GSMA

Quantum Hardware Abstraction Layer for Quantum Computing and Networking

Version 1.0

21 December 2022

GSMA

This is a Whitepaper of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

About the GSMA Internet Group

The GSMA Internet Group (IG) is the key working group which research, analyses and measures the potential opportunities and impacts of new web and internet technologies on mobile operator networks and platforms. We maintain the most up-to-date knowledge base of new internet and web innovations through intelligence gathering of available global research and active participation in key Standards organisations.

www.gsma.com/workinggroups

Table of Content

1 Introduction

1.1 The Second Quantum Revolution

A first quantum revolution started decades ago and has already brought quantum technologies in our everyday life. Chips for computers and smart-phone, systems for medical imaging (Nuclear Magnetic Resonance, Positron Emission Tomography), LED and lasers, etc. are all based on technologies exploiting the quantum mechanics principles. Today a second revolution seems to be underway: in fact, there is an impressive new grow of interests for quantum, with several investments from public and private organizations worldwide targeting new horizons of applications. In particular, there are three quantum phenomena, well known and well tested in Physics, which are not fully exploited yet by Industry. These phenomena are superposition, entanglement, and measurement:

- Superposition concerns the property of quantum objects to stay in linear combination of multiple states until they are observed.
- Entanglement is defined as the possibility that two or more quantum objects to stay intrinsically linked, into an intertwined composite state, regardless of how far apart the objects are from one another.
- Measurement regards the collapse and disruption of a quantum state from coherent probabilistic superposition state into a discrete on.

International innovation activities and Standardization Bodies are pretty aligned in identifying four main applications areas of quantum technologies and services: communications, computing, simulations, sensing and metrology.

- The area of Quantum Communications includes two main sub-domains: the so-called quantum-safe communications and (for the very long term) the “teleporting” of qubits (e.g., Quantum Internet, whose TRL is 1-2). Quantum-safe communications leverage on systems such as Quantum Key Distribution (QKD) and Quantum Random Number Generators (QRNG) and its potential integration with (Post Quantum Cryptography) PQC solutions.
- Quantum Computing concerns the exploitation of the above principles of superposition, entanglement, and measurements, to speed up over classical computers in solving complex optimization and combinatorial problems.
- Quantum simulations concerns all those applications where well-controlled quantum systems are used to simulate the behaviour of other systems, which are less accessible and more complex for a direct simulation (TRL 6-9). Table 2 provides some examples of applications.

Quantum sensing and metrology includes those applications where high sensitivity of quantum systems to environmental influences can be exploited to measure physical properties and timing with more precision (e.g., magnetic and heat sensors, gravimeters, GPS-free navigators, clocks; TRL is 4-9).

Overall, while some quantum applications are already commercially available today (e.g., QKD and QRNG, quantum annealers, quantum simulations, atomic clocks and some quantum sensors) the current use of the second wave of quantum technologies is still relatively limited. This is due to both technical limitations and trade-offs between technical performance and costs. Further progresses are needed.

In quantum communications, for instance, a technological breakthrough is needed for developing quantum repeaters: this would be a key step for both long-distance QKD, distributed quantum computing and the quantum internet. Concerning quantum computing, a roadblock is mitigating the random fluctuations that could occasionally flip or randomize the state of qubits during processing. Quantum software scenario is very active but rather fragmented: major efforts are directed to define languages to enable Programmers to work at high level of abstraction. At the same time, international community is recognizing the disruptive potentialities of these quantum technologies in several markets when breakthroughs will be reached.

1.2 Overview and scope

As mentioned in the previous section, Quantum Computing and Quantum Communications are two the key applications areas of Quantum Technologies. In Quantum Computing, quantum effects are employed to reduce the data-processing time for solving complex problems (e.g., from exponential to polynomial time). In Quantum Communication, quantum effects are employed to transmit digital data in a quantum-secure way or even “teleporting” quantum information.

In general, Quantum Networks will have to be integrated with current network for the purpose of executing methods and protocols which are provably more efficient than the classical counterparts. In particular, it is expected that Quantum Networks will enable quantum security services (e.g., through QRNG, QKD), future quantum computing services (e.g., through Cloud Quantum Computing, Blind Computing, etc) and in the long term even services based on the teleporting of information.

Quantum Networks includes quantum nodes and systems in charge of networking, processing, and storing units of quantum information up to the end-Users. Currently there are several international efforts to define a protocol stack for quantum networks: in fact, interfaces and protocols must be designed and standardize, at least at the physical, data link and network layer in order to consider the requirements introduced by the quantum technologies.

One major obstacle hindering these developments is that, today, the industry has not yet consolidated around one type of quantum hardware technology. In this scenario, a Quantum Hardware Abstraction Layer (Quantum-HAL) - for Quantum Computing and Networking - would allow Applications and Services Developers to start using the abstractions of the underneath quantum hardware (even if today under consolidation): this would simplify and speed-up the development of quantum platforms, services, and applications.

In fact, a Quantum-HAL would provide unified northbound quantum Application Programming Interfaces (APIs) for the higher layers, decoupling from the different types of quantum hardware technologies (e.g., trapped ions, superconducting qubits, silicon photons qubits) for Quantum Computing and Networking.
The activities of design and standardization of a Quantum-HAL - for Quantum Computing and Networking – require coordinated and joint efforts including, where appropriate, existing projects, industry bodies and standard fora (e.g., ITU-T, ETSI, IETF, IEEE, etc…) active in the area.

Scope of the document is to provide:

- Analysis of the state of art of the international activities carried out by existing projects, industry bodies and standard fora on a Quantum-HAL for Quantum Computing and Networking. The analysis will also aim at identifying gaps, challenges, and opportunities for synergies to avoid overlapping efforts.

- Overview of the main architectural principles and the high-level requirements of a Quantum Hardware Abstraction Layer for Quantum Computing and Networking, as derived from the analysis of the state of art.

Detailed technical analysis and specifications are out of scope, but references to the state-of-the-art and best practices are listed for the Readers willing to get more details.

1.3 Abbreviations

Term	Description
QRNG	Quantum Random Number Generator
QKD	Quantum Key Distribution
CV-QKD	Continuous Variable Quantum Key Distribution
DV-QKD	Discrete Variable Quantum Key Distribution
SDN	Software Defined Network

1.4 References

Doc Number	Title
QuInT	D. Awschalom, K. K. Berggren, H. Bernien et alii, Development of Quantum InterConnects for Next-Generation Information Technologies available at https://arxiv.org/abs/1912.06642
Qths	Kurizki G, Bertet P, Kubo Y, Mølmer K, Petrosyan D, Rabl P, Schmiedmayer J. Quantum technologies with hybrid systems. Proc Natl Acad Sci U S A. 2015 Mar 31;112(13):3866-73. doi: 10.1073/pnas.1419326112. Epub 2015 Mar 3. PMID: 25737558; PMCID: PMC4386362.
QHAL	https://riverlane.github.io/QHAL_internal/v0.1.1/general.html
QED-C	https://quantumconsortium.org/members/
QIA	https://cordis.europa.eu/project/id/820445/it
CIVIQ	https://civiquantum.eu/
GSMAWP1	https://www.gsma.com/newsroom/resources/ig-11-quantum-computing-networking-and-security/attachment/ig-11-quantum-computing-networking-and-security-2/
GSMAWP2	https://www.gsma.com/newsroom/resources/quantum-networking-and-service/
QKD-Review	https://mdpi-res.com/d_attachment/entropy/entropy-24-00260/article_deploy/entropy-24-00260-v2.pdf
Eurolab4hpc	https://www.eurolab4hpc.eu/media/public/vision/vision_final.pdf

Doc Number	Title
IRTFQI	W. Kozlowski, S. Wehner, R. Van Meter, B. Rijsman, A. S. Cacciapuoti, and M. Caleffi, “Architectural Principles for a Quantum Internet,” Internet Engineering Task Force (Work in Progress), Mar. 2020.
IRTF-QIRG	https://datatracker.ietf.org/group/qirg/about/
IEEE P1913	http://sg.committees.comsoc.org/files/2018/09/IEEE-P1913-Summary-2018-v0.1.pdf
ETSI GS QKD 004 V2.1.1	Quantum Key Distribution (QKD): Application Interface
ETSI GS QKD 018 V1.1.1	Quantum Key Distribution (QKD): Orchestration Interface for Software Defined Networks
ETSI GS QKD 014 V1.1.1	Quantum Key Distribution (QKD): Protocol and data format of REST-based key delivery API
ETSI GS QKD 020	Quantum Key Distribution (QKD); Protocol and data format of REST-based Interoperable Key Management System API
ETSI GS QKD 015 V2.1.1	Quantum Key Distribution (QKD); Control Interface for Software Defined Networks
ITU-T Y.3805	Quantum Key Distribution Networks - Software Defined Networking Control
ITU-T Y.3810	Quantum key distribution network interworking – framework
ITU-T X.sec_QKDNi	Security requirements for Quantum Key Distribution Network interworking (QKDNi)
ITU-T Y.QKDNf-fr	Framework of Quantum Key Distribution Network Federation
QuvNA	Matthias F. Brandl, “A Quantum von Neumann Architecture for Large-Scale Quantum Computing” https://arxiv.org/abs/1702.02583
ExEQN	Stephanie Wehner Experimental demonstration of entanglement delivery using a quantum network stack https://arxiv.org/pdf/2111.11332.pdf
LLPQN	A. Dahlberg, M. Skrzypczyk, T. Coopmans, L. Wubben, F. Rozpędek, M. Pompili, A. Stolk, P. Pawełczak, R. Knegjens, J. de Oliveira Filho, R. Hanson, and S. Wehner, A link layer protocol for quantum networks, in Proceedings of the ACM Special Interest Group on Data Communication, SIGCOMM ’19 (Association for Computing Machinery, New York, NY, USA, 2019) pp. 159–173.
EuroQCI	https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci
QIA	http://quantum-internet.team /

Doc Number	Title
CIVIQ	https://civiquantum.eu/
UNIQORN	https://quantum-uniqorn.eu/

2 Quantum Infrastructures

This section is reporting definitions and models of Quantum infrastructures, and some specific examples.

