Lux4QCI

EuroQCI

D2.1: Technical Report on National Use Cases and Scenario Selection Appendix B (Public)

Revision: v.3.1

Grant Agreement No.: 101091508
Call: DIGITAL-2021-QCI-01

Topic: DIGITAL-2021-QCI-01-DEPLOY NATIONAL
Type of action: DIGITAL-SIMPLE

APPENDIX B – (PUBLICLY AVAILABLE) TECHNICAL REPORT ON NATIONAL USE CASES AND SCENARIO SELECTION

Work package	WP 2
Task	Task 2.1
Due date	16/02/2024
Submission date	16/02/2024
Deliverable lead	SES Techcom
Annex version	1.0
Authors	Antoni H. Bonet (SES)
Reviewers	Junaid Ur Rehman (UNILU), Zaira Ambu (UNILU) SAB members: Symeon Chatzinotas (UNILU), Vincent Weynandt (LCON), Shivam Singh (INCERT), Christine Muller (SMC); Thomas Baeumer (SES), Carlo Harpes (ITR), Stefan Winter (RES)
Abstract	This document serves as a publicly available annex to Deliverable D2.1 within the Lux4QCI project, summarizing key insights derived from Task T2.1. The purpose of this document is to briefly describe the use cases, scenarios, and potential stakeholders of the LuxQCI system developed within the Lux4QCI project. The stakeholders are governmental and private entities, which have been categorized based on their industry affiliation, such as defence and military, governmental entities, healthcare, financial institutions, IT industry, communication industry, and transport industry. The identified use cases involve the integration of QKD-generated keys into existing security techniques. This, mainly, aims to ensure highly secure data transmission, particularly for the governmental sector, as well as protect long-term stored data, especially within the healthcare sector.
Keywords	QKD, Quantum Communication Infrastructure, use cases, stakeholders, High-security Data Transport, Long-term data storage

Document Revision History

Versio n	Date	Description of change	List of contributor(s)
1.0	16/02/2024	First release of this Annex B	SES, UNILU

Co-funded by the European Union

DISCLAIMER

Co-funded by the European Union

LUX4QCI Luxembourg Experimental Network for Quantum Communication Infrastructure project has been co-funded by the Digital Europe Programme under the Grant Agreement No. 101091508.

“Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them”.

COPYRIGHT NOTICE

Project co-funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	**R**	
Dissemination Level		
PU	*Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project’s page)*	✓
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No 2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No 2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No 2015/ 444*	

* R: Document, report (excluding the periodic and final reports)

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

DATA: Data sets, microdata, etc.

DMP: Data management plan

ETHICS: Deliverables related to ethics issues.

SECURITY: Deliverables related to security issues

OTHER: Software, technical diagram, algorithms, models, etc.

B.1 INTRODUCTION

The European Commission (EC) together with the supporting European Union (EU) member states have initiated the development and deployment of a Quantum Communications Infrastructure (QCI) for Europe. The mid- to long term plan is for the QCI to support distributed quantum computing and the quantum internet. However, in the current stage, the focal point of the QCI is to enable and provide Quantum Key Distribution (QKD) services.

Under this European initiative, each supporting member state shall initiate the development of its own national QCI to interlink it with the other EU member states' QCIs, creating a European wide infrastructure, the so-called European Quantum Communication Infrastructure (EuroQCI). The Luxembourgish Quantum Communication Infrastructure (LuxQCI) is Luxembourg's contribution to the EuroQCI and it will consist of a terrestrial and a space segment.

The LuxQCI programme development involves several phases. In the first phase, the concept of the network and system at the national level providing a QKD service throughout Luxemburg are being further defined and detailed following potential user and stakeholder needs and views. In the second phase, the first terrestrial testbed will be put in place by linking several locations within the country. In the subsequent phase 3 the testbed implementation is planned to be validated, the concept demonstrated, and the network interfaced with the other neighbouring QCIs. The LuxQCI phase 4 is intended to integrate the satellite segment into the terrestrial infrastructure and to roll out the service to additional stakeholders worldwide.

