FGQT Q05 Quantum Technologies Use Cases [written by the CEN-CENELEC Focus Group on Quantum Technologies (FGQT)]

FGQT Q05

Quantum Technologies Use Cases

written by the CEN-CENELEC Focus Group on Quantum Technologies (FGQT)

Release 1 – March 2023

Table of Contents

1 Abbreviations, terms and acronyms **3**

2 Introduction **4**

3 Use cases **5**
3.1 Using a quantum computer as secondary processor in the cloud **5**
3.2 Trapped-ion optical clocks and sensors **6**
3.3 Networks of quantum computers using trapped-ions **8**
3.4 Quantum simulations **9**
3.5 Assembly of an ion-trap quantum computer **10**
3.6 Cloud-based quantum computing **11**
3.6.1 Current setting of classical cloud-services 11
3.6.2 Extending cloud-services with quantum capabilities 12
3.6.3 Desirable functionalities for quantum cloud-services 13
3.7 QKD High security metropolitan area network **16**
3.8 QKD secure cloud archive **17**
3.9 Integrating QKD with other encryption techniques and using KMS implementation to support healthcare services **18**

Annex A – Standardization template for FGQT use cases **22**

References **23**

1 Abbreviations, terms and acronyms

CEN	Comité Européen de Normalisation (European Committee for Standardization)
CEN-CENELEC STAIR	CEN-CENELEC Working Group Standards, Innovation & Research
CENELEC	Comité Européen de Normalisation Électrotechnique (European Committee for Electrotechnical Standardization)
DC	Direct current
ETSI	ETSI Telecommunications Standards Institute
ETSI ISG	ETSI Industry Specification Group (type of standards developing group)
ETSI TC Cyber	ETSI Technical Committee "Cyber"
FGQT	CEN/CENELEC Focus Group on Quantum Technologies
FHIR	Fast Healthcare Interoperability Resources standard
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission, standards organization
ISO	International Organization for Standardization, standards organization
ITU	International Telecommunication Union (of the United Nations)
ITU-T	ITU Telecommunication Standardization Sector
JTC 1	Joint Technical Committee 1 (of ISO and IEC)
KMS	Key-management system
PP	Protection Profile
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution
QT	Quantum Technologies
Qubit	Quantum bit
RF	Radio Frequency
SC27	Sub-Committee 27 (of ISO/IEC JTC1)
SDO	Standards Developing Organization
TC	Technical Committee
TRL	Technology Readiness Level (estimate for technology maturity)
WG	Working Group

2 Introduction

Quantum technologies form a booming field of research areas. Often, we subdivide the field of quantum technologies in quantum computing, quantum communication and quantum sensing. Some also include a fourth: quantum simulation. Each of them has a different level of maturity and therefore different standardization needs.

Standards can help mature a field and allow for interoperability of different devices or parts of a larger device. Especially in the field of quantum technologies, we expect only a small number of parties to be able to manufacture the hardware by themselves. More likely is that a party focuses on only a small part of the hardware or software stack. The output of the products of these parties has to interoperate with the input and/or output of the products of other parties.

The standardization needs and the level of maturity of specific quantum applications may be uncorrelated. Furthermore, it might be difficult to directly define standards for some application. Instead, use cases allow to freely think about some application and how it should interact with the outside world and with other components of a larger system and which interfaces are necessary. From this, we can determine where which standards are needed when and the characteristics of this use-case.

Even though use cases can imply standards or standardization needs, they not have to. Use cases are relevant on their own as they give a sense of what the community is interested in and what applications of quantum technologies are possible.

The use cases presented in this document are unstructured, both in topic and in the readiness or implication on standardization. Each subsection contains a separate use case and starts with a description, enabling technologies and standardization needs. Some use cases follow with a deeper discussion of the aspects where standards are needed or might be beneficial.

3 Use cases

3.1 Using a quantum computer as secondary processor in the cloud

Use case identification: *Using a Quantum Computer as Secondary Processor in the Cloud*

Application domain: *Applications of quantum computing, applications domains with computationally intensive problems*

Submitted by: *Niels Neumann, The Netherlands Organisation for Applied Scientific Research (TNO)*

Date of submission: *December 1, 2020*

Use case description:

This use case describes a situation where a company has a computationally heavy (sub)task which it wants solved. A quantum computer is used to solve this (sub)task specifically, while the rest of the computations are performed on a classical device. Some functionalities are identified which help integrating the quantum process within the larger computational pipeline.

This use case is on using quantum computing in practical settings via cloud services.

Enabling technologies:

The enabling technologies relevant for this use case are high-performance computing, quantum computing and the interaction between them. Furthermore, the application domains of both fields are also relevant here.

Standardization needs:

This use case does not directly identify standardization needs, but it does identify desirable functionalities, which in turn could lead to standards. The desirable functionalities all relate to cloud-based quantum computing within a large computational pipeline.

A user has developed a pattern-recognition algorithm with a specific computationally heavy sub-routine. To optimize both the running time and the results, the user wants to run part of its algorithm on a quantum computer without disclosing it. The rest of the algorithm is programmed in an often-used classical programming language and it is run on a classical cloud (or supercomputer). Only the result of the quantum-subroutine is needed in the rest of the algorithm. The user can either run the software on a new generation quantum computer, mixing quantum and classical computing facilities or optimizing the execution of the software by distributing it over the available resources. In both cases, the user does not want to deal with the selection of the most appropriate mix of computing resources. The user wants to achieve business-relevant results, while taking care to the overall cost for maintaining the software, thereby maximizing its competitive advantage.