2.1 Definitions and Models

In analogy with ‘classical’ network and service infrastructures which lay on a foundation built of interconnected network nodes and information-processing systems, quantum network and service infrastructures rely on quantum network nodes and quantum information-processing systems.

Quantum infrastructures will allow the transmission and manipulation of quantum states (e.g., Qubits) between remote locations. A Qubit is a quantum bit, the counterpart in quantum information to the binary digit or bit of classical information. More in general, in quantum physics, a quantum state is a quantum information entity that provides a probability distribution for the outcomes of each possible measurement on a system.

The transfer of quantum states (e.g., Qubits) between nodes is feasible using photons as carriers, often dubbed flying photons. Quantum Infrastructures are integrated with current classical ones, photons can be transmitted and controlled using standard optical components, in particular exploiting the transmission through optical fibres and satellite communication (free space optics).

Quantum infrastructures will be based on protocols that have no classical counterpart, as based on quantum principles. The range and roadmap of possible quantum applications will mainly depend on the development stage of the underlying hardware.
Figure 1 shows an example extracted from [QuInT].

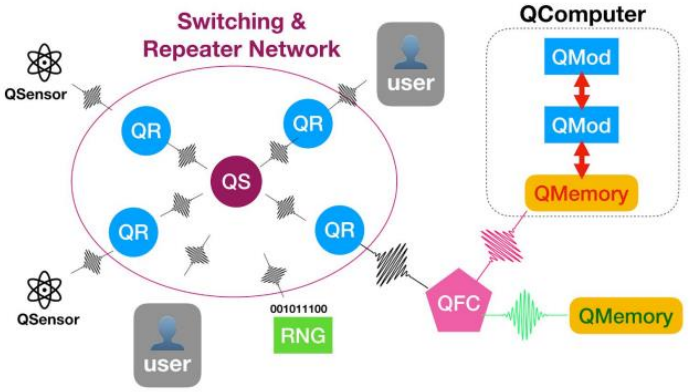


Figure 1 – Example of model of quantum infrastructure (QS = Quantum switch; QR = Quantum repeater; QMod = Modular quantum processor; QFC = Quantum frequency converter; RNG = Random number generator).

Systems, nodes and devices for quantum infrastructures are being implemented with diverse technological approaches, ranging from photons, atoms, and spins to mesoscopic superconducting and nanomechanical structures: the reason is that the different physical properties are better suited than others for specific tasks. For instance, photons are well suited for transmitting quantum information, weakly interacting spins can serve as long-lived quantum memories, etc. Hybrid quantum infrastructure includes node and systems composed of different physical components with complementary functionalities [Qths].

2.2 Examples of Quantum Infrastructures

This section describes some examples of quantum infrastructure, from QKD networks to the Quantum Internet.

2.2.1 QKD Networks

The two GSMA White Paper [GSMAWP1], [GSMAWP2] already provided a picture of applications of quantum technologies for cyber-security. Quantum Key Distribution (QKD) provides an approach to share a key between two remote parties via a quantum channel with quantum-theoretic security. Since the first QKD protocol, BB84, was proposed by Bennett and Brassard in 1983, several types of QKD protocols based on the discrete variables or the continuous variables have been proposed. Remarkably, QKD-based quantum networks testbeds and field-trials are available, including, an integrated space-to-ground architectures [QKD-Review].

2.2.2 Cloud QC/HPC interconnected with quantum links

Another example of quantum infrastructures is based on the interconnection of centralised Cloud Quantum Computing/High Performance Computing facilities with quantum secure links and networks (e.g., QKD networking).

High Performance Computing (HPC) refers to technologies that enable achieving a high-level computational capacity as compared to a general-purpose computer. High-performance computing in recent decades has been widely adopted for both commercial and research applications including but not limited to high-frequency trading, genomics, weather prediction, oil exploration, etc.

Today’s HPC mainly consist of a multitude of nodes and interconnects linked together through a high-speed network. While on-premises HPC will remain the de facto architectural type, at the same time the advantages offered by HPC as a service are getting momentum. In fact, one of the benefits of the cloud approach is that it provides access to on-demand HPC resources at a relatively accessible cost.

According to [Eurolab4hpc] while only 27% of HPC centres worldwide are already experimenting with quantum computing, adoption of the technology will accelerate: by 2023, 76% of HPC centres worldwide will be using the quantum technology — the majority with an on-premises infrastructure.

2.2.3 Quantum Internet

A definition of Quantum Internet has been already reviewed in the Appendix of the GSMA WP [GSMAWP1].

Quantum Internet can be defined as a global network exploiting some principles of Quantum Physics for transmitting, processing and storing qubits: in particular, the communications features of the Quantum Internet concerns distributing entangled quantum states among remote quantum nodes and devices. The quantum channels of the Quantum Internet work in synergy with classical links. Some key characteristics of the Quantum Internet have been recently overviewed by an IETF Quantum Internet Draft [IRTFQI].

3 Management and Control of Quantum Infrastructures

Software Defined Networks (SDN) technologies offer very flexible ways to manage and control functions, resources and services of a telecommunications network.

In general, SDN allows the management and optimization of the entire infrastructure from a logically centralized element, usually called as SDN controller. Moreover, programmability and flexibility brought by SDN technologies reduces drastically times and efforts of integrating new devices and technologies in the network.

In the specific context of Quantum Infrastructures, a key requirement is their integration (at the physical level, but also at the management and control levels) in the existing telecommunications infrastructures. Therefore, flexibility of the SDN management and control has been recognized as a promising approach that allows said integration in a seamless way.

Essentially all Quantum Infrastructures nodes and systems can be modelled similarly to any other traditional network elements (e.g., router, switch) so that a SDN controller will be capable of controlling, integrating and optimising their behaviours. This is basically in line with the ETSI ISG-QKD group where SDN control and orchestration of QKD is being discussed and defined.

3.1 Control and Management

Secure application entities can reside in various network domains within classical communication network. While QKD network domain and secure application entities' network domain can be managed and configured independently via its own SDN controller, a network operator can introduce multi-domain SDN orchestrator for a single and integrated management for both network domains.

Therefore, an SDN controller is deployed for a given network domain while the whole network system is orchestrated by an SDN orchestrator. For the use case of QKD-derived keys' delivery to secure application entities in optical transport network (OTN), with the rich fiber environment in telecom companies and because of steep performance degradation of QKD over optical fiber length compared with the performance of OTN, network operators can choose the deployment of a QKD network with dark fiber to be separated from classical

OTN to operate and manage each network without the performance degradation of each network.

With this separated deployment in the network configuration and each network's operation under the network operator's integrated network management, QKD network domain and OTN network domain need to be interconnected between two nodes which, respectively, belong to each network domain for QKD-derived keys' delivery to secure application entities in OTN. Usually, this kind of interconnection plays the role of providing QKD-derived key delivery API between the key supplier, that is, QKD node and the key receiver, that is, secure application entity.

Under this configuration, QKD does not guarantee that QKD-derived key will be used securely in secure application entity because its use in secure application entity is beyond the responsibility of QKD. However, in this case, as QKD node and secure application entity in OTN node belong to the same network operator's telecom network, the network operator can control both networks and guarantee the secure use of QKD-derived keys with telecom operators' security. For the security from key generation to the use of the key in telecom network, the address matching between QKD node and OTN node in two network domains needs to be resolved before key delivery under the network operator's management.

Therefore, the network operator needs to coordinate both QKD and OTN network domains and a multi-domain SDN (Software Defined Network) orchestrator is required for this reason. In this use case, SDN orchestrator can play the coordinating role with the information received from the SDN controller of QKD network and the information from the SDN controller of OTN, respectively. With this configuration, the network operator can ensure the secure end-to-end QKD service provisioning between QKD network and OTN.

