The Opportunities and Challenges of EuroQCI

Felix Wissel, Oleg Nikiforov, Daniel Giemsa, Matthias Gunkel
Deutsche Telekom Technik GmbH, Ida-Rhodes-Str. 2, 64295 Darmstadt; Germany
Felix.Wissel@telekom.de

Abstract: EuroQCI, the European Quantum Communication Infrastructure, is one of the most ambitious security initiatives in Europe. We will present the status and discuss challenges and opportunities. © 2024 The Author(s).

1. EuroQCI

Since 2019 all 27 EU Member States signed a declaration on a quantum communication infrastructure for the EU (EuroQCI) [1]. The declaration's aim is to create the first operational European platform providing quantum-secure shared secrets to protect governmental communication and other critical infrastructure, like healthcare and financial institutions. This includes facilitating an infrastructure for EU-27 based supply chains and a joint action plan to support the national QCI implementations. EuroQCI is a part of the European Cybersecurity Strategy [2] and will be integrated into the new Secure Space Connectivity initiative 'IRIS²'. These projects position Europe as a global frontrunner in quantum technology, promoting economic growth, fostering innovation, and laying the ground for the future quantum internet.

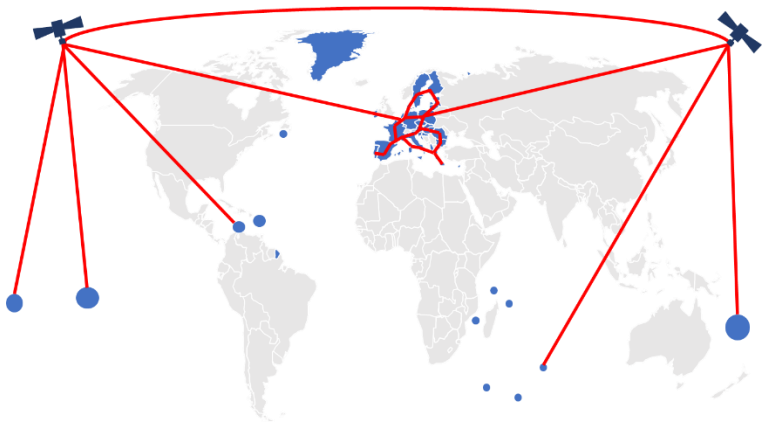

Figure 1 Generic model for a EuroQCI spanning over the European Union and its overseas territories.

EuroQCI will consist of an integrated terrestrial segment and satellite segments spanning the entire European Union including its overseas territories (see Figure 1). The EuroQCI space segment will distribute quantum-secured encryption keys on global scale. According to the concept of operations [3], the terrestrial segment of EuroQCI comprises a federation of national terrestrial QCI networks with cross border links.

The fundamental use case of EuroQCI is to provide a secure key exchange, enabling quantum-secure communication services for European users within the EU and globally. This is based on Quantum Key Distribution (QKD).

2. Overview recent Activities and Approach

To pursue the EuroQCI initiative, several projects were initiated and funded by the European Commission. Based on basic research in the Quantum Technology Flagship, the Horizon 2020 project OpenQKD, led by Austrian Institute of Technology (AIT) between 2019 and 2022 [4], implemented several metropolitan QKD network testbeds in various EU countries. This served for practical explorations of quantum capabilities, use cases and applications.

Additionally, two consortia from industry and academia – QOSAC (led by Airbus) and QCI4EU (led by Thales) – conducted a feasibility study and investigated potential network structures of a European QKD network [5]. These were further followed by two detailed design studies [6], 8TAVO (led by Airbus) and QSAFE (led by Deutsche Telekom), which developed detailed blueprints for a potential EuroQCI architecture, conducted a cost analysis, and described operational models. Most importantly, a preliminary security and risk assessment was elaborated.

The European Commission then released several calls for proposals within the Digital Europe Programme (DEP). They aim to support the development of the EuroQCI on various levels: support of start-ups, SMEs and QKD manufacturers based within the European Union (DIGITAL-2021-QCI-01-INDUSTRIAL); encourage individual Member States to build their own national QCIs (DIGITAL-2021-QCI-01-DEPLOY-NATIONAL and DIGITAL-2022-QCI-02-DEPLOY-NATIONAL). The Coordination and Support Action (CSA) of the national QCI deployments funded under the Digital Europe Programme (DIGITAL-2021-QCI-01-EUROQCI-QKD) is done within the PETRUS [7] project. For this consortium, the former primes of OpenQKD and the before-mentioned detailed studies joined forces. Finally, the European Commission issued a tender for a 'Testing and evaluation infrastructure for the European Quantum Communication Infrastructure (EuroQCI) initiative' [8], which will be implemented by a consortium led by Deutsche Telekom under the project name NOSTRADAMUS. The objectives of NOSTRADAMUS are to describe the blueprint for a testing & validation infrastructure to enable the evaluation and certification of QKD devices and related technologies, as well as to implement and operate a prototypical testbed facility to offer initial evaluation services which are mandatory for the accreditation by a European security authority.

Pursuing the development of the EuroQCI, PETRUS follows the 5P principle to measure the progress and quality of the implementation. This is a general framework of telecommunication industry, including:

- **People**: Operation governance, defined roles, availability of skilled people and their education opportunities.
- **Processes**: Service management processes, security, accreditation, testing etc. across all stakeholders
- **Platforms**: defined architecture and interfaces, available infrastructure, meeting the service levels and operational requirements; safeguarding by the patch and release processes.
- **Providers**: for component delivery, meeting the quality and process requirement.
- **Products**: supply chain for certified products in required quality, with associated service chains which are operated according to demand and requirements.

