30-05-2024

Deliverable D2.1
QKD system architecture plan with QKD methodology

Contractual Date:	30-06-2023
Actual Date:	30-05-2024
Grant Agreement No.:	101081247
Work Package:	WP2
Task Item:	T2.2
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	KIFÜ
Authors:	András Jákó (KIFÜ); Sándor Imre (BME)

Abstract

WP2's primary goal is establishing a country-wide QKD-secured network comprising wide area and metropolitan data communication links. Most of this system's hardware and software components should be commercial off-the-shelf items. Therefore, a public procurement procedure is needed to purchase them. An essential input to this procurement procedure is the planned QKD system architecture described in this report, which will be refined based on the procurement outcome.

Co-funded by the European Union

KIFÜ on behalf of the QCIHungary project. The research leading to these results has received funding from the European Union's Digital Europe Programme under Grant Agreement No. 101081247 (QCIHungary).

Document Revision History

[This section to be deleted or hidden before publication of deliverable]

Version	Date	Description of change	Person
1	08-06-23	First draft issued	A. Jákó
2	12-06-23	Added "Executive Summary" and "Conclusions".	A. Jákó
3	15-06-23	Added link overview figure. Specified BME in-campus link buildings.	A. Jákó
4	29-06-23	Review and delivery	S. Imre, J. Mohácsi
	19-04-24	1st project review required update in the deliverable	
5	15-05-24	Updated content with market consultation results and added optical link parameters.	A. Jákó
6	21-05-24	Update conclusions	J. Mohácsi
7	30-05-24	Clean up	J. Mohácsi
		Approved	

Table of Contents

Table of Figures

Table of Tables

Executive Summary

In the QCIHungary project, a Hungarian national quantum communication network will be established. This report contains the network architecture plan.

From this plan's point of view, the network consists of similar point-to-point data communication links. Each link has

- a regular **network path** that connects the two endpoints of the link,
- a **data encryption subsystem** that encrypts traffic at the ingress endpoint of the link and decrypts it at the egress and
- a **key distribution subsystem** that delivers the same random key bit sequence to the encryption subsystem at the link's endpoints.

The network path and the encryptors use mature technologies. This project focuses on the key distribution subsystem and its interoperation with the encryptors.

The components of the data encryption and the key distribution subsystems must be purchased using a public procurement procedure. Financial rationality dictates that these two subsystems should belong to independent offer parts, but they must interoperate technically. As the interface between these subsystems is in the early stages of standardisation, with little public information on their implementations, we held preliminary market consultations to understand QKD-encryptor interoperability. We refined the technical specifications based on information gathered from these consultations.

1 Introduction

The QCIHungary project aims to lay down the foundations of a national quantum communication infrastructure in Hungary. The capital, Budapest, will be connected with three cities, and a metropolitan network within Budapest will be constructed using commercial off-the-shelf quantum key distribution (QKD) systems.

