Digital Europe Programme (DIGITAL)

Application Form

Technical Description (Part B)

(Digital Europe Standard)

Version **1.0**
01 November 2021

IMPORTANT NOTICE

What is the Application Form?

The Application Form is thetemplate for EU grants applications; it must be submitted via the EU Funding & Tenders Portal before the call deadline.

The Form consists of 2 parts:

- Part A contains structured administrative information
- Part B is a narrative technical description of the project.

Part A is generated by the IT system. It is based on the information that you enter into the Portal Submission System screens.

Part B needs to be uploaded as PDF (+ annexes) in the Submission System. The templates to use are available there.

How to prepare and submit it?

The Application Form must be prepared by the consortium and submitted by a representative. Once submitted, you will receive a confirmation.

Character and **page limits**:

- page limit normally **70** pages (unless otherwise provided in the Call document)
- supporting documents can be provided as an annex and do not count towards the page limit
- minimum font size — Arial **10** points
- page size: A4
- margins (top, bottom, left and right): at least 15 mm (not including headers & footers).

Please abide by the formatting rules. They are NOT a target! Keep your text as concise as possible. Do not use hyperlinks to show information that is an essential part of your application.

⚠ If you attempt to upload an application that exceeds the specified limit, you will receive an automatic warning asking you to shorten and re-upload your application. For applications that are not shortened, the excess pages will be made invisible and thus disregarded by the evaluators.

⚠ **Please do NOT delete any instructions in the document. The overall page limit has been raised to ensure equal treatment of all applicants.**

TECHNICAL DESCRIPTION (PART B)

COVER PAGE

Part B of the Application Form must be downloaded from the Portal Submission System, completed and then assembled and re-uploaded as PDF in the system.

Note: *Please read carefully the conditions set out in the Call document (for open calls: published on the Portal). Pay particular attention to the award criteria; they explain how the application will be evaluated.*

PROJECT	
Project name:	Slovenian Quantum Communication Infrastructure Demonstration
Project acronym:	SiQUID
Coordinator contact:	prof. dr Anton Ramšak, University of Ljubljana, Faculty of Mathematics and Physics (FMF)

TABLE OF CONTENTS

PROJECT SUMMARY

Project summary
SiQUID will implement quantum key distribution (QKD) links between multiple government nodes in Slovenia and a test-bed quantum network between research institutions in Ljubljana for advanced quantum-communication protocols. We will coordinate our efforts with public and industrial stakeholders, and we will train key personnel, young researchers and engineers in quantum technology. The first test nodes implemented will be based on our recent first demonstration of QKD links between three European countries (arXiv:2203.11359-paper attached). We will harness directly modulated laser diodes to ensure the phase randomisation between adjacent pulse sequences, and we will use a high-assurance random number generator to randomise the choice of the state preparation basis. These improvements promise a higher level of security, a larger range, and a higher key rate. This will form the basis for the implementation of the QKD links between government nodes. To reduce the cost of future QKD networks, SiQUID will investigate the feasibility of cheaper alternatives for the detection nodes by balancing cost against the key rates achievable in metropolitan links. At the same time, we will use superconducting nanowire single-photon detectors (SNSPDs) to implement high-efficiency links. We will use these to test long-distance links between distant cities in Slovenia, and to nodes close to neighbouring countries. Moreover, we will test advanced quantum communication protocols like measurement-device-independent (MDI) QKD and the long-distance distribution of entanglement to further increase the security of QKD implementations, and to prepare the ground for a future full-fledged quantum communication network. We are in close contact with QCI initiatives in neighbouring countries to facilitate the harmonisation of the national efforts, and to facilitate future cross-border links and the implementation of the space segment of EuroQCI.

1. RELEVANCE

1.1 Objectives and activities

Objectives and activities *Describe how the project is aligned with the objectives and activities as described in the Call document.* *How does the project address the general objectives and themes and priorities of the call? What is the project's contribution to the overall Digital Europe Programme objectives?*
The endeavour of applying novel quantum-phenomena-based techniques for perfectly securing sensitive communication has been recognized as a strategically important priority of the EU and its member states on the path towards a future "quantum internet". In 2019 Slovenia has committed to participate in this joint undertaking by signing the declaration of cooperation on exploring ways to create a European integrated quantum-secure communication network, upraise Europe's scientific and technological capabilities, and establish its strategic autonomy, which has led to the EuroQCI cooperation framework. Even though Slovenian researchers have an outstanding track record in basic quantum physics research, the transfer of these achievements into some application areas, such as quantum communication, has been lagging behind. Slovenian industry has a significant expertise in secure classical communication technology and its deployment to secure critical public communication, but it has not yet had the right set of circumstances to integrate these with quantum solutions. The Faculty of Mathematics and Physics (FMF) of the University of Ljubljana has recently established a laboratory dedicated to quantum optics and quantum foundations and has put effort into establishing state-of-the-art research in quantum communication and quantum optomechanics. A recent highlight has been the collaboration with researchers from Croatia and Italy to implement a demonstration of quantum key distribution (QKD) between three neighbouring countries during a G20 meeting in Trieste (arXiv: 2203.11359 - paper attached). Still, there have so far been no national nor even local initiatives to build (semi)permanent quantum communication infrastructure. The EuroQCI initiative represents an opportunity to address these challenges. The objective of SiQUID is to establish the national infrastructure for quantum

communication in the form of a number of nodes interconnected by optical fibres, with the key sites at two research organisations (Faculty of mathematics and physics of University of Ljubljana, FMF, and Jožef Stefan Institute, IJS), one industry partner (Beyond Semiconductor, d.o.o., BSC), and seven government institutions at six locations (Ministry of public administration, Ministry of the interior, Ministry of foreign affairs, Ministry of defence, Secretariat-general of the government, Government office for the protection of classified information, and Government information security office), as well as at the location of the future optical ground station for satellite communication (a guarded location in the vicinity of the capital with suitable atmospheric conditions); we will also work toward establishing end points within reach of borders to neighbouring countries: Austria, Croatia, Hungary, and Italy. The Slovenian government has made a strong long-term commitment to the EuroQCI efforts and will co-fund the projects through the Recovery and Resilience Facility funds; the goal is to reinforce national cybersecurity infrastructure and to jump-start and then further develop the national efforts in the domain of advanced quantum technologies, thereby contributing to the joint European efforts in these domains.

In scope of SiQUID, the two research organisations, FMF and IJS, will establish the enabling infrastructure (laboratory space, essential equipment, permanent optical connections between their laboratory spaces) for quantum communication. This will enable the testing of key quantum communication components, their integration into full-stack QKD solutions, the investigation of advanced experimental techniques, the development of scalable solutions for national deployment, and the training of research and technical staff as well as that of end users. The industrial partner, BSC, will work towards combining the QKD solution developed with established classical encryptors for symmetric encryption in order to provide a fully integrated solution for secure communication, with the potential for obtaining approval for the protection of classified information (at a specific level of classification) This will aim to produce advanced quantum-reinforced encryption solutions that could be deployed in all member states and thus contribute towards a Europe-wide ultra-secure communication network. The public authorities in Slovenia will provide the locations to host the government quantum network nodes, investigate use cases of interest, and provide policy guidance on matters of information security.

The objective of deploying advanced national quantum systems and networks will be addressed by setting up a consortium that will work towards the successful completion of this task in several steps. In the planning stage, we will elaborate on the requirements and use case list that has been determined by the public authorities as a basis for preparing this proposal. In collaboration with the providers of optical communication infrastructure, the hosts of the premises to be used for the QKD nodes, and other relevant parties we will investigate the optimal solutions for interconnecting the identified sites (Slovenian quantum network nodes). The planning stage will lead to a detailed deployment plan, detailing the architecture, addressing the feasibility, and exploring the best available options for establishing the national infrastructure. In parallel, very early in the project, we will establish a minimal test-bed network connecting the two academic institutions (FMF and IJS). This initial infrastructure will enable the early testing and the characterization of the experimental hardware, and the development of QKD solutions, while more advances solutions for longer-range connectivity will be prepared. The long-term goal is to secure several permanent optical links operated by the government entities; this will constitute the initial sites of the future national secure network that will be fully equipped with mature equipment in later stages of the EuroQCI programme.

We plan to work on two approaches to QKD. One will be based on well-established and field proven techniques, like the approach that has been successfully demonstrated during the G20 Digital minister's meeting in Trieste in August 2021 with the participation of researchers from FMF, who will coordinate the present project (arXiv: 2203.11359 - paper attached). This approach will be fully developed, tested and characterized in a laboratory setting during the first year of the project. This will be the basis for the setups for the test-bed network, which will, for the most part, use EU27-sourced components. One of these initial setups will be portable, permitting field testing at multiple locations. Having established this early QKD testbed, we will explore the integration with the existing classical encryption devices made by the Slovenian industrial partner in this project. This will allow us to integrate QKD with existing communication appliances and communication networks, and to perform benchmark tests to assess the performance of the QKD equipment as well as the network links. We will also investigate the potential for scaling up and ruggedizing such a solution. This will allow us to assess the characteristics of the general approach and the viability of the specific home-grown QKD solution for the final deployment at multiple sites.

A central goal of future quantum networks will be the distribution of entanglement as a resource to harness the full potential of quantum technologies. In the context of QKD, entanglement offers the potential for increased, device-independent security. To provide the foundation for entanglement distribution in quantum networks and for entanglement-based QKD, we will demonstrate entanglement distribution over long distances and entanglement swapping. We will investigate the potential to ruggedize and industrialise these setups. The experience gained from the experimentation with home-grown solutions will serve as the final input to the deployment plan, which will then receive its final refinement before being put to execution. The goal is to have at the end of the project a fully functional and validated QKD network between the government sites for testing purposes and several trained operators, as well as academic/industrial laboratories for testing advanced quantum communication technologies. In addition, we will have obtained valuable know-how and appreciation for the real-life issues in deploying advanced quantum communication techniques; these will be communicated to colleagues involved in EuroQCI in other member states.

The objective of developing and testing use cases will be addressed by tasks that will elaborate the requirements of the national quantum network in full detail, focusing on the challenge of securing communication between key ministries and government offices and on applications to critical infrastructure where we will be in contact with providers of optical fibre infrastructure (who also operate railways, highways, and electricity distribution networks). We will explore using QKD for securing the communication between high-performance computing sites in the country, one of which is hosting a EuroHPC-procured supercomputer (HPC Vega) that may receive a quantum-simulator update in the future.

Slovenia has ambitions in other fields of quantum technologies, in particular quantum-enhanced sensing, quantum simulators/computers, and harnessing quantum technologies in space. Taking full advantage of many of these technologies will require quantum entanglement as a resource, which will need to be distributed via a quantum network. For this reason, several QKD network sites in the present project will be chosen and set up so that the laboratories developing those technologies will be able to connect to the QKD network through short-distance quantum-secure links. This will facilitate secure communication between those sites, and it will be a major step towards a fully functional quantum network.

The deployment will make use of the best available quantum technologies, by leveraging the quantum-optics know-how from FMF and IJS, and using it to devise original solutions for QKD, the distribution of entanglement, as well as the best available classical security technologies provided by the industrial partner, BSC, such as high-speed encryption devices. By proposing to develop our own complete systems through combining the complementary expertise of the consortium partners, we are thus going significantly beyond the baseline recommendation of deploying components developed and manufactured in the EU, instead contributing even more directly toward the development of the European supply chain. We will also put a significant effort towards ensuring that the quantum solutions do not leak any sensitive information through side channels, which would completely nullify any physical guarantee of security in QKD. We believe this adds a significant value to our proposal.

The testing of use cases will involve the most security-sensitive government institutions (the 6 government sites), which will provide a realistic assessment of the maturity of the technologies in the most demanding environments and provide valuable feedback for further development. In particular, it will provide feedback on the robustness, the dependability, the ease of integration, and on security. This will provide an excellent basis for the next steps of EuroQCI which aim towards scaling up the installations with approved solutions.

Some participants of the project are already developing other quantum components that are not directly within the purview of this call and will not be developed as part of the activities of this project. Nevertheless, the proposed activities would benefit from the availability of a testing infrastructure where those components could be swapped in and out as part of the total setup. Examples include random number generators and solutions for time synchronisation.

The project will have an important educational component, which will be facilitated by the fact that the project coordinator, FMF, is the largest degree-granting institution in physics in the country, while another beneficiary, IJS, is the largest national public research institution and an important employer of researchers trained in quantum physics as well as information and communication technologies, with a strategic ambition to become one of the leading institutions Europe-wide in the field of quantum technologies. Through integrating junior researchers in all phases of this project, planning, development, and deployment, we will train the first generation of quantum technologists that will be able to participate in future endeavours, not only as basic researchers, but also engineers capable of building fully integrated systems and deploying them in the field. The training will also extend to end users from the ministries and government offices, as well as other interested parties (sectors of critical infrastructure, defence, national security).We will also contribute towards the overarching goal of EuroQCI, that of large-scale deployment spanning the EN, by developing solutions to extend the range and the security of QKD solutions by using measurement-device-independent (MDI) QKD and laying the foundation for quantum networks by demonstrating long-distance entanglement distribution and entanglement swapping. Another effort in the direction of increasing distances is the identification of a suitable site for the optical ground station and the securing the required optical connection to the rest of the national QKD network. These preparatory activities will be executed in anticipation of the Connecting Europe Facility call, to which a national QCI consortium is also committed to apply. We have already established contacts with the European Space Agency (ESA) on the topic of Slovenian plans and the question of the required equipment and other resources. We will explore how to best combine the terrestrial and satellite technologies, and how to interface them. Finally, as one of the aims of this project, we will work towards obtaining secure locations and optical connections along key axes towards the neighbouring countries (1st axis: Ljubljana-Celje-Maribor towards Austria and Hungary, 2nd axis: Ljubljana-Postojna-Koper/Sežana towards Italy and Croatia, 3rd axis: Ljubljana-Novo Mesto-Brežice towards Croatia). We will collaborate with EuroQCI teams from the neighbouring countries towards ensuring the compatibility of our QKD systems, permitting an easy bridging of borders, and to exchange lessons learned during the deployment of the respective national networks. Figure 1 shows a schematic of possible future long-distance links that could form backbones for the Slovenian quantum network and potential locations for cross-border relay nodes to connect to neighbouring EU countries. So far, we discussed future connections from Ljubljana towards Graz, towards Zagreb, and towards Trieste as indicated. Given the central location of Slovenia between Austria, Croatia and Italy, it could prove very beneficial in the future to also test a potential additional backbone towards Villach.

Figure 1: Schematic of a possible future realization of the backbones of a Slovenian QKD network and potential connections to neighbouring countries. While we will test the implementation of long-distance connections, optional trusted nodes would be applied in the case that direct connections from Ljubljana to the border or to other cities are not possible. The indicated positions of cross-border relays indicate possible locations that we will coordinate with neighbouring countries. A testbed realization is planned at least for one of directions: Ljubljana to Zagreb, to Trieste or to Graz. The figure also indicates a potential location for an optical ground station to connect Slovenia to the space segment of EuroQCI.

We will strengthen an ongoing research collaboration with the neighbouring countries on topics of quantum communication. A notable example is the already mentioned successful demonstration of QKD links between three countries (Italy-Slovenia-Croatia) during the G20 Digital Minister's meeting in Trieste on 5 August 2021, which involved researchers from FMF, Ruđer Bošković Institute (RBI) in Zagreb, Croatia, the University of Trieste's Department of Physics and CNR in Florence, Italy. FMF and IJS are also collaborating with RBI and Institute of Physics in Zagreb, Croatia, on topics of quantum memory and long-distance entanglement distribution. We will further strengthen these ties in the scope of SiQUID, by doing exchanging lessons learned in implementing the national networks, by collaborating in defining routes and locations for border crossings for future international quantum-network connections, and by investigating the compatibility of the QKD architectures used in the respective national networks.

To highlight our commitment to work closely with our direct neighbours in Europe to facilitate the implementation of cross-border links, we agreed beforehand with the coordinators of the EuroQCI proposals of our neighbouring countries that we would closely coordinate our actions, that we would exchange experiences during the course of the project, and that we would exchange lessons learned. These efforts will significantly help to harmonise the activities in Slovenia with the efforts of its EU neighbours, and it will help integrate the Slovenian quantum community within the European quantum community. To emphasize our commitment to this effort, we attach letters of intent / memoranda of understanding from Austria, Croatia, Italy, Hungary, and Slovenia to the present proposal.

Specifically, these are the objectives of SiQUID and their alignment with the call topics:

Objective 1 (architecture and EuroQCI integration): Provide network architecture, requirements and plan for national deployment of advanced quantum systems and their integration with EuroQCI.

Measurable Assessment criteria:

- Availability of SiQUID requirements, architecture and Specification (D2.1, M3; D2.2 M12)
- Availability of initial network deployment and cross-border links plan (D2.2, M12)
- Availability of Quantum-Enhanced Encryptor (QEE) requirements, performance estimates and other specifications (D3.1, M12; D3.2, M24)
- Availability of revised network deployment and cross-border links plan (D5.1, M24)
- Availability of minimal operation requirements (D5.2, M30)
- Availability of projected performance and characteristics of next generation quantum system (D4.3, M30)
- Availability of measured real-world characteristics of deployed nodes (D5.3, M30)
- Availability of lessons learned during deployment and experimentation with public, academic and critical infrastructure use cases (D6.3, M30)

Rationale and connection to call topic: Network architecture design and planning is essential for successful deployment of quantum systems and their integration with existing networks. It is also iterative by nature, where capabilities, performance and specifications of QEE influence the network architecture and vice-versa. The characteristics, requirements and performance measured in real-world experiments and those projected for the next generation QKD systems are important to support further development and eventual integration with EuroQCI. Furthermore, established contacts and lessons learned exchanged with other member states will facilitate cross border secure connections and integration into EuroQCI.