This requires a quantum-host and infrastructure, such that the user can run the quantum-subroutine (possibly wrapped into classical interfaces exposing it over a traditional network) under the requirements that

— The user can program the algorithm locally in a classical environment using a high-level classical programming language and additional quantum instructions;

— The quantum instructions can be programmed both on a high- and a low-level;

— The high-level quantum instructions are compiled to hardware-agnostic low-level instructions, either locally or at the host. The user should be able to decide on this;

— The low-level quantum instructions should be from a hardware-agnostic standardized gate set;

— If the user decides to compile locally, low-level instructions are sent to the cloud-based quantum computer. The user should then also have the option to integrate hardware specific constraints. Additionally, this should be taken care of by the host if needed;

— The user should have the possibility to apply indistinguishability obfuscation to the hardware-agnostic low-level quantum instructions before sending them to the cloud-based quantum computer;

— The hardware-agnostic low-level quantum instructions should then be translated to hardware backend-specific instructions;

— If the user instead sends high-level instructions to the host, and the instructions are compiled on the host-side, there should be messaging that facilitates debugging. Additionally, the user should be able to integrate specific hardware constraints. Otherwise, the compiler should take care of this;

— The high-level quantum instructions may in this case be directly compiled to hardware-specific instructions;

— The intellectual property of new quantum algorithms should be protected;

— There is a standardized interface allowing for executing (bursts of) quantum instructions, and the algorithm should automatically call the quantum instructions when needed;

— Protocols exist such that the user can use it for sending their quantum instructions to the hardware whenever needed: instructions are processed and results are send back to the user;

— Execution of quantum software is orchestrated by an intermediate software layer using standard interfaces and protocols. This operating system should allow for managing quantum jobs, auditing and billing according to requested SLAs and business relevant parameters (e.g. priorities, execution time, etc.);

— Quantum error-correction routines are applied if needed, the user should have influence on this if desired;

— An interface exists between the quantum computer and (super)computers, potentially hosted in the cloud, to send instructions and provide (intermediate) results;

— The result of the quantum-subroutine can directly be used by classical clouds or su-percomputers running the whole algorithm;

— The quantum routine should be integrated in complex service lifecycles as implement-ed by the users on traditional cloud;

— Such an integration is aimed to reduce costs in the medium term.

3.2 Trapped-ion optical clocks and sensors

Use case identification: *Trapped-ion optical clocks and sensors*

Application domain: *Time and frequency references (e.g., VLBI astronomy), navigation (e.g., GNSS), geodesy, communications (e.g., telecom providers), fundamental research*

Submitted by: *Jonas Keller (PTB), Tanja E. Mehlstäubler (PTB)*

Date of submission: *April 2021*

Use case description:

Precision spectroscopy of optical transitions in trapped-ions is the basis of some of the world's most accurate atomic clocks. Clocks can be employed as stable frequency references for synchronizing signals in very-large baseline interferometers, telecommunication, and navigation, or used as sensors to determine gravitational potentials at unprecedented resolution. However, the desired accuracy for some applications is currently only achieved by highly custom, individually built laboratory setups. For economically feasible production of such devices, a manufacturer will require several components to fulfil strict specifications and to interface with each other. These include an ion-trap, vacuum system, multiple laser systems, electronic control systems, and control software. Autonomous operation of the entire system without the need for human interventions is a prerequisite for developing the current laboratory setups into commercial products. Miniaturization and integration of components will be essential to reach such levels of robustness. Finally, the whole apparatus must be able to exchange frequency information with external devices: A clock needs to output its frequency information, whereas sensors based on frequency measurements will require an external reference.

Enabling technologies:

The central enabling technology for this application is an ion-trap. A wide range of implementations is well established for the use in laboratory environments, but adaptation to commercial applications will rely on further developments in areas such as integrated photonics and electronics as well as optical and electrical interfaces.

Other relevant enabling technologies include further miniaturized components, such as lasers and frequency combs.

Standardization needs:

Standardization of the following aspects is needed for a successful implementation:

- *Specifications for the confining potential of the ion-trap, in particular the aspects affecting systematic frequency shifts (RF and DC field imperfections, thermal environment, etc.)*
- *Electrical interconnects for the RF and DC voltages of the ion-trap*
- *Mechanical mounting of the ion-trap inside the vacuum system*
- *Optical interconnects to provide laser beams to the trapped-ions and read out fluorescence signals (once technology is ready)*
- *External port for the optical frequency information. The output of this port can be linked to frequency transfer modules that convert the frequency signal to the RF domain with an optical frequency comb or transfer the optical signal via pathlength-stabilized optical links*
- *Optical interfacing of laser systems with other modules, allowing for the active stabilization of optical pathlengths across multiple components where necessary.*
- *Electronic interfacing of the laser systems with short-term frequency references (such as optical resonators)*
- *Communication of all components with the control system to monitor their health status and autonomously correct for failures or misalignments.*
- *External access to the control system (hardware and software)*

3.3 Networks of quantum computers using trapped-ions

Use case identification: *Networks of quantum computers using trapped-ions*

Application domain: *Quantum simulation, quantum computing, quantum communication, fundamental research*

Submitted by: *Thomas Monz (AQT)*

Date of submission: *April 2021*

Use case description:

The strength of classical computers is not only their individual computational power, but the power that can be accessed when they are connected to one another. This can be seen from the examples of high-performance computing centers, smartphones, and the Internet-of-Things. As quantum devices are being scaled up, interfaces between these devices will allow for easier scaling, seeing that devices can be copied and connected, rather than redesigned in a larger fashion each and every time. Interfaces between quantum computers will also enable novel applications beyond computing, such as provably secure communication protocols and quantum-enhanced sensor networks. Similar to connections between classical computers, the connections between quantum computers require significant standardization efforts: from protocols on the software side, to automated operation on the firmware side, to agreed-upon mechanical interconnects on the hardware side. Building such connected networks of quantum devices currently faces challenges that will tremendously benefit from standardization on several levels.

Enabling technologies:

The key enabling technology is an ion-trap platform for quantum computing, connecting individual qubits to a network of quantum computers.

