapting the architecture and design of the original use case to fit the demands of the new ideas. The expected delay in execution was not observed, since the QKD devices were not delivered in time anyway.

2.2.2. On the whole project

Since in the new use case the medical data is not related to patients, the need for an ethics approval is no longer there. This also means, the ethics advisory board is not relevant anymore.

More generally, by revising the scope of the medical use case the relevance and impact is markedly increased for the following reasons:

- Genetic data of high-risk pathogens and associated information is highly sensitive because of dual use and biosecurity issues requiring highest cybersecurity solutions.
- By combining the fragmentiX secret sharing technology with QKD we will generate a secure data repository for highly sensitive medical data. Such a data repository can be used to ensure full traceability of high risk pathogens, since the pathogen sequence is not only a unique identifier for the pathogen (like a DNA fingerprint) but also documents the history of the pathogen evolution. This can be done, because the pathogen sequence gets modified by each infection cycle and therefore act like a molecular time stamp.
- In case of a successful demonstration of the establishment of a secure data repository within QCI-CAT, the results may act as blueprint for an international data repository allowing to identify the origin of pathogens in case of unintentional (e.g., accident) or intentional release (e.g., as bioweapon or in context of bioterrorism) of pathogens. The relevance of such a secure multinational data repository has been recently highlighted in context of the discussion on the origin of SARS-CoV-2.

3. Planning and design

In this section the abstract architecture and design are outlined and then detailed down to the network level. The planned roll out to the designated locations is described as far as available as the time of writing. As is true in general for this use case, the changes explained before also influenced the content of this section and made retrospective changes necessary.

3.1. Architecture and Network Design

The network for connecting the two end nodes consist of three QKD links connecting the four locations. The two locations between the Medical University of Graz and the datacenter in Vienna are trusted nodes. These locations are necessary as the distance between Vienna and Graz is far too long for only one QKD system. Using the ADVA encryptors, the traffic between the two end nodes will not be decrypted in the trusted nodes, as they will only function as repeaters to enhance the encrypted signal.

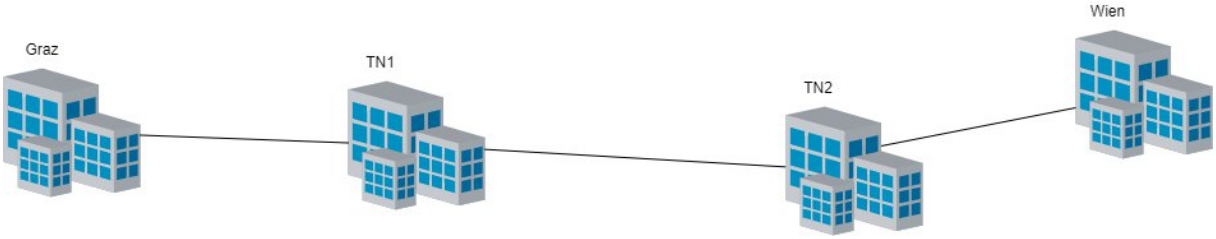


Figure 1: Use case overview of involved sites

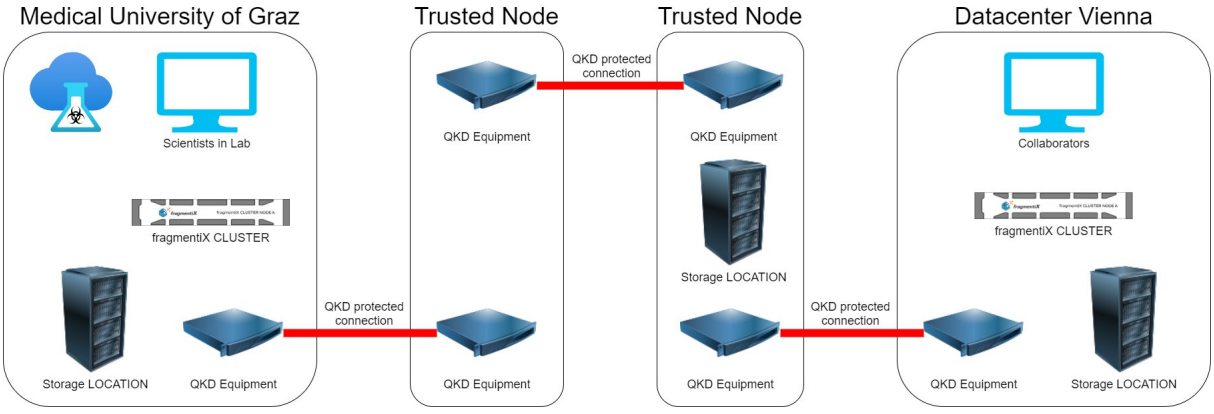


Figure 2: Overview of necessary equipment and connections

The initial design for connecting two university institutes was done in close collaboration with MUG and was modified for the new use case by AIT and FRX.

3.2. Rollout plan

The locations of the two TRNs between Vienna and Graz are under NDA with the provider of glass fiber and therefore only known to those with a clear “need to know”.

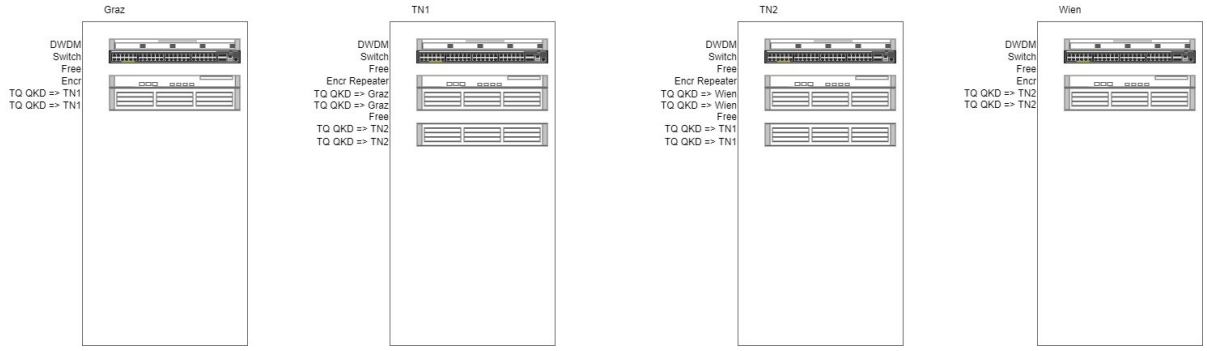


Figure 3: Rack plan for roll out coordination with frX and MUG

As the TRNs were set up in the first half of October, the next step is to get the fibers connected to all nodes. Once this step is concluded the QKD, encryptor, secret sharing and classical hardware can be installed in the nodes. Before connecting the equipment to the fibers, the fibers will be tested with an OTDR to measure the attenuation and reflections throughout the fiber to identify witch fiber of the pair connecting the nodes to use for classical communication and which to use for the QKD signal.

3.3. Adaptation to the new Pathogen use case

The roll out plan needed adaptation, since the infrastructure and facilities were changed

The situation at MUG did not change, since the endpoint for QKD and fragmentiX appliance and storage server can stay in the same room. Only the internal network settings and routing to the relevant participants must be redefined.

With the retreat of the Medical University Vienna, the other endpoint and user side needs to be changed. In the first iteration, only storage server and QKD devices will be deployed in a data center in Vienna, while the fragmentiX appliance is not needed (while it can still be installed and configured if desired) until another institution or organization wants to access the data, stored and distributed by the lab at MUG.