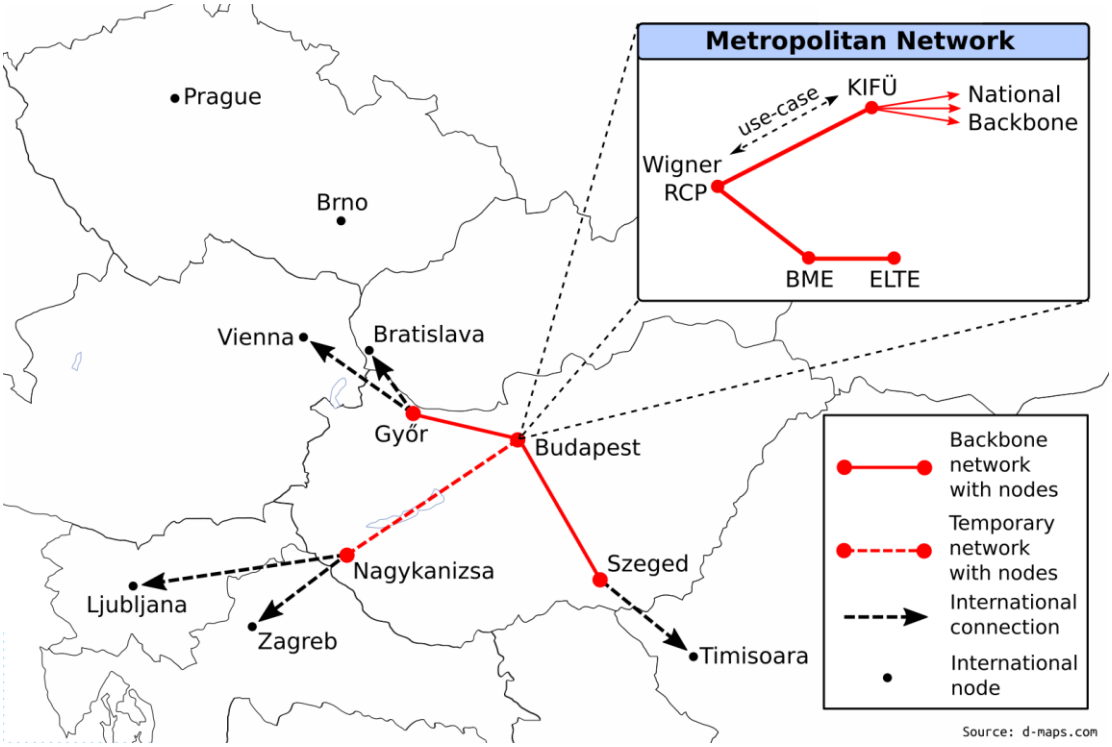

Figure 1: Planned national quantum communication backbone

In addition to the national quantum backbone links, two local connections will be established, one each on BME and ELTE campuses.

From the point of view of the present task, the planned system consists of independent point-to-point data communication links. All links will be used for encrypted data transmission. Encryption keys are provided by a key distribution subsystem per link. Encryption/decryption is performed by the data encryption subsystem, consisting of different tools per link.

The links will be used for diverse purposes:

- to test, study and evaluate the deployed system in WP2
- provide encryption keys for the use-case of WP3
- indirectly sharing results and lessons learnt among other NatQCI projects in WP5
- training in WP6
- testbed for software development in WP7

For some of the links, the current architecture plan includes the key distribution and data encryption subsystems, as well as test traffic generators. For one link, it includes only the key distribution subsystem. There are also links for which all subsystems are outside the current plan's scope.

1.1 Plan Maturity

At this stage of the public procurement procedure for the components of the key distribution subsystem, the amount of QKD nodes needed is yet unknown because the maximum allowed distance (more precisely, the optical attenuation) between neighbouring QKD devices varies among QKD products. We have the optical fibres and possible QKD node locations ready, but skipping some node locations where a QKD device pair can handle concatenated optical sections is certainly possible.

2 Market Research and Preliminary Market Consultation Results

To gather a better understanding of available QKD products, encryptors, and their interoperability, we first studied information available publicly and through our existing vendor contacts, then we conducted preliminary market consultations. Seven vendors, mainly QKD manufacturers, accepted our invitation to the market consultation. The following manufacturers or their representatives provided information in this stage of the planning process:

- Adtran/ADVA
- Cisco Systems
- Fortinet
- ID Quantique
- Juniper Networks
- KeeQuant
- Senetas/Thales

- Telsy/QTI
- ThinkQuantum
- Toshiba

The types of QKD equipment discussed during the market consultations have different technical capabilities and parameters. We have seen equipment operating on one and two optical fibres, equipment capable of interoperating with DWDM systems in various ways, and a variety of capabilities in terms of system operation.

Key conclusions of our market research and the consultations regarding the architecture plan are the following:

- There are multiple protocols for QKD to encryptor key delivery: ETSI GS QKD 004 and 014, Cisco SKIP, and some others. The most widely implemented one is ETSI GS QKD 014, which is much ahead of the others.
- As we have slightly different technical needs from one data communication link to another (we need DWDM interoperability for one of the links only; research- and training-oriented extra capabilities are necessary for two links), it makes sense to split the procurement into several tender lots, as this can result in a lower set of mandatory capabilities per lot, which leads to more competition.
- Quite a few QKD-encryptor interoperability technical demonstrations and proof-of-concept style experiments are published (e.g., as press releases). Although this looks promising, a significant number of them turned out to use internal, unreleased encryptor software/firmware that the vendor does not plan to publish at all or not in the near future.
- Since both one- and two-fiber systems will possibly be considered, we collected data on the availability of a second fibre in all links, see Section 3.1.1.
- Some two-fibre QKD systems tolerate only minor length differences between the two strands.