Standardization needs:

Standardization of the following aspects is needed for a successful adaption towards commercial realization:

- *Devices need to be built upon an initially agreed set of parameters (wavelengths, bandwidths, etc.);*
- *Interoperability via a "data-bus" standard to connect trapped-ions via an interface to other systems, such as rare-earth-ion-doped crystals;*
- *Compatibility of optical interfaces and used wavelengths with the majority of existing telecom infrastructure and control devices (including fibers and switches);*
- *Agreed-upon and ideally standardized protocols for quantum networks that check several aspects of the network such as routing, resource allocation, connection establishment, availability, and loss of transferred information;*
- *It will be important to establish protocols and drivers on how to connect and control such "quantum network cards" at the location of their installation – independent from the initial prototype. These drivers need to be able to communicate with both the OS of the system per se as well as build upon standardized hardware connections.*

3.4 Quantum simulations

Use case identification: *Quantum simulations*

Application domain: *Quantum simulation, quantum computing, quantum communication, fundamental research*

Submitted by: *Thomas Monz (AQT)*

Date of submission: *April 2021*

Use case description:

Quantum simulators can be used to solve problems connected to optimization problems, and as such may offer interesting solutions beyond the capabilities of classical computers in the area of logistics, packaging, power distribution, chip layout, portfolio-optimization and much more. Foremost, the system should be programmable from a standardized interface that facilitates the implementation of algorithms and solutions on the system. In addition, the simulators should be able to interconnect with various classical systems to exchange the results and potentially act both as an independent computing unit as well as a quantum accelerator for a classical computer. The results potentially need to be verified and validated - potentially both with other quantum simulators as well as classically obtained results. This requires procedures and protocols that have been both approved as valid and are standardized to be applicable across various platforms.

Enabling technologies:

The key enabling technology is a quantum simulator which is programmable from a standardized interface being able to also interconnect with classical systems as a quantum accelerator.

Standardization needs:

The use case described here requires the standardization of components and interfaces on various levels:

- *A set of available interactions in the device needs to be communicated in a standardized fashion with the control to ensure that higher-level compilers can optimize algorithms for a given architecture;*
- *Compilers should be able to take system-specific details into account to map algorithms onto hardware;*
- *Algorithms need to be called from classical devices and be forwarded in a standardized fashion to the simulator;*
- *Results of a simulator need to come in a unified format to enable computation and comparison across machines;*
- *Agreed-upon and standardized methods are necessary to provide uncertainties in error propagations of the simulation results before further processing and usage;*
- *A standardized interface to connected quantum simulators with other computers needs to be developed.*

3.5 Assembly of an ion-trap quantum computer

Use case identification: *Assembly of an ion-trap quantum computer*

Application domain: *Quantum simulation, quantum computing, quantum communication, fundamental research*

Submitted by: *Thomas Monz (AQT)*

Date of submission: *April 2021*

Use case description:

A quantum computer producer wants to sell a quantum computing unit that includes both hardware, firmware and software. The producer for many reasons cannot do everything. Therefore the value chain will involve hardware, software, and requires interconnectivity across the full stack. The necessary components include the quantum processor (an ion-trap), which is mounted on a motherboard (a processor-carrier, inside a vacuum chamber), and control capabilities (both electronics and lasers). The system needs to operate in an automated fashion with standardized interfaces (firmware) such that higher-level abstract quantum algorithms can be directly executed on the device.

Enabling technologies:

A quantum computer comprising interconnectable hardware, firmware and software allowing for the direct execution of abstract quantum algorithms on the device.

Standardization needs:

The successful combination of components into a finished product requires:

- *An ion-trap quantum processor with a standardized foot-print and pin-connection, such that it can be installed in different motherboards;*
- *The functionality of the motherboard needs to accommodate a trap carrier (mount) with standardized connections (high voltage, high current, RF signals) which can be used for a variety of trap suppliers;*
- *Standardized interconnects for optical integration that have been tested and are available in bulk would facilitate progress towards further scaling of ion-trap quantum processors;*
- *A standardized interface (both electronics and optics) to connect from outside the vacuum chamber towards the processor will help to adapt and upgrade the housing while maintaining compatibility;*
- *The control electronics of ion-trap quantum processors needs to be able to extract the trap parameters in a standardized fashion to optimize the controls in accordance with the trap specifications;*
- *A layer of standardized abstraction included in the processor firmware to allow the communication of the number of qubits, the connectivity, and special features towards the compiler level to take all system capabilities into account.*

3.6 Cloud-based quantum computing

Use case identification: *Cloud-based quantum computing*

Application domain: *Applications of quantum computing, applications domains with computationally intensive problems*

Submitted by: *Niels Neumann, The Netherlands Organisation for Applied Scientific Research (TNO)*

Date of submission: *August 18, 2021*

Use case description:

Quantum computers are expected to remain cloud-based at least for the near-term. This requires interfaces between different parts of the computing pipeline for a seamless interaction. This use case identifies the need for these interfaces and describes some of the functionalities that these interfaces can offer, all from a user-point of view and in analogy with classical cloud-based computing.

This use case is on which capabilities a cloud-based quantum environment should offer.

Enabling technologies:

The enabling technologies relevant for this use case are high-performance computing, quantum computing and the interaction between them. Furthermore, the application domains of both fields are also relevant here.

Standardization needs:

The standardization needs are interfaces between users and cloud-based quantum platforms and between cloud-based quantum platforms and classical cloud-based platforms. Suggestions are made for the functionalities of these interfaces, however, no requirements are imposed.

This use case serves to identify possible desirable functionalities of future quantum computers from a user perspective, with quantum computers hosted in a cloud-environment. This use case hence also helps in identifying possible requirements for cloud-based quantum computing. It relies on common developments for digital computing, and may also fulfil important needs for end-users of future quantum computers. As such, this use case has the potential to become the most dominant business-case of quantum computing in the future.

3.6.1 Current setting of classical cloud-services

Cloud computing is an all-purpose term for offering a flexible solution to storage, computing power and software. Instead of buying a fixed amount of resources, users can opt for resources for a limited time only. Various types of contracts are possible, for instance, a single hour of computations, or the possibility to flexibly use a software package for a period of three years. Therefore, the structure and way of working of cloud-functionalities are in essence similar to those of local hardware and software. Many companies are already migrating or have already migrated some of their processes to public clouds, as overall, cloud-services require lower upfront investments and can reduce the ICT total-cost of ownership.

In general, three types of cloud-services are proposed: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), with increasing functionalities offered by the cloud-provider. In the first, IaaS, the hardware is provided, typically this includes computers and data storage. In PaaS, the cloud-provides also takes care of the infrastructure, often including the operating system. Finally, in SaaS, a software package or license is provided by the cloud-provider. A key difference between

PaaS and SaaS is that PaaS provides a platform to develop software, whereas SaaS offers the software itself.

There are other types of cloud-services located between the three basic types mentioned above. An example is Container as a Service (CaaS), located between IaaS and PaaS, where services are offered as containers. This is automatically taken care of in PaaS.