For the SDN orchestrator to play the coordinating role between QKD and OTN network domains, the interface between an SDN orchestrator and an SDN controller of QKD network needs to be defined. This interface describes the flow of information between the SDN controller performing as a server and the SDN orchestrator operating as a client. Through this interface, SDN orchestrator can orchestrate QKD network in terms of discovery of QKD network topology, monitoring of QKD network status and resource inventory, end-to-end QKD service provisioning with path calculation in QKD network, management policy, performance management as well as the address matching as described above.

With this configuration extended, an SDN orchestrator can orchestrate multi-QKD network domains from multi-vendors via each SDN controller of each QKD network as well as both QKD and classical optical transport network domains. For the security consideration, contrary to the exposed orchestration interface of the SDN controller in a QKD network, as the SDN controller in a QKD network does not directly handle QKD-derived keys generated and transported inside the QKD network, and the SDN orchestrator does not receive any QKD-derived keys through the orchestration interface from the SDN controller in a QKD network, QKD-derived keys cannot be exposed through the orchestration interface between the SDN controller in a QKD network and the SDN orchestrator. Therefore, the QKD-derived key itself can be secured from the orchestration interface. The introduction of quantum nodes/systems will bring unavoidably to heterogeneous networks that consist of the mixture of quantum and classical communication technologies, both from terrestrial and spatial field. Additionally, the need to integrate the elements coming from different vendor will add to difficulty of operating final product.

Building separate network for QKD assures high performance and isolation but is highly impractical due to high non-incremental up-front cost and is plainly difficult to deploy on commercial level. On the other hand, high complexity of managing life cycle of classical and quantum channels coexisting in the same network and even sharing the same physical media, requires adopting solutions that allow to bring the operational costs down, for example automated algorithms utilizing AI - artificial intelligence - and ML - Machine Learning - to optimize the most power and bandwidth consuming elements in processes like path computing. SDN, already established in optical network architectures, is pacing the path for integrating quantum and classical worlds by enabling vendor agnostic, dynamically configurable control and management, both network and service level. There is wide existing range of security standardisation and recommendation documents related to both SDN and NFV from different bodies (ETSI, ITU-T, etc) to build upon.

As proposed by both ETSI and ITU-T, the functions of SDN controller include application registration, topology acquisition, routing control, policy-based control, session control, configuration control, access control and QKDN virtualization. As both hierarchy and isolation are supported in SDN, according to requirements separate SDN controllers can be defined for multivendor and multi-client/domain network with potential “zero touch” integration. From security concerns point of view, as SDN Controller only provides control and management functions, the key itself is never shared with controller (it does not add new risk to the process).

3.2 Orchestration

When network operators deploy QKD network in order to secure data transported through classical optical network, they need to consider how QKD network will be incorporated in their classical network. With the infrastructure availability and because of steep performance degradation of QKD over optical fiber length compared with the performance of optical transport network (OTN), network operators can choose the deployment of QKD network to be separated from classical OTN to operate and manage each network separately. With this separated deployment and operation in the configuration, both network domains need to be interconnected between two nodes that belong to each network domain for QKD-derived keys’ delivery to secure application entities in OTN. In this interconnection, address matching between nodes at different network domains needs to be resolved. Therefore, the network operator needs to coordinate both network domains, and a multi-domain orchestrator is required for this reason. In this use case, SDN orchestrator can play this role with the information received from the SDN controller of QKD network and from the SDN controller of OTN, respectively. In addition, the network operator can coordinate QKD network and OTN integrally with an SDN orchestrator via each SDN controller to ensure end-to-end service provisioning.

For the SDN orchestrator to play the coordinating role between both network domains, the interface between an SDN orchestrator and an SDN controller of QKD network needs to be defined. This interface describes the flow of information between both entities, the SDN controller being served as a server and the SDN orchestrator being served as a client. Through this interface, SDN orchestrator can orchestrate QKD network in terms of network configuration and topology, management policy, and performance management as well as address matching as described above.

An SDN orchestration can be defined as the continuing process of automatically coordinating the available resources according to optimization criteria to establish and release the end-to-end service provisioning through different network domains controlled by each SDN controller, respectively. SDN orchestration may be used to start the series of automated processes required to satisfy a customer service request generated via a customer website. An SDN orchestrator is a master entity that enables each SDN controller to establish and release multiple paths in its own network domain to conform to customers' end-to-end service provisioning requests through different network domains.
Since quantum cryptography communication networks are built in parallel with optical communication networks in SK Telecom, it was essential for SK Telecom to manage both networks in an integrated way. This task is to develop an interface (SDN Orchestration Interface) standard that includes a software-defined network (SDN) that controls quantum cryptography communication into the telecommunication company's overall network integrated management.

The standardization of the existing quantum cryptography communication has progressed in terms of the function of providing an encryption key in an independent quantum cryptography communication network, but it has been recognized that the standardization of the integrated management standard with the optical communication network is absolutely necessary.

By standardizing ETSI GS QKD 018 [ETSI GS QKD 018], when telecommunication companies introduce quantum cryptography communication networks, it is expected that the technical obstacles to integrated management of the two networks would be alleviated and the commercialization of quantum cryptography communication would be activated.
In addition, when attempting to hack a quantum cryptography communication network, it is immediately recognized and it is easy to connect to a new optimal safe route, and it is expected to be flexibly applied when expanding the service area of the quantum cryptography communication network in the future. In particular, as 5G-based hyper-connected services are expanding, the importance of standardizing quantum cryptography communication standards is further emphasized.

3.3 Interworking and interoperability scenarios

ETSI ISG-QKD initiated the work to specify a REST API that allows key management systems to interoperate to pass keys horizontally between two systems, usually with two different vendors, located in a common trusted node in the draft ETSI GS QKD 020 [ETSI GS QKD 020]. The API enables QKD networks to serve applications that request shared secret keys from key management systems that are not linked by a contiguous chain of systems from the same vendor. It is beyond the scope of the document to describe how the underlying QKD networks agree key material between nodes. URI formats, communication protocols (HTTPS), and the JSON data format encoding of posted parameters and responses (including key material) are supposed to be described.

The primary purpose of the key management system in network of QKD systems is to deliver QKD keys to cryptographic applications. Aligned with the terminology in ETSI GS QKD 014 [ETSI GS QKD 014], cryptographic key-consuming applications at each node are Secure Application Entities (SAEs) and instances of key management software that they connect to are Key Management Entities (KMEs). When an SAE initiates a request to a KME for symmetric keys shared with the "target SAE" it becomes the "initiator SAE". The key management system of the network is responsible for implementing secure key distribution between the KMEs to enable key requests from the initiator and target SAEs to be honoured.

APIs have been specified in ETSI GS QKD 014 [ETSI GS QKD 014] and ETSI GS QKD 004 [ETSI GS QKD 004] that define methods and data formats for the delivery of keys from a KME to a SAE. However, where different parts of a network use key management systems that are incompatible or managed separately etc. a standardized interface is required for KMEs to pass keys horizontally between different parts of the network. The API described in the present document enables such key transfers such that shared keys can be delivered to SAEs that connect to Kem’s in different parts of the network.
An example of a network with several parts using systems from different vendors is illustrated in Figure 1. Each node includes QKD module(s) and at least one KME from the vendor of the links that it connects to. Nodes that are a point of presence in more than one part of the network are referred to as "gateway nodes".