3 QKD System Architecture Plan

Below, we describe the design considerations and assumptions first. Then – advancing from the overall view towards the details – follows the description of the planned network, the architecture of its data communication links, and finally, the building blocks of a single link.

3.1 The Planned Network

This architecture plan concerns potentially eight data communication links secured using terrestrial, optical fibre-based QKD systems. Some links will operate with commercial off-the-shelf QKD equipment, and some will be tested with a system developed in WP4.

Endpoint "A"	Endpoint "Z"	Link Type	Primary Purpose	Required Key Rate [bit/s]
KIFÜ Budapest	Győr	national backbone wide area link	system testing and evaluation in WP2	200
KIFÜ Budapest	Nagykanizsa	national backbone wide area link	system testing and evaluation in WP2	200
KIFÜ Budapest	Szeged	national backbone wide area link	system testing and evaluation in WP2	200
KIFÜ Budapest	Wigner RCP Budapest	national backbone metropolitan link	providing encryption keys for WP3's real use-case, WP4 testing	1000
Wigner RCP Budapest	BME building I	national backbone metropolitan link	WP4 testing	200
BME building I	BME building F	local	training in WP6, WP4 testing	200
BME building I	ELTE Lágymányos campus	local	training in WP6 and software development in WP7	200
ELTE Lágymányos campus	ELTE Trefort campus	local	software development in WP7	1000

Table 1: Data communication links concerned in this plan

The Budapest – Nagykanizsa link will be temporary. It will share the active equipment with the Budapest – Szeged and Budapest – Győr links; only the first or the latter two links will operate simultaneously.

3.1.1 Optical links

As the table below describes, a fibre pair is available on all planned links, although the second fibre can only be used for a fee on some of them. Where only the first strand is free, both strands are also prepared and ready, so we can start using either one or two fibres on these links in an equally short time. Regarding administrative issues: KIFÜ has an existing framework contract with, among others, Magyar Telekom for the lease of such optical links, and Magyar Telekom's commercial offer is also available for the second fibres in question. Accordingly, both single- and dual-fibre QKD systems are acceptable in all cases.

Endpoint "A"	Endpoint "Z"	Owner/Provider	Remarks
KIFÜ Budapest	Győr	Magyar Telekom	The first fibres are Magyar Telekom's in-kind contributions. The second fibres are also ready and available for a fee.
KIFÜ Budapest	Nagykanizsa		
KIFÜ Budapest	Szeged		

Endpoint "A"	Endpoint "Z"	Owner/Provider	Remarks
KIFÜ Budapest	Wigner RCP Budapest		
Wigner RCP Budapest	BME building I		A fibre pair is available free of charge and has already been used by BME.
BME building I	BME building F	BME	A fibre pair is available.
BME building I	ELTE Lágymányos campus	BME+ELTE	Fibre pairs are available. A few universities own a tiny Budapest metropolitan optical network operated by BME. These links include sections on the common metro optical network and the universities' internal fibre infrastructures.
ELTE Lágymányos campus	ELTE Trefort campus		

Table 2: Optical link providers

The financial difference between one- and two-fibre QKD systems can be handled well by life-cycle costing. According to Directive 2014/24/EU on public procurement, Hungarian public procurement law also mandates life-cycle costing when possible. So, we will allow both one- and two-fibre solutions in the technical requirements of the QKD call for tenders and will calculate scores based on the sum of the QKD equipment cost and the fee of the second fibre where applicable.

Optical parameters per section for each planned data communication link are detailed in the tables below. Attenuation at 1550 nm was measured with OTDR or from the KIFÜ operated DWDM system, while 1625 nm values came from a fibre monitoring system operating on another strand in the same optical cable. The required QKD link budget is calculated by adding 2-3 dB to the measured attenuation to leave enough room for potential repairs or any other degradation that increases attenuation.