Note that each of these services also comes with limitations and potential risks: security and vendor lock-in are two of them. Using cloud-services is therefore often a trade-off between cost, performance, flexibility and security aspects.

3.6.2 Extending cloud-services with quantum capabilities

Classical cloud-services have already been around for a long time and have gained significant attention the last few years. Quantum cloud-services on the other hand have been around only shortly and are still emerging.

When considering the three types of cloud-services of the previous section, we mainly see PaaS being available now. The first platforms that offer IaaS or SaaS are currently upcoming. Below we will sketch the situation for each of the three services in the quantum context:

— IaaS: Users are given access to a quantum computer and have complete control over which hardware fundamental operations are applied to which quantum states at what time. This in general requires sufficient knowledge of the quantum device and possibly requires calibration of it.

  - Note that though possible, quantum computer providers will in general be reluctant to opening up their devices to IaaS users. This service is likely most relevant for specific academic contexts or for use by employees of quantum computer providers.

— PaaS: Users are given access to a quantum computer and can program it using a set of operations, which might be parametrized. For gate-based quantum devices this can for instance imply that users have access to the qubits on a quantum device and they may manipulate them using simple rotations around certain axes or a controlled-phase gate between two qubits. The operations can also be more complex, such as a quantum Fourier transform. The user should not be bothered by mapping these instructions to the quantum hardware, i.e., quantum compiling is performed automatically by the system.

— SaaS: Users can directly run quantum algorithms for specific problems. Users are only bothered with specific problem instances they want to solve. Users might be given the option to tweak the algorithm implementation, which in some cases is even a necessity (consider for instance the oracle implementation in Grover's algorithm). The algorithms offered to the users can already be optimized for specific quantum devices or based on specific metrics.

Note that the descriptions above work equally well for a network of quantum computers, instead of an individual quantum computer. In IaaS in a distributed setting, users are given the flexibility how to correspond between which computers in what way. For PaaS, users are flexible in assigning which operations are performed on which device and which non-local operations (between quantum states on different devices) are performed. The way how these are implemented is taken care of for the user. This is not yet applicable for current hardware.

Finally, in hybrid quantum-classical settings, where only part of the computations are performed on a quantum computer, there has to be a seamless integration between the quantum devices and classical (cloud) computers that perform the classical operations and instantiate new quantum operations. Most current quantum-cloud services require the classical computations to be performed on a local device, instead of in the cloud, which might result in communication overhead. This hybrid quantum-classical setting can even be integrated in SaaS, for instance with the classical computations to update the quantum parameters being done automatically by the system in variational quantum eigensolvers.

3.6.3 Desirable functionalities for quantum cloud-services

From a user point-of-view, there are various functionalities that allow for a sufficient adoption of quantum cloud-computing and an integration with classical functionalities. Below we list a few, including some suggestions on how to implement this. Before we present these functionalities, we first give some assumptions on quantum computing:

— There will only be a few quantum computer providers. Their quantum devices can be made available via a self-hosted platform or via a third-party cloud-platform;

— The number of quantum resources will remain limited. Similarly, will the quality and the fidelity of these quantum resources be limited. Error correction will help suppress errors, but will not yet result in fault-tolerant quantum computing. This point will likely hold especially for the near-future;

— Quantum devices can be linked together via a quantum network, possibly via fiber optic cables;

— Mid-circuit measurements and subsequent classically controlled operations are possible;

— There will not be a single agreed upon hardware technology. This holds for both the quantum paradigm (gate-based, photonics, quantum annealing, Hamiltonian simulation and others) and the specific implementation of it (for gate-based e.g. transmon or spin qubits);

— There will not be a single approach to quantum computing (e.g. gate-based quantum computing, quantum annealing or Hamiltonian simulation);

— Users of SaaS are in general only interested in the end-result of a quantum routine. This can be either the measurement results themselves or the interpretation thereof.

Some of the following functionalities relate to the early nature of quantum computing, where especially for the near-future, device characteristics including different noise rates are a key-part in determining the performance of a quantum device. Examples of functionalities which users might request are set out below and are formulated generally, and should be specified for different hardware backend technologies. Therefore, quantum cloud-services should provide:

— **Characterization of quantum devices:** Relevant properties of quantum devices should be characterized correctly such that users can make a conscious choice on which quantum backend to use. For gate-based devices, such properties include for instance the number of qubits, the qubit type, single qubit T1 and T2 times (average and worst-qubit values), topology of the qubits and fidelity of single and two-qubit gates.

  - Preferably these metrics should be presented in a uniform manner across different vendors.

— **User choice in computational device:** Users should have the option to choose the quantum backend on which the computations are run. This choice can be made based on the characteristics of the available quantum devices. If users do not have a preference, any available and sufficient device may be used for the computations.

  - Once quantum computing devices are sufficiently large, a single device may be partitioned to virtually provide multiple smaller devices to the users. This requires sufficient shielding between different parts.

— **Programming opportunities at different complexity levels:** Users should be able to program quantum algorithms on different levels of complexity, i.e., using different granularities. This means that the complexity of the quantum operations given by the user can differ from for instance elementary quantum operations to a higher-order routine, such as *Use Shor's algorithm to decompose this biprime* or *Solve this linear system of equations*.

— **A hybrid programming environment:** Users should be able to program their algorithms in a hybrid programming environment, which can be made available by the vendor. Users should be able to program their algorithm in the classical language of choice, with the option to call quantum subroutines. Results of these quantum subroutines can directly be used in the classical computations.

- At least the most common programming languages should be supported in this hybrid programming environment, including Python and C++/C#

— **Appropriate resource allocation:** With only a limited number of quantum devices, allocating computation time across different users, but also maintenance and calibration time of the device self is an optimization problem. There should be service level agreements between the quantum cloud-host and the users on which quantum devices can be used when.

- Especially for IaaS users this is important, as such users have the most control over quantum devices and their fundamental operations.

— **Security of computations:** The vendor should provide sufficient shielding and isolation between the computations of different users, such that computations by one user are secure and inaccessible to other users.

- Ideally, computations of a user should also be secure against the cloud-provider. Blind quantum computation will offer this security.

— **Possibility to communicate with other devices:** The vendor should make it possible for the quantum device to communicate with other quantum devices, possibly hosted by other parties and/or used by other users.