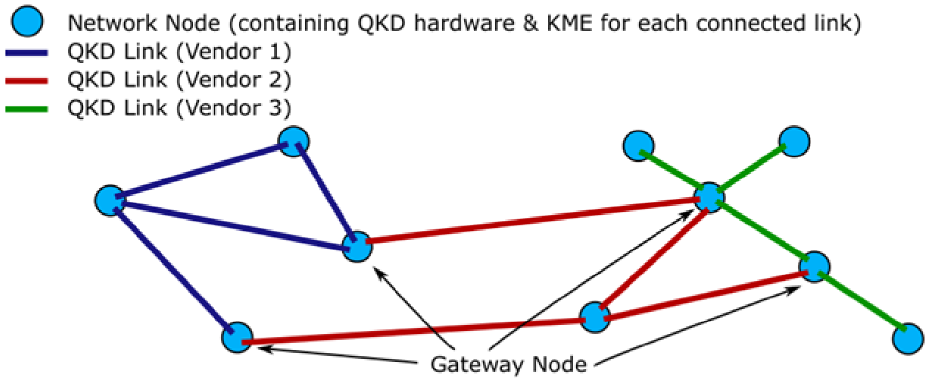


Figure 1: Schematic of multi-vendor QKD network

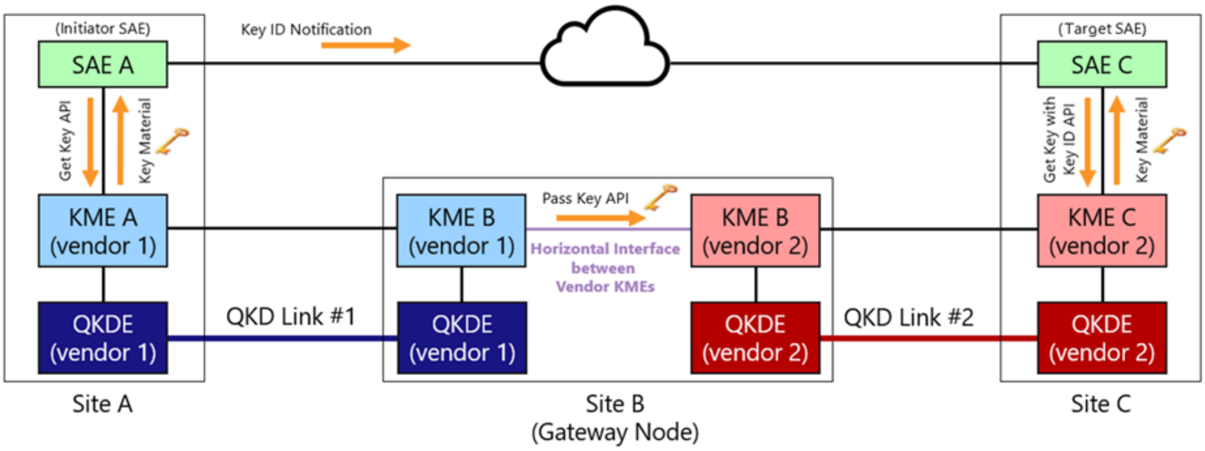


Figure 2: Three-node network illustrating interoperable key management system interface

Figure 2 shows a use-case in which the ext_keys method is used to pass keys horizontally between KMEs in a gateway node of a three-node network comprised of two parts using otherwise incompatible systems from different vendors.

While ETSI ISG-QKD focuses on the interworking interface between multi-vendor environments, ITU-T has been working on a series of recommendations for interworking supporting multiple QKD Network (QKDN) providers. Y.3810 [ITU-T Y.3810] is a recommendation for 'Quantum key distribution network interworking –framework' which is now under final review by ITU-T members for approval and two further recommendations, 'Quantum key distribution interworking – requirements' and 'Quantum key distribution interworking – architecture' are under development. The security perspective for the interworking is also considered and a new work item [ITU-T X.sec_QKDNi] was approved in ITU-T SG17 at last August 2022. QKDN providers may have their own policies for such as service, charging, routing and security. Network topologies and technology which are used in QKDN are confidential information. They don't usually disclose them to other QKDN providers even in interworking cases. QKDNs should be demarcated at a network boundary and connect through interworking interfaces. Interworking interfaces are strictly prohibited to transfer unauthorized information. There are two reference models considered as described below.
Figure 3 shows a reference model for QKDN interworking with Gateway Functions (GWFs.)

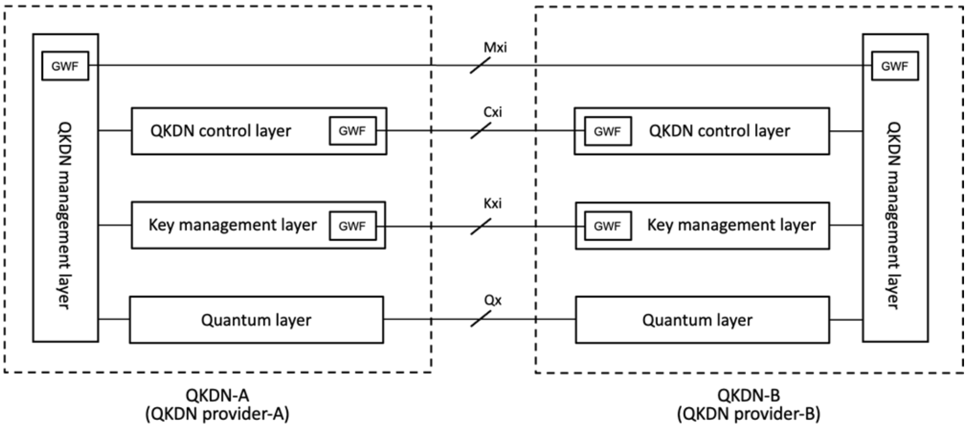


Figure 3: Reference model for QKDN interworking with GWFs

The GWF is located at the border of each QKDN provider. The GWF is a functional entity to support interworking interfaces between two different QKDN providers. The GWF may perform to convert internal protocols in a QKDN to other protocols for QKDN interworking. Even in a case that standardized protocols are used in a QKDN internally, the GWF conducts protocol conversion that gets into alignment with inconsistency of the parameters used in the internal protocol and the interworking protocol such as filtering of confidential parameters.

Figure 4 shows a reference model for QKDN interworking with interworking functions (IWFs).

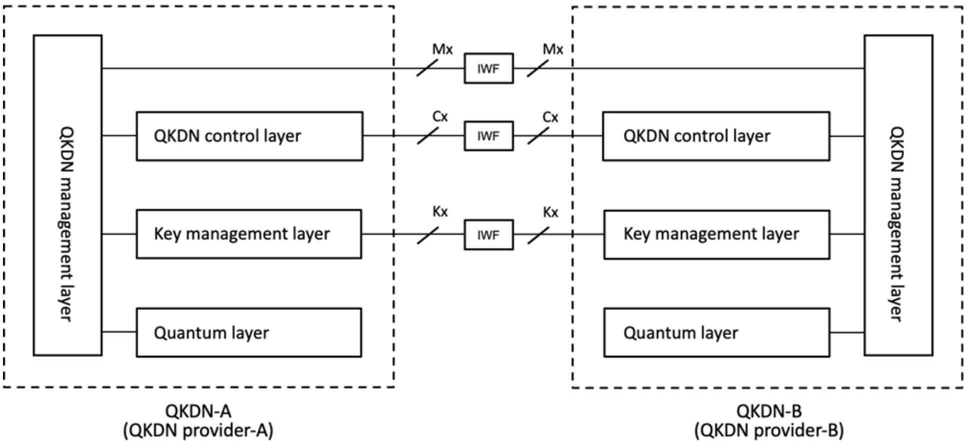


Figure 4: Reference model for QKDN interworking with IWFs

The IWF might be used for connecting QKDNs, as shown in Figure 4. The IWF can be installed in a trusted node other than inside of the QKDN which interworks. The interworking structure with the IWF is one of the variations of the structure using the GWFs for interworking, considering the IWF consists of two GWFs.

Even though the interworking aspects between different QKD providers, this is very start of the large scale of QKDN networks to provide the end-to-end QKD service to cover the large areas to the end users and to provide the QKD service when the end user is not in the area of home network etc. Therefore, the federation of QKDNs to share the resources and capabilities of many QKDN providers shall be considered to create the industry ecosystem including operators, vendors, OEMS and service providers which could lead to eventually a platform to develop additional services in the future. Federation refers to the interaction and coordination between QKDN providers and QKDNs, supporting multi-operator, - network, - vendor environment to provide the seamless QKDN service to the end users. If the end user wishes to have the same level of security which QKDN provides when the end user moves to the region of other QKDN provider, then the end user needs to find the service capability in that region. The relevant QKDN service discovery, network capability discovery, resource allocation and negotiation and the subsequent service provisioning need to be performed. As QKD technology is being deployed around the world, however, still limited coverage exists from QKDN perspective as only some operators deploy them in part of their networks. Therefore, it is good to have the mechanisms to have the same level of security service in the different regions where possible and to combine resources among multiple operators. Furthermore, the QKDN sharing could be also considered where one operator does not have QKDN coverage in certain regions in a certain country. This perspective is considered in ITU-T SG13 to initiate a new work item last July [ITU-T Y.QKDNf-fr].