The initial deployment of the LuxQCI is planned to be a Quantum Key Distribution Network (QKDN) providing QKD services and enable, inter alia, the creation of Quantum Secured Networks (QSNs) and potentially Quantum Internet Networks (QINs). However, to date QIN enabling technologies such as quantum-repeaters and quantum memories cannot be produced with the technologies available today.

Lux4QCI is part of the LuxQCI phase 2, and it is expected to become the backbone of the future LuxQCI network in Luxembourg.

B.2 SERVICE DEFINITION

There is no service associated with Lux4QCI itself. The outcome of the project will be an experimental infrastructure that will have the potential to be integrated or transformed into a fully functional national QCI network at a later stage. This experimental network will allow the Luxembourgish actors to gain experience in the deployment and operations of such novel infrastructure.

Once Lux4QCI becomes a fully tested infrastructure it will also be used to engage potential customers for the forthcoming LuxQCI—the Luxembourgish contribution to EuroQCI—and to address their specific use cases.

The initial service for LuxQCI will be **the distribution of cryptographic keys by using QKD technologies**. The specific usage of these keys is, however, out of the scope of LuxQCI and reserved to the potential users, who can freely use them for their own applications—for instance, to securely transmit or store data. A user subscribing to the service will be able to make use of dedicated equipment installed at their premises—the User End Point (UEP). The equipment provides the user with access to the service through a standardized Key

Co-funded by the European Union

Management System (KMS) interface for obtaining the cryptographic keys in a highly secure way for their own applications.

The system will be designed to distribute pairs of cryptographic keys between distant UEPs which belong to the same entity (e.g. different buildings of a ministry) or to different organisations but also subscribed to the service. Based on the terms and conditions specified in a Service Level Agreement (SLA), the keys will be delivered upon user request. Different quality parameters might be specified in the key request by the user—for instance, the key length, epsilon security value, use/avoidance of trusted nodes, etc.

The Lux4QCI system should, nevertheless, implement the following features for better interaction of the user with the system:

- Implementation of Service Requests
    - Possibility for the User to specify a type of service as per consuming application
    - Possibility to change the amount of keys per delivery period

B.3 STAKEHOLDERS IN LUXEMBOURG

Types of Stakeholders

A set of stakeholders has been identified in Luxembourg. These organisations and entities may have different types of relationships and interests with the national QCI.

- **Operator**: The legal organisations that will operate the LuxQCI system and will grant access to the service to its subscribers (LuxQCI Customers). This organisation will ensure the well-functioning of the infrastructure providing services to customers and users, by managing operations, handling technical aspects, and addressing any issues or concerns that may arise during the system's use.

- **Provider**: Industries and/or institutions that supply services or resources to LuxQCI. They can be suppliers, manufacturers, contractors, or service providers that provide, for instance, networking equipment such as dark fibres, QKD devices, or software solutions for network management or security.

- **Contributor**: Contributors are stakeholders who actively participate in the development of the LuxQCI system. This includes, for instance, the members of the present Lux4QCI consortium.

- **Customer**: Customers are the institutions and industries that are willing to engage in a financial transaction to benefit from the LuxQCI service for their final users.

- **User**: Industries or/and institutions who will benefit directly from the LuxQCI service. They are the primary beneficiaries and consumers of the QKD-generated keys provided by the QCI in order to fulfil their needs and objectives in terms of security. Their needs should be taken into consideration in the development of this project in order to provide accurate solutions and user-friendly tools.

Co-funded by the European Union

Industries and Sectors

The main industries and sectors identified in Luxembourg who could benefit from the Lux4QCI and LuxQCI services are:

- **Military and Defence**
  - The protection of sensitive information would have to be secured with appropriate measures without the risk of the communication being intercepted or hacked.
- **Governmental**
  - The governmental entities need secure communication channels to exchange sensitive information with other entities and protect it from unauthorized access and tampering, in order to uphold privacy and security standards. Besides, these governmental entities need to store personal data, confidential legal documents, contracts, and other sensitive information for extended amount of time.
- **Financial and banking**
  - These institutions require high security data transport that secure communication networks to ensure the confidentiality and integrity of financial transactions and financial records. There is also a need to store large amounts of sensitive data, such as financial records, transaction history, and customer information.
- **Healthcare**
  - Secure communication networks are paramount to protect patient information and maintain the confidentiality of communication among healthcare providers. In addition, ensuring the secure storage of healthcare data is of utmost importance for healthcare institutions. This includes sensitive information such as patient personal data, which often needs to be retained for extended periods. Preserving the confidentiality and integrity of medical findings is also essential to protect intellectual property.
- **IT & Telecom**
  - IT industry needs to ensure reliable and secure communication networks that protect the sensitive information, and to ensure the confidentiality of communication channels. Solutions to keep data secure while in motion across telecoms networks are also needed. Network providers need to enhance the security of their Control and Management layer in order to protect their networks.
- **Transport**
  - Transport entities need to enhance data transport solutions and to ensure the integrity and confidentiality of transportation data operations. Besides, this

sector requires robust security techniques to safeguard the large volumes of sensitive data such as passenger information, transaction records, transportation plans and regulatory documentation.

- **Energy**
    - This sector needs reliable and secure communication networks for real-time monitoring, control, and management of energy systems. In addition, it is crucial to protect sensitive data such as energy consumption records, grid operations information and customer data, in order to ensure the privacy of individuals and organizations.

B.4 NATIONAL USE CASES

Use Cases

Following the industry and sector analysis and the feedback obtained from different stakeholders, the general use cases, as representatives of the most common applications, are:

- High-security data transport—along with key management of the QKD keys involved in the transport protocols.

- Long-term secure storage—for instance, in cloud-based datacentres.

Scenarios

The Lux4QCI will focus on the following two scenarios:

- **Integration of QKD-Keys in VPNs**
    - Use Case: High-security data transport
    - Lux4QCI will aim to enhance VPN security by replacing the key exchange mechanism of a VPN implementation with QKD-generated keys.
    - The user obtains a QKD-generated keys suitable to be used with encryption schemes that provide high-security (e.g., ITS) to data in transport

- **Preloading QKD keys into HSMs**
    - Use Case: Long-term secure storage
    - The QCI supports the exchange of QKD-generated keys for secure storage of data over extended periods, ensuring its integrity and confidentiality.
    - The data stored in an HSM preloaded with QKD keys is encrypted using a symmetric scheme (e.g. AES) where the key is taken from the set of preloaded QKD-generated keys.

Co-funded by the European Union

B.5 CONCLUSIONS

Lux4QCI will offer a comprehensive solution to the key distribution problem through the implementation, procurement and deployment of the Quantum Communication Infrastructure using Quantum Key Distribution technology. This infrastructure is envisaged to address the security needs of organizations across various industries and sizes.

Lux4QCI aims to serve a wide range of user categories, including military and defence, governmental entities, healthcare, financial institutions, as well as communication, IT, energy, and transport industries. These sectors can benefit from the enhanced security solutions provided by Lux4QCI to protect their sensitive information and communications.

It is important to note that Lux4QCI will not provide standalone security services. Instead, it offers secure secret keys through QKD technology, which can be utilized by subsequent cryptographic applications. The security properties, context, and scenarios of use may vary depending on the specific cryptographic applications employed.

The Lux4QCI is being developed to cater to two primary use cases. Firstly, it will ensure high-security data transport by securely transmitting keys, effectively safeguarding against potential threats during the key distribution process. The two specific scenarios of integrating QKD keys along with VPN and with IPSec are identified as the first applications showcasing this use case. Secondly, the QCI will enable long-term data storage, guaranteeing the integrity and confidentiality of stored data over extended periods. The specific scenario of preloading QKD keys into HSMs is identified as a first application showcasing this use case.

As a result, Lux4QCI implementation and deployment will be a significant advancement in the field of secure communications and key distribution for Europe—and for Luxembourg in particular. It will play a crucial role in enhancing data protection and contributing to the secure digital transformation of organizations, by providing robust security solutions and addressing the needs of diverse industries.

Co-funded by the European Union