- This allows for some form of blind computation, where users cannot learn data of other parties, while still being able to do computations with them. Furthermore, quantum teleportation allows for transferring quantum states from one device to another.

— **Automatic quantum operation compiling routines:** Users should be able to have their quantum instructions automatically compiled to hardware-agnostic low level instructions or even further to hardware-specific fundamental instructions. Users should also be able to provide such a compilation themselves.

— **An integration with classical cloud-processes:** The quantum device should be callable directly from a remote user, however, the quantum devices should also be able to communicate and interact with different classical computers hosted in the cloud.

To achieve the points listed above, it is important that various aspects work together seamlessly. Interfaces are a vital concept to achieve these requirements. Therefore, there should be interfaces between quantum computer providers and cloud-providers for a seamless interaction between different relevant components in cloud-based quantum computing. These interfaces furthermore allow modularity, where different parts are provided by different parties.

Below, in Figure 2.6.1, an overview of different interfaces is presented. Note that where the distinction between local and cloud lies, depends in a large part on the services the user rented. Typically, in SaaS, this distinction lies at the User-Software interface, whereas for PaaS and IaaS this distinction is at the Software-Hardware interface. Note that different interfaces, with different functionalities, can both be Software-Hardware interfaces. See Figure 2.6.2 as an example, the interface can be at the Intermediate quantum instructions separation, indicating that quantum instructions are presented at relatively high level and decompositions are performed on the host side. On the other hand, the separation can also be at the Low-level quantum instructions separation, where the quantum algorithm is sent to the host in terms of low-level hardware-agnostic quantum instructions, or even in terms of hardware-specific quantum instructions.

In Figure 2.6.1, also an interface is required between quantum computers and cloud-hosted classical devices. Such an interface is fundamental for a sufficient adoption of quantum computing in complex business processes.

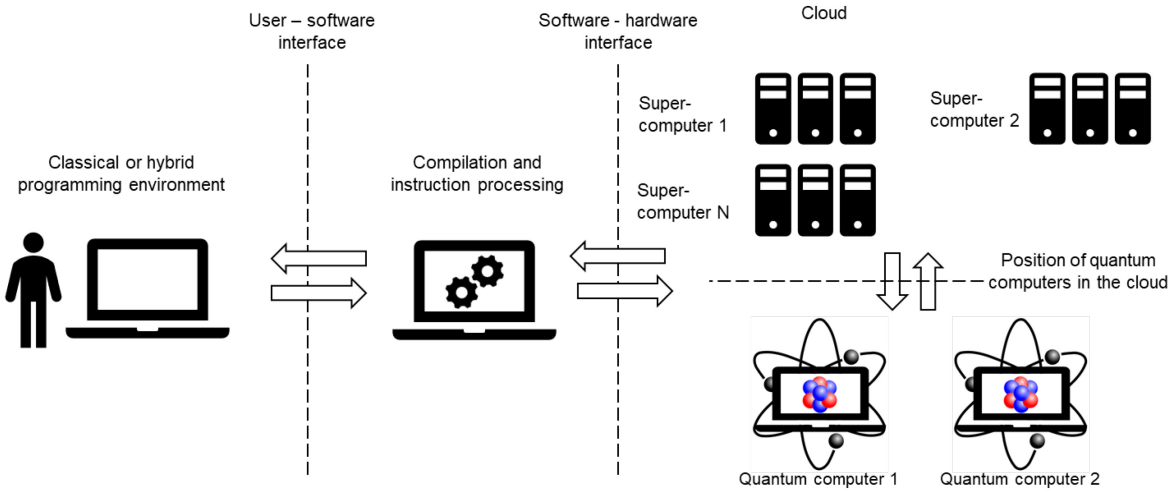

Figure 2.6.1: An overview of different interfaces in a hybrid cloud setting. The separation between a local user an the cloud depends on the services agreed upon.

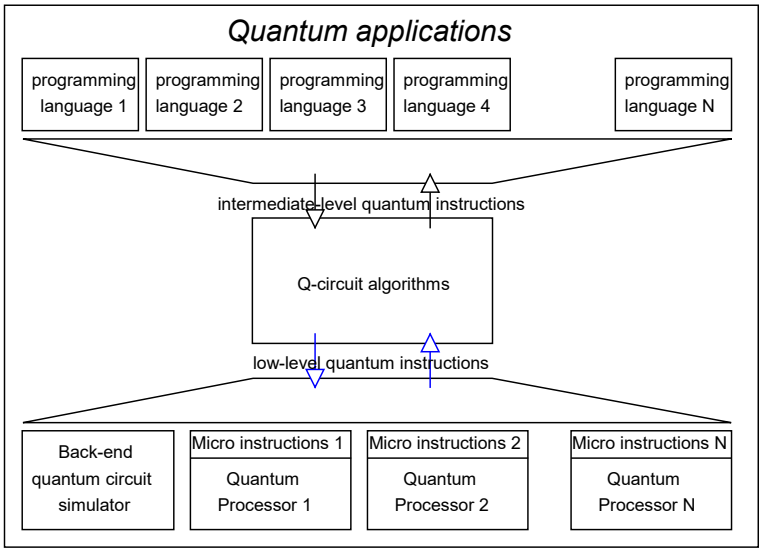

Figure 2.6.2: A software stack for quantum computing (from: [1]).

3.7 QKD High security metropolitan area network

Use case identification: *QKD high security metropolitan area network*

Application domain: *Organizations with branches in a metropolitan area, looking for a high security communications network solution.*

Submitted by: *Thomas Länger, StandICT.eu and IDQuantique Europe GmbH*

Date of submission: *February 21, 2022*

Use case description:

This use case describes a general-purpose high security communications network between several network nodes within distances among adjacent nodes up to 100km. The network uses a dedicated optical infrastructure, completely separated from the internet. QKD systems are used to generate symmetrical cryptographic keys for authentication and encryption of network traffic between nodes. The single nodes are being physically secured by the network owner.

Enabling technologies:

QT enabling technologies to be used: Quantum level sources and detectors; Photonic chips, Control software/electronics; color center materials.

