EuroQCI

Digital Europe Programme Project ***QCI-CAT***
QCI: Proof of Concept – Secure Connectivity Austria
Digital Europe Work Program 2021-2022
EU Secure Quantum Communication Infrastructure (DIGITAL-2021-QCI-01)
Project number: 101091642

Project starting date: fixed date: 1 January 2023
Project end date: 30 June 2025
Project duration: 30 months

Document:	**Deliverable**
Type:	Report
Dissemination Level:	Public
Title:	**Dissemination, communication and exploitation plan**
Work-Package	WP10
Document number:	**D10.2**
Document Owner:	AIT / Hannes Hübel
Contributors:	All Partners
Abstract:	This deliverable provides the dissemination, communication, and exploitation plans of the QCI-CAT consortium as a whole and the plans of the individual partners their foreground knowledge obtained throughout the project.
Key words:	Communication plan, dissemination plan, exploitation plan
Pages	27
Delivery Date Planned	2023-03-31 (M3)

Revision History

Version	Revision Points	Author(s) & Organization	Date
V 1.0	Initial version	M. Kos (AIT)	2023-02-20
V 1.1	Target groups, standardization activities, software exploitation, collaboration with related research activities, scientific publications, public webpage	S. Ramacher, S. Krenn (AIT)	2023-03-10
V 1.2	Social Media, SBA SPOCs, Acronyms	K. Osman (AIT)	2023-03-10
V 1.3	Social Media	K. Osman (AIT)	2023-03-13
V 1.4	National EuroQCI Workshop	S. Ramacher (AIT)	2023-03-15
V 1.5	Social Media	K. Osman (AIT)	2023-03-24
V 1.6	qtlabs Input	J. Pseiner (qtlabs)	2023-03-24
V 1.7	UIBK input	B. Lanyon (UIBK)	2023-03-27
V 1.8	SBA input	S. Raubitzek (SBA)	2023-03-27
V 1.9	TU Graz input	C. Rechberger (TU Graz)	2023-03-27
V 1.10	MUG input	S. Leiner, K. Zaloukal (MUG)	2023-03-28
V 1.11	Small layout changes to figures and tables, new picture for deliverable figure, text for target audience	K. Osman (AIT)	2023-03-29
V 1.12	DAC input	C. Cehovin (AIT)	2023-03-29
V 1.13	X-net input	K. Kloiber (X-net)	2023-03-29
V 1.14	Finalization of deliverable	S. Ramacher, C. Striecks, S. Krenn (AIT)	2023-03-30

Author List

Organization	Name	E-Mail address
AIT	M. Kos	Manuela.kos@ait.ac.at
AIT	S. Ramacher	sebastian.ramacher@ait.ac.at
AIT	K. Osman	karim.osman@ait.ac.at
AIT	S. Krenn	stephan.krenn@ait.ac.at
AIT	C. Striecks	christoph.striecks@ait.ac.at
KBC	T. Huemer	tobias.huemer@k-business.com
qtlabs	J. Pseiner	johannes.pseiner@qtlabs.at
SBA	S. Raubitzek	sraubitzek2@sba-research.org
UIBK	B. Lanyon	ben.lanyon@uibk.ac.at
TU Graz	C. Rechberger	christian.rechberger@tugraz.at
MUG	S. Leiner	stefan.leiner@medunigraz.at
MUG	K. Zatloukal	kurt.zatloukal@medunigraz.at
DAC	C. Cehovin	christian.cehovin@dacoso.com
X-net	K. Kloiber	kk@x-net.at

Reviewer List

Organization	Name	E-Mail address
ALL	QCI-CAT Consortium	-

Copyright Statement

Funding Acknowledgment:

This project has received funding from the European Union's Digital Europe Work Programme 2021-2022 under Project number: 101091642.

Table of content

List of Figures

List of Tables

Executive Summary

This report describes the initial plan and strategy for the dissemination and exploitation of the foreground knowledge as obtained from the QCI-CAT project. On the one hand, it presents a general plan focused on communication, communication channels and target audiences that the consortium expects to reach with its activities. The general plan is supplemented with partner specific plans that the industry and academic partners follow to maximize the impact of their results. The plan also outlines the collaboration with other research initiatives and specifically PETRUS as coordination and support action as well as other DEP 1 and DEP 2 projects building QKD components and deploying national networks. Furthermore, individual exploitation plans are provided by the partners. These plans are based on the partner's involvement in the various use-cases and their components that are demonstrated in these use-cases.

1. Introduction

1.1. Purpose and scope of the document

This deliverable introduces the plan of the individual members of the QCI-CAT consortium and for the project overall to approach the dissemination, communication, and exploitation activities throughout the project. Additionally, the document also outlines the cooperation with the coordination and support action PETRUS and the DEP 1 projects QUARTER and eCausis. Finally, the document also provides a plan for a national EuroQCI workshop for stakeholders with speakers from QCI-CAT and other projects involved in the EuroQCI initiative.

1.2. Target Audience

This document is targeted at the general public.

1.3. Relation to other project work

This deliverable is closely related to D10.1 QCI-CAT webpage which describes the public project webpage. The outcome of workshop planned within this document will be reported in D10.3 National EuroQCI workshop. The results of the other communication, dissemination, and exploitation activities will be reported in the deliverables D10.4 Report on communication, dissemination, enduser workshops, and exploitation activities and D10.5 Report on participation to the EuroQCI initiative and the collaboration with other DIGITAL projects.

1.4. Structure of the document

This document starts with the discussion of the general dissemination and communication strategy. This overall strategy is accompanied with the strategies of the individual partners from academia and industry. Secondly, each partner also provides an initial plan for the exploitation of their QCI-CAT results.

