



EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content and Technology

CNECT.C – Enabling and Emerging Technologies

C.4 – Emerging & Disruptive Technologies

AMENDMENT No AMD-101113143-5

Project: 101113143 — EstQCI

The parties agree to amend the Agreement as follows ('**Amendment**')

1 . Change of Annex 1

Annex 1 is changed and replaced by the Annex 1 attached to this Amendment.

2 . Change of the project duration

The project duration in the **Data Sheet** is changed to 36.

3. Change of the reporting periods

The reporting period(s) in the **Data Sheet** are changed to:

- RP 1: month 1 to month 12
- RP 2: month 13 to month 24
- RP 3: month 25 to month 36

All other provisions of the Agreement and its Annexes remain unchanged.

This Amendment **enters into force** on the day of the last signature.

This Amendment **takes effect** on the date(s) mentioned in the amendment clause(s) (or — if no date was chosen — on the same date the Amendment enters into force).

Please inform the other members of your consortium (if any) of this Amendment.

SIGNATURES

For the coordinator

For the granting authority

Done in English

Enclosures: Grant Agreement Data Sheet
Grant Agreement Annex 1



ANNEX 1



Digital Europe Programme (DIGITAL)

Description of the action (DoA)

Part A

Part B

DESCRIPTION OF THE ACTION (PART A)

COVER PAGE

Part A of the Description of the Action (DoA) must be completed directly on the Portal Grant Preparation screens.

PROJECT	
<i>Grant Preparation (General Information screen) — Enter the info.</i>	
Project number:	101113143
Project name:	Estonian Quantum Communication Infrastructure
Project acronym:	EstQCI
Call:	DIGITAL-2022-QCI-02
Topic:	DIGITAL-2022-QCI-02-DEPLOY-NATIONAL
Type of action:	DIGITAL-SIMPLE
Service:	CNECT/C/04
Project starting date:	fixed date: 1 January 2023
Project duration:	36 months

TABLE OF CONTENTS

Project summary	3
List of participants	3
List of work packages	4
Staff effort	9
List of deliverables	10
List of milestones (outputs/outcomes)	17
List of critical risks	18

PROJECT SUMMARY

Project summary

Grant Preparation (General Information screen) — Provide an overall description of your project (including context and overall objectives, planned activities and main achievements, and expected results and impacts (on target groups, change procedures, capacities, innovation etc)). This summary should give readers a clear idea of what your project is about.

Use the project summary from your proposal.

The purpose of the EstQCI project is to deploy the first experimental QKD network in Estonia in order to be prepared for the full deployment of the EuroQCI. EstQCI should provide the basis for the fast uptake and deployment of quantum security technology by building up the competence of relevant ministries, companies and other entities. In addition, the project would serve as a deployment model for the future deployment of QKD network in Estonia. The project aims to build up a metropolitan QKD network and test long-distance links to be ready for connections with neighbouring countries. In these networks, devices from EU-27 developers will be used, when possible. The main goals of the project are as follows:

- a) Building up the know-how and competence of relevant entities for future deployment of QKD networks and services
- b) Testing the readiness of devices from EU-27 producers to gain information about their suitability for the Estonian conditions and needs
- c) First demonstrations of the use of the network between metropolitan areas as well as for long-distance network in laboratory conditions
- d) Collaborating with neighbouring countries and preparation for cross-border links with Finland, Latvia and Sweden
- e) Sharing knowledge with relevant stakeholders, raise the awareness of companies and other relevant entities about the possibilities of the network to prepare for future secure connectivity/ cyber security applications.
- f) Demonstration of QKD implementation and usage on low latency and high-capacity connections between servers in a round network, securing the Estonian Government cloud services.

One of the important elements of the EstQCI project is coordination with Finland, Latvia, Lithuania, Poland and Sweden to create a foundation for the future cooperation within the margins of EuroQCI project and to prepare for terrestrial cross-border connections between Member States.

As a result of the project we will open our network for interested parties (for example cyber security industry, academia etc) and facilitate the exploration of further use cases of the network. We will build up a wide-scale competence among the relevant stakeholder

LIST OF PARTICIPANTS

PARTICIPANTS

Grant Preparation (Beneficiaries screen) — Enter the info.