Relevant Work Packages: WP2 (network architecture), WP3 (QEE, MDI QKD), WP4 (entanglement distribution), WP5 (network deployment), WP6 (use cases trials).

Objective 2 (improved security): Improved data and network security with QEEs by integrating "classical" network encryptors with quantum technologies, also paying attention to minimization of the side channel leakages.

Measurable Assessment criteria:

- Availability of Network Security Assessment and Requirements (D2.1, M3)
- Availability of QEE security design (D3.1, M12)
- Availability of Theoretical assessment of quantum security guarantees (D4.1, M12)
- Availability of QEE node design and TEMPEST plan (D3.2, M24)
- Availability of QEE node TEMPEST protections (D3.3, M30)
- Demonstration and availability of Entanglement source and distribution for QKD purposes (D4.2, M12; D4.3, M30; D4.4, M30)
- Availability of QEE security evaluation process & artifacts (D5.2, M30)

Rationale and connection to call topic: QKD enables up-to information theoretic security guarantees that can be leveraged in combination with network encryptors to strengthen overall security of communication systems and networks. Independently from QKD and in the interest of improving security, the network encryptors will be upgraded with the most promising post-quantum algorithms. The project will also pay special attention to TEMPEST (side channel leakage) issues that are known to have been responsible for real world security compromises. Furthermore, the design of QEE nodes will take into account interoperability and other issues that reduce availability (and thus security).

Relevant Work Packages: WP2 (security requirements), WP3 (QEE security & TEMPEST), WP4 (theoretical assessment of quantum security guarantees), WP5 (QEE evaluation process and artifacts).

Objective 3 (industrialization): Design and develop experimental advanced quantum systems including QEE with attention on the ease of manufacturability, integration, miniaturization, robustness, cost reduction and other industrialization aspects. Experiment with extending maximum achievable link distance to enable the next generation of long distance QEE.

Measurable Assessment criteria:

- Ka: Longest link achieved as measured in laboratory environment for non-industrialized nodes, by determining the maximum attenuation at which the QKD system still operates and calculating the distance assuming standard 0.2 dB/km fibre attenuation (Ka >= 100km @ M30).
- Availability of SiQUID requirements, architecture and Specification (D2.1, M3; D2.2 M12)
- Availability of QKD proof of concept (D3.1, M12)
- Availability of QEE node design (D3.2, M24)
- Availability of QEE node (D3.3, M30)
- Availability of Entanglement source design, industrialization (D4.2, M12; D4.3, M30)

Rationale and connection to call topic: The industrialization, integration and cost reduction are key enablers in preparation for large-scale deployments. The network (security) requirements and QEE (security) requirements are interdependent and will be thus codeveloped and optimized in accordance with expected future security and large-scale deployment needs. Maximizing the achievable link distance is important in easing deployment and reducing (eliminating) the need for trusted nodes. The distribution of entanglement in combination with quantum memories promises to overcome distance limitation in a future full EuroQCI deployment.

Relevant Work Packages: WP2 (requirements), WP3 (QEE node), WP4 (entanglement distribution, advanced quantum experiments progressing towards quantum internet).

Objective 4 (autonomy): Contribute to strengthening of the European strategic non-dependence in the field of quantum technologies, data assurance and security by focusing design, development and experimentation activities around (in order of priority) national, EU, NATO and if necessary other allied & democratic countries supply chains.

Measurable Assessment criteria:

- Availability of QEE security design (D3.1, M12)
- Availability of QEE node design and TEMPEST plan (D3.2, M24)
- Availability of QEE node TEMPEST protections (D3.3, M30)
- Availability of Entanglement source design, industrialization, and TEMPEST analysis (D4.2, M12; D4.3, M30)

Rationale and connection to call topic: Technological autonomy requires both the control (autonomy) of supply chains and autonomous ability to design, develop, deploy and manage secure quantum communication systems. Furthermore, security and availability of such critical systems could be compromised when relying on components, technologies, supply chains or development and design capabilities of untrusted third parties (and countries). This is why SiQUID will focus on minimizing supply chain risks.

Relevant Work Packages: WP3 (QEE components selection), WP4 (entanglement distribution, advanced quantum experiments progressing towards quantum internet).

Objective 5 (deploy and integrate): Deploy first advanced quantum systems with QEEs and show their integration with existing communication networks.

Measurable Assessment criteria:

- Kn: number of deployed nodes (may not be all operational at the same time) (Kn >= 7 @M30)
- Km: number of member states involved in cross-border collaborations (Km >= 5 @ M30)
- Availability of SiQUID requirements, architecture and Specification (D2.1, M3; D2.2 M12)
- Availability of initial network deployment and cross-border links plan (D2.2, M12)
- Availability of QEEs (D3.1, M12; D3.2, M24)
- Availability of revised network deployment and cross-border links plan (D5.1, M24)
- Availability of measured real-world characteristics of deployed nodes (D5.3, M30)

Rationale and connection to call topic: Before any large-scale deployments it only makes sense to experiment with smaller networks and with different devices and approaches. SiQUID's contribution towards EuroQCI goals includes experimental deployment of nationally produced QEEs and their integration with existing communication networks in support of public, academic and critical infrastructure end users.

Relevant Work Packages: WP2 (deployment plan, network architecture), WP3 (QEE to be deployed), WP5 (deployment).

Objective 6 (measurements and lessons learned): Gather initial reliability, performance and lessons learned related to performance of deployed quantum enhanced systems. Gather initial public, academic and critical infrastructure end-user feedback and lessons learned.

Measurable Assessment criteria:

- Availability of QEEs (D3.1, M12; D3.2, M24)
- Availability of revised network deployment and cross-border links plan (D5.1, M24)
- Availability of planned public, academic, and critical infrastructure use cases (D6.2, M24)
- Availability of measured real-world characteristics of deployed nodes (D5.3, M30)
- Availability of lessons learned during deployment and experimentation with public, academic, and critical infrastructure use cases (D6.3, M30)

Rationale and connection to call topic: Information about real-world behaviour, reliability, and performance of QEEs is critical in preparation for large-scale EuroQCI deployments. The end user feedback and lessons learned will help guide design and deployment of next generation(s) of highly secure communication and data networks.

Relevant Work Packages: WP3 (QEE), WP5 (deployment lessons learned and network measurements), WP6 (end user feedback related to public, academic and critical infrastructure use cases).

Objective 7 (grow national expertise): Concentrate and grow the critical mass of national experts and expertise in the fields of quantum communication technologies and secure communication & data networks.

Measurable Assessment criteria:

- Kp: Number of professionals trained due to SiQUID project (Kp >= 12 @ M30)
- Availability of SiQUID requirements, architecture and specification (D2.1, M3; D2.2 M12)
- Availability of initial network deployment and cross-border links plan (D2.2, M12)
- Availability of QEEs (D3.1, M12; D3.2, M24; D3.3, M30)
- Availability of revised network deployment and cross-border links plan (D5.1, M24)
- Availability of planned public, academic, and critical infrastructure use cases (D6.2, M24)
- Availability of measured real-world characteristics of deployed nodes (D5.3, M30)

- Availability of lessons learned during deployment and experimentation with public, academic, and critical infrastructure use cases (D6.3, M30)

Rationale and connection to call topic: While task T6.3 explicitly focuses on Quantum technologies training and capacity building it is the (inevitable and desired) consequence of this project that many new professionals will gain expertise and experience in quantum-communication technologies, secure communications and data networks. Such critical mass of national experts that have the ability to design highly secure quantum-communication systems if required in order to design and deploy the next generation of secure quantum systems and progress the technological autonomy of European quantum-communications industry. The newly trained quantum workforce will be key in facilitating the full deployment of the EuroQCI.

Relevant Work Packages: WP2, WP3, WP4, WP5, WP6 through project work directly contribute to training of new professionals and thus growing of national and EU expertise in quantum communication technologies.

We now detail some of key activities of this project.

In the planning stage we will:

1) identify the most vulnerable critical infrastructure in Slovenia (weakest links) that requires high resilience and would benefit from the enhanced security provided by QKD;

2) plan possible ways to align the quantum network with the existing transport and electricity distribution networks (which by themselves constitute national critical infrastructure);

3) select specific use cases for testing QKD infrastructure in the final phase of this project.

In order to provide the QKD solutions for government sites, we will explore existing solutions (e.g., through joint procurement within EuroQCI) as well as developing our own solutions. The development of home-grown setups will go in three directions:

1) development of a full BB84 implementation in the form of a full-stack solution, starting with a test-bed installation at the academic institutions, permitting the evaluation of the scaling potential for the final deployment within scope of this project; completed no later than on M12 to permit validation and performance characterization to allow an informed decision for the national deployment; this critical task is feasible due to past experience of the researchers involved in the project and carries low risk;

2) development of a long-distance MDI QKD test setup. Based on the experience with the BB84 testbed solutions, we will first implement an MDI QKD test setup in the FMF lab and then test the deployment over longer distances. In a first test, we will aim to connect the site at IJS Jamova. If this is successful, we will aim to test this advanced QKD technology between two distant sites with the FMF location acting as the relay.

3) development of two high-brightness sources of entanglement with the potential for long-distance entanglement distribution and entanglement swapping, completed in milestone MS2; this task is feasible due to past experience of the researchers involved in the project, and it will provide a solid foundation for connecting Slovenia to future quantum networks.

The national deployment will consist of:

1) an installation of QKD devices and their connection to point-to-point links at the specified government sites;

2) a functional integration with existing communication devices and encryptors.

3) tests of long-distance QKD links within Slovenia to connect key locations within the country (e.g.: Ljubljana, Postojna, Celje, Maribor) and locations close to the borders of neighbouring countries to test the feasibility of future cross-border connections.

4) tests of advanced quantum-communication solutions over long distances. In particular, we will test MDI QKD and the distribution of entanglement and entanglement swapping.

The deployment will be followed up by (or run in parallel with):

1) the validation of innovative solutions in selected application scenarios (t.b.d. in the scope of the project);

2) security assessments of the devices, and the verification of the fulfilment of common criteria that will be established within EuroQCI on the European level;

3) the development of solutions for network monitoring, logging, and alerting in case of failures; these will be based on open-source solutions;

4) the setting up of national quantum communication management structures, and its integration in Europe-wide management structures;

5) the formulation of national QKD policies and their alignment with European standards.

We plan to investigate several use cases. Tentatively, the list includes:

1) communication between data centres;

2) communication between government locations;

3) communication with critical infrastructure (power plants, ports, airports, military bases, network hubs, optical ground station, …);

4) international links to secure the communication with other EU member states.

Training and dissemination of results:

1) a key and integral component of this activity will be to train research staff and engineers. During this project, we will train master students and new professionals (young researchers at PhD or post-doctoral level at FMF and IJS, engineers at BSC and government experts) by sharing knowhow while implementing the test setups and the QKD nodes for the government nodes and for the demonstration setups. We will also train them in more advanced quantum technologies when we implement MDI QKD, entanglement sources, and the distribution and swapping of entanglement. Throughout the duration of the project, we will train master students by having them participate in laboratory work. In this way, the project will contribute to alleviating the shortage of ICT trained personnel, which is already a critical issue that leads to serious security incidents and disruption;

2) training of end users; 1 person per participating government organisation;

3) raising public awareness through outreach activities (newspaper articles aiming general public in national mainstream media);

4) working towards attracting external users (academic, SMEs, industry, public sector) through training sessions (workshops) organised at the academic institutions in the consortium; staff training on topics of QKD deployment, operation and use.

The SiQUID activities will be closely coordinated with the activities in other EU member states. Already during the preparation of this proposal, we have been in contact with the coordinators of national EuroQCI initiatives in all neighbouring countries: H. Hübel (AIT) in Austria, M. Lončarić (RBI) in Croatia, J. Mohacsi (KIFU) in Hungary, and D. Calonico (CARNET) in Italy. In all stages of the project, we will test and validate the equipment based on common criteria and rules established within the EU EuroQCI project (EUROQCI-QKD coordination of national EuroQCI projects and the preparation of large-scale QKD testing and certification infrastructure). We will work towards open solutions.

These efforts will be an essential contribution to strengthening European sovereignty in quantum technologies. This will prepare Europe to build and to maintain its sovereignty in novel technologies that will shape the future of digital technologies. In particular, the establishment of a European quantum network will allow interconnecting future quantum sensors, quantum computers, and quantum simulators. The efforts in SiQUID in close collaboration with the efforts in neighbouring countries will be a strong contribution to the establishment of a European quantum communication infrastructure, and to train a new generation of scientists and engineers in quantum technologies. In addition, we will train key personnel at government institutions in the use of these novel technologies.

1.2 Contribution to long-term policy objectives, policies and strategies — Synergies

Contribution to long-term policy objectives, policies and strategies — Synergies

Describe how the project contributes to long-term policy objectives of the call's domain/area and to the relevant policies and strategies, and how it is based on a sound needs analysis in line with the activities at European and national level.

What challenge does the project aim to address?

The objectives should be specific, measurable, achievable, relevant and time-bound within the duration of the project.

The overall project objectives and a way to measure them is given in 1.1.

The digital transition in Europe will require reliable, fast, and secure network connectivity. Slovenia has identified the key areas where enhanced resilience towards cybernetic attacks is required: government and other public-administration data (including those exchanged across borders with EU partners), connected devices (IoT), energy distribution networks (the electricity grid in particular), district heating, air traffic control, banks, health-care institutions, key digital infrastructure (internet exchange points, data centres, providers of cloud computing to public administration and schools), and other critical infrastructure in line with the EU Cybersecurity Strategy and the Directive on the resilience of critical entities. The long-term goals are to reduce vulnerabilities and to increase the security of critical communication and data infrastructure to enhance the existing security systems based on hardware and software solutions with an additional quantum security layer, and to ensure the integration with the EU Cyber Shield (i.e., the use of Security Operations Centres across the EU to detect signs of attacks and to launch early preventive action). The activities of this project will also support the European long-term strategy of the transition towards a gigabit society (GIGAEurope) with a strong and harmonised European Digital Single Market, by increasing the trust in connectivity through quantum-secured encryption key exchange.

A key long-term aim of EuroQCI is to secure access to optical fibres across Europe for the purposes of QKD and for a future quantum internet. In the scope of this project, we will work towards this goal at the national level. We aim to:

1) provide dark fibres to 6 key government sites in Ljubljana with appropriate point-to-point direct connectivity between the sites (with topology to be determined in the scope of the project), route these to optical-port panels in communication racks, secure space (tentatively 10U) in the racks for the installation of QKD devices and the associated communication equipment. This will be done no later than M24, for the purposes of use case testing; this is expected to be easily achievable since the said sites are located in the central area of Ljubljana where there is an ample supply of optical fibres owned by both state-owned and private companies, and also because the government entities involved have already committed to participate in this project;

2) connect the research sites (UL FMF and IJS at Jamova) using dark fibres at an early stage of the project (no later than M6) for the purposes of early tests and the characterization of QKD solutions built, and for benchmarking, verification and further development; this will be easily achievable due to neighbouring positions of these institutions and the existence of installation channels which can be put to use to establish a permanent fibre connection;

3) establish two long-distance links, connecting Ljubljana (UL FMF site) to sites close to the Slovenian border, for the purposes of establishing cross-border links at a later time, as well as for testing long-range QKD networks in the scope of this project (see below); one such optical link already exists (it was established for the three-country QKD demonstration at the G20

Digital ministers meeting in Trieste, August 2021), but its long-term use will be negotiated in scope of this project, no later than in M12;

4) determine a solution for connecting the optical ground station for satellite communication to the terrestrial segment (government QKD network in Ljubljana); in collaboration with the European space agency (ESA), the solution should be determined by M12 and implemented in the scope of a separate project co-funded by Connecting Europe Facility (CEF); the determination of the connection plan is achievable within this project, while the implementation will depend on securing the required funding within the CEF call (national participation is provisioned in the national Recovery and Resilience Facility (RRF) plan).

We will also work towards two further endeavours, which are however dependent on the commitment of resources by fibre owners:

1) inter-connect the government and research QKD networks through a central location in Ljubljana (Cankarjev dom); this appears technically feasible because the national academic research network ARNES has in use optical fibre connection between the ARNES data centre at IJS on Jamova street and the Cankarjev dom site;

2) additional long-distance connections within the country, with the goal of establishing links along the key corridors in the country, westwards towards Italy, northeast toward Austria and Hungary, and southeast towards Croatia. These activities are aligned with the European goal of establishing 5G corridors along roads and railways within the Connecting Europe Facility. The optical networks are owned and operated by DARS (Slovenian highways agency), Slovenske železnice (Slovenian railways), ELES (Slovenian electrical power distribution), and Telekom (a state-owned telecommunication company).

As part of the activities aiming to provide the dark fibre infrastructure for the terrestrial segment of EuroQCI, we will also perform regular characterization of fibre characteristics (e.g. attenuation measurements).

The links that will be established are schematically presented in Figure 2.