Finally, the document describes the planned interaction with the coordination and support action PETRUS and the organization of a workshop dedicated to the deployment of EuroQCI in Vienna, Austria.

2. Plan for dissemination and communication

2.1. General Strategy and Target Audiences

Dissemination of the project results and communication related to quantum and related technologies in general are key activity areas of the QCI-CAT project. To maximize the effect of these activities and to promote engagement with quantum technologies and the QCI-CAT results specifically, it is paramount to develop a dissemination and communication strategy that identifies the various target audiences, the communication channels to reach the identified target audiences, and finally to produce content that is appropriate for both target audiences and the chosen communication channels.

The first step is to identify the target audiences. With respect to QCI-CAT we aim to interact with a wide variety of different audiences due various tasks planned during the project. Specifically, the following target audiences have been identified:

- The target audience of the results obtained via the research focused tasks is the **scientific and research community**.
- **Academic institutions** are training future computer scientists, physicists, network engineers, and many more working in related areas and hence offer good opportunities to raise interest into quantum-safe technologies in students.
- To bring quantum-safe technologies into practice, **SMEs and large industries** are required beyond the development of the technologies itself. The technologies need to be integrated into networks, small to large-scale applications, and more. Furthermore, companies will also need to be aware of risk management strategies, the necessary maintenance as well as monitoring tasks for successfully operating quantum-safe technology.
- **Authorities and policy makers** play a major role in the deployment of EuroQCI. Authorities such as the Austrian ministries are early-adoptors of quantum-safe technology and are heavily involved in the use-cases of the project. Also, regulation presents a barrier to the deployment of quantum-safe technologies and QKD specifically in certain environments including governmental networks or the financial sector. Therefore, reaching policy makers with our communication strategy is essential to establish the regulatory requirements for deployment in these environments in the future.
- The **general public** may not be aware of the need of quantum-safe technologies and as such awareness regarding its importance for secure communications needs to be raised.
- **Standardization bodies** define interfaces and protocols for the individual components of a QKD network (QKDN) to interact and as such are important to establish interoperability of an EU-wide QKD network.

The identified audiences can be reached via various communication channels. For the scientific community, the main communication media are of course publications in journals and conference proceedings and talks at conferences and workshops. Beyond scientific publications, workshops co-organized by different research projects provide the academic partners with the opportunity to discuss, share, and develop new ideas in the intersection of these projects. Hence workshops — either co-located at larger conferences or organized as a separate event — foster the scientific advance of quantum-safe technologies. Furthermore, with respect to the cryptographic and security communities, discussions of various topics and publications is also happening in online communities and social media such as Twitter or federated Mastodon instances.

The primary channel to reach students at academic institutions are of course lectures, and other forms of classes. With lectures one can provide deep understanding of certain areas of quantum-safe for physics or computer science students during their Master studies. For a broader range of students, a

class touching on quantum-safe technologies on a higher level can be also be taught on a Bachelor level for students of physics, computer science, electrical engineering, or mathematics (among others). For those students that caught interests via the lectures on quantum-safe technologies, Master or Bachelor thesis could be conducted in cooperation with the partners of the QCI-CAT consortium for further specialization into this domain. As many students are also very active online, the use of social media channels also provides an interesting opportunity to interact with interested students.

As SMEs and large industries are often present at more or less specialized industry fairs, booths at such fairs can provide the perfect opportunity to demonstrate the readiness of quantum-safe technologies to companies that could integrate them into their services, software or hardware offerings. Hence, such fairs provide a great opportunity for the industry partners of QCI-CAT to present their advancements with respect to quantum-safe solutions that is ready for deployment. Another option to raise awareness of quantum-safe technologies are customer contacts of participating industry partners to make them aware of QKD and quantum-safe solutions. White papers on the technology may also help to highlight the capabilities of the technologies for companies working in related areas.

Furthermore, for employees of SMEs and large industries having an interest in exploring, working with, or deploying quantum-safe technologies, online course material will provide them with the necessary background knowledge. With a curriculum that covers both basics about quantum key distribution, post-quantum cryptography, QKD networks, and their integration into systems and more detailed topics, it provides professional training opportunities for these employees.

Also, for authorities and policy makers, the aforementioned white papers together with training material can also be used to build the necessary understanding for developing regulations on the use of quantum-safe technologies in restricted domains. Policy briefs that discuss various options for the deployment of the Austrian network as part of the EuroQCI initiative will serve as a vehicle for providing advice required in informed decision-making processes.

Citizens and the general public may be reached by a multitude of different communication channels. To maximize the reach in the general public, all of these channels need to be used in conjunction. These channels include a project website with an introduction to quantum-safe technologies, posts on social media sites to reach different age groups, press releases and non-technical publications, and many more.

Due to the wide area of (technical) topics covered by QCI-CAT, many different standardization bodies and organizations are responsible for defining and maintaining standards in quantum-safe and networking technologies. Standardization efforts can be steered by active participation in the corresponding working groups and standardization meetings.

For this initial dissemination plan, we summarize the identified target groups and the corresponding dissemination and communication plans in **Fehler! Verweisquelle konnte nicht gefunden werden.**. In the following sections, we also discuss the identified channels and how they can be used for communication with the target audiences in more detail.