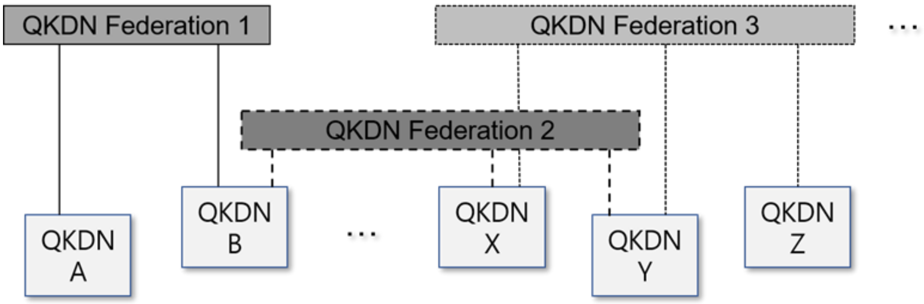
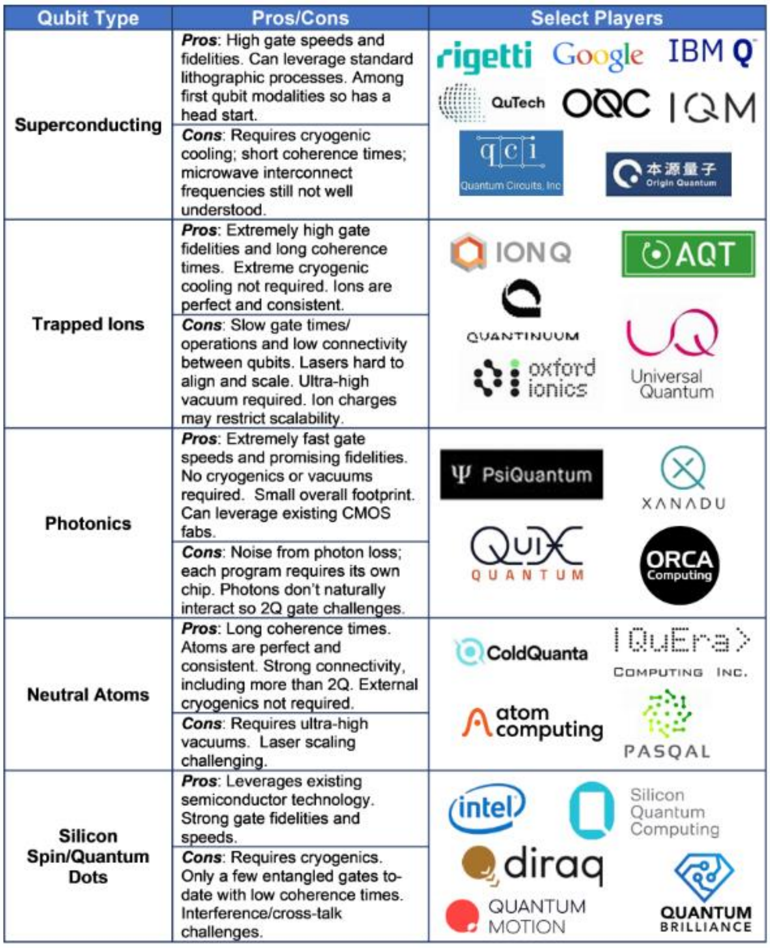


Figure 5: Conceptual model of QKDN federation

4 Quantum-HAL for Quantum Computing and Networking

Quantum-HAL would provide unified northbound quantum Application Programming Interfaces (APIs) for the higher layers, decoupling from the different types of quantum hardware technologies for Quantum Computing and Networking.

The following picture (Figure 6) summarizes a list of quantum hardware technologies, with some of the benefits and challenges along with some of the current Technology Providers. The list provide just an indicative example and it is not exhaustive.



Qubit Type	Pros/Cons	Select Players
Superconducting	***Pros***: High gate speeds and fidelities. Can leverage standard lithographic processes. Among first qubit modalities so has a head start. ***Cons***: Requires cryogenic cooling; short coherence times; microwave interconnect frequencies still not well understood.	rigetti Google IBM Q QuTech OQC IQM qci Quantum Circuits, Inc 本源量子 Origin Quantum
Trapped Ions	***Pros***: Extremely high gate fidelities and long coherence times. Extreme cryogenic cooling not required. Ions are perfect and consistent. ***Cons***: Slow gate times/ operations and low connectivity between qubits. Lasers hard to align and scale. Ultra-high vacuum required. Ion charges may restrict scalability.	IONQ AQT QUANTINUUM Universal Quantum oxford ionics
Photonics	***Pros***: Extremely fast gate speeds and promising fidelities. No cryogenics or vacuums required. Small overall footprint. Can leverage existing CMOS fabs. ***Cons***: Noise from photon loss; each program requires its own chip. Photons don't naturally interact so 2Q gate challenges.	PsiQuantum XANADU QUIX QUANTUM ORCA Computing
Neutral Atoms	***Pros***: Long coherence times. Atoms are perfect and consistent. Strong connectivity, including more than 2Q. External cryogenics not required. ***Cons***: Requires ultra-high vacuums. Laser scaling challenging.	ColdQuanta |QuEra〉 COMPUTING INC. atom computing PASQAL
Silicon Spin/Quantum Dots	***Pros***: Leverages existing semiconductor technology. Strong gate fidelities and speeds. ***Cons***: Requires cryogenics. Only a few entangled gates to-date with low coherence times. Interference/cross-talk challenges.	intel Silicon Quantum Computing diraq QUANTUM MOTION QUANTUM BRILLIANCE

Figure 6: Examples of a list of quantum hardware technologies (Picture credits: https://quantumtech.blog/2022/10/20/quantum-computing-modalities-a-qubit-primer-revisited/)

This section provides some basic definitions about the concept of Quantum-HAL and the possible data modelling language (e.g., YANG) and protocols (E.g., NETCONF)

4.1 High level architectural definitions

In general, the concept of hardware abstraction layers (HAL) of an IT system has been used to indicate ways to provide an interface between hardware and software so that the applications and services developments and executions can be made node/system/device independent.

In classical computing systems, for example, a HAL is a layer that allows a computer OS to interact, through standard API, with a hardware device and components at a general or abstract level rather than at a detailed hardware level.

The concept of Quantum-HAL offers an extension of the HAL applicable for quantum computing and quantum networks. The next two sections will provide some examples.

4.1.1 Examples of Hardware Abstraction Level in Quantum Computing

One of the first examples of the concept of Hardware Abstraction Level for Quantum Computing was formulated in "A Quantum von Neumann Architecture for Large-Scale

Quantum Computing” [QuvNA], with an emphasis on von Neumann quantum equivalence solution.

As the size of quantum systems becomes bigger, more complicated hardware is required to control these systems. In the paper it is argued that to build a large-scale quantum computer, one can use architectural principles, from classical computer architecture, like multiplexing or pipelining, so a Quantum von Neumann architecture is introduced which uses specialized hardware for the different tasks of a quantum computer, like computation or storage. The quantum von Neumann architecture combines the classical von Neumann architecture with the requirements of the DiVincenzo-criteria in Quantum Computing resulting in quantum hardware which incorporates scalability requirements. The schematic diagram of the quantum von Neumann architecture is depicted in Figure 7.

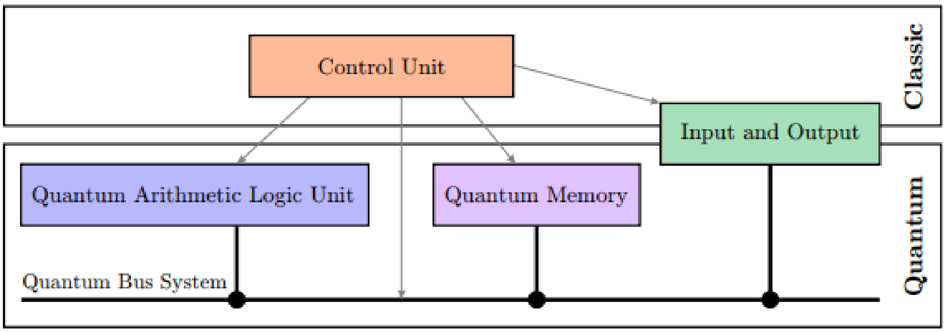


Figure 7: Quantum von Neumann architecture [QuvNA]

Specifically, Figure 8 shows, for instance, the parallelism in Quantum von Neumann architecture: panel (a) shows a multi quantum processor system with a shared quantum memory; panel (b) depicts a multi quantum computer which couple’s multiple quantum computers via a quantum interface.

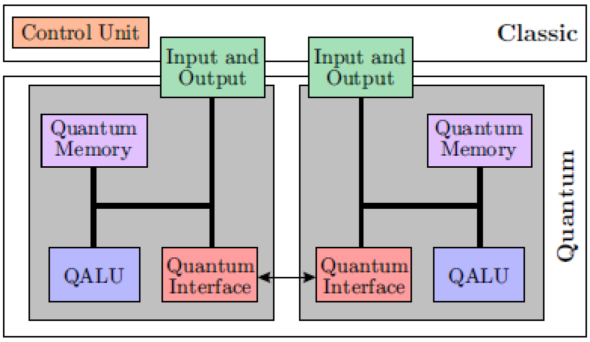


Figure 8: Parallelism in Quantum von Neumann architecture [QuvNA]

4.1.2 Examples of Hardware Abstraction Level in Quantum Communications

The development and exploitation of a large-scale quantum network will require both advancements in quantum hardware capabilities and also robust control of such nodes, systems and devices. Moreover, the abstraction of tasks and services offered by the quantum network should enable platform-independent applications to be executed without knowledge of the underlying physical implementation.