The third storage server will be placed inside one TRN, as originally planned.

4. Hardware and Infrastructure

This section describes the hardware and equipment acquired or developed, necessary to implement the use case. This includes fiber connections, network equipment, TRNs, QDK devices, encryptors, secret sharing appliances and storage systems. Further, the preparation and testing of said equipment is detailed here.

4.1. Fiber links and network equipment

The long distance link between Graz and Vienna will be divided into three links, each about 70 to 80 km in length. This is necessary as the classical and QKD hardware used, is designed to operate with an optical loss up to 20dB in mind.

Each of the three links consists of one pair of fibers. One of those fibers will be used for the quantum channel whereas all classical bidirectional communication will be multiplexed on the other fiber. Once the trusted nodes and the fibers are installed we will measure the attenuation and will decide which fiber will carry which signal. The classical signal will consist of the 10Gb connection for all classical non encrypted communication and another 10Gb connection solely for the encrypted channel. For multiplexing eight channel DWDM multiplexers will be used. Therefore, another six channels could be multiplexed on the same fiber if the need would arise.

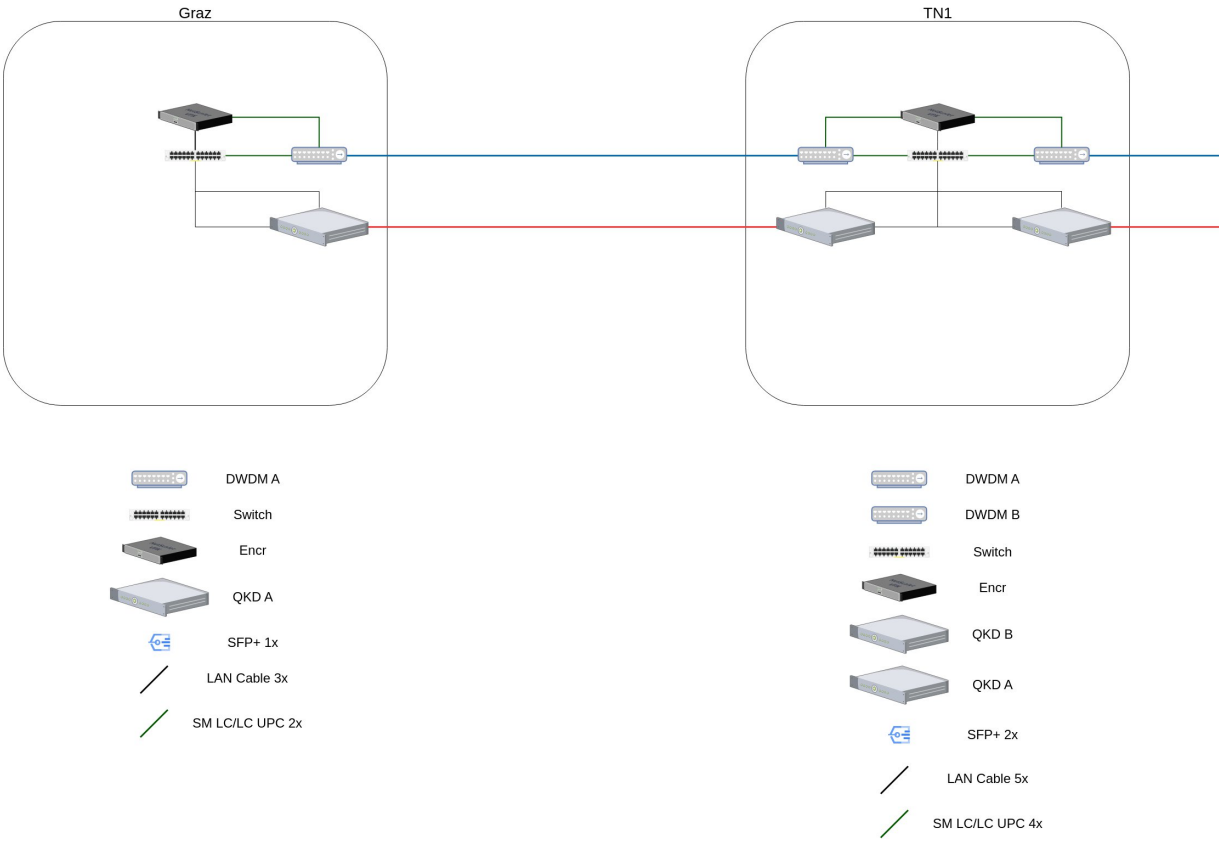


Figure 4: Network plan with all QKD Systems, classical communication hardware and fiber links

Figure 5: Setup and testing of network equipment (DWDM, switch, encryptor)

The single mode DWDM is used to multiplex multiple data channels onto one single fiber. Due to the fact that only a single fiber is used for sending and receiving data, every connection has to use two DWDM channels for transmission.

All management interfaces will be connected to the 10Gb switches which will be located at every location to create a backbone network that will also be used for managing the devices.

The ADVA Encryptors will encrypt and transmit the secret share package between the Medical University in Graz and the datacenter in Vienna.

4.2. Trusted repeater nodes

Since several of the aspects of this solution have to be seen as sensitive and in the near future classified we can only bring a rather generic description of the detailed implementation within this document.

Since the reach of QKD devices is limited by the quality of the fiber and the stability of photon transmission, for long distances (and if fiber domains are crossed, either commercial or political) at some point the signal must be relayed. At this points the QKD generated encryption keys are available in the computer hardware and need special protection against any kind of attacks. A trusted and protected environment is provided by the tamper proof housing/building that contains a server rack with the necessary cryptographic equipment to pass the key to the next pair of QKD devices.

Important tasks are:

- Tempest
- Physical protection of hardware
- Physical protection of generated keys

In order to achieve these targets, the TRN prototypes are equipped with multiple intrusion detection systems, electrical, mechanical and chemical protection systems as well as uninterruptible power supplies. Further a self-destruction mechanism is put in place, to prevent any kind of information leakage by destroying not only the keys, but also all cryptographic equipment in the TRN.

TRNs will be individually customized, depending on the intended usage and the equipment inside. The basic platform are standardized 10 ft. shipping containers that can be hidden in the ground or placed anywhere on a protected area in the field.

In general, it can be stated that several of the national Directors of National Security Authority have been showcased the technologies that are used to protect the TRNs and until now all of them gave “thumbs up” to what they saw.

4.3. QKD devices and encryptors

Three QKD devices of the company ThinkQuantum were procured to cover the distance between Vienna and Graz as they, on paper, can manage up to 25dB of loss. In our testing facility we were able to manage up to 30dB in loss.

The classical equipment, as well as the encryption equipment has a budget of about 24dB of losses, but due to using a DWDM to multiplex the signals, additional 3dB of losses will be added.

The encryption will be handled by ADVA. ADVA uses Layer 1 network communication and therefore needs a dedicated channel on the multiplexer. One Encryption module will be on the end nodes in Vienna and Graz each. In the two trusted node locations hardware for enhancing and boosting the signals will be installed. Thanks to those devices it is not necessary to uncrypt and re-encrypt the transmitted data again on the TRNs.