Target group	Dissemination and exploitation goals	Channels
Research community	• Effectively disseminate project results to enable other researchers to efficiently built on QCI-CAT‘s results • Track scientific progress and establish collaborations to improve the quality of the project‘s results • Co-locate workshops and seminars with major conferences as a discussion forum for ideas, challenges, and results • Liaise with related initiatives and projects on a national and European level to use synergies, to ensure interoperability, and to avoid the duplication of work	• Scientific publications • Personal networks • Conference presentation and invited talks
Academic institutions	• Encourage and organize dedicated courses and lectures on quantum-safe technologies to train future generations of researchers and engineers • Train students at different levels (BSc, MSc, PhD)	• Lecture series and invited lectures
SMEs and large industries	• Gathering experience to being able to provide be customized, high-quality and highly available quantum security solutions for all company sizes • Form new strategic partnerships to develop cross-company synergies regarding quantum security solutions • Gather information about end-user requirements in terms of quantum security	• Publications • Conference presentation and invited talks • Trade fairs participation
Authorities and policy makers	• Ensure alignment of QCI-CAT with national and European strategies • Raise the awareness of benefits of QCI-CAT’s results by politicians and decision makers • Encourage government entities to actively participate in QCI-CAT and prepare for quantum computer threats • Support MoD’s activities to build up stronger resilience against hybrid warfare threats	• Policy briefs (targeted and limited audience) • White papers (targeted and limited audience)
Citizens	• Raise awareness of the need for quantum-safe technologies and explain how QCI-CAT contributes to providing them	• Non-technical publications • Website and social media
Standardizatio n bodies	• Improve quality of standards in the domain of QCI-CAT‘s research • Influence standards to facilitate the widespread adoption of QCI-CAT‘s approaches, concepts, and technologies • Engage in standardization bodies to ensure compatibility of QCI-CAT‘s architectures and concepts with existing standards in the domain	• Direct participation in SDOs

Table 1 - Summary of the target groups, dissemination and exploitation goals, and communication channels

2.1.1. Project logo

AIT contracted an external design consultancy firm to design the logo of QCI-CAT. The logo in Figure 1 depicts the official project logo. A variant of the logo for dark backgrounds is provided in the internal project document repository.

Figure 1 – The official project logo. The I in QCI-CAT is stylized to include the outline of a key to symbolize the output of a QKDN. The logo also includes a cat as a reference to the project name and the thought experiment of Schrödinger's cat.

2.1.2. Project document templates

AIT designed and prepared the official project templates for deliverables, review forms, and presentations. All templates are available to the members of the consortium via the internal document repository (cf. Section 2.1.3). Figure 2 and Figure 3depict these templates.

EuroQCI

Digital Europe Programme Project **QCI-CAT**
QCI: Proof of Concept – Secure Connectivity Austria
Digital Europe Work Programme 2021-2022
EU Secure Quantum Communication Infrastructure (DIGITAL-2021-QCI-01)
Project number: 101091642

Project starting date: fixed date: 1 January 2023
Project end date: 30 June 2025
Project duration: 30 months

Document:	**Deliverable / Agenda / Meeting Minutes / …**
Type:	Report / Demonstration /
Dissemination Level:	Public / Sensitive / EU-Classified
Title:	**Title according to GA**
Work-Package	WP1-WP10
Document number:	**Del. Number According to GA**
Document Owner:	Institution / Name of the Person
Contributors:	Partners
Abstract:	1-2 Sentences
Key words:	2-5 Key Words
Pages	1
Delivery Date Planned	YYYY-MM-DD (M3-30)

Figure 2 - First page of the official template for deliverables.

Figure 3 - Title slide of the official project template for presentations.

2.1.3. Online document repository

As coordinator, AIT prepared an online document repository for collaboration between the consortium members. The document repository serves as storage for all project results and provides access to various project management resources. It also offers an online document editing functionality for efficiently preparing deliverables.