Number	Role	Short name	Legal name	Country	PIC
1	COO	MKM	MAJANDUS JA KOMMUNIKATSIOONIMINISTEERIUM	EE	963638450
2	BEN	Metrosert	AKTSIASELTS METROSERT	EE	994104016
3	BEN	RIKS	STATE INFOCOMMUNICATION FOUNDATION	EE	911424126
4	BEN	EE MoD	KAITSEMINISTEERIUM	EE	905124655

LIST OF WORK PACKAGES

Work packages						
Grant Preparation (Work Packages screen) — Enter the info.						
Work Package No	Work Package name	Lead Beneficiary	Effort (Person-Months)	Start Month	End Month	Deliverables
WP1	Project management and procurement coordination	1 - MKM	27.00	1	36	D1.1 – Technical documents for the 1st review meeting D1.2 – Technical documents for the 2'nd review meeting D1.3 – Gap analysis and roadmap for alignment with the security baseline D1.4 – Procurement overview D1.5 – Technical documents for the 3'rd review meeting
WP2	Development of trustworthy quantum communication network topology in metropolitan area	3 - RIKS	58.00	6	36	D2.1 – Evaluation report for the equipment D2.2 – Network deployment report D2.3 – Deployment plan
WP3	Testing of deployed QCI in metropolitan area	1 - MKM	24.00	13	36	D3.1 – Description of first use cases D3.2 – Evaluation report of the metropolitan networks
WP4	Demonstration of long-distance quantum communication network	2 - Metrosert	57.00	6	36	D4.1 – Long-distance network test report
WP5	Regional coordination and EuroQCI integration	1 - MKM	30.00	1	36	D5.1 – Plan for the cross-border connections in the region D5.2 – Report on participation to the EuroQCI initiative and on the collaboration with other DIGITAL projects, part 1 D5.3 – Report on participation to the EuroQCI initiative and on the collaboration with other DIGITAL projects, part 2 D5.4 – Report on participation to the

Work packages*Grant Preparation (Work Packages screen) — Enter the info.*

Work Package No	Work Package name	Lead Beneficiary	Effort (Person-Months)	Start Month	End Month	Deliverables
						EuroQCI initiative and on the collaboration with other DIGITAL projects, part 3
WP6	Creating impact and dissemination	1 - MKM	28.00	1	36	D6.1 – Communication report, 1st period D6.2 – Communications report D6.3 – Report on dissemination and exploitation

Work package WP1 – Project management and procurement coordination

Work Package Number	WP1	Lead Beneficiary	1 - MKM
Work Package Name	Project management and procurement coordination		
Start Month	1	End Month	36

Objectives
Progress monitoring and reporting Technical specifications for procurements Procurement coordination and execution Alignment with security baseline

Description
Regular project management, including monitoring of progress of all WPs. Necessary updates to project plan and risk analysis. Setting up dedicated channels for information sharing between the consortium and planning of regular meetings. Management of finances and regular reports. Preparation of technical specifications for all devices and other supplies, based on consultation with regional partners and considering the future EuroQCI integration as well as the requirements from the European Commission. Based on the technical specifications, public procurements will be set up and carried out according to Estonian law. Alignment with the security baseline.

Work package WP2 – Development of trustworthy quantum communication network topology in metropolitan area

Work Package Number	WP2	Lead Beneficiary	3 - RIKS
Work Package Name	Development of trustworthy quantum communication network topology in metropolitan area		
Start Month	6	End Month	36

Objectives
Investigation of available channels including the connection between fibre properties Testing of QCI-equipment procured Incorporation of tens of kilometres of fibre optic link realising a standard platform for validation, quantification and comparison of the diverse physical components of a QCI system in a real environment.

Description
Mapping the existing fibre-based network and to assessing accessibility for secure QCI in between two locations in metropolitan area. Procurement of the devices in collaboration with WP1. Testing the devices for the metropolitan network in laboratory conditions. Metrological testing of the devices. The systems tested in the laboratory conditions will be used to build up a metropolitan network.

Work package WP3 – Testing of deployed QCI in metropolitan area

Work Package Number	WP3	Lead Beneficiary	1 - MKM
Work Package Name	Testing of deployed QCI in metropolitan area		
Start Month	13	End Month	36

Objectives
<p>Evaluation of the QCI network implemented for performance</p> <p>First use cases in the networks</p> <p>Dissemination of knowledge</p>
Description
<p>Evaluation of the network performance based on knowledge from the laboratory conditions. Workshops with stakeholders (cyber security industry, possible service providers and government agencies) to identify and to select relevant use cases.</p> <p>Opening of the testbed and demonstration of first use cases in the networks.</p> <p>Information sharing about the possibilities of the testbed, trainings for potential staff for EuroQCI.</p>

Work package WP4 – Demonstration of long-distance quantum communication network

Work Package Number	WP4	Lead Beneficiary	2 - Metroserit
Work Package Name	Demonstration of long-distance quantum communication network		
Start Month	6	End Month	36

Objectives
<p>Evaluation of additional parameters or components that must be used in order to ensure the functioning of real fibre-based QCI system operating in the long distance (i.e. around 70 km-150 km).</p> <p>Test planning and execution of the network in laboratory conditions.</p> <p>Demonstration of long-distance quantum communication.</p> <p>Dissemination of knowledge.</p>