QT components and subsystems to be used: Photonic quantum subsystems; control subsystems; quantum repeaters; QKD senders/receivers

QT platforms and systems to be used: QKD networks; End-to-end QKD systems

Standardization needs:

For this use case, and for QKD in general, standardization activities have been going on since more than a decade in the ETSI Industry Specification Group ISG-QKD: Standards for security proofs and for an application interface are currently being revised. A standard for the characterization of typical optical components of a QKD system has been published. Currently (beginning of 2022) a standardized ISO/EN 15408 "Common Criteria" (CC) Protection Profile (PP) for a QKD link is about to be finished. It is not clear whether that paradigmatic PP will actually be certified (or "certifiable") as several base standards are still missing, or in an insufficient state. Currently, the ETSI has started a new work item for a CC methodology standard. Other SDOs with activities towards standards in QT, most of them ongoing: ISO/IEC JTC1 SC27 WG3, CEN/CENELEC FGQT, ETSI TC Cyber WG QSC, ITUT/SG 13 "Future Networks" and SG 17 "Security" plus few other SDOs in the very beginning stages.

An overview of the QKD standardization landscape, and the single standards already published and currently in development was produced by the Horizon Europe project OpenQKD and published in March 2021 [4] and the current state is/will be maintained by the FGQT Standardization Roadmap, including a specific roadmap for QKD security specification.

Relevant standards for the security certification of QKD are currently being developed by two SDOs:

The ETSI ISG-QKD works on a standard DGS/QKD-016 "Common Criteria Protection Profile for QKD", which is a standardized Common Criteria Protection Profile for a "prepare and measure" QKD system. The standard draft is edited by Deutsche Telekom Security GmbH, Evaluation Facility, with German BSI as sponsor.

ISO/IEC SC27 WG3 has two standards currently under development: ISO/IEC 23837-1 "In-formation security—Security requirements, test and evaluation methods for quantum key distribution—Part 1: Requirements" (containing predefined security functional requirements for use in QKD PPs) and "ISO/IEC 23837-2 (…) Part 2: Test and evaluation methods".

The following aspects call for standardization:

— *Authentication architecture;*

— *Protocols and handling;*

— *Interfaces, wavelengths both for fiber and free space applications;*

— *Methods to test and validate QKD in order to allow authorization bodies the "approve" a QKD system.*

The basic problem addressed is that organizations with highest communications security requirements are currently relying on communication networks that are either using dedicated network infrastructures or are layered upon the internet. In both cases cryptography is used to protect communication confidentiality and integrity, the security of which is either based on computational or intractability assumptions—with uncertain current and long term security.

The solution is to use a communications network with advanced security guarantees on a dedicated optical infrastructure. The advanced security guarantees are provided by QKD links, delivering a continuous stream of symmetrical secrets used to authenticate and secure the communication between adjacent nodes of the network.

End users can rely on the security of their proper network infrastructures, even in the long term. They produce their cryptographic secrets with the high security guarantees of QKD.

Advantages in comparison to alternative solutions: QKD offers key distribution with stronger security guarantees than other non-quantum key distribution primitives. The use of dedicated infrastructure, not directly connected to the internet ensures a relatively smaller attack surface towards attackers from the outside.

This use case was demonstrated in several research projects. The first network was that of the European FP6 project "SECOQC" in 2008, [2] followed by the "Tokyo QKD Network" [3].

3.8 QKD secure cloud archive

Use case identification: *QKD secure cloud archive*

Application domain: *Individuals and organizations looking for an improved storage solution in the cloud with advanced security and privacy guarantees.*

Submitted by: *Thomas Länger, StandICT.eu and IDQuantique Europe GmbH*

Date of submission: *February 21, 2022*

Use case description:

End user data are distributed among several cloud storage providers in order to remain available, even when some of the cloud providers are not reachable at the moment. A particular cloud software ensures that the data remains integrity protected as well as confidentiality protected against storage providers, other tenants of the involved storage clouds, as well as other non-entitled third parties. End users may at any time decide to exchange one cloud provider for another, without any consent or action required of the cloud provider, in a way that no exploitable information remains at the revoked cloud provider.

Enabling technologies:

Same as for the "QKD High security metropolitan area network" use case.

Standardization needs:

The following aspects call for standardization:

— *Authentication architecture;*

— *Protocols and handling;*

— *Interfaces, wavelengths both for fiber and free space applications;*

— *Methods to test and validate QKD in order to allow authorization bodies the "approve" a QKD system.*

Same as for the "QKD High security metropolitan area network" use case.

The basic problem addressed by this use case is that an end user might want to use a cloud storage in order to profit from its flexibility and availability features. Specific data with highest confidentiality and integrity requirements cannot be stored and archived in external public cloud services without adequate protection. The use of encryption in a long term storage scenario requires safeguarding of cryptographic keys for long periods of time, and advances in technology might render the employed algorithms insecure. Cloud providers may become unreachable, lose the entrusted data, or even disappear as companies with all the hosted data. Furthermore, in order to verify data availability, potentially big chunks of data need to be downloaded and decrypted. Another problem is that users may not find it easy to change to another storage provider (vendor lock-in).

The solution is to use a cloud archive with advanced privacy and security guarantees, based on a provably secure Shamir secret sharing primitive, and secure the data links to the single storage providers with QKD links. The secret sharing primitive allows to split the data into multiple shares, which are given to different storage providers. The secret sharing primitive has the advantage that one single share does not contain exploitable information on the original data. A minimum number of shares, the threshold, is required to access the information. The threshold (e.g. 3 out of 5 shares) can be arbitrarily selected by the data owner. Together with QKD secured transport links, such a system yields a keyless cryptographic solution with highest security and availability guarantees (clearly under a dedicated "non-collusion assumption" of cloud providers). Furthermore, specific protocols can remotely verify that the single storage providers have intact shares, without having to download all shares and recombine them. In a long term scenario, single shares can be invalidated and be replaced with new shares, potentially at another cloud provider—thus solving the 'vendor lock-in' and secure deletion issues.

Advantages for end users: The use case counters some of the most severe threats in current cloud solutions and provides a distributed cloud archive with advanced data availability guarantees, as well as provable long term confidentiality and integrity guarantees.

Advantages in comparison to alternative solutions: The used cryptographic technologies exhibit information-theoretic security and are thus impossible to break, even with unlimited resources.

The use case was implemented and demonstrated in several research projects [5, 6].