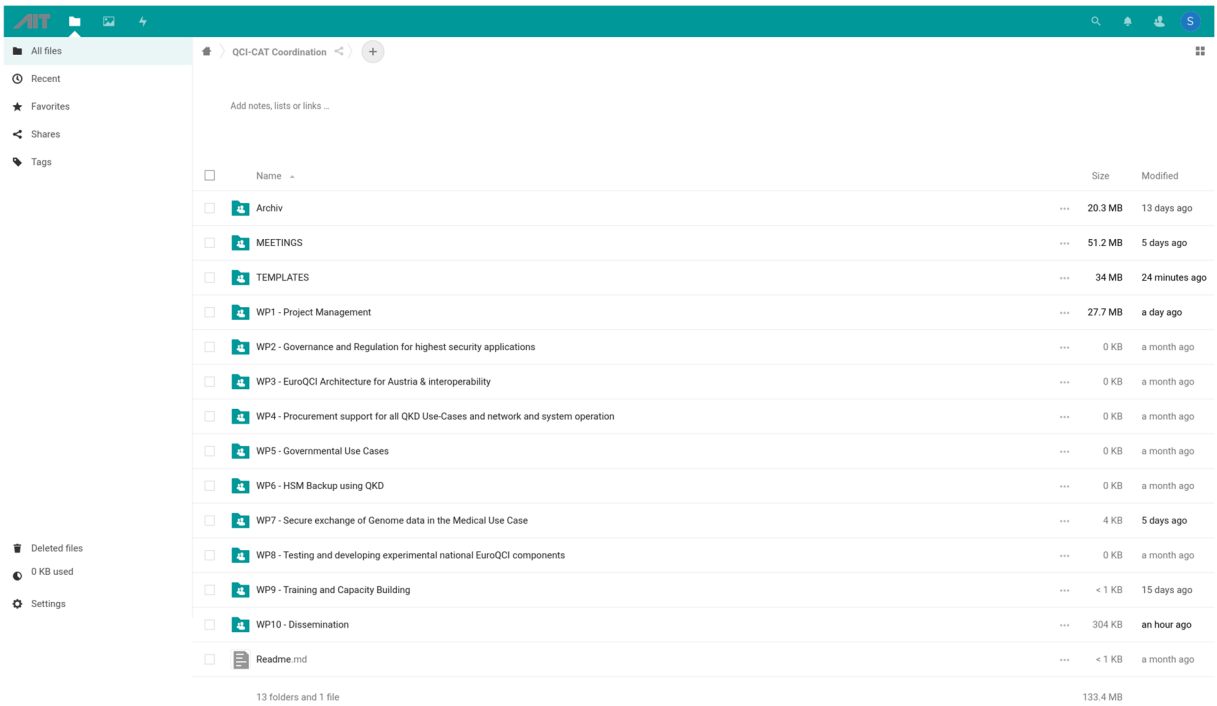

Figure 4 - Landing page of the online document repository hosted by AIT.

2.1.4. Public webpage

The public webpage is available via https://qci-cat.eu, https://qci-cat.at, and https://qci.at. The webpage will be used to highlight the results, events organized by the consortium and related material to make them widely available to the general public. As such, it will serve links to all public deliverables and scientific publications. For a complete description of the webpage, we refer to the deliverable D10.1 which is dedicated to the webpage and gives a complete overview.

2.1.5. Social media

Social media has become an important tool for the dissemination and communication of national and international research and innovation projects due to its wide reach, ease of use, and accessibility. Specifically, the diverse range of participants reachable via a variety of social media channels helps QCI-CAT to engage with experts and the wider research community. Social media can also serve as a tool to promote the curriculum to students during their studies and as lifelong learning opportunity to computer scientists, software engineers, electrical engineers, and others that are working in related fields.

Hence the consortium is committed to use social medial channels to reach specific audiences to promote QCI-CAT and its results, EuroQCI activities, and quantum technologies in general.

On LinkedIn, the consortium will connect with representatives of the European quantum technology industry and members of all DEP 1 and DEP 2 projects. The communication channel will be used to highlight the major technological achievements and to announce national and international workshops on EuroQCI that are of particular interest to industry partners and users from various application domains.

Twitter will be used to promote events organized or attended by members of the consortium whereas the focus is on scientific events. Thereby the consortium will be able to reach the broader scientific community and experts that are represented on Twitter. Furthermore, scientific publications will also be announced via this channel to widen their visibility among researchers.

Finally, on Instagram, the consortium plans to upload pictures made at various events, the project logo as well as short videos (reels) with short statements on different quantum technologies, which will sometimes include a link to our QCI-CAT curricula for engineers, technicians and management in order to promote the online courses. With over 30% of users belonging to the age group of 18-24 years and another 30% belonging to the group of 25-34-year-olds,[1] it is expected to reach students as well as prospective junior employees with the curricula and thereby raising their awareness and interest into quantum technologies.

2.1.6. Leaflets, Poster, newsletters and other dissemination materials

The consortium plans to prepare leaflets and posters for meetings, workshops, scientific conferences, and industry and trade fairs. Hence, official leaflets and posters will be designed and kept up-to-date with new results during the project lifetime. The consortium is also committed to preparing a periodic newsletter (e.g., every three months) discussing quantum technologies and project results. The project website will offer a registration form for the newsletter and it will also contain an archive of all newsletters. Furthermore, a project roll-up will be prepared by AIT that can be borrowed by members of the consortium for booths at conferences and fairs.

[1] https://www.statista.com/statistics/325587/instagram-global-age-group/ (03/22/2023)

2.1.7. Collaboration with related research activities

The QCI-CAT consortium will seek collaboration with national and international research activities working in related areas to foster scientific collaboration and use synergies to avoid duplicated work. The partners of the QCI-CAT consortium are involved in the following research activities that are of relevance for QCI-CAT:

- HARMONIC (SESAR 3 JU) completes key developments of the Demand and Capacity Balancing (DCB) operational concept in air traffic management to make the implementation of the operational concept more efficient. Among others, it leverages privacy preserving data spaces via potentially information theoretically secure multiparty computation (MPC) to foster collaboration between all stakeholders in real-time.
- DISCRETION (EDIDP) integrates and combines Software Defined Network (SDN) and Quantum Key Distribution (QKD) technologies on top of legacy optical networks to build a highly secure, scalable, and resilient network control architecture for advanced military tactical operation services.
- QSNP (HEU), Qu-Test (HEU), Qu-Pilot (HEU) are projects within the Quantum flagship programme and aim at supporting open testing and experimentation for quantum technologies in Europe. Among others, work items focus on quantum communication and quantum computing, the supply chain of quantum hardware, and the support of the European quantum industry.
- QIA (Quantum Internet Alliance, EU, Horizon Europe) is a project within the Quantum Flagship program whose mission is to build a global Quantum Internet made in Europe – by developing a full-stack prototype network validating all key sub-systems and by driving an innovative European Quantum Internet ecosystem capable of scaling all sub-systems to world-leading European technology.
- QKD4Gov (FFG KIRAS) establishes a secure communication network between public authorities in Austria to investigate novel encryption schemes based on quantum key distribution (QKD) and post-quantum cryptography (PQC).

The collaboration with EuroQCI activities is discussed in Section 4.

2.2. Dissemination plans per partner

Since the QCI-CAT consortium includes companies from different areas of the industry, universities, and RTOs, their individual dissemination plans vary. The following sections give an overview of planned communication and dissemination activities beyond the already outlined strategy.