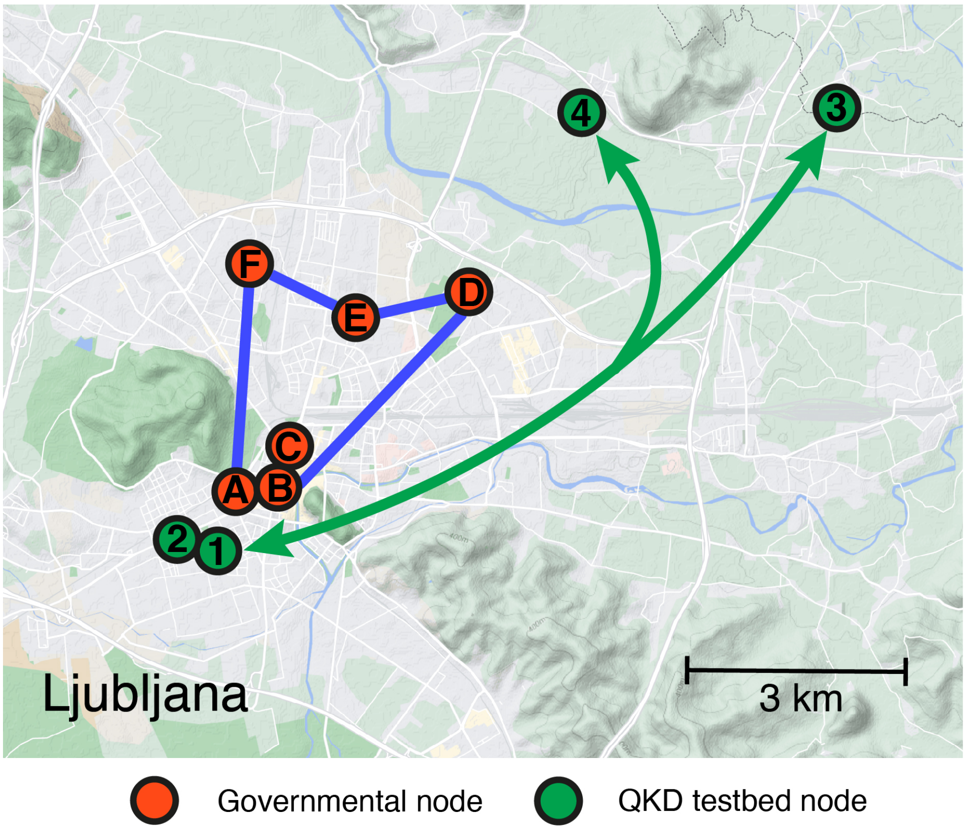


Figure 2: Governmental nodes (A-F) will be connected in QKD links to demonstrate the feasibility of securing the exchange of sensitive information via quantum-enhanced encryption. The indicated topology of the QKD network connections is only schematic. The final network

topology will depend on the available fibre links, and different topologies may be used for test purposes. The green arrows indicate quantum communication links of the test and demonstrator setups. The nodes involved are: 1 ~ FMF, 2~IJS, 3 ~IJS/Reactor and 4~BSC.

1.3 Digital technology supply chain

Digital technology supply chain

Explain to what extent the project would reinforce and secure the digital technology supply chain in the EU.

⚠ *This criterion might not be applicable to all topics — for details refer to the Call document.*

SiQUID project will develop a QKD system that will use critical components from national and EU suppliers wherever reasonably possible. The assembly and production of QKD system and its integration into QEE will be performed within EU granting an additional level of supply chain control and security. All the software (apart from standard & open-source software) and hardware logic description (RTL e.g. required by hardware encryptors) will be of national and thus EU origin only. Furthermore, we will aim to acquire the equipment required for the experimental demonstrators and the equipment related to the QKD nodes from European Suppliers. Most key technologies are available from European Suppliers. For the budget planning for this grant application, we already contacted potential suppliers for the equipment we will need. We focused on identifying potential European Suppliers. Apart from a very few exceptions, we were successful. Given that European suppliers will receive many similar inquiries in the course of the EuroQCI initiative, we are confident that this will signal European suppliers an increasing demand for those technologies. In the final documentation for this project, we will provide an overview of equipment and material bought, and which supplier we purchased it from. We will clearly indicate any non-European suppliers, and we will describe why we could not choose a European supplier in those cases. Possible reasons are: (a) there is no European supplier (with required functionality and performance), or (b) potential European suppliers are unreasonably and far more expensive than non-European alternatives, or (c) that European suppliers were not able to deliver at all or in time.

1.4 Financial obstacles

Financial obstacles

Describe to what extent the project can overcome financial obstacles such as the lack of market finance.

⚠ *This criterion might not be applicable to all topics — for details refer to the Call document.*

The main reason for lack of market financing for QKD related technologies lies in low (commercial) demand for QKD protected systems. This is understandable since QKD promises advancement of security above that achievable with “classical” encryptors (which is already very high), but at a relatively high additional cost (in terms of limitations of range, trusted nodes issues, device costs, fibre costs and other complexities). It does not help that in more than one occasion QKD systems didn’t offer any (even classical) level of security due to various design issues. Thus, the very use cases that require the highest level of security and would thus be the most natural first adopters avoid production use of the technology due to its immaturity, especially in terms of high assurance guarantees.

The project will work towards addressing above mentioned obstacles by:

- Integrating QKD with already existing high assurance hardware encryptor accredited for protection of national, EU and NATO classified information
- Focusing on security, implementing additional post quantum algorithms and above all making sure that in no circumstances the security of the system would be lower that achievable with “classic” high assurance hardware encryptor.
- Focusing on side channel protections of QKD and integration with high assurance encryptor

- Improving industrialization aspects of QEE, driving down the product cost, improving reliability, ease of use, etc.
- Working on increasing maximum distance between QKD nodes and in progressing towards eliminating the need for trusted nodes
- Developing use cases implemented on QKD protected systems to drive demand
- Testing advanced quantum communication protocols that overcome a possible dependence of security on device characteristics (measurement-device-independent QKD), or that use entanglement, which promises the maximum security achievable with QKD and which can overcome the need for trusted nodes.

We believe that the above are the key aspects that need to be addressed to drive market adoption (and thus market financing) of QKD systems.

Furthermore, one of the most high-risk obstacles that we, but also other participants to EuroQCI could face is the availability of dedicated dark fibres. These would be the ideal connections for quantum networks and for QKD. However, while fibre owners sometimes are willing to provide fibre connections for free or for a significantly reduced rate for a limited time window, this is not a permanent solution. In the future, we anticipate that users of quantum applications will be able and willing to pay the rent for the required optical fibre links. For the current purpose of demonstrating European quantum network connections and QKD, there is of course no direct market finance. For that reason, we (a) have already discussed with various providers of optical fibre connections in Slovenia to identify the most suitable providers for the purpose of the present project but also for the purpose of permanent connections. Also, (b), we reserved part of the project budget in case we will need to pay for the rental of fibres in the source of this project. If the rental for some of the fibre connections proved too expensive given the budget reserved, we will aim to (I) get a reduced price for example by highlighting the continuous usage of the fibres, or by arguing to the supplier that the demonstration will be a valuable advertisement for them, or to (II) solve this issue by talking to alternative suppliers, or (III) choose a different route if possible.

2. IMPLEMENTATION

2.1 Maturity

Maturity

Explain the maturity of the project, i.e. the state of preparation and the readiness to start the implementation of the proposed activities.

The Faculty of Mathematics and Physics at the University of Ljubljana (UL-FMF) is well equipped and ready to lead this project, and to implement the proposed activities. In 2020, the UL-FMF finished setting up a state-of-the-art quantum optics lab led by R. Kaltenbaek (RK). RK published high-impact research in long-distance quantum communication, optical quantum computation, and quantum optomechanics, and he is one of the lead scientists for quantum technologies in space. His experience in long-distance free-space and fibre-based quantum communication links, his seminal research on quantum interference and entanglement swapping with independent sources, and his contributions to harnessing quantum technology in space render him uniquely qualified for implementing large-scale quantum networks. Since RK joined the UL-FMF in 2019, the faculty has become a key player in quantum technology in South-Eastern Europe. In particular, RK initiated close contacts with partners in Croatia and in Italy and invited the latter to also join the QUAPITAL initiative, which research groups from central and South-Eastern European countries formed to share experience in the implementation of quantum networks. This was the basis for a bilateral research project between Slovenia and Croatia. In this project, RK and A. Ramšak (AR) have been collaborating since 2020 with researchers at the Jozef Stefan Institute (IJS) and with researchers in Croatia to implement sources of entangled photons and to couple them to atomic quantum memories. Since early 2022, the research of RK's group (FMF), of Rok Žitko and that of researchers from the IJS has been supported by a new research program of the Slovenian Research Agency (ARRS) dedicated to quantum technology.

In August 2021, RK and AR led the Slovene part of a trilateral demonstration experiment between Croatia, Italy and Slovenia at a G20 meeting in Trieste. Following this demonstration, AR and RK were contacted by Branko Drobnak from the Business Angels of Slovenia to explore possible collaborations with Slovenian companies. In particular, this led to regular meetings with FMF, IJS, BSC and the service provider T-2 to explore possible applications of quantum technology and market potential of those applications.

BSC previously delivered, deployed and maintains a number of classified and non-classified systems, nationally and internationally, that are based around XIPHRA hardware encryptors. The experience with government classified and critical infrastructure deployments will help guide SiQUID requirements, architecture and execution in direction of minimizing the time in which QKD protected systems can be deployed and used for protection of the most critical classified information.

In 2012, Peter Jeglič put together a group of researchers to set up the first Slovenian laboratory in the field of quantum technologies. Together with Erik Zupanič they have started a new independent line of research in quantum simulations, sensors and devices with cold atoms. Their experience in building and designing complex experimental setups is a valuable contribution to this project. Their expertise covers a variety of experimental methods and techniques, including photon frequency conversion, phase and frequency locking of light sources, photon storage and slow light. These are the basis of atom-based quantum memory, which is an important building block of long-distance QKD and beyond-QKD technologies.

The experimental demonstration at the G-20 meeting in Trieste was the first to show long-distance and cross-border QKD between three European countries. This working principle is a very mature technique that has been used successfully in many QKD demonstrations in the lab and over long distances. We will use this technique as the basis for our activities in order to implement working QKD demonstrators as quickly as possible after the start of this project. These will form the basis for further development and industrialization, and their implementation will serve as an ideal opportunity to train young researchers at the FMF and colleagues at the IJS and BSC in quantum communication. This will provide a solid foundation for subsequent tasks in this project by increasing the scientific expertise of Slovenian researchers and engineers.

2.2 Implementation plan and efficient use of resources

Implementation plan

Show that the implementation work plan is sound by explaining the rationale behind the proposed work packages and how they contribute to achieve the objectives of the project.

Explain the coherence between the objectives, activities, planned resources and project management processes.

Show how the project integrates, builds on and follows up on any pre-existing work or EU funded projects. Provide details (including architecture and deliverables) about pre-existing technical solutions.

The work in the project is divided into work packages. Conceptually it falls into three groups:

- Development, experimentation, industrialization and integration of QKD and related quantum technologies with field proven hardware network encryptor (WP3, WP4): This is where the core of the research, development and experimentation work will be performed with goal to adjust all parts of QKD system in order to optimize the trade-off between security, cost, performance, ease of deployment, ease of use and other metrics that will be identified as important during project execution (mainly in WP2, WP5 and WP6). The key outcome of this activities is QEE that will be used for deployment (WP2 and WP5).
- Deployment of SiQUID network and required preparation work (WP2, WP5): The initial SiQUID requirements elicitation will be performed in WP2 which will guide the development and experimentation activities in WP3 and WP4. The required node locations and optical fibres are going to be secured. The QEE will be deployed taking into account security requirements and minimal operating requirements as will also be determined in the WP2 and WP5. The behaviour of deployed network will be monitored

and measured to facilitate further QEE improvements. Plans for cross border connection will be prepared with other member states.

- Explointation of SiQUID network (WP6): The deployed network will be made available to public (governmental), academic and critical infrastructure users to gather their feedback and experiences. The lessons learned will tackle back to the level of network deployment (WP5) and design of the underlining node hardware and software (WP3, WP4) to enable further improvements.

The precise link of work packages and overall SiQUID objectives is given in section 1.1. The main interactions between work packages are shown in the Pert chart (section 4.1).

Building on the experience with this successful »Trieste demonstration«, we will first aim to implement QKD nodes using similar protocol based on decoy-state BB84 using time-bin encoding in sequences of weak pulses. We will, however, implement improvements to increase the bandwidth and the security of the protocol. These improvements will be based on successful demonstrations by the group of A. Shields (Toshiba Europe Ltd, Cambridge, UK). We will use pairs of gain-switched and injection-locked laser diodes to implement the sender nodes. This will allow achieving increased security compared to the Trieste demonstration because of the intrinsic phase randomization between subsequent pulse sequences. In addition, this approach promises significantly higher transmission rates.

These initial simple nodes will provide a fail-safe backup option while we will also aim to implement protocols promising enhanced security and longer range. In particular, we will (A) aim to achieve BB84 links over longer distances by using superconducting nanowire single-photon detectors (SNSPDs), and (B) to implement measurement-device-independent (MDI) QKD. For this, we will harness SNSPDs in combination with the enhanced sender nodes described above. To train researchers and engineers in Slovenia in techniques for the next steps in implementing a European quantum-communication network, we will (C) implement a state-of-the-art source of entangled photons at a telecom wavelength and demonstrate the distribution of entanglement and the swapping of entanglement over long distances. In all these activities, researchers from IJS will participate, at first to learn about techniques how to implement quantum communication protocols and later to help implement additional nodes for IJS, for demonstration purposes, and for nodes connecting government institutions.

The project will benefit from the availability of the field-proven (developed by BSC) XIPHRA line of high assurance hardware encryptors that are accredited for protection of national, EU and NATO classified information. These will be extended with appropriate interfacing with QKD and additional post quantum security measures in a way that will guarantee (regardless QKD) no worse security than that of already deployed XIPHRA devices. Many QKD projects start with QKD system that gets coupled with “some” symmetric encryption functionality (that is often software only, but usually not accredited). SiQUID will start with already field proved design of hardware encryptor and extend its security guarantees with those uniquely offered by QKD. We believe that such an approach is needed to convince security demanding end users to seriously consider QKD systems for critical production use.

BSC also has a number of technological building blocks available that may be reused or extended in context of SiQUID, including PCB modules with FPGAs, time precise synchronization IP, various hardware (RTL) IP, silicon proven secure boot IP, quantum random number generator, hardware true random source with DRBG, etc. These, together with experience of designing (side channel) secure, industrialized complex electronics systems will be beneficial in the design and industrialization of QKD devices.

Describe the measures planned to ensure that the project implementation is of high quality and completed in time.

Describe the methods to ensure good quality of monitoring, planning and control activities.

Describe the evaluation methods and indicators (quantitative and qualitative) to monitor and verify the outreach and coverage of the activities and results. The indicators proposed to measure progress should be specific, measurable, achievable, relevant and time-bound.

The project management will be handled at FMF by A. Ramšak (AR) as **Project Coordinator**, B. Dorić (BD) as Project Manager and R. Kaltenbaek (RK) as **Scientific & Technical Coordinator**. All three have ample experience in the administrative and scientific management of national and international research projects. BD leads the research & development and project office at FMF. AR and RK have been the PIs of numerous successful national and international research projects. AR currently is the vice rector of the University of Ljubljana and, until very recently, he was the dean of FMF. Since 2020, he has been the project lead of a bilateral (Croatia-Slovenia) research project on quantum communication. AR and RK managed the Slovenian part of the demonstration of QKD between Italy, Croatia and Slovenia during a G20 meeting in Trieste.

Management structure, milestones and procedures:

Consortium Board (CB): The CB is the primary and top-level decision-making body responsible for the overall strategic and technical planning and control. It includes the Project Coordinator, the Project Manager, and one representative per partner. The CB is chaired by the Project Coordinator. The CB meets at the project start and at least once per quarter. These meetings can be arranged via video conferences. The CB decides on: (i) Work plan changes, agreed by the funding agency (FA); (ii) Changes to the Consortium Plan; (iii) Transfer of budget and work between partners; (iv) Approval of reports to the FA.

Coordinator: FMF has the overall responsibility for project implementation, management, administrative, financial matters and liaison with the FA. The Coordinator will: (i) Monitor compliance with obligations by the Partners; (ii) collect information on progress every 3 months via a progress sheet and conference call, and, if necessary, propose modifications of the Work Plan to the CB; (iii) Collect, review and submit reports; (iv) Prepare CB meetings; (v) Administer FA financial contributions to partners;

Project Manager: B. Dorić (BD) is an experienced project manager to support the Project Coordinator. They will handle administrative/financial aspects of the project, coordinate the content and timing of communication and participation in events.

Work Package Leaders (WPL): are responsible for executing activities in their respective WPs. Each WPL establishes a detailed WP schedule, monitors progress, and organizes regular WP teleconferences (e.g., monthly or bi-monthly) with all partners involved.

Risk monitoring: Monthly conference calls will be organized with all partners to assess risks and monitor delays. The coordinator will maintain a register assessing external/internal risks for project implementation (technology, scientific, acquisition, security, performance). It will be updated every 3 months together with the progress sheet.

Quality assessment: The WPLs are responsible for the quality and completeness of the deliverables prepared in their respective WPs. Project deliverables are prepared on the corresponding task at WP levels and validated by the corresponding WPL before they are presented to the CB for approval.

Conflict resolution will first occur at WP level before going to the higher project level: from task to WP, from WP to Project Coordinator and CB, where WPLs will act as mediators.

Rights management: The Project Coordinator is very experienced with project organisation, and they will be in close contact with industrial consortium members and with legal counsel with respect to rights management. Intellectual-property (IP) ownership terms will be detailed in the Consortium Agreement and signed by all members. Due to clear separation of work responsibilities in the project it is expected that IP delineation between consortium members will be straight forward. Entities will retain the freedom to enter into individual to party or multi-party IP agreements. Notably, when work is carried out jointly by several partners, with no prior agreement and with no possibility to ascertain their share, joint ownership of the foreground IP will apply. FMF will perform IP audits as deemed necessary to identify IP origin, ownership, and exploitation potential of created results. For each result, protection options will be proposed and discussed yearly with the objective to maximise knowledge transfer towards scientific and commercial communities.