3.9 Integrating QKD with other encryption techniques and using KMS implementation to support healthcare services

Use case identification: *Integrating QKD with other encryption techniques: Securing cloud-based healthcare data implementing a hybrid security approach by integrating QKD systems with encryption techniques and using KMS implementations*

Application domain: *Healthcare, cloud-based, homomorphic encryption, PQC, cloud-based AI services, telecoms, KMS*

Submitted by: *Homer Papadopoulos, NCSR Demokritos, Sydnesis Ltd*

Date of submission: *August 30, 2022*

Use case description:

Cloud technology can potentially support a wide variety of healthcare use cases such as provide a cost-efficient way for a trustworthy storage of medical datasets and Electronic Health Records (EHR) and access to patient health records from anywhere, transfer of healthcare data to external servers for second opinion or analysis from AI models for decision support and others. In all these scenarios the end-users (doctors and patients) are concerned with the privacy of personal health information. Furthermore, quantum computers seem to be able to undermine all conventional cybersecurity systems of the present and to threaten soon several of the cryptographic primitives used in cloud technologies. Therefore, it is crucial that "quantum-safe" cybersecurity systems are developed and refined before quantum computing becomes commonplace.

QKD4IntelligentHealth pilot within the realm of the OPENQKD project believes that to enhance the security and privacy of the healthcare data that are stored and analyzed in cloud based Electronic Health Records (EHR), hybrid security approaches should be adopted. These hybrid approaches could better guarantee the security and privacy of personal medical data in different real-life scenarios.

Furthermore currently, it is not possible to generate a sufficient amount of quantum keys to provide stable quantum cryptography communication network services for verticals like healthcare based on the QKD technology, and there is a lack of relevant standards for quantum key management and integration of quantum keys with encryption technologies like PQC. This is becoming more complex when the QKD nodes are increasing. This pilot is trying to demonstrate how to secure the transfer and analysis of private health data over the cloud integrating and managing QKD with different encryption techniques. Therefore QKD4IntelligenceHealth proposes a hybrid combination of many-level cyber-security measures:

— *Apply advanced cryptographic algorithms such as post-quantum algorithms;*

— *Homomorphic encryption techniques for communication and the exchange of Electronic Health Record datasets to remote servers that host AI models and algorithms;*

— *Application of QKD technology (integrated at the application layer) to facilitate network communication.*

Implementation of an intelligent Key Management System (KMS) aiming to achieve the right balance between security, usability (interoperability with existing EHRs), cost and ease of use.

Enabling technologies:

The enabling technologies that interoperate in this use case are among the others the following:

— *Authentication and encryption protocols;*

— *KMS able to interoperate between PQC and QKD;*

— *QKD devices with increased generation rate of secret keys.*

Standardization needs:

What seems to be missing is a lack of standards for quantum key management and integration of quantum keys with encryption technologies like PQC. This is becoming more complex when the QKD nodes are increasing. Certification of QKD and KMS products is missing as well. Standardized KMS interfaces that will allow KMS to accommodate heterogenous vendor devices are necessary as well.

The pilot demonstrates the transfer of homomorphic encrypted datasets (e.g. Vital signs, X-rays, MRI files) from FHIR EHRs to external servers that host Machine Learning trained models to analyze and diagnose the transferred datasets. The scenario uses a KMS system that gets the keys from quantum cryptography (quantum key distribution, QKD) to encrypt and securely transmit the datasets between the two servers.

The pilot integrates QKD with other cryptography methods (Post Quantum Cryptography – PQC) to provide a hybrid security guarantee.

The KMS distributes several symmetric and asymmetric keys (PQC, AES, TLS certificates, partially homomorphic encryption asymmetric keys). The KMS integrates and manages the high-entropy source of keys coming from QKD over their full lifecycle to enable the implementation of strong encryption.

The pilot is being implemented within the campus of the NCSRD organization, with two QKD nodes that serve many end points utilizing dedicated optical fiber to connect two remote buildings. The pilot will be updated with more nodes within the realm of the HellasQCI project pilot including Large Hospitals and Public authorities within the Greek territory. Within this National network we will adopt the Trusted Repeater QKD Networks approach although other network architectures like the Switched QKD Networks, Security without Trusted Repeaters and QKD Overlay Networks will be considered as well in the relevant architecture design deliverables.

The QKD4IntelligentHealth project aims to demonstrate that QKD can be combined with other encryption technologies to increase the security and privacy of healthcare services over the cloud. The pilot following the QKD network layer description [7] conducted activities and developed modules that concern the Key Management and the communication layers:

— A quantum layer where a secure symmetrical key is established;

— A key management layer used to verify and manage the previously established key;

— A communication layer where the established key is used to secure data traffic.

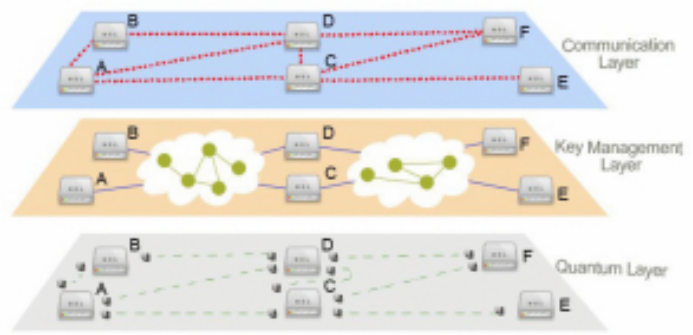

Figure 2.9.1: QKD network hierarchy with quantum, key management, and communication (key usage) layers.

The QKD modules in the quantum layer had to be integrated with other encryption techniques in the communication layer to support an application in the health sector that requires a high level and long-term security (as indicated in ITU UC-V-040). Thus, the whole architecture of the network and the KMS was designed. First, we designed (by referencing the ETSI [8] and ITU-T standards) the interface and connection structure of QKD-KMS-transmission and exchange equipment. Then we constructed the layers of the KMS as shown in the following architecture. The KMS has adopted the standards of the ITU-T / X.1714 and ITU-T/Y.3803.