2.2.1. Dissemination AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH

Together with their national and international partners, AIT plans to generate high visibility of project results within the scientific and non-scientific community:

- Scientific publications in conferences and journals, and participation in workshops and conferences, will be the key instrument to reach the scientific community. Related to quantum-technologies, the team will aim for venues like the Journal of Physics, Applied Optics, Optics Express, Journal of light wave technologies, and Physical Review X. In the domain of PQ-cryptography, the AIT team will aim for highly visible venues, including, e.g., top-tier conferences like ACM CCS, the USENIX Security Symposium, ESORICS, or all conferences organized by the International Association of Cryptologic Research (IACR).
- In collaboration with university partners, AIT envisions to supervise theses, especially on a BSc and MSc level, within the context of the project. Also, teaching activities – either as dedicated

lectures or as invited lectures in existing courses – are planned to educate students in the domains relevant for QCI-CAT.

- As a forum for discussion of novel ideas or results, academic workshops with open calls for papers will be organized in close collaboration with our liaison projects.
- To also reach a broader audience, AIT will additionally aim for non-scientific technical publications such as the ERCIM newsletter

The standardization of QKD and PQC related technologies is pursued by international standardization organizations. AIT will continuously monitor the results of QCI-CAT and their suitability for standardization, and it will also monitor the ongoing standardization activities in relevant working groups. Thereby, the highest level of compatibility of QCI-CAT components can be ensured. Among the standardization organizations, the following list has been identified as relevant for QCI-CAT:

- The European Telecommunications Standards Institute (ETSI) has members from more than 60 countries promoting a greater harmonization of (European) telecommunication systems. The Industry Specification Group (ISG) on QKD is working and standardizing interfaces between the individual components of QKD network. The Technical Committee (TC) Cybersecurity (CYBER) is — among other areas of interest — working on post-quantum secure cryptography.
- The International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) is covering numerous fields within telecommunication and information technology. Study Group 12 - Future Networks (Q16/13 and Q6/13), Study Group 17 – Security (Q15/17), and Focus Group on Quantum information technology for networks (FG-QIT4N) publish recommendations and standards on QKD networks.
- The National Institute of Standards and Technology (NIST) is a physical sciences laboratory federal agency of the United States of America promoting innovation, measurement science, and standards. NIST is well known for running international competitions for the selection of symmetric and asymmetric cryptographic schemes. NIST is currently running the Post-Quantum Project to select post-quantum secure digital signatures, public-key encryption schemes and key encapsulation mechanisms for standardization.
- The Internet Engineering Task Force (IETF) is an open standards organization, developing and promoting voluntary and open Internet standards named Request for Comments (RFC). Widely used protocols such as Transport Layer Security (TLS) and the integration of current and future cryptographic schemes are specified as part of IETF activities.
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), as part of their joint subcommittee on Information security, cybersecurity and privacy protection (JTC1/SC27) recently launched an internal study period for the standardization of post-quantum cryptographic primitives within WG2. Furthermore, WG3 has developed standards on requirements for, and the evaluation of, QKD devices.

2.2.2. Dissemination FRAGMENTIX STORAGE SOLUTIONS GMBH

fragmentiX will prepare various versions of reports about the use of fragmentiX secret sharing together with QKD for a) sensitive medical data like full human genome data sequencing and b) the use within at least 5 federal ministries of the Austrian Government.

fragmentiX will in addition also provide a very generic non detailed explanation and description of the „trusted nodes“ developed and built at prototype level. These documents will only be shared with the desired group of potential users of such trusted nodes within the EU27 countries and at a later stage with NATO countries.

Due to the very sensitive functionality of a „trusted node“ per-se it is not intended to share technical details, concepts or any other potentially sensitive details of the development outside the responsible

government domain. The „Need to Know“ principle will be honored to its full extent even within government entities.

2.2.3. Dissemination UNIVERSITAET INNSBRUCK

As a fundamental research institution, we will disseminate our QCI-CAT project outcomes by publishing in scientific research journals. This is our core approach to disseminating research results to other scientists around the world. We always aim for broad-scope physics, or even all science, journals to ensure the biggest reach across scientists. We will ask our University press office to create a press release for each major scientific publication.

We will ensure that our QCI-CAT results are communicated to other related national and European projects in which we are involved. Specifically, we will report QCI-CAT results to our partners in the European flagship project `Quantum Internet Alliance'. We will also disseminate our results and communicate our project goals and context, to our partners at `ACOnet': an Austrian wide optical fiber network that connects Austrian Universities.

We will also attend at least two international research conferences per year in which scientists working in the field of quantum communication are in attendance. At those conferences we will either present our QCI-CAT results, when they are available, or present the project in some capacity.

2.2.4. Dissemination QUANTUM TECHNOLOGY LABORATORIES GMBH

The dissemination and communication plan of qtlabs can be topically divided into three parts: First, the academic aspect to educate stakeholders and citizens, second, the consulting aspect prepares national and international partners to develop a quantum-safe cybersecurity strategy plan and third, shaping and driving standardization developments of QKD and PQC related technologies. These three areas entail the following activities:

1. Educate and train stakeholders and engineers around the future vulnerabilities of their IT infrastructure. Here, qtlabs is offering introductory and expert level online courses as well as B2B consulting. This helps to build up knowledge of quantum-safe cybersecurity within the core security team and raises awareness in a broader community of decision makers in the relevant business areas. Moreover, together with University of Vienna and Vienna University of Technology, qtlabs plans to supervise and educate Master and PhD students, to train future quantum engineers.
2. An all-encompassing cybersecurity strategy will not stand on a single pillar, but its core strength will be to include several ankers ranging from technology, education, awareness, privacy, and policy strategies. In the context of the space segment of Euro-QCI, qtlabs ensures visibility for technological readiness and quality assurance for both national and international partners, using the respective findings and results obtained in QCI-CAT. Finally, due to experiences in relevant EU projects, qtlabs is in the excellent position of shaping and preparing the relevant stakeholders for the EU-wide legislation on the NIS2 cybersecurity.
3. Standards facilitate the integration of equipment from various vendors, enabling Quantum Key Distribution products to seamlessly integrate into existing infrastructure. They encourage the establishment of a supply chain by outlining interfaces and specifications for components and modules within equipment or distributed systems. To aid these developments, qtlabs will work together with the pertinent task groups of QCI-CAT carrying out standardization endeavors.