Due to a mechanical problem some components of the encryptors produced short circuits and a RMA process needed to be started during which an error in production was discovered because of which all encryptor hardware had to be shipped back for inspection and repairs.

All encryptors are already back at AIT where they were again fully assembled and configured to a certain level till the testing of the connection to the KMS systems is concluded.

4.4. Secret Sharing appliances and storage server

To implement the secret sharing network on top of the QKD infrastructure, fragmentiX secret sharing appliances are prepared and configured. These appliances connect to the three storage systems, assembled for the use case, and distribute the protected data.

4.4.1. Secret Sharing appliances

From the beginning of QCI-CAT both fragmentiX CLUSTER appliances were ready for deployment.

> *"fragmentiX CLUSTER® is the high-performance model of the fragmentiX® storage appliance product family for GDPR-compliance, privacy protection, and data loss protection enabling real digital sovereignty. The highly efficient and redundant design of the cluster hardware is perfectly suited for use in datacenters of enterprises, service providers and governments."*

The fragmentiX CLUSTER® 's hardened operating system - was developed by fragmentiX® to make it both secure and easy to use for users and administrators. All functions are kept up to date through regular updates, which can be carried out locally by the administrator.

All data stored with the fragmentiX CLUSTER® is divided into fragments using threshold cryptography and stored on the predefined LOCATIONs to achieve better security and resilience than any other single storage solution can offer. Using multiple of the 10Gb/s SFP+ WAN interfaces, a combination of multiple storage types can be used:

- S3 and S3 compatible hybrid/multi cloud storage on the internet and/or intranet
- Microsoft Azure Blob storage
- NFS compatible storages

For a high performance connection to the user/client workstations, the LAN interfaces of the fragmentiX CLUSTER are SFP+ 10Gb/s interfaces as well. For the scope of this use case, only one of the LAN interfaces is needed.

While the progress in this use case was halted by external factors, the development of the operating system frXOS was focused on. This allows us to make use of features that were not available a year ago:

- Include more advanced network and routing settings according to MUG requirements
- Simplification of configuration process and available options
- WebDAV interface for communication with Linux workstations
- More approved cloud storage providers (e.g., Austrian and EU27 providers like IT&Tel and ionos)
- Full support of S3-object locking mechanism
- Improved cryptography for more performance

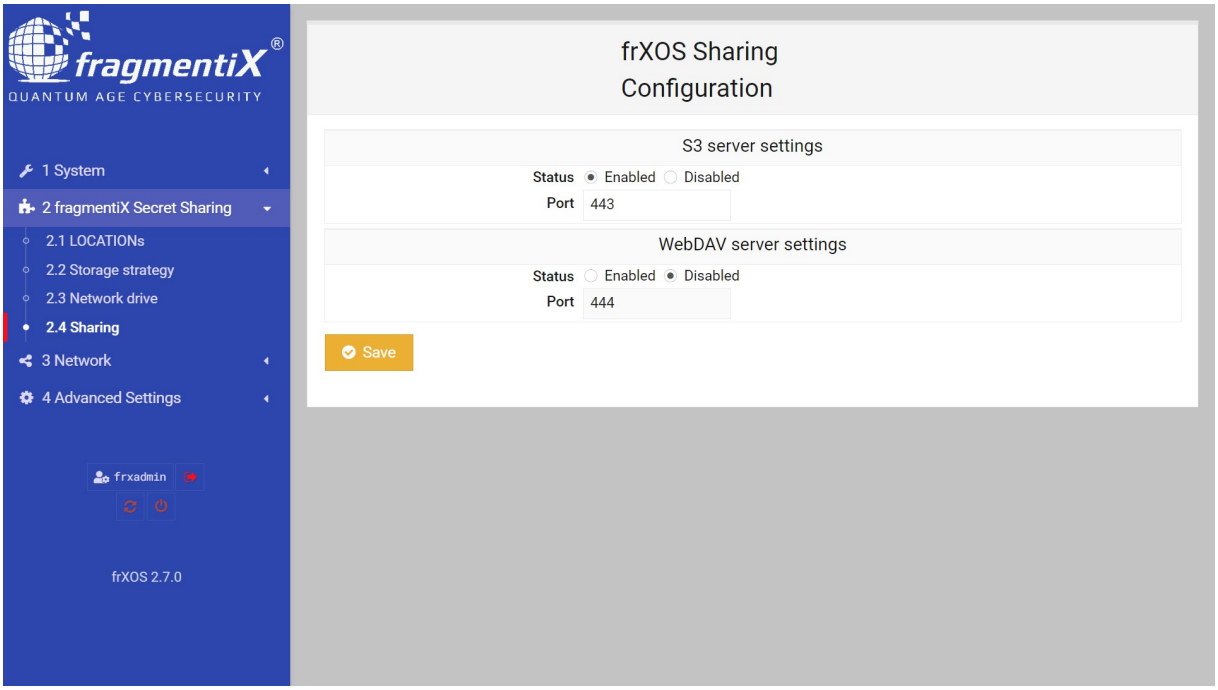


Figure 6: fragmentiX configuration interface with newly implemented features: WebDAV

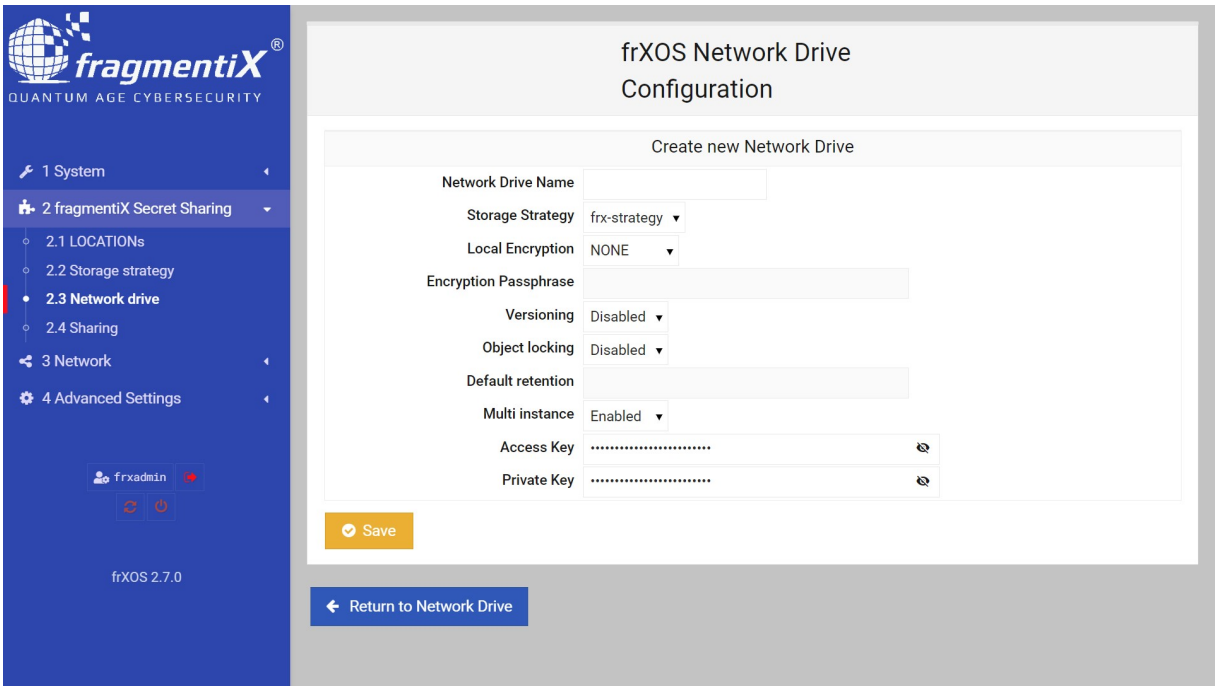


Figure 7: fragmentiX configuration interface with newly implemented features: object locking

To further improve the security of fragmentiX appliances, a penetration testing process was started as part of WP5.