The project progress, its outreach and results achievements will be monitored through:

- **Milestones** that were selected such that they clearly indicate the state of what was accomplished in the project, roughly "Plan" (MS1), "PoC" (MS2), "Ready for full SiQUID Deployment" (MS3), "SiQUID Fully Deployed" (MS4). More precise description of milestones and means of verification are given in Section 4.2 Work packages and activities.
- **Regular project status updates** monitored at task level, deliverable level, work package level and overall project level.
- **Key Performance Indicators (KPIs)** that were selected to measure progress towards the accomplishment of key project goals independently of milestones, deliverables or status reports of task leads, work package leads and the project leads. K1: measures number of deployed nodes (may not be all operational at the same time), K2: number of member states involved in cross-border collaborations (targeting to cover all neighbouring countries), K3: number of professionals trained due to SiQUID project and K4: Longest link achieved (which will be measured in laboratory environment, by determining the maximum attenuation at which the QKD system still operates and calculating the distance assuming standard 0.2 dB/km fibre attenuation).

KPI	Description	Target M12	Target M24	Target M30
K1	Deployed Nodes	>= 2	>= 4	>= 7
K2	Member states involved	>= 2	>= 4	>= 5
K3	Number of professionals trained	>= 5	>= 10	>= 12
K4	Longest link achieved (assuming 0.2 dB/km fibre attenuation)	>= 10 km	>= 50 km	>= 100 km

Summary of project KPI's is given in the table above.

Cost effectiveness and financial management *(n/a for prefixed Lump Sum Grants)*

Describe the measures adopted to ensure that the proposed results and objectives will be achieved in the most cost-effective way.

Indicate the arrangements adopted for the financial management of the project and, in particular, how the financial resources will be allocated and managed within the consortium.

⚠ *Do NOT compare and justify the costs of each work package, but summarize briefly why your budget is cost effective.*

The key approach to achieving cost effectiveness will be based on utilizing the previously acquired knowledge, experience and results, specifically the research work and experiments on quantum technologies (FMF, IJS), the accredited high-assurance network encryptors (BSC) and expertise on security guidelines and standards (URSIV, UVTP).

The project plan was developed by identifying the required work to reach the SiQUID objectives and then assigning the resources where they are most efficient. We went through several optimization rounds to maximize cost effectiveness.

The equipment and the material to be bought in this project will only be what is essential to (a) implement a sufficient number of QKD nodes to connect multiple locations of the government institutions participating in the project consortium, (b) to demonstrate QKD over long distances to illustrate the potential for implementing a Slovenian quantum backbone, (c) to demonstrate QKD links to nodes close to the borders with neighbouring countries, and (d) to enhance Slovene experience in preparation for advanced applications of quantum communication, implementing future-safe and state-of-the-art quantum-communication.

We will first implement a BB84-based QKD link to serve as the blueprint for the implementation of additional links and protocols in this project, and it will serve as the basis for attempts to ruggedize/industrialize our implementation of this protocol. We will replicate this design several times to implement multiple nodes of a QKD network within this project. In addition, we will implement two long-distance links based on the same technology but using state-of-the-art superconducting nanowire single-photon detectors (SNSPDs) to increase the range of the protocol used. In addition, we will implement a demonstrator of measurement-device-independent (MDI) QKD. The senders in this protocol will use the same technology as for the BB84 links to minimize the resources required. MDI QKD also promises an increased range and an increased level of security. We will implement this demonstration with SNSPDs to achieve optimal performance. To train young researchers and stake holders in Slovenia on advanced quantum applications and future-proof technology, we will also implement bright sources of entangled photons, we will aim to distribute the entanglement over long distances using SNSPDs, and we will aim to perform a proof-of-principle demonstration of entanglement swapping over long distances, which will be the basis for future quantum-repeater-enhanced quantum networks.

The SNSPDs used for these demonstrations will be mobile such that we can demonstrate long-distance links between different nodes of the Slovenian quantum network in a time-multiplexed fashion. In total, there will be three sets of SNSPDs to allow implementing three long-distance links using varying protocols. Having three such links will allow demonstrating a small-scale long-distance network with multiple nodes with the potential of connecting key locations in Slovenia like, e.g., Ljubljana, Postojna, Celje and Maribor.

Another key part of the costs of the project are personnel costs. We ensured the cost effectiveness of these costs by discussing beforehand with the consortium partners the best way of splitting personnel resources. For example, we will have one postdoctoral researcher employed by IJS but effectively working at FMF to be trained on the techniques required for implementing the quantum networks. This way, that researcher will directly contribute to the workload of FMF while gaining expertise to later train young researchers at IJS and to help them implement the nodes at IJS and to distribute the nodes in the field at a later stage. Similarly, researchers from FMF and IJS will work closely with engineers from BSC to share knowledge and expertise between those partners. BSC will contribute expertise in the industrialization of the implemented nodes, while FMF and IJS will contribute share expertise in quantum technology and quantum communication. The researchers of FMF and IJS will also train key personnel at UVTP and URSIV in these technologies and instruct them in using the equipment built during this project on dedicated experimental demonstrators. Based on these instructions, the key personnel will later be able to operate the QKD nodes at UVTP and URSIV and to instruct other personnel.

The budget is focused on maximizing the project contribution towards building national and EU Quantum Communication Infrastructure, Expertise and Capabilities. The allocation of the overall resources is: 46% for personnel, 34% for equipment, 10% for material, 7% overhead and the rest for the rent of optical fibres, for services in the context of installing nodes at government locations, for travel costs, etc.

Most of the budget is allocated to the personnel implementing the project, which includes young researchers and engineers that will be trained in quantum technologies. Another significant amount of the budget will be for equipment that will be necessary to implement the QKD links. For example, this contains superconducting nanowire single-photon detectors (SNSPDs), which will be essential for testing the feasibility of implementing long-distance or high-bandwidth links. We will also use them for tests of advanced quantum technologies like measurement-device-independent QKD, which promises higher security and a longer range for QKD. Moreover, we will test the long-distance distribution of entanglement and entanglement swapping. This will be key for future full-scale quantum networks, and it will be crucial to train researchers and engineers in Slovenia in these future technologies. The budget reserved for the rental of optical fibres will be essential to ensure that we will be able to implement semi-permanent or quantum network links in Slovenia.

The equipment in this budget is the minimum required to achieve the described objectives. Because of the high costs of this equipment, and because we will buy it specifically for this project, will claim these equipment costs under the fully capitalized equipment-cost scheme.

Of this, besides TEMPEST equipment which important for security aspects of QEE, 25% will be for governmental nodes and a link to the industrial consortium partner BSC. 47% will be for the demonstration of long-distance links from Ljubljana to other cities in Slovenia and to locations close to the borders with neighbouring EU member states (Austria, Croatia, Hungary, and Italy). 28% will be for the testing of advanced quantum communication protocols like MDI QKD and the distribution and swapping of entanglement over long distances.

Most of the project budget (63%) will be used for the development of the QEE, the deployment of a quantum network to connect multiple government nodes, and to test advanced QKD protocols (MDI QKD)-WP3. This will address many of the main objectives of the call. In addition, the development of entanglement sources and the long-distance distribution of entanglement (WP4) will require 13% of the budget, and 7% of the budget will be used for deploying long-distance connections from Ljubljana to other cities in Slovenia and to locations close to the borders to neighbouring countries (WP5). 4% of the budget are planned for personnel costs in WP1 for project coordination. 5% of the budget are planned for WP2 to design the quantum network architecture, the requirements etc, and 8% of the budget are planned for dissemination, exploitation, communication, and impact creation in WP6.

Critical risks and risk management strategy

Describe critical risks, uncertainties or difficulties related to the implementation of your project, and your measures/strategy for addressing them.

Indicate for each risk (in the description) the impact and the likelihood that the risk will materialise (high, medium, low), even after taking into account the mitigating measures.

Note: *Uncertainties and unexpected events occur in all organisations, even if very well-run. The risk analysis will help you to predict issues that could delay or hinder project activities. A good risk management strategy is essential for good project management.*

Risk No	Description	Work package No	Proposed risk-mitigation measures
R1	(low) A consortium partner or a key member of a consortium partner leaves the project.	WP1-WP6	In case a key member of a consortium partner leaves the project, the consortium partner will aim to replace that member to fulfil its obligations within the project. If that is not possible, other consortium partners will aim to take over the responsibilities of that consortium partner impacted by this change. If a consortium partner leaves the project, the remaining consortiums partners will aim to take over the effort, and they will evaluate the possibility of subcontracting in the affected parts or the project, including costs and possible delays. If no viable options are found, the project objectives affected will be adapted or dropped.
R2	(medium) Failure to secure required materials and equipment in time	WP3-WP5	The consortium partners will look for possible alternative equipment or alternative suppliers. Ideally, the respective equipment and material should allow achieving the targeted system performance. If this is not possible, we will aim to find equipment/material with comparable performance. If that is not possible, we will look for possible alternatives from non-EU sources and precisely document the cause of the failure (delivery times, lack of performance, non-availability from EU

			sources, …). If no alternative can be found, the objectives of the project will be adapted
R3	(medium) technical issues limit the targeted performance of the quantum-communication protocols as defined in WP2.	WP3-WP5	Fall back to more basic quantum-communication protocols. For example, if the MDI QKD approach does not work, fall back to BB84-based QKD. If the long-distance distribution of entanglement does not work, fall back to shorter link distances and introduce intermediate trusted nodes. If the envisioned lower-cost QKD nodes do not work, fall back to established receiver technology comparable to the demonstration at the G20 event in Trieste. If we can only achieve the targeted performance for a small number of nodes, use them in a time-multiplexed way to test the feasibility of a larger-scale quantum network.
R4	(medium) Difficulties with securing affordable access to dark fibres to connect the network nodes. The price for renting fibre connections might be too high.	WP2	The goal will be to ensure fibre access for the duration of the project or at least for the duration of the field tests envisioned. If possible, we will aim to get in-kind access to these fibre by highlighting the contribution of the providers in publications and in online reports. To mitigate this risk, we allocated funds in the budget to cover potential costs for fibre access. To keep within this budget even in the presence of high rental prices, we can reduce the time we need the fibres by testing individual links in a time-multiplexed fashion with the goal of minimizing the overall costs for the fibres required. Alternatively, we can adapt our network topology to avoid overly expensive connections.

2.3 Capacity to carry out the proposed work

Consortium cooperation and division of roles (if applicable)

Describe the participants (Beneficiaries, Affiliated Entities and Associated Partners, if any) and explain how they will work together to implement the project. How will they bring together the necessary expertise? How will they complement each other?

In what way does each of the participants contribute to the project? Show that each has a valid role and adequate resources to fulfil that role.

***Note:** When building your consortium you should think of organisations that can help you reach objectives and solve problems.*

The consortium was assembled with the goal for the partners to complement each other and to have a good mix of (I) quantum & research expertise (FMF, IJS), (II) industrial research and development (BSC) and (III) security and network deployment expertise (UVTP, URSIV, BSC, IJS). The work on the project will be performed collaboratively, with contributions from multiple entities to most tasks.

FMF: The FMF has a fully functional quantum-optics laboratory led by R. Kaltenbaek (RK). RK has ample experience in quantum communication, the distribution of quantum information and entanglement over long distances via free-space and fibre links, and with quantum technology in space. RK is well connected internationally with leading research groups in quantum communication and quantum technology, and he has close contacts to space industry and space agencies in Europe, and in the US. RK was hired by the FMF in 2019 to bring expertise in quantum technology to Slovenia, to perform high-impact state-of-the-art research, and to train the next generation of young researchers in those topics. RK's "quantum optics and quantum foundations" laboratory was built from scratch and to state-of-the-art specifications.

The laboratory became fully operational in 2020, and several students have already been training on quantum-optics experiments for some time by now. In 2021, AR and RK and one of RK's PhD students actively participated in the first demonstration of QKD between three European countries – a pilot realization of part of a future EuroQCI network. This demonstration itself as well as initial characterization measurements of the long-distance fibre links relied on equipment from RK's laboratory and the active participation of RK's team. This experience will allow RK and AR to provide essential input to the planning and the definition of the specifications of the network architecture (T2.1 and T2.2), and RK's past experience with experimental quantum communication, and his close contact with experts in other countries (to name a few, in Austria, Croatia, Italy, Hungary, and in the Netherlands) will provide a sound foundation for achieving the interoperability of QKD protocols between member states of the EU (T2.3).

The experience gained in that demonstration experiment in combination with RK's long experience with quantum communication protocols and experiments will provide a firm foundation for the realization of the QKD nodes and links for the present project. We already defined a rough layout of the setups to better estimate the components we will need to order, to get the quotations and to define the number of components needed.

For the more advanced test setup for MDI QKD (T3.3), we based the design to a large part on the first BB84 QKD nodes. That means, at this point, we will be able to count on additional experience gained during implementing the initial BB84 setup. The most important additional effort in MDI QKD is a two-photon measurement at a central of three nodes. This type of measurement is a simple version of Bell-state measurements that RK often used in past experiments, e.g., for entanglement swapping, quantum teleportation, and in the preparation of multi-photon entanglement.

Another advanced quantum communication protocol we will implement is the generation of entanglement in multiple entanglement sources (T4.2 and T4.3) and the distribution of that entanglement over large distances (T4.4). All these are things that RK demonstrated in many experiments in the past. In particular, RK's master thesis was on quantum state teleportation over long distances, and he contributed to the first long-distance free-space distribution of entanglement. RK's PhD thesis was on building multiple high-fidelity entanglement sources and using them for entanglement swapping. We will build on that experience in Task T4.4 for the distribution of entanglement over long distances, and when attempting to demonstrate entanglement swapping with the entanglement sources we will implement at FMF and IJS. During his PhD and his first employment as a postdoctoral researcher, RK designed and built several high-fidelity sources of entanglement for quantum communication and for quantum computation.

Based on past experience and on experience gained during the implementation of the QKD protocols in WP3, AP and RK will be well placed to provide scientific and technical advice for the deployment of the QKD nodes in WP5. RK's team of young researchers at FMF will by this time be well trained in quantum communication, and in the implementation and handling of QKD nodes. They will actively support the teams from IJS and BSC in the deployment of QKD nodes (T5.4) and in the characterization and monitoring of the nodes (T5.4).

At the Faculty of mathematics and physics, the field of quantum mechanics is well represented on all levels of study. In particular, in the second year of study in Modern physics and the third year, Quantum mechanics is an important subject. At the master level, quantum mechanics continues in Advanced quantum mechanics, Quantum optics and Quantum field theory. Also, in the PhD programme of physics, quantum mechanics represents the main field. In SiQUID several master students will be included along with planned 3 PhD students. Throughout the project, we will train the master students, the young researchers, and engineers in quantum technologies, and we will train key personnel at the government nodes in the operation of the QKD nodes we will implement (T6.3).

The experience of the FMF team in designing and implementing the core equipment for the QKD nodes and for advanced quantum communication protocols will be ideally supplemented by the other consortium partners.

IJS: The Jožef Stefan Institute (IJS) is the leading Slovenian scientific research institute, covering a broad spectrum of basic and applied research. The research staff of more than 850, working in 28 research departments and several centres, has a broad range of expertise in natural sciences, life sciences and engineering. IJS brings a broad range of knowledge and expertise in the project through participation of three research departments: Laboratory for cold atoms, Department of communication systems and Laboratory for open systems and networks.

In particular, the Laboratory for cold atoms at IJS led by Peter Jeglič will be involved in proof-of-concept and experimental tasks (T3.2, T4.2 and T4.4). Together with FMF they will implement two academic nodes for QKD at IJS. The first node will be located in the vicinity of FMF, whereas the second node will be located next to the Laboratory for cold atoms at Reactor Center Podgorica, about 12 km northeast of Ljubljana. The lab infrastructure already fulfils the highest possible standards for highly complex and sensitive experimental equipment including optical tables, air-sock air-conditioning, dedicated electric power supply and ultra-high vacuum chambers with optical access (pressure in the 10^-11 mbar range). The estimated total investment of 1 million EUR was provided by Slovenian Research Agency research programmes and projects. One of their experimental setups is dedicated to development of atom-based quantum memories, which are the basis for advanced QKD and beyond-QKD protocols.

The Department of Communication Systems (DCS) will contribute with its expertise in traditional communication networks and protocols, as well as in prototyping and piloting networking solutions, mostly based on the experience obtained in EU FP and H2020 projects. The core expertise of the department is in research, development and design of next generation communication networks, technologies and services; embedded and sensor systems; and parallel and distributed computing. DCS will be first involved in definition of use cases and network architecture specification and planning (T2.1), interoperability between traditional and quantum network as well as between networks in neighbouring countries (T2.3). It will support the deployment (T5.3) and monitoring (T5.4) of the QKD network and investigate its applicability in critical infrastructure related use cases (T6.2).

The Laboratory for open systems and networks has a long tradition of supporting applications of advanced networking and security technologies in national, European and worldwide experimentation and piloting. The Laboratory primary expertise is in applied cryptography, information security, privacy and critical infrastructure protection. The laboratory will be involved in use cases collection and system security requirements elicitation from T6.2 to tasks T2.1, T2.2 and T5.1. The Laboratory will assess risks of QKD technology introduction and interconnection with existing security systems and propose needed adaptations to existing security policies to mitigate the risks. Theoretical assessment will be supported through T4.1. End user prioritized use cases will be studied for implementation through work in T6.2. Laboratory will support QKD network deployment in T5.3.