Section	Length [km]	Attenuation Measured		Required QKD Link Budget [dB]
		@ 1550 nm [dB]	@ 1625 nm [dB]	
KIFÜ Budapest – BG1	48	13.490	13.5	16
BG1 – BG2	27	7.221	7.3	10
BG2 - Győr	75	18.567	17.4	21

Table 3: KIFÜ Budapest – Győr link sections

Section	Length [km]	Attenuation measured		Required QKD link budget [dB]
		@ 1550 nm [dB]	@ 1625 nm [dB]	
KIFÜ Budapest – BN1	34	8.200	8.4	11
BN1 – BN2	61	13.027	14.5	16
BN2 – BN3	57	13.710	14.3	16
BN3 – BN4	59	13.724	14.0	16
BN4 – BN5	32	7.635	8.0	10
BN5 - Nagykanizsa	60	14.192	15.8	17

Table 4: KIFÜ Budapest – Nagykanizsa link sections

Section	Length [km]	Attenuation measured		Required QKD link budget [dB]
		@ 1550 nm [dB]	@ 1625 nm [dB]	
KIFÜ Budapest – BS1	76	N/A	18.0	21
BS1 – BS2	58	11.589	11.9	14
BS2 – BS3	33	6.515	7.7	9
BS3 – Szeged	70	15.222	16.1	18

Table 5: KIFÜ Budapest – Szeged link sections

Section	Length [km]	Attenuation measured		Required QKD link budget [dB]
		@ 1550 nm [dB]	@ 1625 nm [dB]	
KIFÜ Budapest – Wigner RCP Budapest	21	8.658	N/A	11

Table 6: KIFÜ Budapest – Wigner RCP Budapest link

Section	Length [km]	Attenuation measured		Required QKD link budget [dB]
		@ 1550 nm [dB]	@ 1625 nm [dB]	
Wigner RCP Budapest – BME building I	21	7.604	N/A	10

Table 7: Wigner RCP Budapest – BME building I link

Section	Length [km]	Required QKD link budget [dB]
BME building I – BME building F	5	6

Table 8: BME building I – BME building F link

Section	Length [km]	Required QKD link budget [dB]
BME building I – ELTE Lágymányos campus	3	5

Table 9: BME building I – ELTE Lágymányos campus link

Section	Length [km]	Required QKD link budget [dB]
ELTE Lágymányos campus – ELTE Trefort campus	8	6

Table 10: ELTE Lágymányos campus – ELTE Trefort campus link

3.2 The architecture of a data communication link

A point-to-point data communication link in this network consists of three main building blocks:

- A regular **network path** connects the two endpoints of the data communication link.
- The **data encryption subsystem** encrypts traffic at the ingress endpoint of the data communication link and decrypts it at the egress.
- The **key distribution subsystem** delivers the same random key bit sequence to the encryption subsystem at the endpoints of a point-to-point data communication link.