Figure 8: fragmentiX CLUSTER Node A and storage controller server in preparation for deployment at fragmentiX' offices

Figure 9: Storage extensions for two storage systems in preparation for deployment at fragmentiX' offices

4.4.2. Storage systems

The three storage systems for the medical use case were assembled, tested, installed and configured at the fragmentiX offices. Final configuration and updates to the latest software versions will be executed, when the rest of the setup is installed.

One storage system is already in place at the server room at MUG, while the other two systems were kept at the fragmentiX offices until their final destination is agreed on. They will be deployed together with all other equipment (QKD devices, fragmentiX Appliances, encryptors, ...).

- Each of the three storage systems consists of a Dell PowerEdge R730xd (or R720) server with LSI SAS Storage controller.
- Using two redundant SAS cables, each server is connected to a Dell Storage Enclosure with two Bays.
- Each Enclosure is equipped with 56 hard drives (of 6TB each), totaling an amount of ca. 336TB available disk space.
- On each Dell server, we installed Debian12 with MinIO as open source S3-storage-server solution.

4.5. Prototype testing

AIT has developed a QKD prototype system based on the Coherent One Way Protocol (COW). The symbol coding scheme of this protocol is conceptually similar to time-bin encoded BB84 protocols, but simplified due to the coherent phase relation between pulses (see Figure 10).

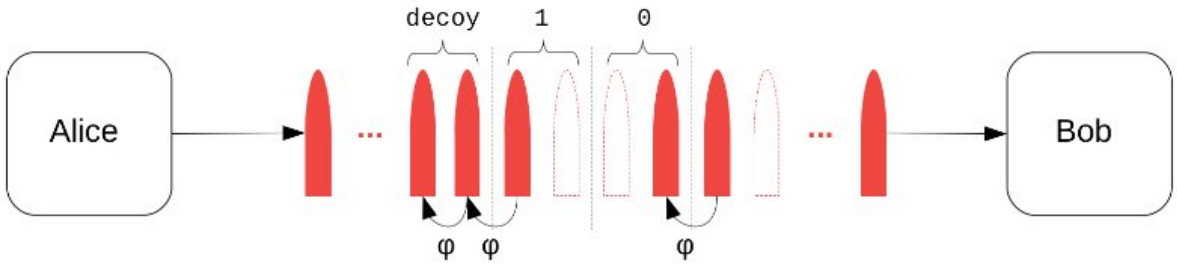


Figure 10: Encoding scheme of the COW protocol

Details about the technical implementation can be gleaned from the block diagrams in Figure 11 and Figure 12. While the technical implementation is not the main focus of this report, we want to stress that the way the prototype was implemented, allows it to be used with a single fiber connecting transmitter (Tx) and receiver (Rx) modules, by multiplexing the (quantum) payload and the (classical) sync signal, as shown below. This is of particular advantage in fiber-scarce scenarios.

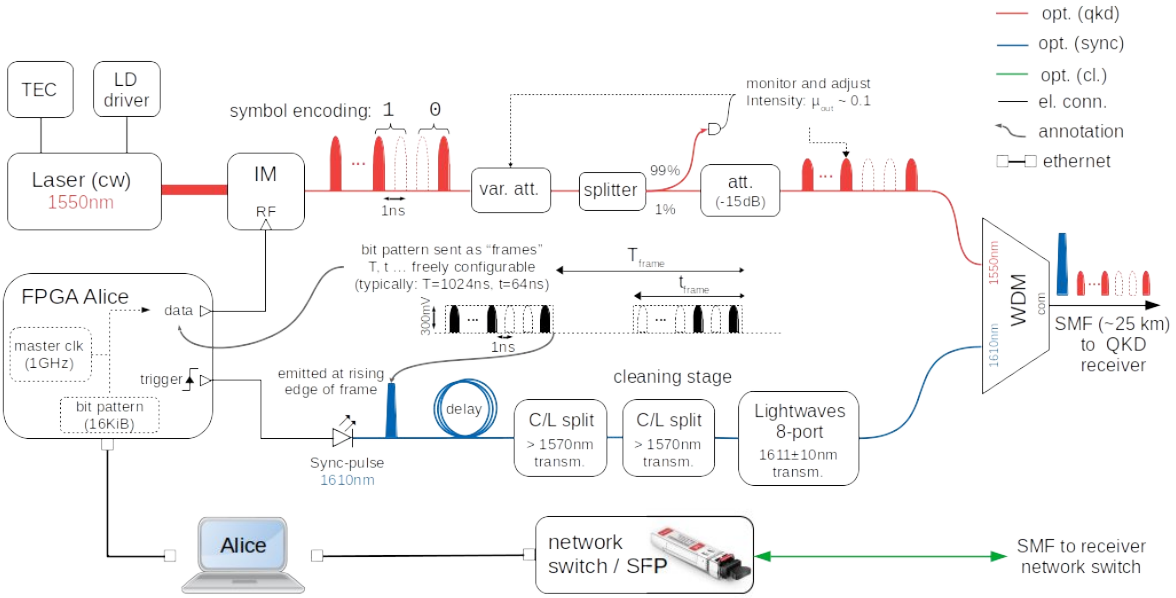


Figure 11: Block diagram COW transmitter (Tx) module. Optical paths are colored for easier distinguishability. The pulse train generated by and exiting the Tx is shown left-to-right. Acronyms: temperature controller (TEC), laser diode driver (LD), continuous wave (cw), intensity modulator (IM), attenuator (att.), optical (opt.), classical (cl.), electrical connection (el. conn.), wavelength division multiplex (WDM), small form factor pluggable (SFP), single mode fiber (SMF)