BSC: Beyond Semiconductor is electronics research and development company that is licensing its general purpose, security and signal processing technologies to many of the worlds most recognized semiconductor corporations.

Some of the company's products based on its technology include network encryptors accredited for protecting national, EU and NATO classified information. The company is active in NATO CIS3 Partnership and participates in NATO SCIP (Secure Communications Interoperability Protocol) and NINE (Network and Information Infrastructure Internet Protocol Network Encryption) working groups.

Main products are network encryptors, data diodes, thin clients and other devices for protection of classified information and products in the field of semiconductor intellectual property (IP), including 32-bit processors, security and cryptographic IP cores, image and video compression IP, GPS IP, communication and digital signal processing IP.

Beyond Semiconductor has expertise in PCB design, FPGA and ASIC design, embedded software, security and functional safety.

BSC will provide its know-how to design and develop certifiable QEE devices and will (I) aim to integrate the secure keys generated via QKD with their classical cryptography modules, (II) provide their expertise in designing TEMPEST-proof solutions, and (III) provide expertise in designing field-programmable gate-array (FPGA) boards for controlling the laser diodes and active optical elements in the QKD senders and receivers. As an alternative option for short-distance and low-bandwidth links, we will also investigate together with BSC (IV) the feasibility of building cheaper QKD nodes based on cheaper, off-the-shelf components. Ideally, this would allow such nodes will be built in Slovenia using local expertise and adding to the portfolio of European expertise in quantum technology.

URSIV: The Slovenian Government Information Security Office (URSIV) is the national information security authority and the single point of contact for cross-border cooperation with the relevant authorities in other countries. URSIV coordinates stakeholders in the national cybersecurity system. URSIV is also the national cybersecurity certification authority and the national coordination centre for cybersecurity and it incorporates the Government CERT. URSIV will provide security guidelines for the identified node locations, as well the project documentation for the national part of project financing and reporting to Slovenian authorities. Marjan Kavčič is the Slovenian Sherpa in EuroQCI.

The personnel budget assigned to UVTP and URSIV is relatively small because they will be participating mainly in security advisory roles and liaison roles to other governmental institutions involved in deployment. However, their contribution is critical for the project goal to address public and critical infrastructure use cases and show the path to designing of QEE devices that can surpass the security guarantees offered by the classical means.

UVTP: The Slovenian Government Office for the Protection of Classified Information (UVTP) leads the development and implementation of physical, organisational and technical standards for the protection of classified information by state authorities and organisations. UVTP will offer its expertise to provide guidelines for security aspects of QKD solutions and thus streamline their development. It will also assist in providing security guidelines and connectivity to the identified node locations. Mojca Mikac is a member of the EuroQCI Security Group.

Project teams and staff

Describe the project teams and how they will work together to implement the project.

List the staff included in the project budget (budget category A) by function/profile (e.g. project manager, senior expert/advisor/researcher, junior expert/advisor/researcher, trainers/teachers, technical personnel, administrative personnel etc. and describe briefly their tasks.

Name and function	Organi-sation	Role/tasks/professional profile and expertise
Anton Ramšak	FMF	Project lead, Professor of physics, teaching Quantum mechanics at Physics department of UL FMF. For the last two decades, he has been conducting research on the theory of quantum nanoscopic systems, more specifically on the physical properties of quantum dots and quantum wires, the generation of quantum entanglement, the manipulation of quantum bits and quantum phases, and the properties of topological insulators. He has also investigated the phenomenon of quantum entanglement in the context of interpretations of quantum mechanics. He has led the Slovenian research group in several international and domestic projects. For the term 2021-2025 he is Vice-Rector for research and development at the University of Ljubljana.
Rainer Kaltenbaek	FMF	Scientific and technical lead, head of the Quantum Optics and Quantum Foundations Laboratory at FMF. Research in quantum technology, quantum communication, quantum optomechanics, optical trapping, and fundamental tests of physics. Experience in long-distance quantum communication, advanced quantum communication protocols, optical quantum computing, quantum

		sensing and quantum technology in space. Principle Investigator of the MAQRO proposal for a space mission to test quantum physics with high-mass test particles.
Primož Potočnik	FMF	Senior researcher, head of the national ARRS programme “Computationally intensive methods in theoretical computer science with applications”. Expertise in the mathematical theory of networks (graphs) and the study of symmetry in combinatorial objects, including connections with coding theory. His many influential works include a computer-based generation of exhaustive datasets of highly symmetrical network models.
Tilen Marc	FMF	Senior researcher with PhD in mathematical theory of networks and research expertise in cryptography, with scientific publications researching classical and post-quantum cryptographic schemes. Experienced as a senior software developer with a focus on security. Coauthor of cryptographic libraries for functional encryption and zero-knowledge proofs. Leading Slovenian research group in European H2020 projects KRAKEN and ARCADIAN-IoT.
Enej Ilievski	FMF	He obtained a PhD in theoretical physics (University of Ljubljana, 2014). He has been working in the areas of quantum statistical physics and mathematical physics for more than a decade, with main expertise in the topics of complex many-body phenomena, dynamical systems out of equilibrium, quantum transport and open systems with dissipation.
Barbara Dorić	FMF	Project manager, administrative personnel. She has ample experience in planning, monitoring and reporting on individual projects. Also experienced in preparing applications for public calls for tender. She has worked on and coordinated many research projects.
Rok Žitko	IJS	Senior researcher, head of the national ARRS programme "Physics of quantum technologies". Computational scientist in quantum many-body theory with experience in large-scale computer installations and (classical) network deployments. Experience with quantum device measurement theory, control systems, digital electronics, and FPGAs. In this project he will have an advisory role.
Peter Jeglič	IJS	Senior research fellow, head of Laboratory for cold atoms. He has 10 years of experience in cold-atom technology and more than 20 years in experimental physics with magnetic resonance techniques. In 2012, he founded the Laboratory for cold atoms with the goal of building a system for the preparation, manipulation, and detection of ultra-cold caesium atoms and molecules. In 2016, his group achieved the first Bose-Einstein condensation in South-Eastern Europe. In parallel, his team entered the field of quantum sensors and devices by starting to develop caesium magnetometers and quantum memories.
Denis Arčon	IJS	Senior research fellow, head of Solid-state physics department and Programme leader for “Physics of quantum and functional materials” research programme, full professor at UL-FMF. He is internationally recognised researcher in the field of quantum materials and has published more than 200 articles in international journals, has around 4500 citations and h-index of 33. He has over 20 years of experience in leading national and international (EU, NATO) projects.

Erik Zupanič	IJS	Senior researcher with over 20 years of experience in designing and building novel scientific equipment, e.g., cold atoms experiments, atom magnetometry, UHV and LT SPMs, MEMS based sensor systems etc. He is head of the Scanning probe microscopy lab at IJS and ass. prof. at the University of Ljubljana.
Mihael Mohorčič	IJS	Scientific Counsellor and head of the Department of Communication Systems. He has more than 25 years of research experience in communication networks, protocols and services, including in experimental testbeds and piloting in national and more than 15 Framework Programme projects since FP4.
Gregor Cerar	IJS	Postdoc researcher at the Department of Communication Systems with PhD in Information and Communication Technologies obtained in 2021. He has more than a decade of experience with Linux systems and 5+ years of experience in networking technologies, and is a Certified Cisco Network Associate (CCNA), having obtained certificate levels CCNA 1-3.
Dušan Gabrijelčič	IJS	Senior researcher, more than 25 years of experience in securing internet applications, applied cryptography, privacy, critical infrastructure protection and systems specification, development, implementation and piloting. He has been working in research, innovation and piloting on European level and projects since Framework Programme 5. He is author of number of scientific publications.
Samed Bajrić	IJS	He received the Ph.D. degree in mathematics from University of Koper in 2014. His main research interests include cryptology and in particular symmetric-key cryptography with emphasis on the design of cryptographic Boolean function. He is currently with Laboratory for Open Systems and Networks.
Tomaž Klobučar	IJS	Senior researcher and head of the Laboratory for Open Systems and Networks with more than 25 years of experience in cybersecurity research and development. He coordinated two CEF projects and participated in 15 EU projects from the cybersecurity domain.
Matjaž Breskvar	BSC	Lead architect of many BSC products, including several XIPHRA encryptor products, security related semiconductor IPs and multiple processor architectures. He has more than 25 years of experience in Linux, Networking and cyber security. He will mainly contribute to high level architecture and, as required, be involved where technical challenges arise.
Jure Ciglič	BSC	Technical lead responsible for FPGA logic design of XIPHRA encryptors and numerous semiconductor IP blocks, including secure boot for leading video processing ASIC and video link authentication for automotive application. He will contribute to QKD logic design and hardware aspects of integration of QEE.
Aleksandar Lukić	BSC	Chief security officer, oversees accreditation of company’s XIPHRA encryptor products. Co-designer and developer of hardware-accelerated cryptographic primitives, more than 20 years of experience with the development of communication systems and embedded software. He will manly contribute to tasks with security impact and security assessments.

Rok Pirnat	BSC	Technical lead in numerous complex printed circuit board (PCB) design including for complete XIPHRA product line. Supervised the design of hardware based true random number generators (TRNG) and quantum random number generator (QRNG) and lead the effort to achieve required TEMPEST protection of selected XIPHRA products. He will contribute mainly to industrialization efforts, time synchronization, mechanical design and development and analysis of TEMPEST protections.
Mitja Pufič	BSC	Senior engineer with more than 20 years of Linux, Networking and security experience. Managed deployment and maintenance of several complex mission critical systems. He will contribute mainly to SiQUID planning, architecture and deployment.
Marjan Kavčič	URSIV	Head of Raising Resilience Division at URSIV, Slovenian Sherpa in EuroQCI. He headed the preparation or prepared several national strategic documents (the National Cybersecurity Strategy of 2016, the Information Security Act of 2018, the first National cybersecurity threat analysis of 2018). He is primarily involved in capacity building in the field of cybersecurity. He will provide expertise for guidelines for security aspects of QKD solutions and assuring the coordination with appropriate national institutions.
Mojca Mikac	UVTP	Senior Adviser, Member of the EuroQCI Security Group, she will offer her expertise to provide guidelines for security aspects of QKD solutions.

Outside resources (subcontracting, seconded staff, etc) *If you do not have all skills/resources in-house, describe how you intend to get them (contributions of members, partner organisations, subcontracting, etc.) and for which role/tasks/professional profile/expertise* *If there is subcontracting, please also complete the table in section 4.*
During the course of the project, the goal will be to involve master students in the project to train the next generation of quantum scientists and quantum engineers in Slovenia. In particular, we will aim to always have one master student involved in all aspects of the implementations of the various QKD and quantum-communication solutions we aim to implement in this project. In particular, that means involvement in T3.2 for the implementation of the BB84 node and in designing the experimental implementation of MDI QKD. This will be followed by the implementation of an MDI QKD demonstration in T3.3, One more master student will be trained in the course of the development of a state-of-the-art source of bright entanglement in T4.2, and in the implementation of that source of entanglement (T4.3), and in the demonstration of entanglement distribution and entanglement swapping (T4.4). At any time during the project, this will mean the involvement of at least two master students in RK's group at the FMF: These students will be trained by RK, and by young researchers in his group (the two postdoctoral researchers and the three PhD students). This will be an important part of task T6.3 to train a new generation of scientists and engineers in quantum technology. While we have already been in contact with several telecom companies in the past to temporarily get access to dark fibres for the QKD demonstration for the G20 event, the requirements for the present project will be different, and we will be in close contact with telecom companies in the course of defining the network architecture (T2.1). We will aim to ideally get free access at least to some dark fibres for testing links within Slovenia and within the metropolitan area of Ljubljana. At the same time, we will aim to discuss the possibility of semi-permanent or permanent access to fibre links. At the very least, we will need access to the fibres for the duration during which we will test long distance links to nodes close to

neighbouring countries and within Ljubljana to connect the planned government nodes. In those cases where we cannot get specific fibre links for free, we will aim to find possible alternate routes or to rent the fibres for as long as needed for this project.

In particular for the connection of the government nodes as well as for the future connection to an optical ground station, we will attempt to find semi-permanent or permanent solutions, and we reserved some budget within this project to cover the costs of renting dark fibres.

Consortium management and decision-making risk(if applicable)

Explain the management structures and decision-making mechanisms within the consortium. Describe how decisions will be taken and how regular and effective communication will be ensured. Describe methods to ensure planning and control.

Note: *The concept (including organisational structure and decision-making mechanisms) must be adapted to the complexity and scale of the project.*

The project management will be led by FMF. The administrative tasks will be led by B. Dorić, who is the head of research & development and project office at FMF, and the project coordination will be led by A. Ramšak with support by R. Kaltenbaek in scientific and technical questions. This core team at FMF will be in close contact with teams at the other consortium partners in order to coordinate the project management, the writing of reports, the scientific dissemination and the acquisition of equipment.

The team at FMF will coordinate the action via regular meetings, and it will collect regular updates from the other consortium partners to monitor the progress of individual tasks and work packages. This will be used for risk management as well as for dissemination purposes (e.g., updating the project website and social-media feeds). In particular, the FMF team will contact all team leaders weekly via e-mail to collect the latest progress estimates, and to keep track of the occurrence of any challenges in the fulfilment of the individual tasks and work packages.

The team leaders and key personnel of the consortium will be invited to monthly meetings by the FMF team to discuss updates on the progress of work packages, on acquisitions and collected progress statements from team members. This will be shared in a newsletter among team members. This newsletter will form the basis for monthly updates on the consortium website and in social-media channels.

3. IMPACT

3.1 Expected outcomes and deliverables — Dissemination and communication

Expected outcomes and deliverables

Define and explain the extent to which the project will achieve the expected impacts listed in Call document.

The link to the deliverables as a way to measure progress towards expected outcomes and connection to expected impacts listed in Call document is presented by linking expected outcomes (this section) with objectives (in section 1.1), which are further linked to deliverables and the Call document expected impacts.

<u>Expected Outcome 1 (deployed experimental networks)</u>**: Deployed initial experimental QKD networks enabling experimentation with advanced QKD & quantum network concepts and use cases, established contacts and plans for cross border QKD connections, all contributing to increased readiness for the full deployment of the EuroQCI.**

This outcome will be realized by SiQUID mainly by a combination of the following project objectives:

- **Objective 1 (architecture and EuroQCI integration):** Addresses requirements elicitation and planning to facilitate experimental deployment and integration with EuroQCI, including planning of cross border links and interoperability aspects.

- **Objective 3 (industrialization):** Addresses design and development of experimental QEE focused on ease of manufacturability, integration, robustness, cost, and other industrialization aspects that are of key importance for large-scale deployments.
- **Objective 5 (deploy and integrate):** Provides deployed QEE nodes that integrate with existing communication infrastructure.
- **Objective 6 (measurements and lessons learned):** Enables real-world end user experimentation, while running realistic public, academic and critical infrastructure use cases. Such real-world feedback, measurements and lessons learned are critical to prepare for the future large-scale EuroQCI deployments.

<u>Expected Outcome 2 (national high assurance QEE)</u>: Experimental nationally produced high assurance QEE leveraging components sourced (in order of priority) nationally or from EU, NATO and if necessary other allied & democratic countries. Contribution to strengthened European quantum communication autonomy.

This outcome will be realized by SiQUID mainly by a combination of the following project objectives:

- **Objective 2 (improved security):** Addresses the key requirement of QEE: increase of data security stemming from application of quantum technologies, while paying attention that such improvements are not jeopardized by integration with “classical” encryptor, its implementation or side channel leakages.
- **Objective 3 (industrialization):** Addresses the practicality of large-scale deployments of QEEs. While improved security is welcome, it is also important to minimize impact on reliability, cost, manufacturability and other industrialization aspects of QEE.
- **Objective 4 (autonomy):** Improves security of supply of QEE, both from perspective of availability (assurance of QEE device supply) and its trustworthiness (assurance of authenticity and non-maliciousness of used components). Also, prioritizing sourcing of components from national and EU suppliers strengthens such suppliers and provides incentives for new players to enter the market thus strengthening European quantum technology autonomy.
- **Objective 7 (grow national expertise):** Strengthens Slovenian quantum communication industry and reduces reliance on non-European actors.
- **Objective 6 (measurements and lessons learned):** While there will be limited time to incorporate lessons learned in the SiQUID into QEE the gathered information will help shape the roadmap for future improvements contributing to QEE relevance, thus strengthened European quantum technology autonomy and contributing towards future large-scale EuroQCI deployments.

<u>Expected Outcome 3 (EuroQCI readiness and new trained professionals)</u>: Improved preparedness of Slovenia for the full EuroQCI and high security data network deployments with sufficient number of new professionals trained in quantum communication and secure data networks.

This outcome will be realized by SiQUID mainly by a combination of the following project objectives:

- **Objective 7 (grow national expertise):** Addresses requirements of Slovenia for the design and deployment of next generation of highly secure communication and data networks.
- **Objective 6 (measurements and lessons learned):** Lessons learned, gathered measurements and other information obtained running experimental SiQUID networks will help Slovenia to prepare for the future large-scale EuroQCI deployments.
- **Objective 4 (autonomy):** Addresses the need to have reliable and trustworthy source of QEE for future large-scale deployments. Prioritizing sourcing of components from national and EU suppliers strengthens such suppliers and provides incentives for new players to enter the market thus strengthening Slovenian quantum communication industry and contribute towards European quantum technology autonomy.
- **Objective 3 (industrialization):** Addresses the need for deployment optimized (cost effective, manufacturable in quantities, …) QEE to support future large-scale EuroQCI

deployments while at the same time providing opportunity to train new professionals "on the job".