Additionally, qtlabs will strive to increase its visibility within the relevant community by participating in prominent events such as QCrypt, Space Expo, and CLEO - top-tier conferences that provide excellent exposure.

2.2.5. Dissemination X-NET SERVICES GMBH

X-Net will present publicly available information about the project as well as project results at the it-sa Expo&Congress in Nuremberg. The it-sa takes place once a year and X-Net will use the platform there to disseminate project results and show the progress in QCI-CAT and post-quantum cryptography. The next it-sa takes place from 10th – 12th of October 2023.

Further on, X-Net is demonstrating secure video links between various ministries. It is planned to publish evaluation results and testbed descriptions in form of reports and summaries. It is secured that sensitive information will not be contained, all dissemination and publication activities will only use anonymized and approved information.

2.2.6. Dissemination DACOSO GMBH

dacoso will gain experience for the framework of QKD network use cases (mainly installation support services for the testing of the fibre links, installation services for network devices including provisioning and monitoring, including training of users for operation), which can be used to consult customers and partners to build new critical infrastructure based on QKD and link encrytors, complementing the usage of new knowledge from other dacoso R&D projects in Germany (AI-NET-Protect, SEQRET, ISQQKMS).

Furthermore, dacoso can use the knowledge, gained in the QCI-CAT Project, for presentations at various events and trade fares (e.g., security conferences like it-sa Nurnberg) as well as in customer and partner workshops.

2.2.7. Dissemination MEDIZINISCHE UNIVERSITAT GRAZ

The Medical University (MedUni) Graz will provide and manage the end-node of the long-distance link formed between Graz and Vienna. Furthermore, MedUni Graz will provide a use case and push ethical constraints by utilizing genomic data, which by its nature is highly sensitive as well as personal identifiable data. This will require the approval by the research ethics committees of the Medical Universities in Graz and Vienna, a process which will be supported by years of previous experience. Furthermore, a major administrative challenge is to implement the QCI-CAT technical solution in compliance with the hospital and university IT requirements. The experience gained in this task will serve as blueprint for wide implementation of advanced cybersecurity solutions in universities and hospitals and will be described in scientific publications and presented at international conferences.

2.2.8. Dissemination SBA RESEARCH GEMEINNUTZIGE GMBH

SBA Research gemeinnützige GmbH (SBA) will provide the link between the security experts of the involved partners, the involved ministries, and medical institutions by organizing a series of workshops and a detailed gap, risk, and threat analysis. This will result in three reports. The first of these reports will contain the results of a security and gap analysis, thus complementing and describing the governance of the proposed government architectures and the medical use case. The second report will describe a proposed communication infrastructure for the Austrian Ministry of Defense. The third report contains the gap analysis and roadmap to align with the active security baseline fully. Further, this final report will list all changes to the proposed architecture and a section on the interaction between the NSA and NCSA, thus describing their guidance during this process.

The workshop series organized by SBA will consist of two main blocks: The first one, consisting of 4 workshops, dealing with the context establishment, risk identification, risk analysis, and risk evaluation for the proposed architecture, and the second one, consisting of 2 workshops, conducting a national gap analysis, including experts from the Austrian Security Ministries.

The workshops and the corresponding reports will provide information and a roadmap for implementing a QKD-secured communication infrastructure. Due to the sensitivity of the processed and gathered data, and their respective owner, detailed information about the

proposed/implemented architecture cannot be communicated publicly. Thus, only generic information and ideas already known to the scientific community will be communicated and discussed openly.

2.2.9. Dissemination K-BUSINESSCOM AG

K-BusinessCom AG will create a strategy paper comparing the differences between the various approaches to key-wrapping. Furthermore, KBC will describe the experience with this use-case and compare the collected data with the pre-defined KPIs for the Use-Case. The knowledge, gained in the QCI-CAT Project, will be used to highlight the advantages of the refinement of lines via Quantum key distribution and Hardware Security Modules (HSM), in conferences and client proposals, as well as panel discussions and workshops.

2.2.10. Dissemination TECHNISCHE UNIVERSITAET GRAZ

TU Graz aims to disseminate research results at top venues, including, e.g., top-tier conferences like ACM CCS, the USENIX Security Symposium, ESORICS, or all conferences organized by the International Association for Cryptologic Research (IACR).

TUG envisions to supervise thesis, especially on a BSc and MSc level, within the context of the project. Also, teaching activities together with AIT – either as dedicated lectures or as invited lectures in existing courses – are planned to educate students.

3. Plan for exploitation of foreground

3.1. General strategy

3.1.1. Exploitation AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH

AIT will develop various software prototypes as part of QCI-CAT that are directly related to AIT's Key Management System (KMS) for QKD networks. Depending on the maturity and the evaluation results, AIT will investigate the integration of the prototypes into its KMS. To make these newly integrated functionalities available to the wider EuroQCI and European quantum technologies community, licensing options will be explored at later stages of the project.