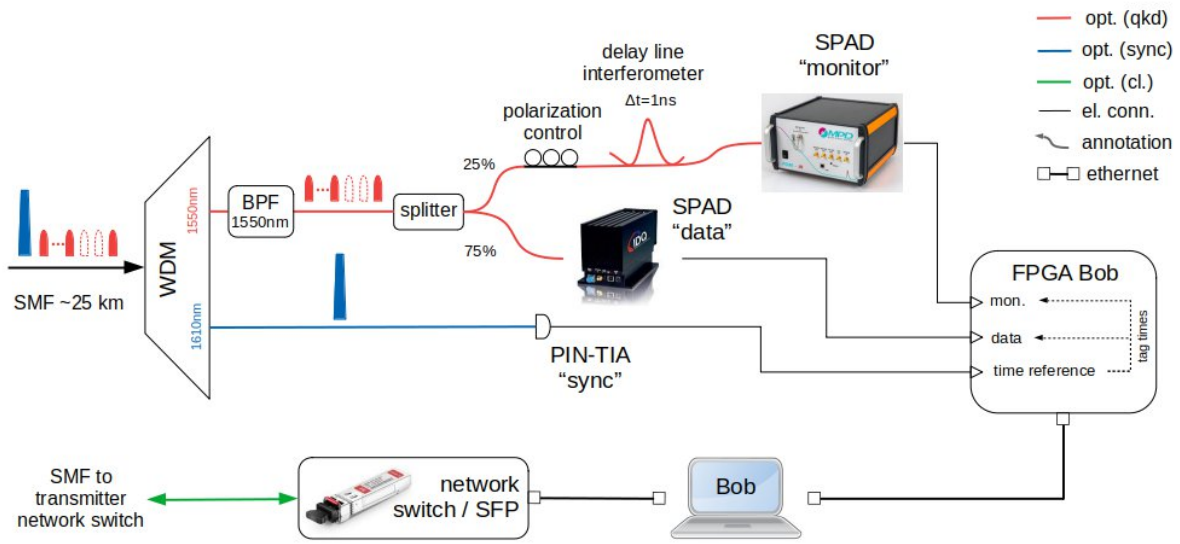


Figure 12: block diagram COW receiver (Rx) module. Optical paths have been colored for easier distinguishability. The incoming pulse train from the Tx is shown to the left. Used acronyms: band-pass filter (BPF), single photon avalanche detector (SPAD)

The Tx and Rx modules are contained in standard 19 inch rack mountable chassis, as show in Figure 13. The Tx module has 1.5 height units, while the Rx module has 3 height units, which is a result of having to contain the cooling solution necessary for single photon detection (Figure 14).

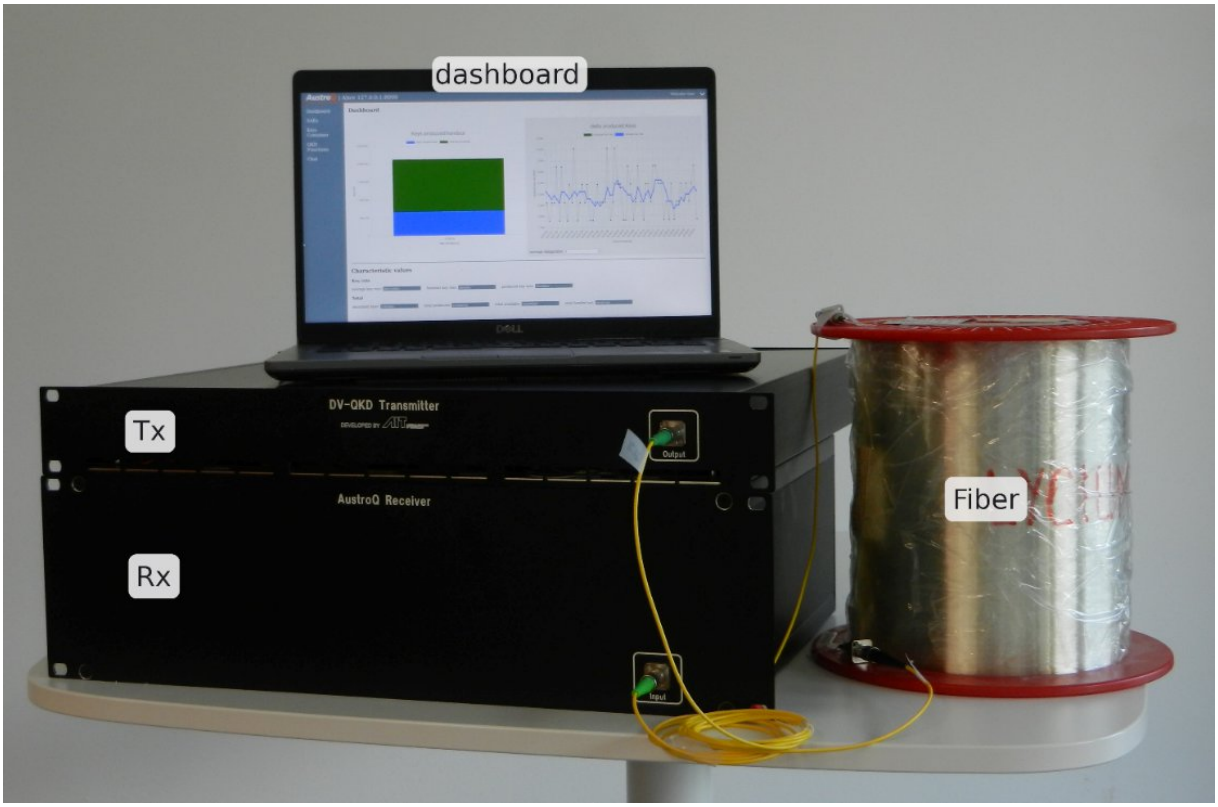


Figure 13: COW QKD system, Tx and Rx modules are connected by 25km fiber coil and the KMS dashboard for live monitoring key generation statistics.

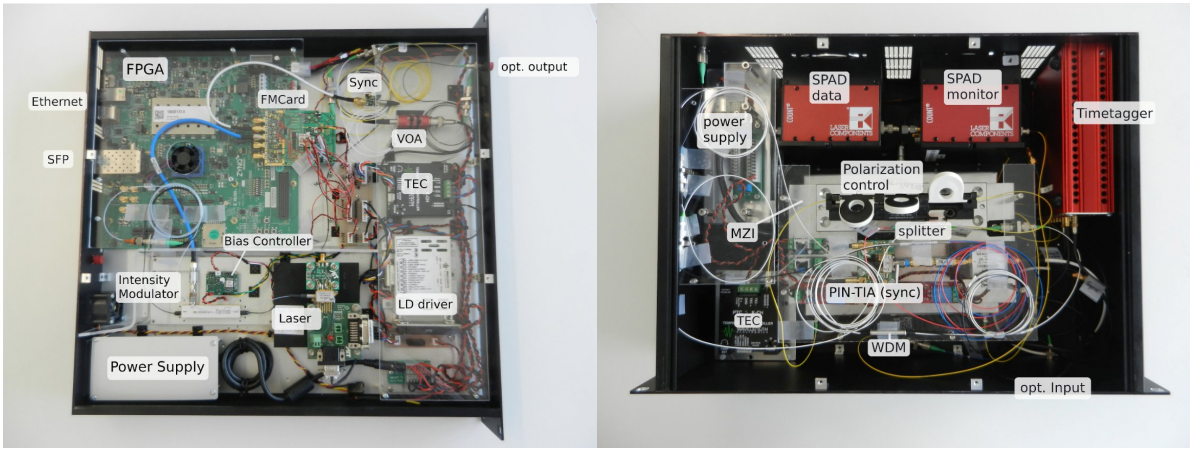


Figure 14: Internal arrangement of components in COW QKD system: Tx (left) and Rx (right). The components still under development for continuous 24/7 operation concern the LD driver (left, Tx) and the polarization controller (right, Rx)

The QKD modules can be connected to AIT's QKD-R10 post-processing software (running directly on the individual control PCs of each system), which allow for live / continuous generation of secure keys. The post-processing pipeline itself is able to interface with an in-house developed, ETSI014 compliant key management system (KMS). Internals of the KMS (key production statistics, SDN functionality) can be gleaned from a web-based dashboard (see Figure 13).