Description
<p>Evaluation of different long-distance QCI technologies. Procurement of the devices in collaboration with WP1. Planning the tests and execution of the long-distance network in laboratory conditions.. Demonstration of long- distance QCI Depending on the regional discussions (WP5) the long-distance network in the field is planned (taking into account the future cross-border connections for EuroQCI). Different possible routes are analysed, taking into account possible end users and the quality of the fibre).</p>

Work package WP5 – Regional coordination and EuroQCI integration

Work Package Number	WP5	Lead Beneficiary	1 - MKM
Work Package Name	Regional coordination and EuroQCI integration		
Start Month	1	End Month	36

Objectives
<p>Planning of next phases of EuroQCI</p> <p>Regional cooperation</p> <p>Coordination with the European Commission and Member States</p> <p>Participation in the EuroQCI initiative and collaboration with the DIGITAL topic 3 project (co-ordination and support action CSA) and with other EuroQCI projects.</p>

Description
Cooperation with Latvia, Lithuania, Poland, Sweden and Finland to identify the best routes for terrestrial connections

with Central-Europe, including the planning of the end points, and facilities for a long-haul network. Discussions between Member States on future network setup, standardisation and lessons learned.

Based on discussions with the neighbouring countries, tests are planned between the countries (for example, between Finland and Estonia). Discussions will be based on knowledge acquired in the WPs 2 to 4.

The possibility for regional satellite interconnection is explored.

Regional workshops will be organised to gain a broader understanding of possible use cases and prepare for the future services.

Synergies are ensured between the projects to reach the full impact of the common goals of the EuroQCI initiative.

Work package WP6 – Creating impact and dissemination

Work Package Number	WP6	Lead Beneficiary	1 - MKM
Work Package Name	Creating impact and dissemination		
Start Month	1	End Month	36

Objectives

Implementation of the communication and dissemination plan
 Workshops and events for academia and industry to define future use cases
 Planning of future support measures for QCI services development for the industry
 Informing the general public

Description

The communication plan is drafted and implemented, target groups and communication messages are defined, events are held and media coverage is ensured.

To ensure future engagement of academia and industry, events are organised to bring together possible developers, service providers and end users from public and private sector. Discussions are held with the regulators and policy makers to secure the legal and regulatory basis for quantum communication in Estonia.

Planning of future support measures for academia and industry. The possibility to include R&D in the field of quantum communication in the existing support measures is analysed and explored. When necessary, new support measures are designed.

STAFF EFFORT

Staff effort per participant							
Grant Preparation (Work packages - Effort screen) — Enter the info.							
Participant	WP1	WP2	WP3	WP4	WP5	WP6	Total Person-Months
1 - MKM	3.00		6.00	6.00	10.00	10.00	35.00
2 - Metrosert	4.00	29.00	6.00	31.00	2.00		72.00
3 - RIKS	16.00	29.00	6.00	20.00	14.00	12.00	97.00
4 - EE MoD	4.00		6.00		4.00	6.00	20.00
Total Person-Months	27.00	58.00	24.00	57.00	30.00	28.00	224.00

LIST OF DELIVERABLES

Deliverables <i>Grant Preparation (Deliverables screen) — Enter the info.</i> <i>The labels used mean:</i> <i>Public — fully open (🚩 automatically posted online)</i> <i>Sensitive — limited under the conditions of the Grant Agreement</i> <i>EU classified —RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision 2015/444</i>						
Deliverable No	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month)
D1.1	Technical documents for the 1st review meeting	WP1	1 - MKM	R — Document, report	SEN - Sensitive	12
D1.2	Technical documents for the 2'nd review meeting	WP1	1 - MKM	R — Document, report	SEN - Sensitive	26
D1.3	Gap analysis and roadmap for alignment with the security baseline	WP1	1 - MKM	R — Document, report	R-UE/EU-R - EU Classified	36
D1.4	Procurement overview	WP1	1 - MKM	R — Document, report	SEN - Sensitive	12
D1.5	Technical documents for the 3'rd review meeting	WP1	1 - MKM	R — Document, report	SEN - Sensitive	36
D2.1	Evaluation report for the equipment	WP2	2 - Metrosert	R — Document, report	SEN - Sensitive	24
D2.2	Network deployment report	WP2	3 - RIKS	R — Document, report	SEN - Sensitive	36
D2.3	Deployment plan	WP2	3 - RIKS	R — Document, report	SEN - Sensitive	12
D3.1	Description of first use cases	WP3	1 - MKM	R — Document, report	PU - Public	24
D3.2	Evaluation report of the metropolitan networks	WP3	2 - Metrosert	R — Document, report	SEN - Sensitive	36
D4.1	Long-distance network test report	WP4	2 - Metrosert	R — Document, report	SEN - Sensitive	36

Deliverables

Grant Preparation (Deliverables screen) — Enter the info.