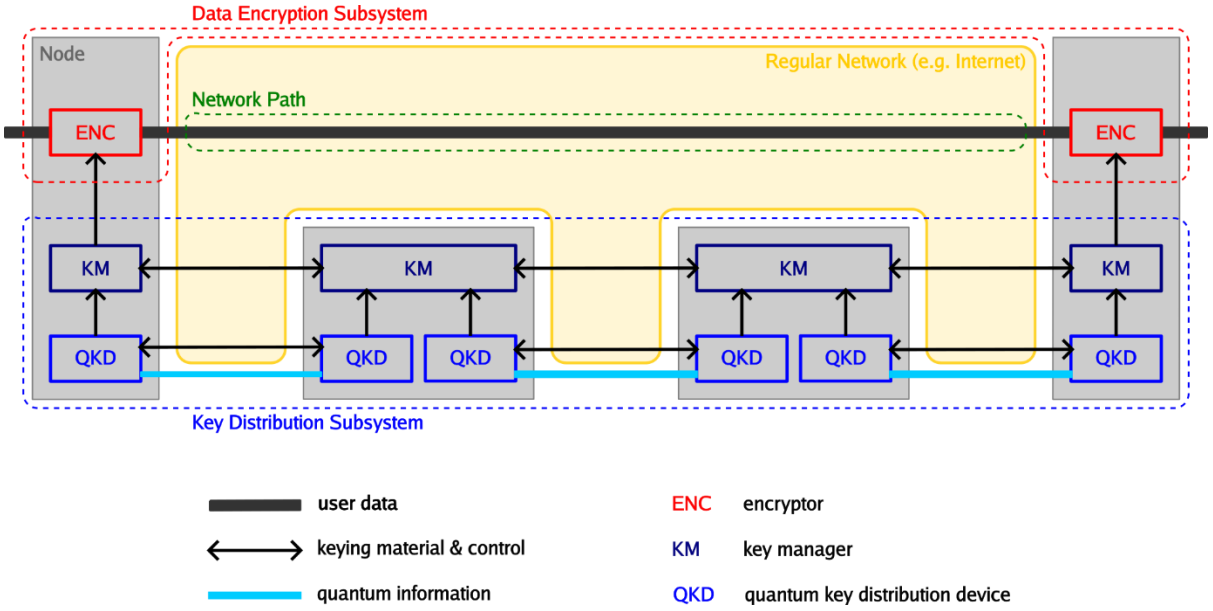

Figure 2: Link architecture overview

3.3 System Building Blocks

The three main building blocks mentioned in the previous chapter will be described here in detail. For some links, a pair of test traffic generators are planned, too, described afterwards.

3.3.1 Network Path

Data between the two data communication endpoints travel on a regular network path in both directions. The network path can be a path in an IP or an Ethernet network, a WDM service, or any digital data communication connection.

Data transmitted on the network path may be observed, recorded or even modified by adversaries. Hence, the encryption subsystem is needed to secure communications on the network path against eavesdropping and other attacks.

3.3.2 Data Encryption Subsystem

The data encryption subsystem's task is to encrypt traffic at the ingress endpoint of the data communication link and decrypt it at the egress. As the link topology is point-to-point, the subsystem's primary (or the only) component is a pair of encryptor devices that encrypt the traffic passing through them in one direction and decrypt in the opposite direction.

The encryption subsystem uses symmetric key cyphers that are computationally cheap and resist cryptoanalysis even by quantum computers (according to state-of-the-art science).

Network traffic encryption is possible at multiple protocol stack layers, including the data link, network, and presentation layers. To gather broad knowledge and experience, we decided to use diverse encryptors operating at the lower OSI layers.

3.3.2.1 Encryptor Types

IPsec

The IPsec encryptor routes and forwards IP packets and encrypts/decrypts them using IPsec. It acts as a router with at least two interfaces: One to the network path leading to the other end of the data communication link and at least one to the client(s) of the data communication link. Configuration settings specify which part of the traffic should be encrypted/decrypted.

MACsec

The MACsec encryptor switches Ethernet frames and encrypts/decrypts them using MACsec. It acts as a bridge with at least two ports: One to the network path leading to the other end of the data communication link and at least one to the client(s) of the data communication link.

In-line

The in-line encryptor transmits data streams (Ethernet frames or PDUs belonging to a lower OSI layer) between a cleartext and a cyphertext port. When inserted into an appropriate data link, it encrypts data traffic passing through it in one direction and decrypts it in the opposite direction. Its cyphertext port connects to the network path leading to the other end of the data communication link.

3.3.3 Key Distribution Subsystem

The same encryption key is necessary for the encryption subsystem's symmetric cyphers at the data communication endpoints. This means the confidentiality problem is shifted from the data traffic to the encryption key by applying symmetric key encryption. Distributing the encryption key is most commonly handled by public key algorithms in current hybrid schemes or by using a separate channel secured by entirely different means (e.g. a courier). In our case, the key distribution subsystem delivers the same random key bit sequence to the pair of encryptor devices operating at the endpoints of a point-to-point data communication link, and the encryption keys are derived from these identical key bit sequences.

The subsystem is composed of

- one or more **quantum key distribution (QKD) device pairs**,
- **optical fibre** connecting the members of every QKD device pair and
- **key management system (KMS)** devices orchestrating QKD devices and key derivation.

Distance between the members of a QKD device pair is limited; therefore, we expect the inter-urban (wide area) links to be too long for any single QKD device pair. In that case, the key distribution subsystem shall be built from daisy-chained sections, one QKD device pair per section.

3.3.3.1 Components

Optical Path

ITU-T G.652 optical fibre (or fibre pair) connects the members of every QKD device pair. The quantum channel of the QKD device pair uses the first (or the only) fibre.