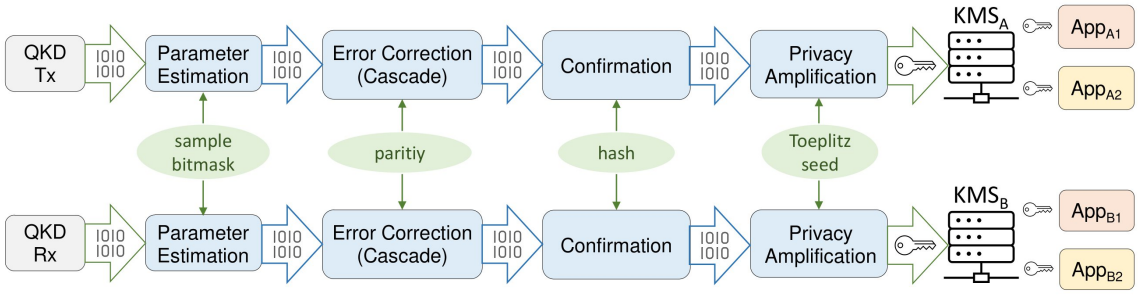


Figure 15: Post-processing pipeline QKD-R10 and ETSI014-compliant KMS, both compatible with COW QKD system

A requirement for this use case is fully autonomous 24/7 operation of the system, without the need for manual calibration (during startup, etc.). In order to achieve this, the system mainly needs to account for active compensation of polarization drift and optical phase. AIT has developed an automated calibration loop for compensation of polarization drift and is currently working on the calibration loops for compensation of polarization drift, as reported in T8.2.

Specific to this use case and in anticipation of the high attenuations that the associated fiber link might impose and that the QKD system thus has to deal with, AIT has performed comparative measurements between the Rx module using InGaAs SPADs (Figure 14) and super-conducting nanowire single photons detectors (SNSPD). While the former allow use and system demonstration in the field, due to their relatively compact size, the latter enable the system to generate keys for much longer distances / higher attenuations. This is due to the inherently better SNR of SNSPDs, resulting from both the better single-photon detection efficiencies and lower dark-count rates. The cryogenic cooling necessary to achieve super-conducting operation makes the detectors quasi-static though, meaning that the Rx module has to remain at AIT premises if operated with SNSPDs.

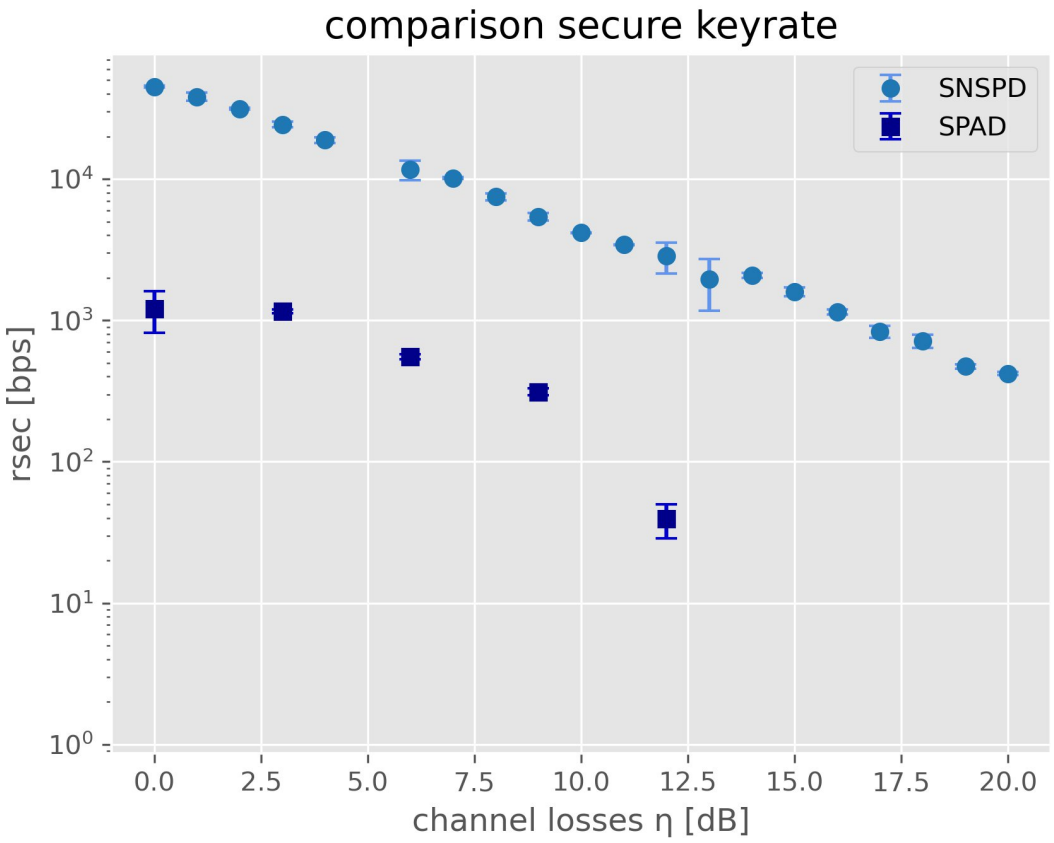
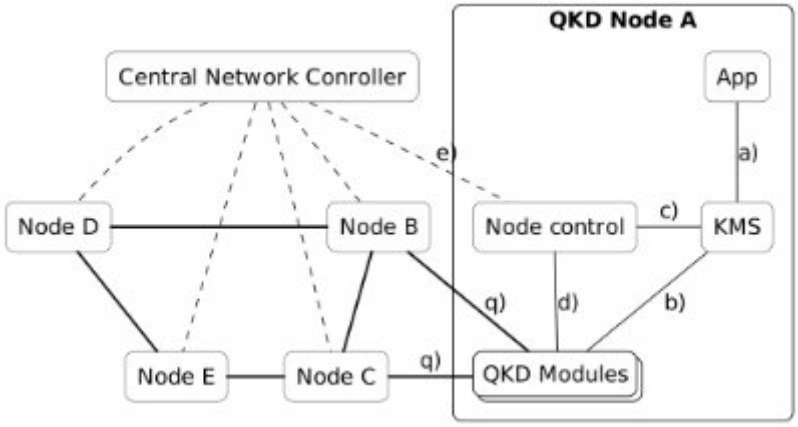


Figure 16: Secure key generation rates of the COW QKD system, comparison between operating the Rx module with SNSPDs vs InGaAs SPADs.

AIT also further developed its key management system (KMS).[1] The role of the KMS is to provide the link between the network of QKD devices and the application layer requesting key material. Therefore, it is a central tool in a QKD network as soon as the network contains two or more links. Keys are retrieved by the application via the ETSI 014 interface, that provides a REST-style interface.



[1] More information on the KMS can be found at https://qkd-kms.ait.ac.at/.