The labels used mean:

Public — fully open (🚩 automatically posted online)

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](#)

Deliverable No	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month)
D5.1	Plan for the cross-border connections in the region	WP5	1 - MKM	R — Document, report	SEN - Sensitive	36
D5.2	Report on participation to the EuroQCI initiative and on the collaboration with other DIGITAL projects, part 1	WP5	1 - MKM	R — Document, report	PU - Public	12
D5.3	Report on participation to the EuroQCI initiative and on the collaboration with other DIGITAL projects, part 2	WP5	1 - MKM	R — Document, report	PU - Public	26
D5.4	Report on participation to the EuroQCI initiative and on the collaboration with other DIGITAL projects, part 3	WP5	1 - MKM	R — Document, report	SEN - Sensitive	36
D6.1	Communication report, 1st period	WP6	1 - MKM	R — Document, report	PU - Public	12
D6.2	Communications report	WP6	1 - MKM	R — Document, report	PU - Public	36
D6.3	Report on dissemination and exploitation	WP6	1 - MKM	R — Document, report	PU - Public	6

Deliverable D1.1 – Technical documents for the 1st review meeting

Deliverable Number	D1.1	Lead Beneficiary	1 - MKM
Deliverable Name	Technical documents for the 1st review meeting		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	12	Work Package No	WP1

Description
Documents and presentations for the review meeting are prepared according to the requirements of the grant agreement.

Deliverable D1.2 – Technical documents for the 2'nd review meeting

Deliverable Number	D1.2	Lead Beneficiary	1 - MKM
Deliverable Name	Technical documents for the 2'nd review meeting		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	26	Work Package No	WP1

Description
Documents and presentaions for the review meeting are prepared according to the grant agreement. The financial figures are available 30 days after the reporting period, therefore the Review documents are available within 60 days of in accordance with the grant agreement pdata sheet point 4.2.

Deliverable D1.3 – Gap analysis and roadmap for alignment with the security baseline

Deliverable Number	D1.3	Lead Beneficiary	1 - MKM
Deliverable Name	Gap analysis and roadmap for alignment with the security baseline		
Type	R — Document, report	Dissemination Level	R-UE/EU-R - EU Classified
Due Date (month)	36	Work Package No	WP1

Description
Gap analysis and roadmap (including costs and timeline) arr prepared to achieve full alignment with the security baseline. Document, English.

Deliverable D1.4 – Procurement overview

Deliverable Number	D1.4	Lead Beneficiary	1 - MKM
Deliverable Name	Procurement overview		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	12	Work Package No	WP1

Description
Overview of the state of play of procurement procedures. Document, English

Deliverable D1.5 – Technical documents for the 3'rd review meeting

Deliverable Number	D1.5	Lead Beneficiary	1 - MKM
Deliverable Name	Technical documents for the 3'rd review meeting		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	36	Work Package No	WP1

Description
Documents and presentations for the review meeting are prepared according to the grant agreement. The financial figures are available 30 days after the reporting period, therefore the Review documents are available within 60 days of in accordance with the grant agreement pdata sheet point 4.2.

Deliverable D2.1 – Evaluation report for the equipment

Deliverable Number	D2.1	Lead Beneficiary	2 - Metrosert
Deliverable Name	Evaluation report for the equipment		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	24	Work Package No	WP2

Description
Testing of the devices for the metropolitan network in laboratory conditions and Metrological testing of the devices is carried out. Report of testing and evaluation of the in laboratory conditions is prepared.

Deliverable D2.2 – Network deployment report

Deliverable Number	D2.2	Lead Beneficiary	3 - RIKS
Deliverable Name	Network deployment report		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	36	Work Package No	WP2

Description
Report of the deployed metropolitan and round network is prepared.

Deliverable D2.3 – Deployment plan

Deliverable Number	D2.3	Lead Beneficiary	3 - RIKS
Deliverable Name	Deployment plan		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	12	Work Package No	WP2

Description
Deployment plan of the metropolitan network. Document, English

Deliverable D3.1 – Description of first use cases

Deliverable Number	D3.1	Lead Beneficiary	1 - MKM
Deliverable Name	Description of first use cases		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	24	Work Package No	WP3

Description
Based on workshops with stakeholders (cyber security industry, possible service providers and government agencies) relevant use cases are identified and a report is prepared. Document, in English and Estonian.

Deliverable D3.2 – Evaluation report of the metropolitan networks

Deliverable Number	D3.2	Lead Beneficiary	2 - Metrosert
Deliverable Name	Evaluation report of the metropolitan networks		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	36	Work Package No	WP3

Description
Evaluation of the network performance based on knowledge from the laboratory conditions and round network tests is carried out and a report is prepared (document, English, Estonian).