- **Objective 2 (improved security):** Addresses the projected security requirements of the future large-scale EuroQCI deployments.
- **Objective 1 (architecture and EuroQCI integration):** Addresses network architecture, requirements and plan for future integration with large-scale EuroQCI.

In this project, we will deploy an experimental QKD network in Slovenia in coordination with public authorities, with several research institutions, and with corporate stake holders. We will implement several QKD links connecting government institutions, research institutions and industrial stake holder. In addition, we will investigate the feasibility of integrating the QKD equipment built with existing classical cryptography solutions in order to provide a firm basis for future industrialisation and certification. The core of the deployed network will be based on QKD technology that has been recently demonstrated in the field to show QKD between Italy, Croatia and Slovenia in the course of the G20 meeting in Trieste in 2021. We will improve upon that implementation to increase the range and the security of these core QKD links, and in order to train young researchers and engineers in Slovenia in state-of-the-art quantum technology, and to we will train government stake holders in the use of the QKD solutions implemented.

In addition to those core nodes, we will implement multiple nodes to allow long-distance QKD by (1) using state-of-the-art superconducting nanowire single-photon detectors (SNSPDs), and (2) by demonstrating measurement-device-independent (MDI) QKD using SNSPDs. To prepare Slovenia for future developments in quantum communication, we will also implement state-of-the-art sources of entanglement, distribute that entanglement over long distances and demonstrate entanglement swapping. This will provide Slovenia with field expertise in advanced quantum-communication techniques, and it will provide the basis for future upgrades of the quantum network by integrating it with quantum memories to provide the foundation for augmenting the network with quantum repeaters.

Together with BSC, who have a high level of expertise in providing high-end classical cryptography solutions, we will aim to integrate the quantum links implemented with classical cryptography modules into pilot devices that will form a sound foundation for a future industrialisation of these solutions.

In the course of this project, we will design and optimize the network architecture for the Slovenian quantum network, and we will be in close contact with telecom providers and ARNES to acquire the required optical fibres to connect the nodes of the quantum network at least for the duration of the demonstration experiments and ideally for the full duration of this project from the moment we will be ready to deploy the network nodes.

The network architecture will include connections between several government institutions, and we will demonstrate long-distance connections in order to connect distant key locations in Slovenia (e.g., Ljubljana, Postojna, Celje and Maribor). Moreover, we will demonstrate QKD connections to locations close to the borders of neighbouring countries (Austria, Croatia, Hungary, and Italy). We already made contact with the coordinators of the national deployment efforts in those countries during the proposal phase, and we plan to keep contact with them during the run-time of this project in order to coordinate the locations of the network nodes, to keep each other up to date with respect to the work progress, information on possible European suppliers of equipment, to harmonize the quantum communication protocols used, and to exchange lessons learned. This will facilitate the next steps in deploying a European-scale quantum network.

In order to prepare for the future integration between the terrestrial and space segments of the European Quantum Communication Infrastructure, we have already identified possible locations for a ground station in Slovenia as well as the technical requirements for such a ground station (requirements on the telescope, optical equipment, fibre connections, fast tracking of LEO satellites, issues of light pollution, cloud coverage etc.).

Already in the proposal phase, we contacted many possible suppliers for equipment in order to (a) identify European suppliers, (b) identify equipment where it may be challenging to find European suppliers, (c) get proper price estimates for the equipment to optimize the budget efficiency.

Dissemination and communication of the project and its results

If relevant, describe the communication and dissemination activities, activities (target groups, main messages, tools, and channels) which are planned in order to promote the activities/results and maximise the impact. The aim is to inform and reach out to society and show the activities performed, and the use and the benefits the project will have for citizens

Clarify how you will reach the target groups, relevant stakeholders, policymakers and the general public and explain the choice of the dissemination channels.

Describe how the visibility of EU funding will be ensured.

⚠ *In case your proposal is selected for funding, you will have to provide a more detailed plan for these activities (dissemination and communication plan), within 6 months after grant signature. This plan will have to be periodically updated; in line with the project progress.*

The dissemination and communication activities will carefully consider information to be published. The dissemination and communication will use the following tools to reach members of the public:

- An up-to-date project website
- News-feed to social-media channels (Facebook, Instagram, Twitter, Linkedin)
- Youtube videos of experimental setups and demonstrations
- Press releases to newspapers, television, and radio
- Public demonstrations (QKD demonstration with public stake holders and/or with public participation, entanglement distribution over long distances), to which we will invite journalists and members from public authorities
- News-feed to be provided for the websites of participating public authorities

In addition, we will aim to also reach scientifically interested audience or fellow scientists:

- Scientific publications in high-impact journals
- Collaboration with international partners on joint publications – e.g. reviews or quantum-communication tutorials
- Presentation of results at international conferences/workshops

In order to train young researchers and engineers in Slovenia, and to make them aware of this EU-funded project, we will post regular updates on the newsfeed of FMF and IJS (websites and social-media channels). In addition, we will provide opportunities for students and engineers at collaborating Slovenian companies to visit our laboratories to see the QKD and quantum-communication setups in operation.

To reach representatives of the Slovenian government, we will aim to coordinate demonstration events at government facilities. The activities related to involved government institution will enable to inform the institutions on progress of the project activities and as well to collect relevant feedback from the institutions as end users on target use cases, their implementation and deployment.

The visibility of the EU funding will be ensured on multiple levels. We will mention the EU funding in all public announcements, on the project website, and on our social-media channels. The EU funding will, of course, also be acknowledged in all publications resulting from this activity, we will highlight the EU funding at all demonstration events and in all presentations about the results of this project.

3.2 Competitiveness and benefits for society

Competitiveness and benefits for the society

Describe the extent to which the project will strengthen competitiveness and bring important benefits for society

The implementation of an operational, Europe-wide quantum network will face a number of challenges. Some of these challenges are already identified and addressed by this call itself, which has the main objective to deploy national QCI systems and networks across EU member countries with an outlook for their interconnection in the next step. To be more specific, challenges such as *unbalanced distribution of expertise and knowledge in quantum communications*, *disproportional representation in quantum communication programs across Europe*, and *concentration of ongoing activities in non-widening countries*, are tackled by definition, as these are national projects aiming to reduce the uneven geographical distribution in the level of knowledge, know-how and industrialisation in quantum communications. On the other hand, challenges such as *inconsistent choice of QKD technologies*, *going beyond QKD*, and *standardisation of quantum networks* are those that we are paying particular attention to in SiQUID. Addressing these challenges by a combination of existing EU-sourced and own developed equipment as proposed in SiQUID will strengthen Slovenia's competitiveness in the European region, as well as Europe's competitiveness against other global players in quantum communication and cybersecurity industry.

Without any coordination we can assume that each country will choose different QKD technologies on the national level. This becomes problematic when integrating different QKD approaches (such as continuous variable QKD, discrete variable QKD, trusted-mode concepts or entanglement-based solutions). The challenge is in understanding the advantages and disadvantages of the different technologies and how they can complement each other. In SiQUID, we are addressing this challenge mainly in T2.3. In cooperation with our Austrian, Croatian, Hungarian and Italian colleagues, and their regional and national government representatives and companies, we will aim to align QKD technologies with a vision to enhance Europe’s competitiveness on the global security scene and, eventually, the wealth of industrial products that Europe can offer.

In the near term, quantum networks will primarily serve QKD applications because QKD at this point has a significant higher technological maturity than other quantum communication protocols. Moreover, and with concrete impact to data privacy and security that is at the core of European values, QKD promises a significant enhancement of security for highly sensitive data as well as security against the threat that quantum computers will pose for many established cryptography schemes. However, in the longer term, most quantum communication and quantum networks will require entanglement as a resource to teleport qubits, and to interconnect quantum computers, simulators and sensors. For example, using entanglement to connect multiple quantum computers can boost their collective computing power. It is thus of key importance to ensure a complete supply chain of critical components (for example optical sources, receivers, transmitters, firmware, software, protocols and services) and infrastructure for quantum communication for Europe in the near future. This is required to achieve a high level of independence and competitiveness. In addition, Europe may lose its leadership in the standardisation of quantum networks. Worldwide industrial standards are being developed, with Europe lagging behind. In SiQUID, we dedicate WP3 to develop a QKD demonstrator using a decoy-state BB84 protocol, to demonstrate a measurement-device-independent (MDI) QKD and to investigate the feasibility of integrating the QKD setups with industrial cryptography solutions provided by Slovenian high-tech company Beyond Semiconductor (BSC). In terms of involvement, this industrial partner is equally committed to SiQUID yet complementary in expertise to academic partners FMF and IJS that contribute the necessary knowledge and stimulating research environment. For security and industrial standards, SiQUID will be in close contact with Coordination and Support Actions that will be launched within the EuroQCI programme. In this way, SiQUID will provide an opportunity for Slovenia to overcome the above challenges, catch-up with the state-of-the-art developments in quantum communications in Europe and the world, and compete with other global players.

While the BSC will take care of the integration of QKD into existing cyber security products (WP3) and will lead the deployment of national QKD protected nodes (T5.3), FMF and IJS will be responsible for the experimental and technical aspects of QKD (T3.2) and beyond QKD (WP4), and most importantly for the training of new generation of engineers skilled in quantum communications (T6.3). At the moment, the entire Slovenian community actually working on quantum communications numbers at most 10 people, of which the majority are researchers at FMF and IJS and maybe a few individuals at BSC and UVTP. At the end of the project, we will have trained at least 12 professionals means that we will multiply the pool of available workforce that can be employed as tomorrow's leading researchers in academia and in quantum industry. Having expertise in these novel fields of technology will be essential to provide Slovenians with attractive opportunities to study and work in Slovenia with state-of-the-art technologies, and it will form the basis for the foundation of quantum start-up companies (T6.3).

The SiQUID project represents the first step in building quantum communication infrastructure in Slovenia, and establishing a community of its operators and users. In doing so we will define an initial set of representative use cases (T2.1), such as securing communication and data exchange, support secure operation of critical infrastructure (smart energy grids, communication networks, nuclear facilities), etc., and elaborate on the suitability of the deployed quantum network for their support as well as extension to other application domains from interconnection of data centres to financial and healthcare sector, both on the national and Europe-wide levels (T6.2). This will help (i) identifying further beneficiaries and individuals for training in the use of quantum communication infrastructure and thus extending the base of its users in subsequent steps, as well as (ii) raising awareness on the need for and capabilities of quantum communication networks in the modern economy and society.

The SiQUID project is extremely important for Slovenian government as well. SiQUID, as a pilot project, will enable transfer of knowledge from research to government institutions and help to build alert awareness about QKD and quantum technologies. Addressed and implemented use cases will help the government institutions to understand the technologies, their potential use, management and integration with existing systems in finer details. After the project, the government institutions will be better equipped to further plan, develop, purchase and use QKD and quantum technologies applications for their own needs. Raised awareness will offer as well an opportunity to research organizations and industry to develop the field even further for mutual benefit of multiple stakeholders and society as a whole.

3.3 Environmental sustainability and contribution to European Green Deal goals

Environmental sustainability and contribution to European Green Deal goals

Describe the extent to which the project will contribute to environmental sustainability and in particular to European Green Deal goals

⚠ *This might not be applicable to all topics — for details refer to the Call document.*

The industrialization, miniaturization and cost reduction of encryption devices is of key importance for wide deployment. These technical goals directly relate with and contribute to reduced consumption of resources (both in terms of materials and energy) for device production as well as reduced operational energy consumption.

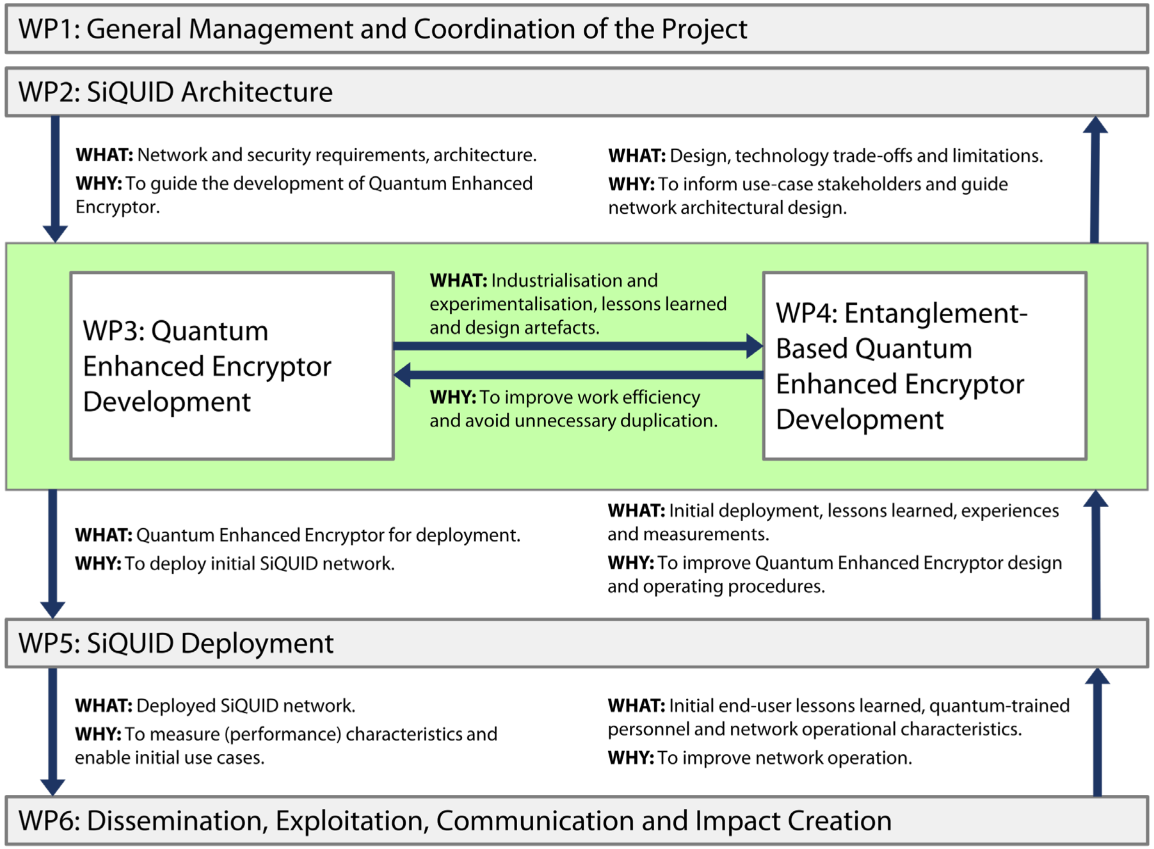
Specifically, wide deployment of equipment that requires cryogenic cooling is infeasible. The contribution of the project in experimenting with and developing of techniques and components that operate at room temperature with a smaller physical footprint and at lower power consumption simultaneously contributes towards both European Green Deal goals.

4. WORK PLAN, WORK PACKAGES, TIMING AND SUBCONTRACTING

4.1 Work plan

Work plan

Provide a brief description of the overall structure of the work plan (list of work packages or graphical presentation (Pert chart or similar)).



4.2 Work packages and activities

WORK PACKAGES
This section concerns a detailed description of the project activities. *Group your activities into work packages.* ***A work package means a major sub-division of the project****. For each work package, enter an objective (expected outcome) and list the activities, milestones and deliverables that belong to it. The grouping should be logical and guided by identifiable outputs.* *Projects should normally have a minimum of 2 work packages. WP1 should cover the management and coordination activities (meetings, coordination, project monitoring and evaluation, financial management, progress reports, etc) and all the activities which are cross-cutting and therefore difficult to assign to another specific work package (do not try splitting these activities across different work packages). WP2 and further WPs should be used for the other project activities. You can create as many work packages as needed by copying WP1.* *For very simple projects, it is possible to use a single work package for the entire project (WP1 with the project acronym as WP name).* *Work packages covering financial support to third parties (⚠ only allowed if authorised in the Call document) must describe the conditions for implementing the support (for grants: max amounts per third party; criteria for calculating the exact amounts, types of activity that qualify for financial support (closed list), persons/categories of persons to be supported and criteria and procedures for giving support; for prizes: eligibility and award criteria, amount of the prize and payment arrangements).* ⚠ *Enter each activity/milestone/output/outcome/deliverable only once (under one work package).*

Work Package 1

Work Package 1: General Management and Coordination of the Project			
Duration:	M1 - M30	**Lead Beneficiary:**	FMF
Objectives *List the specific objectives which this work package aims to achieve*			
▪ Collect weekly progress updates from team leaders ▪ Documentation of project progress ▪ Organizing monthly meetings between consortium partners ▪ Internal reporting and reporting to funding agency			

- Publishing non-sensitive results in peer-reviewed scientific journals, and in platforms for the general public
- General administration, cost & schedule control

Activities (what, how, where) and division of work

Provide a concise overview of the work (planned tasks). Be specific and give a short name and number for each task.

*Show who is participating in each task: Coordinator (COO), Beneficiaries (BEN), Affiliated Entities (AE), Associated Partners (AP), indicating **in bold** the task leader.*

Add information on other participants' involvement in the project e.g. subcontractors, in-kind contributions.

Note:

In-kind contributions: In-kind contributions for free are cost-neutral, i.e. cannot be declared as cost. Please indicate the in-kind contributions that are provided in the context of this work package.

The Coordinator remains fully responsible for the coordination tasks, even if they are delegated to someone else. Coordinator tasks cannot be subcontracted.