The strategy for software that is not directly connect to the KMS and the QKD software stack that is developed to support research papers and scientific results is different. For this type of software results, AIT will aim at publishing the source code with an open-source license to provide the results to a large audience.

3.1.2. Exploitation FRAGMENTIX STORAGE SOLUTIONS GMBH

fragmentiX will continue to help government and enterprises protect sensitive data against espionage, theft and loss on the highest possible technical and operational level.

Based on the experiences from QKD4GOV and other projects like QSAFE and OPENQKD fragmentiX will improve usability, performance and ease of integration into existing applications and environments.

Due to already established international collaborations within the EU27 countries and like-minded NATO countries fragmentiX is preparing for worldwide sales activities.

The development and first prototype level production of two trusted nodes will be the core of intended future business segment at fragmentiX. The now produced prototypes will be on a high level of protection - qualifying them for future accreditation for EU SECRET and NATO SECRET.

After the successful test of this high-end trusted nodes there will follow models with only a subset of the features that will allow the usage also in existing protected datacenters in Austria, the EU27 and NATO countries. To become a trusted supplier for this kind of highly security sensitive equipment

fragmentiX must keep a very strong tenure of personal and facility security including all the relevant EU and NATO clearances. This can and will be achieved by implementation of strict rules within the company and within the company's engagement in projects like QCI-CAT.

3.1.3. Exploitation UNIVERSITAET INNSBRUCK

The foreground knowledge generated during the QCI-CAT project will be exploited in the follow ways:

One of our particular focuses at UIBK is developing the fundamental building blocks of the next generation of quantum networks, often referred to as the "quantum internet" and capable of much more than quantum key distribution. During the QCI-CAT project knowledge will be generated as new technologies for a quantum internet are taken outside the lab for the first time, integrated into the existing fiber network and deployed in that real-world scenario. We will exploit this knowledge and experience to identify the issues facing realizing a quantum internet across Austria and develop a research strategy towards a fiber-based (ground) quantum internet across Austria for the years beyond the QCI-CAT project.

A second focus at Innsbruck is on developing the fundamental building blocks for satellite-based quantum communication. During QCI-CAT a concept for satellite part of the Austrian EuroQCI network will be developed. We will exploit that knowledge to inform our research strategy to implement satellite-based quantum communication, using our Innsbruck ground station, over the coming years.

3.1.4. Exploitation QUANTUM TECHNOLOGY LABORATORIES GMBH

The findings and results can aid the further development of QKD systems tailored to the QCI infrastructure. Gaining knowledge on classical cryptographic devices such as e.g., KMS and HSM, the development in interfacing crucial systems of the overall QKD implementation can be further undertaken by qtlabs, ultimately increasing performance, and enhancing usability.

3.1.5. Exploitation X-NET SERVICES GMBH

X-Net will demonstrate the use of secure video links and implement at least one testbed in QCI-CAT. Findings and results will be used for further development and investments in security solutions that are ready for post-quantum technologies. Governments and organizations with sensitive data will be supported to build up secure infrastructure using these technologies and to enhance processes.

3.1.6. Exploitation DACOSO GMBH

As an experienced integrator and provider for security operation centers and a provider of encrypted optical connectivity solutions dacoso can use its gained knowledge for QKD networks to promote these use cases to a wider audience in our industry in order to consult, implement and operate QKD based networks.
dacoso will gain knowledge for the security assessment part (including the optical fiber links, QKD, KMS, Link Encryptor, Secret Sharing Appliance and Storage), as well as for governance procedures (i.e., installation) and threat analysis for the proposed government architectures to be used to consult and support follow-up projects in similar QKD use cases.

3.1.7. Exploitation MEDIZINISCHE UNIVERSITAT GRAZ

Our long-term plan is to further build up existing infrastructure with the aim of eventually integrating quantum key distribution systems as well as secret sharing. Thereby we leverage state-of-the-art cryptography schemes into the daily workflow of scientists to improve collaborative research and data sharing.

Based on results obtained within QCI-CAT, a series of industrial products will be developed by fragmentix with features tailored to different user groups. For example, it will be proposed to relevant EU-projects including the European Health Data Space to create secure and trusted data spaces.

Additional future user groups are organizations handling highly sensitive data (e.g., high security laboratories or critical manufacturing infrastructure) but also industry and SMEs, in general.

3.1.8. Exploitation SBA RESEARCH GEMEINNUTZIGE GMBH

The knowledge obtained from proposing and analyzing the quantum-safe architecture will provide documents and guidelines for future applications, e.g., to extend the medical use case or involve further government-related institutions.

Further, the conducted work on proposing, establishing, and finally certifying a quantum-safe infrastructure in Austria will provide a basis for future Austrian-made security solutions and thus contribute to Austria becoming more secure and both, more autonomous and connected, within the EU in this sector.

Further, by establishing a quantum security standard, SBA Research gemeinnützige GmbH (SBA) will gain knowledge on how to guide future quantum security analysis and thus be able to advise, within the current restrictions, possible partners in establishing a quantum-secure status themselves and/or provide gap/threat/risk analysis for future quantum-safe infrastructures.

3.1.9. Exploitation K-BUSINESSCOM AG

As a long-established company with more than 130 years of experience and the leading provider of ICT solutions and services, K-BusinessCom AG will use its expertise as a security facilitator.

KBC will establish key material stored in Hardware Security Modules which are used for sensitive crypto operations like certificate generation and/or verification, signing operations for firmware and other critical IT infrastructure operations. Typical HSMs allow for so-called key-wrapping to transfer sensitive key material from one HSM to another and in some cases vendor proprietary solutions which are hard to audit and verify. A refinement of these lines will happen by protecting the link between two HSMs via a QKD based VPN to make it impossible for an attacker to gain access to the data exchanged between the HSMs.