Deliverable D4.1 – Long-distance network test report

Deliverable Number	D4.1	Lead Beneficiary	2 - Metrosert
Deliverable Name	Long-distance network test report		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	36	Work Package No	WP4

Description
Planning the tests and execution of the long-distance network in laboratory conditions has been carried out and an evaluation report is prepared (document, English, Estonian).

Deliverable D5.1 – Plan for the cross-border connections in the region

Deliverable Number	D5.1	Lead Beneficiary	1 - MKM
Deliverable Name	Plan for the cross-border connections in the region		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	36	Work Package No	WP5

Description
Cooperation with Latvia, Lithuania, Poland, Sweden and Finland to identify the best routes for terrestrial connections

with Central-Europe, including the planning of the end points, and facilities for a long-haul network. Plan of the future connections is prepared. Document, English.

Deliverable D5.2 – Report on participation to the EuroQCI initiative and on the collaboration with other DIGITAL projects, part 1

Deliverable Number	D5.2	Lead Beneficiary	1 - MKM
Deliverable Name	Report on participation to the EuroQCI initiative and on the collaboration with other DIGITAL projects, part 1		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	12	Work Package No	WP5

Description

Document, english. Report on the project contributions to the broader EuroQCI initiative, and on the collaboration with other EuroQCI projects in the first half of the project.

Deliverable D5.3 – Report on participation to the EuroQCI initiative and on the collaboration with other DIGITAL projects, part 2

Deliverable Number	D5.3	Lead Beneficiary	1 - MKM
Deliverable Name	Report on participation to the EuroQCI initiative and on the collaboration with other DIGITAL projects, part 2		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	26	Work Package No	WP5

Description

Document, english. Report on the project contributions to the broader EuroQCI initiative, and on the collaboration with other EuroQCI projects in the second period of the project.

Deliverable D5.4 – Report on participation to the EuroQCI initiative and on the collaboration with other DIGITAL projects, part 3

Deliverable Number	D5.4	Lead Beneficiary	1 - MKM
Deliverable Name	Report on participation to the EuroQCI initiative and on the collaboration with other DIGITAL projects, part 3		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	36	Work Package No	WP5

Description

Document, english. Report on the project contributions to the broader EuroQCI initiative, and on the collaboration with other EuroQCI projects in the third period of the project.

Deliverable D6.1 – Communication report, 1st period

Deliverable Number	D6.1	Lead Beneficiary	1 - MKM
Deliverable Name	Communication report, 1st period		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	12	Work Package No	WP6

Description
Document, English. Communication and dissemination activities are described for the first period of the project.

Deliverable D6.2 – Communications report

Deliverable Number	D6.2	Lead Beneficiary	1 - MKM
Deliverable Name	Communications report		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	36	Work Package No	WP6

Description
Document, English. Communication and dissemination activities are described for the entire period of the project.

Deliverable D6.3 – Report on dissemination and exploitation

Deliverable Number	D6.3	Lead Beneficiary	1 - MKM
Deliverable Name	Report on dissemination and exploitation		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	6	Work Package No	WP6

Description
Document, English. Description of planned dissemination and exploitation activities.

LIST OF MILESTONES

Milestones					
Grant Preparation (Milestones screen) — Enter the info.					
Milestone No	Milestone Name	Work Package No	Lead Beneficiary	Means of Verification	Due Date (month)
1	Management setup	WP1	1 - MKM	Feedback from partners	3
2	Technical specifications	WP1	1 - MKM	All specification tables filled	6
3	Procurements	WP1	1 - MKM	All tenders available in the public procurement portal	9
4	Deployment plan for metropolitan network	WP2	3 - RIKS	Document is available	12
5	Equipment tested	WP2	2 - Metrosert	Test report and data available	18
6	Metropolitan network deployed	WP2	3 - RIKS	Network is available for use cases and testing	30
7	Evaluation report of the metropolitan network	WP3	2 - Metrosert	Evaluation report available for all participants	36
8	First use cases of the metropolitan network	WP3	1 - MKM	At least two use cases in the network, description of use cases available.	30
9	Long-distance network technologies evaluated	WP4	2 - Metrosert	Evaluation report	18
10	First demonstration of the long-distance network	WP4	2 - Metrosert	Test report, data	30
11	Plan for a long-distance network	WP4	3 - RIKS	The deployment plan is available	30
12	Identification of cross border partners	WP5	1 - MKM	At least two cooperation agreements with neighbouring countries.	36
13	Design of the cross-border network	WP5	1 - MKM	Document is available as a part of cooperation agreements	36
14	Feasibility analysis for the satellite link	WP5	3 - RIKS	Study report	36
15	International stakeholder cooperation	WP5	1 - MKM	At least two international events held.	36