The following Figure 9 shows an example of Quantum network node architecture [ExEQN] which includes an HAL. At the application layer, a simple platform independent routine is sent to the network controller. The network controller implements the platform-independent stack—in this work only the link layer protocol—and a hardware abstraction layer (HAL) to interface with the physical layer's device controller. An instruction processor dispatches instructions either directly to the physical layer, or to the link layer protocol in case a remote entangled state is requested by the application. The link layer schedules entanglement requests and synchronizes with the remote node (on a local area network, LAN) using a time-division multiple access (TDMA) schedule computed by a centralized scheduler (external).

At the physical layer, the device controller fetches commands from—and replies with outcomes to—the network controller. Driven by a clock shared with the neighbouring node, it performs hard-real-time synchronization for entanglement generation using a digital input/output (DIO) interface. By controlling the optical and electronic components (among which an arbitrary waveform generator, AWG), the device controller can perform universal quantum control of the communication qubit in real-time, as well as attempt long-distance entanglement generation with the neighbouring node.

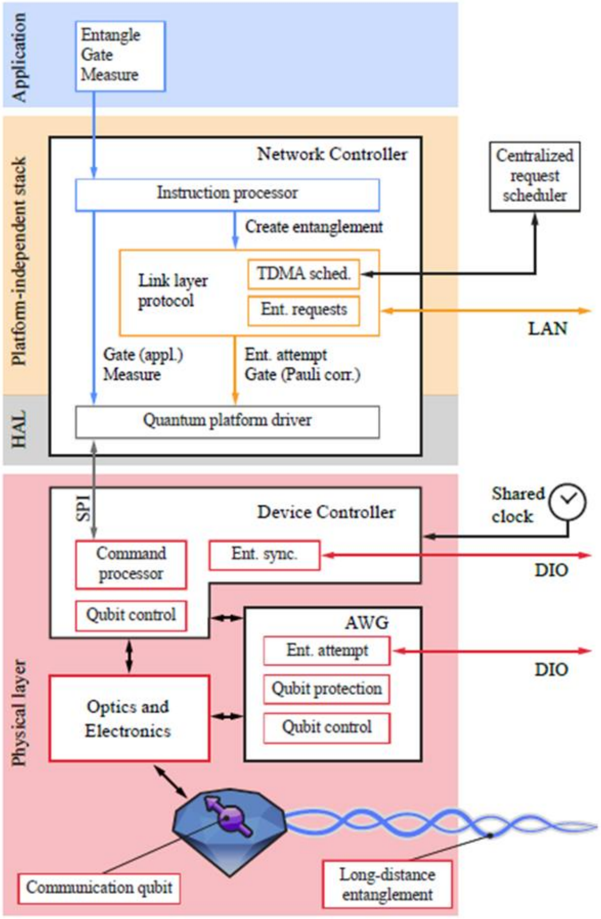


Figure 9: Example of Quantum network node architecture

The next picture (Figure 10) is an illustration of (Quantum) Hardware Abstraction between Physical and Link layers [LLPQN]:

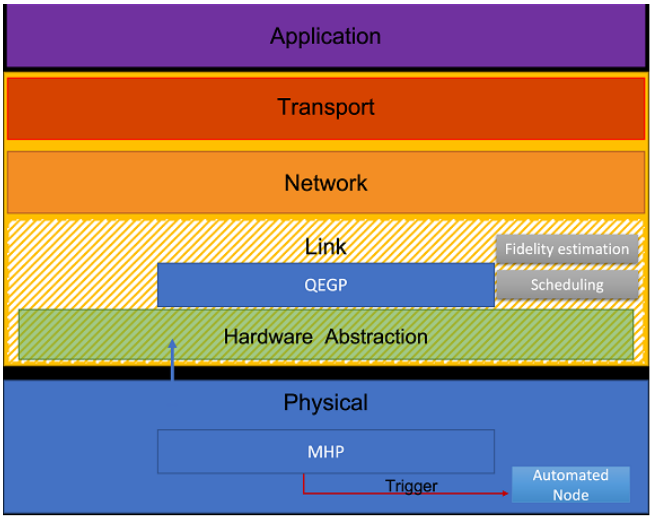


Figure 10: Example of Quantum Hardware Abstraction between Physical and Link layers

In the picture, the acronyms QEGP and MHP stand for Quantum Entanglement Generation Protocol and Midpoint Heralding Protocol, respectively.

The QEGP protocol, as originally designed, relies on the underlying quantum physical layer protocol to achieve accurate timing synchronization with its remote peer and to detect inconsistencies between the local state and the state of the remote counterpart. To satisfy such requirements, QEGP is accompanied by a quantum physical layer protocol, called Midpoint Heralding Protocol (MHP), designed to support QEGP on heralded entanglement-based quantum links.

4.2 Possible Data modelling languages and protocols

YANG is a data modelling language used to model configuration and state data. Together, NETCONF and YANG provide the tools that network administrators may use for management and control tasks across heterogeneous nodes and systems in infrastructures adopting Software Defined Network (SDN) paradigms.

YANG has been developed by the IETF NETCONF Data Modelling Language Working Group (NETMOD) to be easily read by humans and as of this writing. The YANG specification is published as RFC 6020 and YANG types as RFC 6021.

Using YANG for data modelling has two main advantages: firstly, it has been positioned as the main modelling language for network elements, systems and services while the main network control plane protocols already use it to structure their internal data; secondly, it is easy to define, read and extend base when introducing new technologies and services.

5 State-of-the-art on abstractions and data modelling

5.1 Standardization Bodies

5.1.1 ETSI – QKD

The parameters and modelling defined in ETSI GS QKD 015 [ETSI GS QKD 015] relate to the management interface of QKD modules (one or multiple) that connects them to an SDN controller. The requirements for such an interface and further integration are described as a YANG model and as associated workflows for the main functional use cases. This architectural design permits a controller to centrally orchestrate the QKD resources to optimize the key allocation per link based on demands and automate the creation of either direct (physically connected through an uninterrupted quantum channel) or virtual (multi-hop-based) QKD links, where the keys are relayed from one hop (direct QKD link) to the next in the chain connecting the initial with the final points. The workflows would be implemented by using any of the well-accepted network management protocols used in SDN architectures, which are based on YANG information models for their internal data structures. However, it is out of the scope of ETSI GS QKD 015 [ETSI GS QKD 015] to define which specific protocol, data structures or specific implementation is chosen to carry the YANG-structured information defined.

ETSI GS QKD 018 [ETSI GS QKD 018] provides a definition of an orchestration interface between an SDN orchestrator and an SDN controller of a QKD network. This orchestration interface defines the abstract information models and workflows for QKD network resource management, configuration management, performance management, service provisioning, notifications and management of multi-domain QKD networks. Interfaces between an SDN orchestrator and SDN controllers of classical optical transport networks are out of scope. The YANG model proposed in the ETSI GS QKD 015 [ETSI GS QKD 015] and ETSI GS QKD 018 [ETSI GS QKD 018], are available at ETSI Forge, where users of ETSI standards can download software that has been produced collaboratively by ETSI delegates.

5.1.2 ITU-T Q16/SG13

ITU-T SG13 Q16 published the recommendation Y.3805 [ITU-T Y.3805] which specifies the requirements, functional architecture, reference points, hierarchical SDN controller and overall operational procedures of SDN control based on the QKDN control layer in their architectural model.

5.1.3 IEEE P1913

IEEEP1913 [IEEEP1913] is about the configuration of quantum devices in a communication network to dynamically create, modify, or remove quantum protocols or applications and facilitate cross-device information flow. The control protocol resides at the application layer and communicates over Transmission Control Protocol/Internet Protocol. The standard defines a set of quantum device configuration capabilities that control the transformation, transmission, and reception of quantum states. These device commands contain parameters that describe quantum state preparation, measurement, and readout. Stakeholders include Quantum key distribution companies, Quantum communication device manufacturers, Critical infrastructure owners and developers, Communication network managers and Quantum Computing device manufacturers.

The adopted model assumes that the quantum services offered by a device can be expressed in terms of quantum circuits composed as a series of connected quantum gates. These can be well-known gates or custom transformations There is also an ongoing focus on optical implementation of quantum circuits, as such is today's typical realization of quantum hardware. Likewise, a quantum-key-distribution-specific module is being elaborated as a common application and use case. Future versions of this standard will consider other quantum frameworks (e.g., annealing), implementations (e.g., topological), and use cases (e.g., teleportation, superdense coding, etc.) [IEEEP1913].