The KMS adopts an architecture that consists of three layers whose implementations are completely customizable independently of each other:

a) Key management distribution where hybrid methods (conventional ECDH/Elliptic Curve Diffie–Hellman Key Exchange, PQC and QKD) are used to create the keys;

b) Homomorphic encryption techniques for communication and the exchange of Electronic Health Record datasets to remote servers that host AI models and algorithms;

c) State-of-the-art data sharing schemes leading to sensitive infrastructure (EHRs) protection.

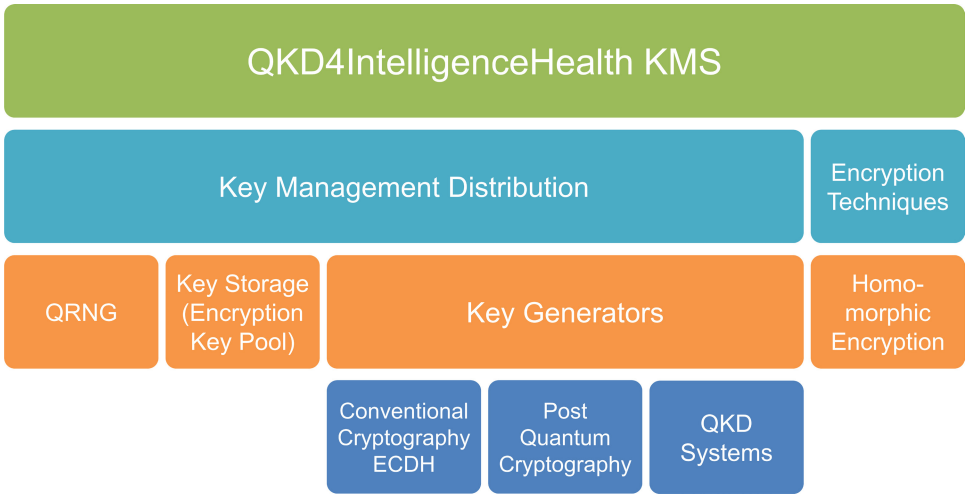

Figure 2.9.2: Architecture of the QKD4IntelligentHealth KMS

The flexibility of the KMS makes it an extremely promising framework for integrating conventional cryptography, (PQC) algorithms that are used to generate keys and encrypt information in a way that is safe against quantum computers, QKD systems able to manage and distribute keys among a network in a secure way and other encryption techniques like Homomorphic encryption and sharing schemes.

The QKD4IntelligentHealth KMS can become the basis of applying state of the art encryption techniques and of the key distribution for quantum-safe cybersecurity systems globally.

Annex A – Standardization template for FGQT use cases

This template is intended to collect information relating to standardization needs on use cases that concern quantum technologies.

Use case identification: *Name of the use case*

Application domain: *Industry / Application scenario and field / end users, organizations, administrations, companies*

Submitted by: *Name/organization of contributor*

Date of submission: *Date of initial submission*

Use case description:

Use cases could be presented in a storytelling fashion. In addition each identified technology (or set of technologies) could be accompanied by the following indicative information:

— *A description of the problem and the needs and gaps of the use case (Rationale of the use case);*

— *Information about the context in which the technology could be shown feasible;*

— *Current technical solution (only non-quantum) that solve the same problem;*

— *A high-level description and a functional architecture of the quantum technology based solution;*

— *Figures and relevant diagrams;*

— *Market description and its potential for financial sustainability;*

— *And cost of the potential market structure, the size, and;*

— *Technical advantage from the quantum technology;*

— *An estimation of the TRL of the technology and timeline for the solution;*

— *Key publications.*

Enabling technologies:

Indicative content of this topic could be:

— *Supply chain for the enabling technologies;*

— *Interoperability gaps with the enabling technological modules;*

— *Technology gaps; and the*

— *Extra research needed to increase the TRL level of the proposed solution.*

Standardization needs:

Indicative content of this topic could be:

— *Existing or planned standards relevant for the use case;*

— *Extra standardization needs in terms of interoperability, performance and metrics.*

References

[1] R. F. van den Brink, N. M. P. Neumann and F. Phillipson, "Vision on Next Level Quantum Software Tooling", Computation Tools, 978-1-61208-709-2, 2019

[2] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J.F. Dynes, S. Fasel, S. Fossier, M. Fürst, J. D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer. T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyoneus, O. Maurhart, L. Monat, S. Nauerth, J. B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z.L. Yuan, H. Zbinden and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna", New J. of Phys. 11 075001 (37pp), 2009

[3] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network Optics Express", 19 11 pp. 10387-10409, 2011

[4] M. Loeffler, C. Goroncy, T. Länger, A. Poppe, A. Neumann, M. Legré, I. Khan, C. Chunni-lall, D. López, M. Lucamarini, A. Shields, E. Spigone, M. Ward and V. Martin, "Current Standardization Landscape and existing Gaps in the Area of Quantum Key Distribution", . online https://openqkd.eu/wp-content/uploads/2021/03/OPENQKD_CurrentStandardisationLandscapeAndExistingGapsInTheAreaOfQuantumKeyDistribution.pdf, 2022

[5] T. Lorünser, C. B. Rodriguez, D. Demirel, S. Fischer-Hübner, T. Groß, Th. Länger, M. des Noes, H. C. Pöhls, B. Rozenberg and D. Slamanig, "Towards a New Paradigm for Privacy and Security in Cloud Services", 4th Cyber Security and Privacy Innovation Forum, https://arxiv.org/abs/1506.05980v2, 2015

[6] J. Braun, J. Buchmann, D. Demirel, M. Geihs, M. Fujiwara, S. Moriai, M. Sasaki and A. Waseda, "LINCOS – A Storage System Providing Long-Term Integrity, Authenticity, and Confidentiality", 13th ACM Asia Conference on Computer and Communications Security, https://eprint.iacr.org/2016/742.pdf, 2017

[7] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher and M. Voznak, "Quantum Key Distribution: A Networking Perspective", ACM Comput. Surv., https://doi.org/10.1145/3402192, 2020

[8] T. Langer and G. Lenhart, "Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD", New Journal of Physics 11.5 (2009): 055051. ETSI, "Quantum Key Distribution (QKD); Protocol and data format of key delivery API to Applications," GS QKD 014, V1.1.1 (2018) ETSI, "Quantum Key Distribution Control Interface for Software Defined Networks", GS QKD 015 Quantum Key Distribution (QKD), V1.1.1 (2021).