Milestones					
<i>Grant Preparation (Milestones screen) — Enter the info.</i>					
Milestone No	Milestone Name	Work Package No	Lead Beneficiary	Means of Verification	Due Date (month)
16	Communication plan	WP6	1 - MKM	All relevant target groups reached (industry, academia, regulatory, general public)	36
17	Stakeholder involvement	WP6	1 - MKM	Event reports indicate involvement of at least 25 different stakeholders	36
18	Interim review	WP1	1 - MKM	Interim review report	14
19	Second intermin review	WP1	1 - MKM	Second Intermin review report	26

LIST OF CRITICAL RISKS

Critical risks & risk management strategy			
<i>Grant Preparation (Critical Risks screen) — Enter the info.</i>			
Risk number	Description	Work Package No(s)	Proposed Mitigation Measures
1	Costs of QQI systems rise due to high demand from EU countries	WP2, WP3, WP4	Procurements based on price. Eventual changes in the project plan to use less devices.
2	Equipment is not working as foreseen	WP2, WP3, WP4	Close collaboration with partners to exchange experiences and best practices. Availability of non-EU devices which might be more advanced.
3	Low interest of stakeholders to develop new products and services	WP3	Proactive engagement to bring together international stakeholders to exchange ideas and find potential services and customers.
4	Too few experts in Estonia to fulfil the tasks of the project.	WP2, WP3, WP4	Collaboration with other Member States to train experts.

Critical risks & risk management strategy*Grant Preparation (Critical Risks screen) — Enter the info.*

Risk number	Description	Work Package No(s)	Proposed Mitigation Measures
5	Neighbouring countries (Latvia, Lithuania) are not interested in developing networks and cross-border connections.	WP5, WP4	Proactive close collaboration with other Baltic countries. Alternatively prepare EuroQCI connections through Finland, who is well advanced in the project.
6	Project amendment to incorporate the round network to the project is not approved or not approved in time to be able to purchase the needed equipment in 2023.	WP2, WP1, WP3	Careful and thorough preparation of the amendment justification and supporting documentation is crucial for a successful proposal. It ensures that all the necessary information is provided, and the rationale for the amendment is clear and well-documented.



Digital Europe Programme (DIGITAL)



Technical Description (Part B)

for EstQCI project amendment - AMD-101113143-5

Version 9.0
8 October 2024



TECHNICAL DESCRIPTION (PART B)

COVER PAGE

PROJECT	
Project name:	Estonian Quantum Communication Infrastructure
Project acronym:	EstQCI
Coordinator contact:	Ingrid Linnas, RIKS

TABLE OF CONTENTS

TECHNICAL DESCRIPTION (PART B)	2
COVER PAGE	2
PROJECT SUMMARY	3
1. RELEVANCE	3
1.1 Objectives and activities.....	3
1.2 Contribution to long-term policy objectives, policies and strategies — Synergies	4
1.3 Digital technology supply chain	5
1.4 Financial obstacles	5
2. IMPLEMENTATION	5
2.1 Maturity	6
2.2 Implementation plan and efficient use of resources	6
2.3 Capacity to carry out the proposed work	11
3. IMPACT	14
3.1 Expected outcomes and deliverables — Dissemination and communication	14
3.2 Competitiveness and benefits for society	15
4. WORK PLAN, WORK PACKAGES, TIMING AND SUBCONTRACTING	15
4.1 Work plan	15
4.2 Timetable	16
4.3 Subcontracting	17
5. OTHER	17
5.1 Ethics.....	17
5.2 Security	17
1. SUMMARY OF THE PROJECT SECURITY ISSUES.....	17
2. SENSITIVE INFORMATION WITH SECURITY RECOMMENDATION	17
3. CLASSIFIED INFORMATION	18
3.1 Security aspects letter (SAL)	18
CONDITIONS UNDER WHICH THE BENEFICIARY MAY SUBCONTRACT	20
SECURITY CLASSIFICATION GUIDE	20
3.2 The security classification guide (SCG) (appendix B of the SAL)	20
3.3 Request for visit (appendix C of the SAL).....	21
3.4 Facility Security Clearance Information Sheet (FSCIS) (appendix D of the SAL)	21
3.5 Minimum requirements for protection of EUCI in electronic form at RESTREINT UE/EU RESTRICTED level handled in the beneficiary's CIS (appendix E of the SAL).....	21
4. SECURITY STAFF	24
4.1 Project security officer (PSO)	24
4.2 Security advisory board (SAB)	24
5. OTHER PROJECT-SPECIFIC SECURITY MEASURES	24
APPENDIX C	26
APPENDIX D	32
6. DECLARATIONS	36

ANNEXES.....	37
LIST OF PREVIOUS PROJECTS	37
PURCHASES AND EQUIPMENT	37
MKM support letter for round network.....	42
HISTORY OF CHANGES.....	44

PROJECT SUMMARY

Project summary

See Abstract (Application Form Part A).