Figure 17: QKD system architecture of a QKD node with the KMS as central link between the Application and the QKD modules. (from [JLRT23])

To implement the core functionality of KMS, it needs to provide the following functionalities:

- **Key Forwarding (or key relay):** Key forwarding is one of the core functions of a KMS. It is the process of establishing an end-to-end key using the intermediate trusted nodes of the QKD network by sampling a random key at the initiator, encrypting it using the key from the QKD link. At each node, the key is decrypted and then encrypted with the QKD key from the next link. The receiver node decrypts the key and forwards it to the application. The nodes in the middle – trusted nodes - must be trustworthy, since during forwarding they temporarily obtain the final key.
- **Key management:** The use of TNs means that a breach of QKD keys is one of the worst-case scenarios. Therefore, to reduce the harm that compromised keys can cause, QKD keys that are not used within a certain time period are deleted. For the same reason, securely deleting keys after delivery is important. Key management also keeps track of the state of keys, such as whether a key has been synchronized or if a reserved key has been delivered to one node but is not yet at the corresponding node.
- **Database synchronization:** Essentially, all KMS instances of a QKD network can be considered a distributed database system. Therefore, the KMS instances must ensure database consistency. This includes verifying that the data on peer KMS instances is consistent as entries are created, re-sized, deleted or changed.
- **Quality of Service (QoS) management:** The KMS reports key performance indicators to the network controller so that an optimal path, at the required bandwidth, can be selected. The KMS must enforce the performance values agreed with the apps and network provider, such as key consumption rate.

The central functionality for deployment in a large network is the implementation of key forwarding.

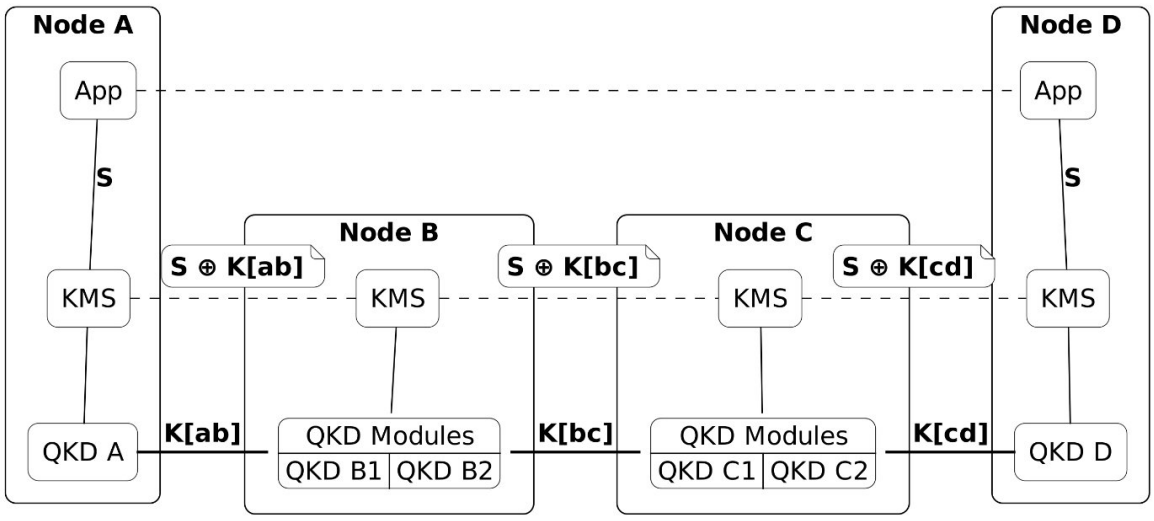


Figure 18: Decentralized key forwarding with keys S sent encrypted between using the QKD links to encrypt the key between Nodes S and D (from [JLRT23]).

Figure 18 illustrates the forwarding of keys through intermediate nodes when an application requests keys for its peer application on a QKDN node with which it has no direct connection. The Network Controller configures the forwarding tables of the KMS instances that are in the chosen path through the QKDN to the destination node. The source KMS then generates a random value, to be used by both applications as a key, and encrypts it using the key generated by the QKD device on the next directly linked node. The encrypted key is forwarded to the KMS on the next node in the path, which then

decrypts it, obtaining the randomly generated value, re-encrypts it using QKD generated keys and forwards it. The common ITS de- and encryption method is a One Time Pad (OTP) with bitwise exclusive or (XOR) operations This forwarding process continues until the final destination is reached at which point the two end-nodes, which are not connected directly, share symmetric keys that can be provided to the applications.

We note that this is not the only technically feasible approach to implement key forwarding. However, it is the method currently implemented by the KMS at AIT. Compatibility with an KMS from a different vendor is established using the ETSI GS QKD 020 interface, which is planned to be implemented until the end of the project.

Furthermore, we discuss the central interfaces between the KMS, the application, and other components of a QKD network that are currently implemented by AIT's KMS:

ETSI GS QKD 004 defines an API between an application and the KMS. While it is defined between KMS and application, it is often used for implementation by a simpler KMS ("local KMS") running on the QKD hardware to manage the keys of a specific link. The standard defines the following interface:

- open_connect: The application requests from the KM a key stream between the supplied source and destination endpoints with the characteristics defined in the Quality of Service (QoS) parameter. The KM responds with a key stream id, and optionally a QoS proposal, or rejects the request.
- get_key: The application requests keys for the given key stream id. Additional metadata can be supplied.
- close: The application requests that the key stream is closed. Keys already allocated for this key stream are held until the other endpoint also sends a close request or the key stream's Time To Live (TTL) parameter expires.

Applications need keys on demand whilst QKD devices deliver keys when generated because resource constraints make secure data storage difficult. Thus the KMS layer in-between the application and local KMS running on a QKD module is able to bridge this gap by either pulling keys from the QKD modules or receiving them via a push mode. The latter is specifically of interest for QKD modules since it removes the need to store key material on the QKD hardware moves this task to the network-wide KMS.

ETSI GS QKD 014 defines a RESTful API for communication between an application and a KMS. In the standard the application initiating the communication is referred to as the "master" and the responding application is called the "slave".[2] Communication is performed using the HTTPS protocol with TLS 1.2 or above. The API is composed of three methods:

- Get status: Returns the KMS' status data and information regarding the keys available.
- Get key: Returns key data to the master application, with optional parameters specifying additional key delivery requirements. The slave application may then request matching keys from its KMS using the key ID provided in the response.
- Get key with Key IDs: Returns key data for the specified key ID to the calling slave application.

ETSI GS QKD 015 introduces the concept of Software Defined Networks (SDN) for QKD networks. SDNs separate data and control by having the main control logic in a centralized SDN Controller. The standard defines an API between the SDN Controller and the SDN Agents which is deployed on the nodes to configure the node sub-modules, such as the KMS.

[2] This terminology is outdated and does not reflect the currently common use in networking. The standards are however still specifying the roles with the old terminology.

A more detail analysis of the design and implementation aspects of the KMS is also presented in [JLRT23].

The KMS is developed following modern and industry grade best practices for secure software development and several tools from an extensive test suite to tools for code analysis aid the developers in this process. Test driven development with unit-tests running in the CI pipeline are maintained during development at a high coverage is a central concept in the software development approach. Integration tests and test deployment in a QKD network simulation are executed as well to ensure that the software confirms to the expectations by other network components. Modern secure implementation techniques are also applied. A zero-warning policy is in place and the CI pipeline executes a static code analysis tool for every pushed commit. Dynamic code analysis is also used to ensure a safe and sound execution of the KMS.

The result of the still ongoing development work has been presented at the QKD network demonstration at ECOC 2024[3] where the KMS by AIT was picked to implement the KMS of the Austrian domain. Overall, the showcase consisted of three national domains (Austria, Germany and Spain), and modeled a small EuroQCI. The main novelty of the demonstration was showing the different domains connected together. To further mimic the EuroQCI the three organizational domains were assigned to the country that implements the KMS layer, therefore a Spanish domain, a German Domain and an Austrian Domain were showcased.