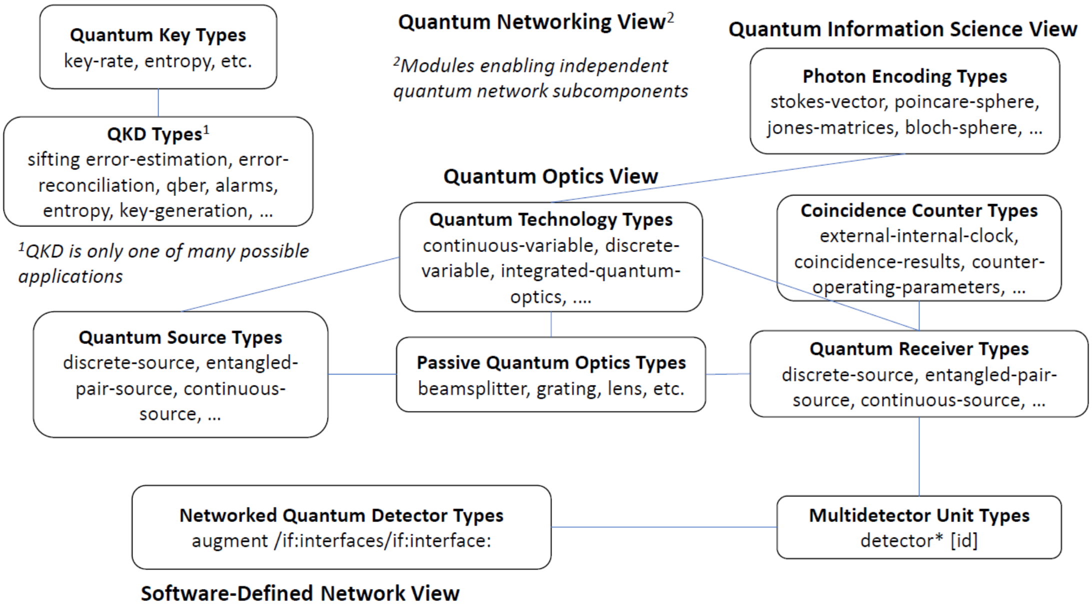

Quantum Key Types
key-rate, entropy, etc.
Quantum Networking View2
2Modules enabling independent quantum network subcomponents
Quantum Information Science View
Photon Encoding Types
stokes-vector, poincare-sphere, jones-matrices, bloch-sphere, ...
QKD Types1
sifting error-estimation, error-reconciliation, qber, alarms, entropy, key-generation, ...
1QKD is only one of many possible applications
Quantum Optics View
Quantum Technology Types
continuous-variable, discrete-variable, integrated-quantum-optics, ...
Coincidence Counter Types
external-internal-clock, coincidence-results, counter-operating-parameters, ...
Quantum Source Types
discrete-source, entangled-pair-source, continuous-source, ...
Passive Quantum Optics Types
beamsplitter, grating, lens, etc.
Quantum Receiver Types
discrete-source, entangled-pair-source, continuous-source, ...
Networked Quantum Detector Types
augment /if:interfaces/if:interface:
Multidetector Unit Types
detector* [id]
Software-Defined Network View

Figure 11: Examples of YANG modules under development in IEEE P1913 (Picture credits: Stephen F Bush presentation in July 2022 at the GSMA QNS WI meeting)

5.1.4 IRTF on Quantum

Overall, the goal of the QIRG is to address the question of how to design and build quantum networks. Some of the problems that need to be addressed includes Routing, Resource allocation, Connection establishment, Interoperability, Security, API design. Some other problems that can be tackled by the QIRG: Applications for a Quantum Internet and Multi-party states and multi-party transfers such as network coding

Concrete work items that QIRG may produce include an architectural framework delineating network node roles and   definitions, to build a common vocabulary and serve as the first step toward a quantum network architecture.

[IRTFQI] represents a roadmap of technical capability milestones for quantum networks. Mapping these milestones to concrete use cases will help to determine the order and timing of classical protocols that will be needed.

5.2 Example of related activities in European Projects

Figure 12 shows some examples of the initiatives related to quantum technologies and services launched in by European Commission.

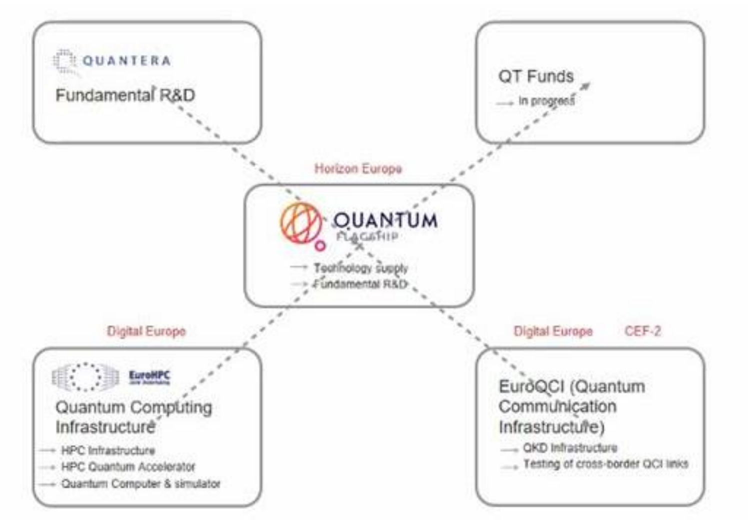


Figure 12: Initiatives related to quantum technologies and services launched in by European Commission

The H2020 Quantum Flagship was launched in 2018 with a budget of €1 billion and a duration of 10 years, the flagship brings together research institutions, academia, industry, enterprises, and policy makers, in a joint and collaborative initiative on Quantum Technologies and Services.

Examples of projects dealing with the topics covered by the white paper include QIA, CIVIC and UNIQORN (Figure 13).

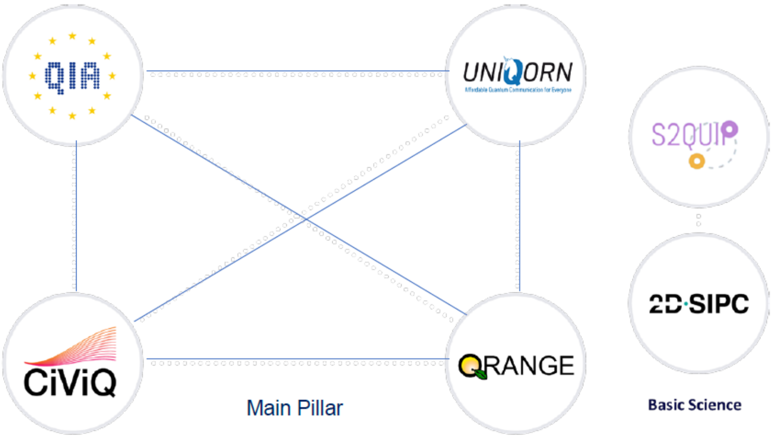


Figure 13: H2020 Quantum Flagship

Since June 2019, all 27 EU Member States have signed the European Quantum Communication Infrastructure (EuroQCI) Declaration, signalling their commitment to the EuroQCI initiative. The participating countries are working with the European Commission and the European Space Agency (ESA) to design, develop and deploy the EuroQCI. The aim is for it to be fully operational by 2027.

According to the official EU website [EuroQCI], the EuroQCI aims at protecting sensitive data and critical infrastructures by integrating quantum-based systems into existing communication infrastructures, providing an additional security layer based on quantum physics. It will reinforce the protection of Europe's governmental institutions, their data centres, hospitals, energy grids, and more, becoming one of the main pillars of the EU's new Cybersecurity Strategy for the coming decades.

5.2.1 Example of project: Quantum Internet Alliance (QIA)

The Quantum Internet Alliance (QIA) is an international project which received funding from the European Union's Horizon 2020 research and innovation program. QIA targets a Blueprint for a pan-European Quantum Internet by ground-breaking technological advances, culminating in the first experimental demonstration of a fully integrated network stack running on a multi-node quantum network.

QIA aims at pushing the frontier of technology in both end nodes (trapped ion qubits, diamond NV qubits, neutral atom qubits) and quantum repeaters (rare-earth-based memories, atomic gases, quantum dots) and demonstrate the first integration of both subsystems. Objectives includes: to achieve entanglement and teleportation across three and four remote quantum network nodes, thereby making the leap from simple point-to-point connections to the first multi-node networks; to demonstrate the key enabling capabilities for memory-based quantum repeaters, resulting in proof-of-principle demonstrations of elementary long-distance repeater links in the real-world, including the longest such link worldwide [QIA].

5.2.2 Example of project: CIVIQ

The goal of the CiViQ project has been to investigate an avenue towards flexible and cost-effective integration of quantum communication technologies, and, in particular, Continuous-Variable QKD, into emerging optical telecommunication networks [CIVIQ].

CiViQ aimed at a broad technological impact based on a systematic analysis of telecom-defined user-requirements. To this end CiViQ engages a broad interdisciplinary community of 21 partners, involving major telecoms, integrators, and developers of QKD. The work targeted advancing both the QKD technology itself and the emerging "software network" approach to lay the foundations of future seamless integration of both.

5.2.3 Example of project: UNIQORN

UNIQORN's goal has been to provide the enabling photonic technology to accommodate quantum communications, by shoehorning complex systems, which are presently found on metre-size breadboards, into millimetre-size chips. These systems will not only reduce size and cost but will also bring improvements in terms of robustness and reproducibility [UNIQORN].