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 events since February 2022 have forced us to put even more emphasis on security in this geopolitically interesting corner of Europe. 99% of Estonian governmental services are offered online. Thus, the functioning of our state is highly dependent on state-of-the-art cyber security solutions. Considering the rapid deterioration of the security situation in Europe during the recent year, the need for securing the vital e-Government services and ensuring a secure communication between different EU (and eventually NATO) Member States becomes even more evident. In addition, it has been recently demonstrated that conventional ways of securing information might not be robust enough as post-quantum cryptographic approaches have proven to be vulnerable¹.

In 2020, Estonia joined the EU cooperation framework for quantum communication, taking the commitment to participate in the preparation of the EuroQCI network. In 2022, the need for securing critical infrastructure and encryption systems against cyber threats, protecting smart energy grids, air traffic control, banks, healthcare facilities and more from hacking is more evident than ever. Estonia's cyber security strategy for the years 2019 to 2022 highlights the role of cyber security as an integral part of the functioning of the state, the economy and of internal and external security.

Estonia has been a pioneer in converting public services into flexible e-solutions for its citizens and e-residents. Thus, it is important to ensure that there are no major cyber incidents that would compel citizens to abandon the online services that have been developed since the early 2000s and are an integral part of the Estonian governance structure. There is a profound understanding in Estonia that creation and development of a successful digital state requires strategical coherence between developing information society and ensuring cyber security.

The implementation of the Government Cloud solution provides an excellent foundation for public e-services and solutions, making Estonia the most digital country in the world. With the Government Cloud solution, Estonia is taking the next step in its digital evolution to expand its ICT society. The Estonian Government Cloud will lead to the modernization and renewal of existing information systems, to embrace the opportunities offered by cloud technology and allow more agility in provision of e-services by the Estonian government agencies and critical service providers to residents and e-residents. Estonian public institutions will gradually transition from existing legacy systems to the new Government Cloud solution. Therefore, Estonia's cybersecurity strategy aims to become the most secure digital state to protect government data and ensure the state's longevity. With the advancement of quantum computing, this vision requires an understanding of possible uses of quantum technology for cybersecurity, the development of competences and infrastructure while supporting the relevant industry.

¹ https://www.quantamagazine.org/post-quantum-cryptography-scheme-is-cracked-on-a-laptop-20220824/?fbclid=IwAR0d2KItxINeV47MF_taj9NBj9LQe-MNKnIR3llhj6iKWSAuGtaspB_DiWA

The Estonian State is currently constructing a new round network between data centers that will house the Government Cloud. The EstQCI project has the opportunity to enable Estonia to be the first state to secure its Government Cloud with Quantum Communication Technology. The Estonian QCI project aims to lay the foundation for scaling up the respective competence in Estonia and providing infrastructure for the industry to secure e-Government services. Implementing QKD technology in the round network of data centers will enable us to enhance the privacy and cybersecurity of our citizens' data, which is currently stored and managed by existing legacy systems, including state registries, healthcare, social benefits, vehicle and transportation systems, to name a few.

The project aims to build up a metropolitan QCI networks and long-distance link to be ready for connections with neighboring countries.

In these networks, devices from EU-27 developers will be used, when possible. The main goals of the project are as follows:

- a) Building up the know-how and competence of relevant entities for future deployment of QCI networks and services
- b) Testing the readiness of devices from EU-27 producers to gain information about their suitability for the Estonian conditions and needs
- c) First demonstrations of the use of the network between metropolitan areas as well as for long-distance network in laboratory conditions
- d) Collaborating with neighboring countries and preparation for cross-border links with Finland and Latvia
- e) Sharing knowledge with relevant stakeholders, raise the awareness of companies and other relevant entities about the possibilities of the network to prepare for future secure connectivity/ cyber security applications.
- f) Demonstration of QKD implementation and usage on low latency and high-capacity connections between servers in a round network, securing the Estonian Government cloud services.

One of the important elements of the EstQCI project is coordination with Finland, Latvia, Lithuania, Poland and Sweden to create a foundation for the future cooperation within the margins of EuroQCI project and to prepare for terrestrial cross-border connections between Member States.

As a result of the project we will open our network for interested parties (for example cyber security industry, academia etc) and facilitate the exploration of further use cases of the network. We will build up a wide-scale competence among the relevant stakeholders in Estonia and facilitate international collaboration of relevant companies and academia. The purpose of this action is to prepare for the further development of quantum cyber security industry in Estonia and in Europe with the focus on secure e-services.

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.

One of the main objectives of the Digital Europe program is to build up essential capacities to secure EU's digital economy, society and democracy through reinforcing EU's cybersecurity industry and competitiveness. The EstQCI project will contribute to building up the necessary infrastructure in Estonia to ensure that the essential capacities are in place for further developments in the area of quantum communication. Additionally, the project will build up a strong base of knowledge among Estonian enterprises and academia to enforce competitiveness of Estonia's cyber security industry.