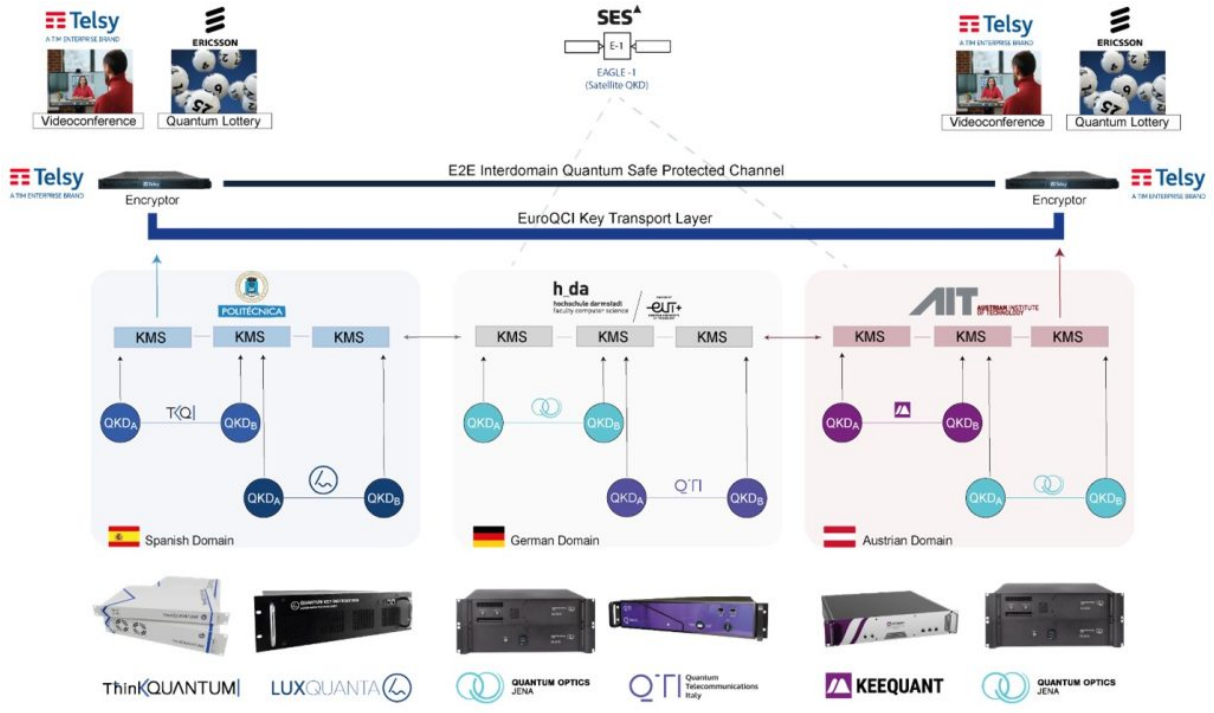


Figure 19: Setup the demonstration at ECOC 2024 of three national domains (Spain, Germany, Austria) with the hardware and software components provided by different vendors.

The AIT KMS performed very well during the three days and, received, synchronized, forwarded and delivered QKD keys. The main interfaces used was ETSI GS QKD 014 towards the QKD devices and to the upper layer. The key forwarding with information-theoretically secure encryption and authentication proved performant and reliable.

With this first test of the KMS with different hardware (KeeQuant and Quantum Optics Jena) and software vendors we are confident that the KMS will serve its role as part of the use case

[3] https://qkd-kms.ait.ac.at/2024/10/01/kms-successfully-showcased-at-ecoc-2024-exhibition/

implementation. There are however some differences in the deployment in the QCI-CAT network. The devices for the network between Vienna and Graz is built using ThinkQuantum devices. Therefore, testing of the KMS with these devices and their implementation of the KMS-facing interfaces has still to be conducted. An additional step is to also test the integration of the KMS with the application on top, meaning the systems built and implemented for the demonstration of the medical use case. The KMS developed by AIT is ready to be integrated with these systems, but the integration itself will happen later during the project runtime.

5. Setup, Integration and Demonstration

In general, it has to be said, that due to the delays and other problems mentioned before, the demonstration has not started yet. Nonetheless some preparation could be done and is detailed below.

5.1. Connection infrastructure

Two locations on the way from Vienna to Graz have been selected and prepared for the installation of the two TRNs. In October the TRNs have been delivered and put in place. Final configurations are ongoing.

Currently there are fibers in place between the Arsenal data center in Vienna and the TU Graz. These fibers are rented for the duration of the project from a commercial provider and ready to be used. At the intermediary locations of the TRNs, the fibers are available, but must be connected inside the TRNs.

5.2. Application layer

At the Medical University of Graz, the use case has been well prepared in that a database has been established where the original pathogen sequence and associated data of the high containment laboratory is documented. The data is encrypted by using the fragmentiX server that is located in the data center of the Medical University Graz.

6. Next Steps

In order to efficiently advance the progress of the use case, the following steps will be executed in the near future or are currently worked on:

- Enhancement of the TRNs at the deployment sites
- Connecting the MUG server room to the fiber network terminating at TU Graz
- Deploying network equipment at all four sites
- Deploying QKD devices and encryptors at all four sites
- Deploying fragmentiX secret sharing appliances and storage systems at three sites
- Determining and training the users of the secret sharing network

Later in the project, it is planned to extend the QDK network to St. Johann.

Summary

Summarizing the progress made in the implementation of the medical use case, it has to be said once again, that the circumstances changed because of the events in the first project year.

The re-planning and adaptation took almost a full year and final confirmation and approval is still under negotiation.

Nonetheless, the preparation of the secret sharing and storage appliances was done, while waiting for the QKD devices and deployment schedules. Further the Testing of the AIT QKD device was prepared and started as well.

The TRN prototypes, developed in WP8, were deployed and await their final network and power connection in the near future (planned for November 2024).

The next step, after the final connection of all involved sites, is to install the hardware and start testing, as it has been prepared already in the lab.

Once, the demonstration is in place, an extension of the QKD network to St. Johann is planned together with the other use case.

Appendix A - List of Acronyms

BSL4 - BioSafety Level 4

QKD - Quantum Key Distribution

DWDM - Density Wavelength Division Multiplexing

KMS - Key Management System

RX - Receiver

TX - Transmitter

RMA - Return Merchandise / Material Authorization

COW - Coherent One Way

LD - Laser Diode

SNSPD - Superconducting Nanowire Single Photons Detectors

SPAD - Single Photon Avalanche Detector

SNR - Signal to Noise Ratio

LAN - Local Area Network

WAN - Wide Area Network

S3 - Simple Storage Service (Amazon)

NFS - Network File System

frXOS - fragmentiX' Operating System

DNA - DesoxyriboNncleic Acid

NDA - Non Disclosure Agreement

OTDR - Optical Time Domain Reflectometer

QoS - Quality of Service

ITS - Information Theoretic Security

OTP - One Time Pad

API - Application Programming Interface

TTL - Time To Live

SDN - Software Defined Networks

CI - Continuous Integration

Appendix B – Bibliography

[JLRT23] Paul James, Stephan Laschet, Sebastian Ramacher, Luca Torresetti: Key Management Systems for Large-Scale Quantum Key Distribution Networks. ARES 2023: 126:1-126:9