The optical path may consist of one or more sections based on the data communication link length and QKD device pair reach. A secured location is provided at the section boundaries for links consisting of multiple sections.

QKD

Both quantum key distribution device pair members deliver an identical random key bit sequence. Key bits are delivered with certainty that an attacker having access to the optical fibres cannot reveal them unnoticed. Quantum physics laws ensure this by ultimately binding key information to physical parameters that unauthorised observation corrupts in a way detectable by the QKD system.

KMS

For longer data communication links composed of multiple sections, the key management system derives the key bit sequence to be delivered by the key distribution subsystem from the keys provided by the per-section QKD device pairs. Based on the WP5 discussion and maturity of the QKD and KMS implementation we selected ETSI GS QKD 014 interface for exchanging key material.

3.3.4 Test Traffic Generators

The wide area (Budapest – Győr, Budapest – Nagykanizsa, Budapest – Szeged) and BME's local intra-campus data communication links secured by the key distribution and data encryption subsystems are used for testing, evaluating, or studying quantum key distribution. For these purposes, test traffic generators are also needed.

As there are no special requirements, ordinary computers with general-purpose operating systems will be used to send and receive test traffic. BSD UNIX or Linux operating systems will be used as these are very suitable for remote access, have low hardware requirements, and are highly customisable, allowing us to compose test traffic producers and consumers easily.

4 Conclusions

This deliverable serves as both a guideline for the public procurement procedures and an introduction to the QCIHungary network, which will be utilized throughout the project. It was developed based on the project's overarching goals and outlines a comprehensive set of requirements to be specified in the technical description of the procurement procedure.

Due to project financing delays, we conducted preliminary market consultations and gathered all relevant details about the underlying dark fiber infrastructure that will form the backbone of our QCIHungary network. These efforts summarised in a complete set of technical requirements, which were documented in the appendix of the revised version of this deliverable.

For our procurement process and the overall architecture of the QCIHungary network, we are using D2.1 as a foundational reference.

Appendix A Technical Description Requirements

(preliminary system requirements)

Based on the architecture plan described in this report, here we present the requirements to be specified in the technical description of the public procurement procedure.

A.1 Data Encryption Subsystem

- Encryption keys provided by the QKD system via the ETSI GS QKD 014 interface are used in a way that decryption is not possible without these keys. (Using keys other than those provided by the QKD is possible if combined suitably with keys received from the QKD.)
- Operates on 230V 50Hz AC power, with 1+1 redundant hot swap power supplies.
- Encryptors must be rack mountable in standard 19-inch telecommunication frames. Maximum height is 1 RU.
- Can be managed via CLI and SNMP. The CLI is available over TIA-232-F serial console and SSH.
- Has out-of-band management Ethernet interface.
- At least 800 Mbit/s throughput (per direction).

A.1.1 IPsec Encryptor

- At least 16 10/100/1000 Mbit/s copper twisted pair Ethernet interfaces.
- Route and forward IP packets. Capable of using (logically separated) virtual router instances.
- Can do policy-based routing.
- Encrypt/decrypt IP transit traffic with IPsec, as defined by the configuration settings. AES-CBC and AES-GCM are available for ESP. AES-CBC, AES-GCM, SHA-256 and SHA-384 can be used for IKEv2.
- Can use QKD-provided keys (PPK) for IKEv2 according to IETF RFC 8784.
- At least 2000 concurrent IPsec tunnels.
- Maximum power consumption is not higher than 600W.

A.1.2 MACsec Encryptor

- At least 2 10 Gbit/s and 12 or more 10/100/1000 Mbit/s Ethernet interfaces.

- Forward Ethernet frames according to the IEEE 802.1 family of standards.
- MACsec encryption/decryption using 256-bit AES algorithm.
- 9000-byte jumbo frame support.

A.1.3 In-line Encryptor

- At least 2 1000BASE-T Ethernet data interfaces.
- Transmit data streams (Ethernet frames) between two ports of the device so that incoming traffic on the cleartext port is encrypted and sent out on the cyphertext port, while encrypted traffic received on the cyphertext port is decrypted and sent out on the cleartext port.
- 9000-byte jumbo frame support.
- Uses symmetric key encryption.
- Can encrypt Ethernet frames, including their header, so that no data can be observed in the encrypted data stream without decryption.
- Maximum power consumption is not higher than 100W.