K-BusinessCom AG will use the gained experience in the QCI-CAT Project to establish itself as leading expert regarding the refinement of either existing or new lines through the QKD and HSM key wrapping technology as well as an expert for operational management of these types of networks

3.1.10. Exploitation TECHNISCHE UNIVERSITAET GRAZ

There is no specific exploitation plan from TU Graz.

4. Relations to PETRUS and EuroQCI projects

As all other DEP 1 and DEP 2 projects, QCI-CAT is being advised and supported by PETRUS. Thereby, advances in the deployment of the EuroQCI networks among the member states can be coordinated to ensure compatibility of the networks in the long run.

PETRUS forms the Coordination and Support Action of the current Digital Europe Programme Calls. Together, they cover all relevant fields to successfully prepare the next steps towards a fully functional and harmonized EuroQCI, consisting of coordinated national QCIs such as QCI-CAT.

Together with PETRUS, members of the QCI-CAT consortium can connect to other national EuroQCI and industry projects to share knowledge, standardize interfaces, and to also avoid the duplication of work. Furthermore, QCI-CAT plans on inviting PETRUS members to demonstrations, larger meetings, and workshops such as the National EuroQCI Workshop. Apart from that, there are regular conference calls between PETRUS members and a selection of QCI-CAT project members. QCI-CAT will attend every relevant PETRUS appointment and support PETRUS activities.

Beyond the collaboration and information exchange with PETRUS, members of the QCI-CAT consortium will seek collaboration with the following projects from the DEP 1 and DEP 2 calls for joint standardization, testing, and evaluation activities:

- QUARTER (DEP 1) aims at increasing the maturity and readiness of quantum cryptography technologies for the deployment within EuroQCI. Among others, the project focuses at improving QPS and KMS software stacks and hence AIT will liaise with the QUARTER consortium on these topics.
- The goal of eCausis (DEP 1) is to advance the industrialisation of European QKD technology for a successful go-to-market with reduced costs. On the software side, KMS is a core focus of the project opening another opportunity for cross-project collaboration.
- HellasQCI (DEP 2) will implement three metropolitan communication networks in Athens, Thessaloniki, and Heraklion utilizing QKD, terrestrial optical fibre, and satellite technologies. Joint testing and evaluation activities will be carried out with QKD devices and entangled sources from AIT.

These collaborations ensure a wide compatibility of the technologies and components which are developed as part of the work in QCI-CAT.

5. National EuroQCI Workshop

Raising awareness for EuroQCI and related technologies among the Austrian stakeholders including end-users, industry, network operators, and suppliers is a central task of the dissemination and communication WP. As such, AIT will organize a workshop for Austrian stakeholders to discuss and interact with national and international experts on QKD and QCI and representatives of the other EuroQCI initiatives. Speakers from academia and industry will be invited to present current developments that advance the field scientifically and technically. Suppliers of QKD equipment will also be given the opportunity to demonstrate their products and offerings.

The workshop will be organized as two-to-three-day event with the following tracks:

- National EuroQCI Networks: This track focuses on national EuroQCI networks that are deployed as part of the DEP 2 projects. A small set of projects will be invited to present their unique use-cases and how they are supported by their QKDNs. Attendees will therefore have the opportunity to gain a wide overview of the European QCI landscape and the progress of designing and developing the national networks.
- QKD Industry: In this track, EU-27 companies producing hardware or software components that find application in EuroQCI will be given the opportunity to present their products. Specifically, industry partners involved in QCI-CAT and projects from the DEP 1 call will be invited as speakers. The talks will be accompanied by panel discussions with audience participation.
- Standardization and Certification: This track will provide updates on ongoing standardization activities in various standardization bodies. As certification of components for QKDNs is of interest to end-users and network operators, speakers will be invited from to discuss relevant developments on protection profiles and more.
- QCI Tutorial: This tracker offers a short introduction on all core technologies for establishing a secure large-scale QKDN. Based on the curriculum that is developed as part of WP9, short talks on QKD, network architectures, SDNs, PQC, and more will provide the attendees with a basic understanding of the technologies. The tutorial talks will specifically cater to the needs of the Austrian stakeholders.

AIT co-organized "QKD Days 2022 Madrid" and conducted an online survey with the attendees to gather their feedback on the event. Attendees would have appreciated more opportunities to interact with the other attendees and to visit booths of companies. For the organization of the EuroQCI workshop, this feedback will be taken into account by offering a dedicated room where companies can put up small booths.

An update on the National EuroQCI Workshop will be reported in the deliverable D10.3.

Summary

This document outlined the general and per partner dissemination, communication, and exploitation strategy for QCI-CAT. The partners will adapt the outline plan as the project progresses. The ultimate goal is to advance the state-of-the-art of quantum-safe technologies and to also communicate these advances as well as background knowledge to stakeholders, companies, and the general public. This document summarizes the overall strategy towards dissemination of projects results to specific target audiences via appropriate channels. Especially, for the industry partners this document also documents their exploitation strategies that formulate a plan to integrate quantum-safe technologies beyond the end of the project.

Appendix A - List of Acronyms

- DEP: Digital Europe Programme
- HSM: Hardware Security Module
- KMS: Key Management Service
- QCI: Quantum Communication Infrastructure
- QCI-CAT: QCI: Proof of Concept – Secure Connectivity Austria
- QKD: Quantum Key Distribution
- QKDN: Quantum Key Distribution Network