If there is subcontracting, please also complete the table below.

Task No (continuous numbering linked to WP)	Task Name	Description	Participants		In-kind Contributions and Subcontracting (Yes/No and which)
			Name	Role (COO, BEN, AE, AP, OTHER)	
T1.1	Project Coordination	Coordination of the communication between consortium members and communication with the funding agency. Coordination and fulfilment of administrative tasks, documentation of the project progress and preparation of reports.	**FMF**, IJS, BSC, UVTP, URSIV	COO, BEN, BEN, BEN, BEN	no
T1.2	Data, Quality and Risk Management	Collecting regular progress updates, documentation of task progress, monitoring with respect to deliverables and task progress. Informing consortium members of upcoming milestones and deadlines for deliverables. Compiling new updates for consortium members to facilitate the timely conclusion of tasks required to fulfil task dependencies.	**FMF**, IJS, BSC, UVTP, URSIV	COO, BEN, BEN, BEN, BEN	no
T1.3	Scientific and Technical Management	Supervise the design of the demonstrator and node setups, supervising and instructing young researchers and participating engineers and key personnel at government nodes. Monitor the specifications achieved in the test setups and network nodes and	**FMF**, IJS, BSC	COO, BEN, BEN	no

		direct improvements if necessary to achieve the specifications required.			

Milestones and deliverables (outputs/outcomes)

Milestones *are control points in the project that help to chart progress. Use them only for major outputs in complicated projects. Otherwise leave the section on milestones empty.*

Means of verification are how you intend to prove that a milestone has been reached. If appropriate, you can also refer to indicators.

Deliverables *are project outputs which are submitted to show project progress (any format). Refer only to major outputs. Do not include minor sub-items, internal working papers, meeting minutes, etc. Limit the number of deliverables to max 10-15 for the entire project. You may be asked to further reduce the number during grant preparation.*

For deliverables such as meetings, events, seminars, trainings, workshops, webinars, conferences, etc., enter each deliverable separately and provide the following in the 'Description' field: invitation, agenda, signed presence list, target group, number of estimated participants, duration of the event, report of the event, training material package, presentations, evaluation report, feedback questionnaire.

For deliverables such as manuals, toolkits, guides, reports, leaflets, brochures, training materials etc., add in the 'Description' field: format (electronic or printed), language(s), approximate number of pages and estimated number of copies of publications (if any).

For each deliverable you will have to indicate a due month by when you commit to upload it in the Portal. The due month of the deliverable cannot be outside the duration of the work package and must be in line with the timeline provided below. Month 1 marks the start of the project and all deadlines should be related to this starting date.

The labels used mean:

Public — fully open (⚠ automatically posted online on the Project Results platforms)

Sensitive — limited under the conditions of the Grant Agreement

EU classified — RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision 2015/444.

Milestone No (continuous numbering not linked to WP)	Milestone Name	Work Package No	Lead Beneficiary	Description	Due Date (month number)	Means of Verification

Deliverable No (continuous numbering linked to WP)	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month number)	Description (including format and language)
D1.1	The Quality Assurance and Risk Management Plan	1	FMF	R	SEN	3	A report describing the project's quality management and risk assessment plan. Language: English

D1.2	Data Management Plan	1	FMF	R	SEN	6	A report describing the project's data management plan. Language: English

Estimated budget — Resources WP1 *(n/a for prefixed Lump Sum Grants)*												
Participant	Costs											
	A. Personnel		B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties		D.2 Internally invoiced goods and services	D.3 PAC procurement costs *(for PAC Grants for Procurement)*	E. Indirect costs	Total costs
FMF	31 PM	102300	0	0	0	2000	0	0	0	0	7301	111601
IJS	3.5 PM	14945	0	0	0	0	0	0	0	0	1046	15991
BSC	8 PM	39200	0	0	0	0	0	0	0	0	2744	41944
URSIV	1.5 PM	6000	0	0	0	8000	0	0	0	0	980	14980
UVTP	1.5 PM	4200	0	0	0	0	0	0	0	0	294	4494
Total	45.5 PM	166645	0	0	0	10000	0	0	0	0	12365	189010

Work Package 2

Work Package 2: SiQUID Architecture						
Duration:	M1 - M12	**Lead Beneficiary:**	IJS			
Objectives *List the specific objectives which this work package aims to achieve*						
▪ Collaborate with public authorities to establish their requirements and select use cases to be considered ▪ Establish detailed plans for the deployment phase of the project, including fibre acquisition ▪ Assess security requirements and establish national policies for QKD ▪ Investigate issues of interoperability (terrestrial-satellite, different systems and protocols) and long distances						
Activities (what, how, where) and division of work						
Task No (continuous numbering linked to WP)	Task Name	Description	Participants		In-kind Contributions and Subcontracting (Yes/No and which)	
			Name	Role (COO, BEN, AE, AP, OTHER)		
T2.1	Architecture, specification and planning	Elaboration of requirements based on the use cases to be tested, with consideration of geographical, technical, and organisational constraints. Identification of relevant sites within Slovenia, verification of availability (dark fibres, rack space) and feasibility. Establish network topology that minimizes resource use and fulfils connectivity requirements. Devise methods to formulate and solve the ensuing constrained optimization problem. Obtain necessary agreement from all participating parties.	**IJS**, FMF, BSC, UVTP	BEN, COO, BEN, BEN	no	
T2.2	Security Assessment and Requirements	Establish security assessment and guidelines for trusted node sites and for endpoints. Assess proposed node locations from the security	**URSIV**, UVTP,	BEN, BEN, BEN, BEN, COO	no	

		perspective. Define policies and procedures for adding further nodes on the quantum network.	IJS, BSC, FMF		
T2.3	QKD Protocol Interoperability and Cross-border Planning	Study interoperability issues regarding connections to neighbouring countries. Determine optimal places for nodes within reach of the border. Study possible interoperability issues regarding the planned satellite connection.	**FMF**, IJS, BSC	COO, BEN, BEN	no

Milestones and deliverables (outputs/outcomes)

Milestone No (continuous numbering not linked to WP)	Milestone Name	Work Package No	Lead Beneficiary	Description	Due Date (month number)	Means of Verification

Deliverable No (continuous numbering linked to WP)	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month number)	Description (including format and language)
D2.1	Initial SiQUID requirements, architecture, and specifications	2	IJS	R	SEN	12	Report detailing the requirements, architecture, and specification (technical solutions for QKD, microlocations of nodes, dark fiber procurement). Language: English
D2.2	Initial network deployment and cross-border-links plan	2	IJS	R	SEN	12	Detailed deployment plan with an actionable specification of required tasks (procurement, site preparation, hardware

							installation, initial testing, full system integration, use case testing). Language: English

Estimated budget — Resources WP2 *(n/a for prefixed Lump Sum Grants)*													
Participant	Costs												
	A. Personnel		B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties		D.2 Internally invoiced goods and services	D.3 PAC procurement costs *(for PAC Grants for Procurement)*	E. Indirect costs	Total costs
FMF	6 PM	19800	0	0	0	0	0	0	0	0	1386	21186
IJS	16 PM	68320	0	0	0	0	0	0	0	0	4782	73102
BSC	17 PM	83300	0	0	0	0	0	0	0	0	5831	89131
URSIV	5 PM	20000	0	0	0	0	0	0	0	0	1400	21400
UVTP	4 PM	11200	0	0	0	0	0	0	0	0	784	11984
Total	48 PM	202620	0	0	0	0	0	0	0	0	14183	216803

Work Package 3

Work Package 3: Quantum-Enhanced Encryptor Development			
Duration:	M2 – M30	**Lead Beneficiary:**	**BSC**

Objectives

List the specific objectives which this work package aims to achieve

- Development of a QKD demonstrator using a decoy-state BB84 protocol
- Demonstration of measurement-device-independent (MDI) QKD
- Investigating the feasibility of integrating the QKD setups with industrial cryptography solutions
- Design of Quantum-Enhanced Encryptor with strengthened security with focus on EU supply-chains, industrialization and TEMPEST

Activities (what, how, where) and division of work

Task No (continuous numbering linked to WP)	Task Name	Description	Participants		In-kind Contributions and Subcontracting (Yes/No and which)
			Name	Role (COO, BEN, AE, AP, OTHER)	
T3.1	Quantum-Enhanced Encryptor Security Evaluation Procedure	Monitoring of security related design decisions during development. Preparation of security evaluation procedures enabling certification and accreditation of QKD enhanced encryptors for protection of classified information. BSC: preparation of proposals.	**UVTP**, BSC, URSIV, FMF	BEN, BEN, BEN, COO	No
T3.2	QKD Lab Proof of Concept	Experiments showing QKD performance using different (key) components and architectures. Development of QKD device and proof of concept in a lab environment. BSC: Industrialization	**FMF**, BSC, IJS	COO, BEN, BEN	No

		advice, contribute to integration. IJS: setting up two nodes to test middle-distance QKD in real environment.			
T3.3	QKD Industrialization Concept and Experiments	Experiments and development focused on suitability for mass production, compactification, cost reduction, room temperature operation, op-ex reduction. Special attention (performance) trade-off related to component availability, supply chains and EU non-dependence. Design to minimize TEMPEST / side channel leakage. FMF: advice and theoretical guidance.	**BSC**, FMF	BEN, COO	No
T3.4	Strengthened Encryptor Security, Interoperability and TEMPEST	Design and integration of simple QKD emulation with Encryptor. Encryptor security and interoperability strengthening as identified and decided in the project based on based on security and functionality requirements, and may include addition of post quantum crypto algorithms, new key exchange algorithms, new protocols support, TEMPEST, monitoring & control functionality, etc. FMF: advice and theoretical guidance	**BSC**, FMF	BEN, COO	No
T3.5	QKD Integration and TEMPEST	Integration of QKD with Encryptor, ensuring proper combined operation. Development of TEMPEST test plan, countermeasures and measurements for QKD + encryptor combination. FMF: advice and theoretical guidance.	**BSC**, FMF	BEN, COO	No

Milestones and deliverables (outputs/outcomes)

Milestone No (continuous numbering not linked to WP)	Milestone Name	Work Package No	Lead Beneficiary	Description	Due Date (month number)	Means of Verification

Deliverable No (continuous numbering linked to WP)	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month number)	Description (including format and language)
D3.1	QKD proof-of-concept and	3	FMF	R	SEN	M12	The report describing QKD proof-of-concept, the

	Quantum-Enhanced Encryptor Security Design.						expected performance characteristics of the devices to be deployed taking into account also industralization aspects. Includes security aspects focusing on security evaluation procedure. Language: English.
D3.2	Quantum-Enhanced Encryptor Nodes Design and TEMPEST Plan	3	BSC	R	SEN	M24	The report describing specification of Quantum-Enhanced Encryptor, QKD Emulation, overview of interoperability, protocol and security encryptor enhancments and identification of new critical TEMPEST side channels. Language: English.
D3.3	Quantum Enhanced Encryptor Nodes Improvements and TEMPEST Protections	3	BSC	R	SEN	M30	The report describing Integration results, final Quantum-enhanced encryptor node design key performance characteristics and achieved TEMPEST level. Language: English.

Estimated budget — Resources WP3 *(n/a for prefixed Lump Sum Grants)*												
Participant	Costs											
	A. Personnel		B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties		D.2 Internally invoiced goods and services	D.3 PAC procurement costs *(for PAC Grants for Procurement)*	E. Indirect costs	Total costs
FMF	56.5 PM	186450	0	0	513637	97600	0	0	0	0	55838	853525
IJS	15.5 PM	66185	0	0	235964	76555	0	0	0	0	26509	405213
BSC	80 PM	392000	0	0	494090	196529	0	0	0	0	75783	1158402
URSIV	1 PM	4000	0	0	110975	0	0	0	0	0	8048	123023
UVTP	8 PM	22400	0	0	110975	135000	0	0	0	0	18786	287161
Total	161 PM	671035	0	0	1465641	505684	0	0	0	0	184965	2827325

Work Package 4

Work Package 4: Entanglement-Based Quantum-Enhanced Encryptor Development			
Duration:	M1 - M30	**Lead Beneficiary:**	FMF

Objectives

List the specific objectives which this work package aims to achieve

- Build two stable and high-brightness sources of entanglement
- Demonstrate entanglement distribution over long distances
- Test the feasibility of entanglement swapping

Activities (what, how, where) and division of work

Task No (continuous numbering linked to WP)	Task Name	Description	Participants		In-kind Contributions and Subcontracting (Yes/No and which)
			Name	Role (COO, BEN, AE, AP, OTHER)	
T4.1	Theoretical Security Assessment of Quantum Security Guarantees	Theoretical assessment of the security enhancement achievable with entanglement-based QKD in the context of a Slovene quantum network.	**IJS**, FMF, BSC, URSIV, UVTP	BEN, COO, BEN, BEN, BEN	no
T4.2	Entanglement Source Development	Design of a state-of-the-art high-bandwidth source of entangled photons in the telecom C band. Training of IJS researchers to design and build a source.	**FMF**, IJS, BSC	COO, BEN, BEN	no
T4.3	Entanglement Source Implementation, Industrialization and TEMPEST	Implementation of one entanglement source at FMF. Duplication of the source at IJS. BSC and FMF	**BSC**, FMF, IJS	BEN, COO, BEN	no

		investigating industrialization of the entanglement source.			
T4.4	Demonstration of Entanglement Distribution for QKD Purposes	Demonstrate entanglement distribution between FMF and IJS as well as between FMF and distant nodes. Demonstrate entanglement swapping with sources at FMF and IJS.	**FMF**, IJS, BSC	COO, BEN, BEN	no

Milestones and deliverables (outputs/outcomes)

Milestone No (continuous numbering not linked to WP)	Milestone Name	Work Package No	Lead Beneficiary	Description		Due Date (month number)	Means of Verification
Deliverable No (continuous numbering linked to WP)	**Deliverable Name**	**Work Package No**	**Lead Beneficiary**	**Type**	**Dissemination Level**	**Due Date** (month number)	**Description** (including format and language)
D4.1	Theoretical assessment of quantum security guarantees for SiQUID schemes	4	IJS	R	SEN	12	A report describing the theoretical security assessment of the various QKD protocols investigated in the context of the Slovene security landscape. Language: English.
D4.2	Entanglement source	4	FMF	DEM	PU	12	Design and implementation of a state-of-the-art source of entangled photons on the telecom C-band. The emphasis for the source will be stability, compactness and a high source brightness and

							entanglement quality. Language: English.
D4.3	Entanglement-source design, industrialization, and TEMPEST analysis	4	BSC	R	SEN	30	Report on the design of the entanglement source, its potential for industrialization. Analysis of the entanglement source with respect to TEMPEST. Language: English.
D4.4	Entanglement Distribution for QKD purposes	4	FMF	DEM	PU	30	Report on the demonstration of entanglement over long distance, characterization of the demonstrator performance and its potential for future implementations of entanglement-based QKD, and as a resource for future quantum networks. Language: English.

Estimated budget — Resources WP4 *(n/a for prefixed Lump Sum Grants)*													
Participant	Costs												
	A. Personnel		B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties		D.2 Internally invoiced goods and services	D.3 PAC procurement costs *(for PAC Grants for Procurement)*	E. Indirect costs	Total costs
FMF	60 PM	198000	0	0	29561	0	0	0	0	0	15929	243490
IJS	32.5 PM	138775	0	0	35030	46962	0	0	0	0	15454	236221
BSC	19 PM	93100	0	0	0	0	0	0	0	0	6517	99617
URSIV	1 PM	4000	0	0	0	0	0	0	0	0	280	4280
UVTP	1 PM	2800	0	0	0	0	0	0	0	0	196	2996
Total	113.5 PM	436675	0	0	64591	46962	0	0	0	0	38376	586603

Work Package 5

Work Package 5: SiQUID Deployment						
Duration:	M13 – M30	**Lead Beneficiary:**	**IJS**			
Objectives *List the specific objectives which this work package aims to achieve*						
▪ Security Evaluation of QKD Protected Encryptor Nodes ▪ Deployment of QKD Protected Encryptor Nodes ▪ QKD Enhanced Nodes Operators Training ▪ Evaluation of QKD Network						
Activities (what, how, where) and division of work						
Task No (continuous numbering linked to WP)	Task Name	Description	Participants		In-kind Contributions and Subcontracting (Yes/No and which)	
			Name	Role (COO, BEN, AE, AP, OTHER)		
T5.1	Minimal Operational Requirements	Elaboration of minimal device, network and system security requirements, including, security evaluation of WDM sharing of QKD and BLACK traffic, procedures if QKD link fails but not the IP connectivity, installation requirements, physical security requirements, etc.	**UVTP**, BSC, FMF, IJS, URSIV	BEN, BEN, COO, BEN, BEN	no	
T5.2	Quantum-Enhanced Encryptor Security Evaluation Artifacts	QKD relevant security evaluation artifacts required for national certification. Includes formal proof of combined QKD + encryptor key exchange (shared secret establishment).	**BSC**, UVTP, FMF	BEN, BEN, COO	no	

T5.3	Deployment of QKD Protected Nodes	Establishing cabling to network rack optical-fibre patch panels and verifying the link quality (attenuation measurements). Installation of lab prototype QKD device, integration with classical encryptor and with classical networking equipment. Testing at device and link level. Deployment of QKD protected encryptors. Setup of Key Management System (KMS). KMS controller. Securing trusted nodes (access controls, cyber security).	**BSC,** IJS, FMF	BEN, BEN, COO	no
T5.4	Deployed Network Monitoring, Behaviour & Reliability Assessments	Establish monitoring infrastructure based on open-source solutions (Observium, Icinga) for monitoring all components (quantum and classical) of the deployed network in real-time, alarming. Measurement of key metrics in real time (e.g. key rates for all links), logging of time-series data (Prometheus or Loki), visualisation (Grafana). Test network maintenance procedures.	**IJS**, BSC, FMF	BEN, BEN, COO	no