A.2 Key Distribution Subsystem

- The system is composed of one or more QKD device pairs. The quantum channel operates on ITU-T G.652 fibre.
- The service channel may use the same fibre as the quantum channel, another G.652 fibre, or an IP connection.
- An IP connection is available at each node, which can be used by the service channel and operations/management.
- If the link is required to operate on a fibre shared with a DWDM transport system, the QKD system may use the O band and one 100 GHz C band ITU-T G.694.1 channel. Multiplexers and demultiplexers to merge/split QKD and DWDM signals must be included.
- If a single QKD device pair cannot operate on the complete data communication link due to its long distance, then the QKD system is built from sections, one QKD device pair per section. Section device pairs are daisy-chained, and together, they provide the key bit sequence at the data communication endpoints. The system derives the key bit sequence delivered at the data communication endpoints from the key bits issued by the QKD device pairs in each section. Possible optical sections and node locations are specified as described in the tables above. Skipping nodes is permitted if a QKD device pair can handle the attenuation of concatenated sections.
- A QKD device may be a member of one or two QKD device pairs. In the latter case, it communicates on the quantum channel with its two neighbours through time division.

- In the case of QKD systems consisting of multiple QKD device pairs operating on multiple optical sections, the Contracting Entity provides location and environmental conditions for installing and operating the QKD equipment at the section boundaries, including preventing unauthorised access. Concerning the security of the QKD system, it is assumed that no unauthorised access will occur at the section boundaries.
- KMS must be included, either integrated into the QKD or as separate equipment.
- QKD and KMS equipment must be rack mountable in standard 19-inch telecommunication frames. All equipment at a node must fit in 6 or 8 rack units (8U where DWDM interoperability is required). Total electric power consumption must be 1 kW at most per node.
- QKD devices must operate on 230V 50Hz AC power, with 1+1 redundant hot swap power supplies.
- The key bit sequence delivered by the QKD system must be random. The QKD system must provide its randomness without using an external source. If the QKD protocol uses random numbers, included QRNG must be used as the random source.
- The key bit sequence delivered at the two data communication endpoints must be identical.
- The QKD system may deliver key bits only if it is certain that they have not been compromised, according to the laws of quantum mechanics.
- The QKD system must interoperate with data encryption network devices specified in the other offer parts in such a way that these encryptors use the key bit sequence delivered by the QKD system as the encryption key as described in ETSI GS QKD 014 standard.
- Actual key rate and QBER are available at the administrative interface.
- Remote operational/administrative access is possible using CLI over SSH, GUI or REST API over HTTPS, or SNMP.

A.3 Test Traffic Generators

- 64-bit Intel or AMD processor with at least four cores, clocked at 2 GHz or more
- at least 8 GByte operational memory
- 2 1 Gbit/s Intel Ethernet interfaces
- at least 64 GByte SSD
- HDMI output
- 2 USB 3.2 ports
- without an operating system

Glossary

AES	Advanced Encryption Standard
API	Application Programming Interface
BME	Budapest University of Technology and Economics
BSD	Berkeley Software Distribution
CBC	Cypher Block Chaining
CLI	Command Line Interface
DWDM	Dense Wavelength Division Multiplexing
ELTE	Eötvös Loránd University
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
GCM	Galois Counter Mode
GUI	Graphical User Interface
HDMI	High-Definition Multimedia Interface
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector
KIFÜ	Governmental Agency for IT Development (Hungarian NREN)
KMS	Key Management System
MACsec	Media Access Control security
OSI	Open Systems Interconnection model
OTDR	Optical Time Domain Reflectometer
PDU	Protocol Data Unit
PPK	Post-quantum Pre-shared Key
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QRNG	Quantum Random Number Generator
RFC	Request for Comments
SHA	Secure Hash Algorithm
SKIP	Secure Key Integration Protocol
SNMP	Simple Network Management Protocol
SSD	Solid State Drive
SSH	Secure Shell
WDM	Wavelength Division Multiplexing
Wigner RCP	Wigner Research Centre for Physics