This approach allows to consider all relevant stakeholders and subareas that are expected to be impacted and that are required for a smooth implementation and operation of any communication platform.

3. Challenges

There are several fundamental limitations and challenges of QKD technology impacting the EuroQCI developments. Obviously, there is the reach limitation due to attenuation and the fact that the usage of optical amplifiers as in classical transport technology is impossible when the quantum nature of single photons should be exploited. This requires utilizing so-called Trusted Nodes and implies the necessity of trust in the infrastructure and the respective operators. However, it is often forgotten, that a certain amount of trust in for example certification authorities is already required today, and that there are ways to counter those challenges for QKD. Another challenge, that is often neglected, is that the actual quantum part of a QKD network is relatively small compared to the classical environment around the quantum network elements. This comprises all the required components to plan, build and run a QKD network and includes for example operations, monitoring systems, spare part management and trained personnel.

The greatest challenge is found in the fact that up to now there is less market request for QKD as the threat that QKD counters, i.e. quantum computer and its capabilities to crack classical quantum-vulnerable public-key cryptography, is not yet tangible for most stakeholders. Hence, the usual market mechanisms for reaching high Technical Readiness Levels (TRL) do not apply for QKD. For other innovations, a typical development can be observed: early adopters, friendly users, and technology enthusiasts are using new gadgets even though the maturity and feature sets of those products are not fully developed yet. This allows manufacturers and providers to already create revenue which can be used to further invest and increase the quality of next-generation products, which in turn attract more users until a mass market production can be reached. This results in decreasing costs and prices, and only when the technology itself is rather mature, security features are implemented to meet the requirements of more conservative user groups (see schematic illustration in Figure 2).

This characteristic behaviour is currently not observable in QKD. The technology is not widely in use, so price erosion effects could not yet take place. Additionally, user groups with the highest demands in security also have the highest security requirements on the used technology. Such users are typically governments, ministries, or national (cyber) security authorities. Especially when classified payload is considered, beta versions or low TRLs are not

accepted. This results in a dead lock situation, because other user groups, which also deal with sensitive information that requires protection, usually follow the advice and example of those security agencies. Thus, the evolution of currently commercially available QKD devices must be squeezed into a rather short time frame to meet higher security requirements. This affects not only the devices themselves, but also the required development of a proper framework for their evaluation and certification to allow usage for classified data encryption.

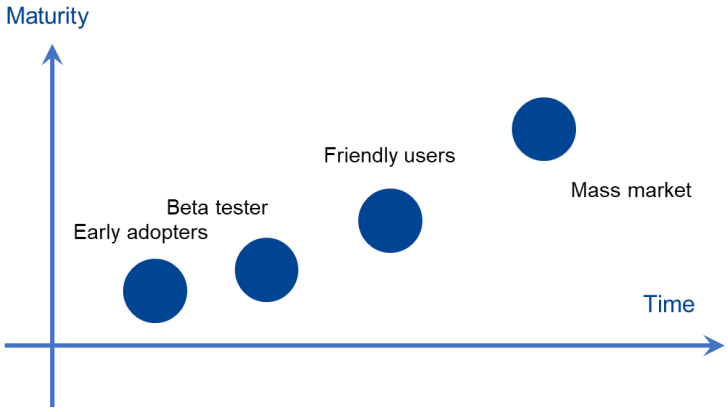

Figure 2 .The typical development rule of a generic technology. Maturity increases with time.

4. Outlook

Despite the above-described challenges, EuroQCI is on a good track and much progress has been made in the recent years. There will be major benefits from a fully implemented EuroQCI: The most obvious one is the increased security and the inherent protection of democracy and free European societies and the maintenance of sovereignty of the European Union and its Member States. Additionally, new expert profiles are created for operating a quantum network which goes along with progress in education like for example a dedicated degree as quantum engineer. Through EuroQCI new high-skill job positions will be required at all levels of the value chain from scientific research over component development and manufacturing up to system and platform engineers.

5. Bibliography

[1] “The European Quantum Communication Infrastructure (EuroQCI) Initiative,” [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci .

[2] The European Parliament and the Council, “The EU's Cybersecurity Strategy for the Digital Decade,” 2020.

[3] R. J. Steiner, “EuroQCI Concept of Operations,” 19 06 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/euroqci-conops-concept-operations.

[4] AIT Austrian Institute of Technology GmbH, “OpenQKD Project,” [Online]. Available: https://openqkd.eu/. [Accessed 24 01 2024].

[5] “Study On The System Architecture Of A Quantum Communication Infrastructure (Ref: EC H2020 SMART 2019/0086)”.

[6] “Detailed system study for a Quantum Communication Infrastructure (Ref: CNECT/LUX/2020/CPN/0062)”.

[7] Deutsche Telekom Global Business Solutions Belgium NV/ SA, “PETRUS,” [Online]. Available: https://petrus-euroqci.eu/.

[8] European Commission, CNECT, “Testing and Evaluation Infrastructure for EuroQCI Tender Details,” [Online]. Available: https://etendering.ted.europa.eu/cft/cft-display.html?cftId=14339.