Milestones and deliverables (outputs/outcomes)

Milestone No (continuous numbering not linked to WP)	Milestone Name	Work Package No	Lead Beneficiary	Description	Due Date (month number)	Means of Verification

Deliverable No (continuous numbering linked to WP)	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month number)	Description (including format and language)
D5.1	Revised network deployment and cross-border links plan	5	IJS	R	SEN	24	Detailed report on the methods used for the security evaluation and on the outcomes of that evaluation. Language: English
D5.2	Quantum-enhanced encryptor security	5	BSC	R	SEN	30	Functioning physical-level QKD protected encryptor communication network

	evaluation process & artifacts						between selected trusted node sites. Language: English
D5.3	Measurements, behaviour and reliability of deployed network	5	IJS	R	SEN	30	Detailed report on performance and reliability of deployed QKD network. Language: English

Estimated budget — Resources WP5 *(n/a for prefixed Lump Sum Grants)*												
Participant	Costs											
	A. Personnel		B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties		D.2 Internally invoiced goods and services	D.3 PAC procurement costs *(for PAC Grants for Procurement)*	E. Indirect costs	Total costs
FMF	12 PM	39600	0	0	0	0	0	0	0	0	2772	42372
IJS	18.5 PM	78995	0	0	0	0	0	0	0	0	5530	84525
BSC	32 PM	156800	0	0	0	0	0	0	0	0	10976	167776
URSIV	2 PM	8000	0	0	0	0	0	0	0	0	560	8560
UVTP	10 PM	28000	0	0	0	0	0	0	0	0	1960	29960
Total	74.5 PM	311395	0	0	0	0	0	0	0	0	21798	333193

Work Package 6

Work Package 6: Dissemination, Exploitation, Communication & Impact Creation			
Duration:	M1 - M30	**Lead Beneficiary:**	FMF

Objectives

List the specific objectives which this work package aims to achieve

- Disseminate the results of the project to stakeholders in Slovenia, and to partners in neighbouring countries to share lessons learned
- Disseminate the activities of the project to the general public and to the scientific community
- Identify end-user use cases and exploit the deployed quantum network
- Train young researchers, engineers, and key government personnel

Activities (what, how, where) and division of work

Task No (continuous numbering linked to WP)	Task Name	Description	Participants		In-kind Contributions and Subcontracting (Yes/No and which)
			Name	Role (COO, BEN, AE, AP, OTHER)	
T6.1	Dissemination and Communication	Dissemination of the activities, their goals and the progress to the public, to the research community and to public and industrial stakeholders.	**FMF**, BSC, IJS	COO, BEN, BEN	No
T6.2	Exploitation of Deployed Quantum Network	Investigate possible end-user use cases, in particular within Slovenia and for international links with neighbouring countries. Exploit the deployed quantum network considering these use cases. Collect lessons learned and feedback.	**IJS**, FMF, URSIV, UVTP, BSC	COO, BEN, BEN, BEN, BEN	No

T6.3	Quantum Technologies Training, Capacity and Community Building	Raise awareness in research institutions and public universities about quantum technologies and quantum communication. Identify interfaces with those research institutions and potential joint interests. Identify potential gaps in the market in Slovenia that would benefit from quantum-technology start-ups. Train young researchers at FMF and IJS as well as engineers at BSC in the laboratory. Train stakeholders at UVTP and involved government institutions in the use of QKD equipment. Provide on-hand experience in demonstrator setups.	**FMF**, BSC, IJS, UVTP	COO, BEN, BEN, BEN	No

Milestones and deliverables (outputs/outcomes)

Milestone No (continuous numbering not linked to WP)	Milestone Name	Work Package No	Lead Beneficiary	Description	Due Date (month number)	Means of Verification
MS1	Initial SiQUID requirements	1, 2	IJS	Agreement of all consortium members about the measures to be taken to assure the quality of the network nodes and links to be implemented, and about the plan for risk management. Evaluation of use cases to test and requirements for the deployed national quantum network. Agreement of all participating parties that the elaborated initial plan defines all requirements that are necessary for the deployed solution to addresses all envisioned use cases.	3	Initial SiQUID Requirements, Architecture and Specifications ready (D2.1) Prepared the quality assurance and risk management plan (D1.1).
MS2	SiQUID Component Level PoC and Initial Security	2, 3, 4	FMF	Theoretical assessment of quantum security guarantees for the nodes to be implemented in SiQUID. Completion of the initial QKD demonstrator nodes, characterization of their performance and security assessment.	12	Initial network deployment and cross-border links plan ready (D2.2). QKD proof-of-concept performed and Quantum Enhanced Encryptor security design ready (D3.1). Characterization of the entanglement source: measurement

	Requirements			Demonstration of the generation of high-visibility entanglement with high spectral brightness.		of the pair rates produced, the spectrum of the generated photons, and the visibility of the entanglement generated (D4.2).
MS3	SiQUID Quantum-Enhanced Encryptor and Node Locations available	3,4,5,6	BSC	Performance tests and TEMPEST analysis of the integrated quantum-enhanced encryptors. Comparison of measured characteristics with the specifications required for establishing the links between government nodes (intra-city links). Demonstration of entanglement distribution and entanglement swapping between research institutions. Performance characterization, comparison and evaluation of initial nodes deployed. Identifying the planned public, academic, and critical infrastructure use cases	24	Availability of quantum enhanced encryptor, measured key characteristics and identification of new TEMPEST sensitive signals (D3.2). Performance characterization of the two sources of entanglement implemented: pair rate, photon spectrum, entanglement visibility, violation of a Bell-type inequality (D4.2). Revised network deployment and cross-border links plan ready (D5.1). Agreement of the consortium partners on the list and on the description of the use cases. Successful demonstration of quantum-enhanced encryption between the specified network nodes. Report on the planned public, academic, and critical infrastructure use cases (D6.2).
MS4	SiQUID Network deployed and initial end user lessons learned	3,4,5,6	FMF	Improvements of Quantum Enhanced Encryptor design based on TEMPEST measurements, deployment and use cases feedback. Demonstration of entanglement distribution and entanglement swapping over large distances. Evaluation of deployed national QKD protected encryptors and QKD network performance. Deployment, community building, and exploitation.	30	Availability of improved quantum enhanced encryptor design (D3.3). Feasibility considerations for the industrialization of the entanglement source, and TEMPEST characterization of the source (D4.3) Performance characterization of entanglement swapping: four-fold coincidence rates, visibility of the two-photon

						interference for the Bell-state measurement, visibility of the swapped entanglement, violation of a Bell-type inequality with the swapped entanglement (D4.4). All specified public administration requirements fulfilled (D5.2, D5.3). Report describing deployment, community building and use cases results (D6.3).

Deliverable No (continuous numbering linked to WP)	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month number)	Description (including format and language)
D6.1	Dissemination and Communication Plan	WP1, WP6	FMF	R	SEN	6	Detailed report on the plan to disseminate the results and to communicate them to the the public, to the funding agency, and to partners in other EU countries. Language: English
D6.2	Planned public, academic, and critical infrastructure use cases	WP6	IJS	R	PU	24	Description of the use-cases identified. List of potential end-users in Slovenia, a description of their use cases, and a description of their capabilities and requirements. Language: English
D6.3	Report describing deployment, community	WP6	FMF	R	PU	30	Report about the activities towards community building and identifying

	building and use cases results						possible opportunities for start-ups and gaps in the Slovene market that could be targeted. Listing members of the Slovene Quantum Community, their capabilities, interests and possible use cases. Language: English

Estimated budget — Resources WP6 *(n/a for prefixed Lump Sum Grants)*												
Participant	Costs											
	A. Personnel		B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties		D.2 Internally invoiced goods and services	D.3 PAC procurement costs *(for PAC Grants for Procurement)*	E. Indirect costs	Total costs
FMF	32 PM	105600	0	5000	0	0	0	0	0	0	7742	118342
IJS	18 PM	76860	0	3600	7188	2396	0	0	0	0	6303	96347
BSC	15 PM	73500	0	5000	0	0	0	0	0	0	5495	83995
URSIV	2.5 PM	10000	0	1000	0	0	0	0	0	0	770	11770
UVTP	5.5 PM	15400	0	1500	0	0	0	0	0	0	1183	18083
Total	73 PM	281360	0	16100	7188	2396	0	0	0	0	21493	328537

Overview of Work Packages (n/a for Lump Sum Grants)

Staff effort per work package

Fill in the summary on work package information and effort per work package.

Work Package No	Work Package Title	Lead Participant No	Lead Participant Short Name	Start Month	End Month	Person-Months
1	General Management and Coordination of the Project	1	FMF	1	30	45.5
2	SiQUID Architecture	2	IJS	1	12	48
3	Quantum-Enhanced Encryptor Development	3	BSC	1	30	161
4	Entanglement-Based Quantum-Enhanced Encryptor Development	1	FMF	1	30	113.5
5	SiQUID Deployment	2	IJS	13	30	74.5
6	Dissemination, Exploitation, Communication, and Impact Creation	1	FMF	1	30	73
				Total Person- Months		515.5

Staff effort per participant

Fill in the effort per work package and Beneficiary/Affiliated Entity.
Please indicate the number of person/months over the whole duration of the planned work.
Identify the work-package leader for each work package by showing the relevant person/month figure in ***bold****.*

Participant	WP 1	WP 2	WP 3	WP 4	WP 5	WP 6	Total Person-Months
FMF	31	6	56.5	60	12	32	197.5
IJS	3.5	16	15.5	32.5	18.5	18	104
BSC	8	17	80	19	32	15	171
URSIV	1.5	5	1	1	2	2.5	13
UVTP	1.5	4	8	1	10	5,5	30
Total Person-Months	45.5	48	161	113.5	74.5	73	515.5

4.3 Timetable

Fill in cells in beige to show the duration of activities. Repeat lines/columns as necessary.
Note: *Use actual, calendar years and quarters. In the timeline you should indicate the timing of each activity per WP. You may add additional columns if your project is longer than 6 years.*

ACTIVITY	YEAR 1				YEAR 2				YEAR 3	
	Q 1	Q 2	Q 3	Q 4	Q 1	Q 2	Q 3	Q 4	Q 1	Q 2
Task 1.1 Project Coordination										
Task 1.2 Data, Quality and Risk Management										
Task 1.3 Scientific and Technical Management										
Task 2.1 Architecture, Specification and Planning										
Task 2.2 Security Assessment and Requirements										
Task 2.3 QKD Protocol Interoperability and Cross Border Planning										
Task 3.1 Quantum-Enhanced Encryptor Security Evaluation Procedure										
Task 3.2 QKD Lab Proof of Concept										
Task 3.3 QKD Industrialization Concept and Experiments										
Task 3.4 Strengthened Encryptor Security, Interoperability and TEMPEST										
Task 3.5 QKD Integration and TEMPEST										
Task 4.1 Theoretical Security Assessment of Quantum Security Guarantees										
Task 4.2 Entanglement Source Development										
Task 4.3 Entanglement Source Implementation, Industrialization and TEMPEST										
Task 4.4 Demonstration of Entanglement Distribution for QKD purposes										
Task 5.1 Minimal Operational Requirements										
Task 5.2 Quantum-Enhanced Encryptor Security Evaluation Artifacts										
Task 5.3 Deployment of QKD Protected Nodes										
Task 5.4 Deployed Network Monitoring, Behaviour & Reliability Assessments										
Task 6.1 Dissemination and Communication										
Task 6.2 Exploitation of Deployed Quantum Network										
Task 6.3 Quantum Technologies Training, Capacity and Community Building										

	SiQUID WBS	LEAD	Start	End	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
WP1	**General Management and Coordination of the Project**	**FMF**	**1**	**30**																														
T1.1	Project Coordination	FMF	1	30																														
T1.2	Data, Quality and Risk Management	FMF	1	30			D1.1			D1.2																								
T1.3	Scientific and Technical Management	FMF	1	30																														
WP2	**SiQUID Architecture**	**IJS**	**1**	**12**																														
T2.1	Architecture, Specification and Planning	IJS	1	12																														
T2.2	Security Assessment and Requirements	URSIV	1	12			D2.1									D2.2																		
T2.3	QKD Protocol Interoperability and Cross Border Planning	FMF	2	12																														
WP3	**Quantum-Enhanced Encryptor (QEE) Development**	**BSC**	**1**	**30**																														
T3.1	QEE Security Evaluation Procedure	UVTP	1	12																														
T3.2	QKD Lab Proof of Concept	FMF	1	12												D3.1																		
T3.3	QKD Industrialization Concept and Experiments	BSC	1	24																														
T3.4	Strengthened Encryptor Security, Interoperability and TEMPEST	BSC	1	24																								D3.2						
T3.5	QKD Integration and TEMPEST	BSC	9	30																														D3.3
WP4	**Entanglement-Based QEE Development**	**FMF**	**1**	**30**																														
T4.1	Theoretical Security Assessment of Quantum Security Guarantees	IJS	1	12												D4.1																		
T4.2	Entanglement Source Development	FMF	1	12												D4.2																		
T4.3	Entanglement Source Implementation, Industrialization and TEMPEST	BSC	12	30																														D4.3
T4.4	Demonstration of Entanglement Distribution for QKD purposes	FMF	12	30																														D4.4
WP5	**SiQUID Deployment**	**IJS**	**13**	**30**																														
T5.1	Minimal Operational Requirements	UVTP	13	30																														D5.2
T5.2	QEE Security Evaluation Artifacts	BSC	13	30																														
T5.3	Deployment of QKD Protected Nodes	BSC	13	30																								D5.1						D5.3
T5.4	Deployed Network Monitoring, Behaviour & Reliability Assessments	IJS	16	30																														
WP6	**Dissemination, Exploitation, Communication and Impact Creation**	**FMF**	**1**	**30**																														
T6.1	Dissemination and Communication	FMF	1	30						D6.1																								
T6.2	Exploitation of Deployed Quantum Network	IJS	1	30																								D6.2						D6.3
T6.3	Quantum Technologies Training, Capacity and Community Building	FMF	1	30																														
							MS1									MS2												MS3						MS4

Given here is a more detailed Gantt chart that was developed during project preparation.

4.4 Subcontracting *(n/a for prefixed Lump Sum Grants)*

Subcontracting

Give details on subcontracted project tasks (if any) and explain the reasons why (as opposed to direct implementation by the Beneficiaries/Affiliated Entities).

Subcontracting — Subcontracting means the implementation of 'action tasks', i.e. specific tasks which are part of the EU grant and are described in Annex 1 of the Grant Agreement.

***Note:** Subcontracting concerns the outsourcing of a part of the project to a party outside the consortium. It is not simply about purchasing goods or services. We normally expect that the participants have sufficient operational capacity to implement the project activities themselves. Subcontracting should therefore be exceptional.*

Include only subcontracts that comply with the rules (i.e. best value for money and no conflict of interest; no subcontracting of coordinator tasks).

Work Package No	Subcontract No (continuous numbering linked to WP)	Subcontract Name (subcontracted action tasks)	Description (including task number and BEN to which it is linked)	Estimated Costs (EUR)	Justification (Why is subcontracting necessary?)	Best-Value-for-Money (How do you intend to ensure it?)
N/A						

Other issues: *If subcontracting for the entire project goes beyond 30% of the total eligible costs, give specific reasons.*	N/A

5. OTHER

5.1 Ethics

Ethics *If the Call document contains a section on ethics, the ethics issues and measures you intend to take to solve/avoid them must be described in the annexed Ethics issues table .*
See annex Ethics issue table

5.2 Security

Security *Describe security issues that may arise during the project implementation in the annexed Security issues table.* *Indicate if there is need for EU classification of information (Decision 2015/444) or any other specific security measures.* ***Note:** Beneficiaries must ensure that their projects are not subject to national/third country security requirements that could affect the implementation or put into question the award of the grant (e.g. technology restrictions, national security classification, etc).*
See annex Security issues table

6. DECLARATIONS

Double funding	
Information concerning other EU grants for this project ⚠ *Please note that there is a strict prohibition of double funding from the EU budget (except under EU Synergies actions).*	**YES/NO**
We confirm that to our best knowledge neither the project as a whole nor any parts of it have benefitted from any other EU grant *(including EU funding managed by authorities in EU Member States or other funding bodies, e.g. Erasmus, EU Regional Funds, EU Agricultural Funds, European Investment Bank, etc)*. If NO, explain and provide details.	YES
We confirm that to our best knowledge neither the project as a whole nor any parts of it are (nor will be) submitted for any other EU grant *(including EU funding managed by authorities in EU Member States or other funding bodies, e.g. Erasmus, EU Regional Funds, EU Agricultural Funds, European Investment Bank, etc)*. If NO, explain and provide details.	YES

Financial support to third parties (if applicable) *If in your project the maximum amount per third party will be more than the threshold amount set in the Call document, justify and explain why the higher amount is necessary in order to fulfil your project's objectives.*
N/A

ANNEXES

LIST OF ANNEXES

Standard
List of previous projects
Ownership control declaration
Ethics issue table
Security issues table

Special
Letter of Authorization
LOI Slovene
LOI Croatia
LOI Italy
LOI Austria
LOI Hungary
Paper Deploying an inter-European quantum network

HISTORY OF CHANGES		
VERSION	PUBLICATION DATE	CHANGE
1.0	01.11.2021	Initial version (new MFF).