Starting with advanced components optimised for quantum applications UNIQORN has shoehorned entire quantum-optic systems into system-on-chip (SoC) realizations, leading to highly miniaturized solutions for further system- and network-level integration. Selected quantum applications beyond simple quantum key distribution will build on UNIQORN's highly integrated and yet cost-effective technology and has been evaluated in lab and field.

5.3 QED-C

The Quantum Economic Development Consortium (QED-C) is a consortium of stakeholders that aims to enable and grow the U.S. quantum industry. QED-C was established with support from the National Institute of Standards and Technology (NIST) as part of the Federal strategy for advancing quantum information science and as called for by the National Quantum Initiative Act enacted in 2018.

Today, QED-C has support from multiple agencies and a diverse set of industry, academic, and other stakeholders. QED-C participants are working together to identify gaps in technology, standards, and workforce and to address those gaps through collaboration [QED-C].

5.4 Other Projects and Initiatives

5.4.1 ISCF Project for Quantum Technologies

The UK Government's Industrial Strategy Challenge Fund (ISCF) brings together leading research and business to tackle the big societal and industrial challenges today.

Several major quantum communications projects have been funded since 2018, involving many Hub partners and, in some cases, further exploiting Hub developed technologies. Some examples of ISCF funded projects are given below.

- 3QN: Towards a New UK Industry for Novel Quantum Receivers in Nascent Satellite QKD Global Markets
- Overcoming technological barriers to the commercialisation of QRNGs
- Developing flexible, low cost and user-friendly prototypes for quantum-safe communication networks

Figure 14, describes the model of Hardware Abstraction Layer (HAL) defined in the project [QHAL]

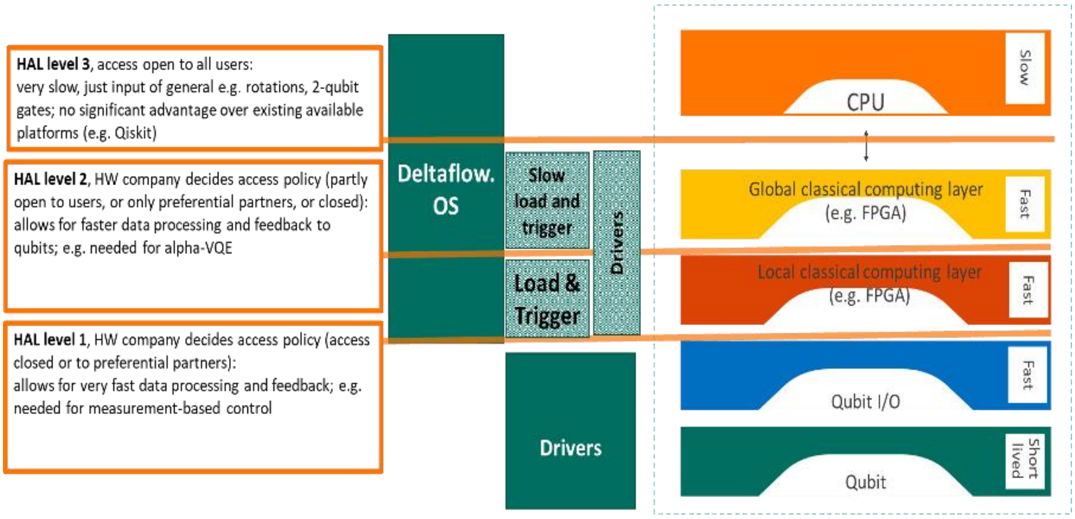

HAL level 3, access open to all users:
very slow, just input of general e.g. rotations, 2-qubit gates; no significant advantage over existing available platforms (e.g. Qiskit)
HAL level 2, HW company decides access policy (partly open to users, or only preferential partners, or closed): allows for faster data processing and feedback to qubits; e.g. needed for alpha-VQE
HAL level 1, HW company decides access policy (access closed or to preferential partners):
allows for very fast data processing and feedback; e.g. needed for measurement-based control
Deltaflow. OS
Slow load and trigger
Load & Trigger
Drivers
Drivers
CPU
Slow
Global classical computing layer (e.g. FPGA)
Fast
Local classical computing layer (e.g. FPGA)
Fast
Qubit I/O
Fast
Qubit
Short lived

Figure 14: Positions of Multi-level HAL layers within the Quantum Processing Unit (QPU) system (Picture credits: https://riverlane.github.io/QHAL_internal/v0.1.1/general.html)

According to [QHAL] the HAL must be capable of supporting advanced algorithms with different degrees of quantum/classical interaction. Current algorithms can be reconducted into three main groups with growing requirements in classical to quantum latency. We associate these groups to three levels of HAL as follows.

The highest level is 3, the ability to run large batches of a static circuit. This is implementable in a setting with high latency, typically much larger than the decoherence time, and is equipotent to commercial quantum devices available over the cloud.
In level 2, there is no change to the quantum device's abilities, but the latency of the classical control is now in order of qubit decoherence time. The controlling hardware can now make circuit updates based upon a single circuit's results, without a significant proportion of qubit "dead time".

In level 1, the ability to make mid circuit measurements, and control of the QPU based on the measurement outcome, is included. This requires the controlling device to make changes or store results on the gate time order on the quantum device and hence well below the decoherence time, so communication must also be of very low latency. The following table summarises the HAL levels 3-1, the timescales and corresponding algorithms considered in the first version of the specification. A general aim is to define a multi-level HAL flexible enough to cater to future developments and additions.

6 Conclusions and Recommendations

A first quantum revolution has already brought quantum technologies in our everyday life since decades. Chips for computers and smart-phone, systems for medical imaging (Nuclear Magnetic Resonance, Positron Emission Tomography), LED and lasers, etc. are all based on technologies exploiting the quantum mechanics principles.

Now a second revolution seems to be underway, leveraging on the three quantum principles of superposition, entanglement, and measurement. It is safe to predict that a second wave of quantum technologies could potentially have a major impact in many markets, ranging from Telecom and ICT, to Medicine, to Finance, to Transportation, and so on. Significant work is still needed to develop enabling components and systems but in light of the potential opportunities and threats, significant investments are being made worldwide across the public and private organizations.

International innovation activities and Standardization Bodies are pretty aligned in identifying four main applications areas of quantum technologies and services: communications, computing, simulations, sensing and metrology.
Standardization efforts are also set to help coordinating and accelerating progresses of quantum technologies. Multiple groups such as ANSI, ITU, IETF, ETSI, GSMA and IEEE are producing significant efforts.

The main conclusions and recommendations provided by this white paper are:

- **A common terminology and language on quantum technologies and** services are essential at all steps from innovation to equipment and platforms developments and exploitations. Infact, one major obstacle delaying roadmaps, standardization and initial deployment of Quantum Networking and Computing infrastructure is the lack of a common terminology and language. An agreement on terminology will enable governments, industry, and the research community to more effectively interact and operate towards the common goal of developing quantum ecosystems. **While terminology and definitions are currently under development within several SDOs, so it is important to reach an overall harmonization of these efforts to reach a common language and modelling approach;**

- **A Quantum Hardware Abstraction Layer (Quantum-HAL) would simplify and speed-up the development of quantum platforms, services, and applications.** Infact, another major obstacle hindering developments and large deployments of Quantum Networking and Computing infrastructure is that, today, the industry has not yet consolidated around one type of quantum hardware technology. In fact, Applications and Services Developers to start using the abstractions of the underneath quantum hardware (even if today under consolidation). Again, as shown by this white paper, **these concepts are already under development in several innovation initiatives, but more efforts are required also to get an overall standardized perspective (e.g., in**

terms of architecture and interfaces) valid for Quantum Infrastructures (integrating Quantum Computing and Quantum Networking).

- Today, QKD is the most mature technology application of Quantum Technologies (i.e., with the higher TRL around 7-8) for the cybersecurity of telecom infrastructures. **Standards on management, control and orchestration of QKD systems in current infrastructure are absolutely mandatory (and the ongoing trend is about using the SDN paradigm).** At the same time, in the same domain of cybersecurity of telecom infrastructures, there is a growing interest also on Post-Quantum Cryptography (PQC). PQC does not use any quantum technologies, but it refers to cryptographic algorithms that are thought to be secure against a cryptanalytic attack by quantum computers. **It is likely that QKD and PQC have different applicability scenarios in future Quantum Infrastructures, also including their potential integration in end-to-end cybersecurity services in future telecom infrastructures. This is an innovation avenue that requires techno-economic analysis and investigations.**

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
V1.0	21 December 2022	New White Paper Publication Acknowledgements Fabio Cavaliere, Ericsson Diego R. Lopez, Telefonica Antonio Manzalini (Telecom Italia - TIM) Dong Hi Sim (SK Telecom) Olivier Le Moult (Orange)	IG/TG	Antonio Manzalini (TIM)

A.2 Other Information

Type	Description
Document Owner	Internet Group
Editor/Company	Antonio Manzalini / Telecom Italia (TIM)