The EstQCI project intends to use products from EU-27 companies, supporting the growth of an EU-27 value chain with feedback based on actual tests in the field. During the project we can identify specific ways how research institutions and companies in Estonia can contribute to EU-27 value chain in the domain of quantum communication. Estonia's cyber industry is well advanced, and its added value is 20 years of knowledge of securing a digital state and governmental e-services.

Estonian is advanced in their e-Government services from which many are already running on our Government Cloud servers. In cooperation with the Estonian State IT Centre and the Estonian Information Systems Authority, the EstQCI project will test the QKD systems on real life low latency and high speed connections between data centers that house the Government Cloud. The experience obtained through

these demonstrations is valuable input for further developments in the area of quantum communication implementation for securing large capacity networks. In addition, the results from these tests will lay the foundation of future National Cyber Security policies and strategies.

The implementation of QKD to the Government cloud will enable us to lay the foundation to start using the cloud services to share Classified information within the state and after the connections of EuroQCI also internationally.


Furthermore, Estonia has been building up competences in the field of quantum metrology, which allows us to contribute to the metrological testing and traceability of EU-27 devices and services for example in the field of low photon flux detectors. Metrological testing of devices and networks will add an additional layer of trust to the QCI network.

The expected outcome of the EuroQCI project is a QCI network covering all Member States of the EU. EstQCI project will lay the foundation for connections between Finland and Latvia (and possibly Sweden) to ensure that the countries in Northern Europe, where satellite links might not work as effectively because of weather conditions, will not remain in isolation.

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.

The number of EU27 industrial providers of needed technology solutions and equipment is small. As technology is continuously developing, still most of the work is conducted within single laboratories and is country-specific. Therefore, it is essential to closely collaborate with EU-27 providers in the preparation phase of the network to find devices that are most suitable for the Estonian QCI.


Although a number of EU-27 producers have started to offer products for QCI systems, several of them will probably not be able to offer a product that is market-ready in time for the EstQCI project (for example KeeQuant, Q*Bird B.V. or LuxQuanta). Regardless, it is important to discuss and exchange information with these producers to ensure that their future applications are appropriate for the large-scale deployment of the EuroQCI network. Other producers such as ID Quantique Europe, QTI or ThinkQuantum are more advanced in their approaches and offer market-ready solutions that can be considered for the EstQCI project.

Cross-EU quantum communication infrastructure requires a standardised approach. This project will contribute to elaboration of standardised approach in establishing co-operation with neighbouring EU Member States and European Commission. Moreover, by implementing and testing equipment available from EU-industries, activities of the present project will facilitate enhanced performance, ease of use and availability of equipment for future cyber-security applications.

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.

For the project execution, no major financial obstacles are foreseen. The project has been prepared within the relevant ministries that are responsible for securing governmental funds necessary to execute the project.

The further development of QCI network in Estonia depends on the future initiatives from the European Union as well as the development of the market for cyber security solutions involving QCI. Ideally, the services provided on the network will cover the cost of maintaining the network (for example the rent of fibre) after the project period. For this reason, the involvement of relevant stakeholders and providing the basis for future development of services is important.

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.

Tasked by the Ministry of Economy and Communications, Metroserf and RIKS have been preparing the project since the end of 2021 in close cooperation with Finland. The change of regional security situation in the beginning of 2022 challenged the long-term planning of R&D and infrastructure projects due to increased uncertainty of the security in the region. However, as Estonia joined the Quantum Initiative already in 2020, it was clear that further development in this area must be prioritized. Estonian representatives have participated in EuroQCI Sherpa meetings, NSA/NCSA meetings and other relevant online events and meetings. We have also discussed further developments with representatives of neighboring countries to prepare for the next phases of the EuroQCI project (cross-border connections).

Estonia is advanced, with more than 20 years of experience, in securing a digital state and governmental e-services. The development and implementation of Governmental Cloud is bringing Estonia to the next step in its digital evolution to expand its ICT society. The long experience will contribute to developing and testing the QKD systems in real life environments and give valuable input to the development of Quantum technologies.

In parallel, Metroserf has been participating in research projects in the field of quantum metrology in past 10 years to build up the competence for exact measurements in quantum optics. One of ongoing projects for example aims to develop bright entangled photon sources based on different application-oriented platforms and to exploit high-purity single-photon sources to demonstrate the quantum advantage achievable using these sources for specific measurements. For the purposes of these research projects, Metroserf has built up specific laboratory conditions as well as secured that in house scientific expertise is available for measurements and R&D in quantum optics. These laboratory conditions are ready to facilitate the development and testing of the QCI network for the purposes of this project.

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 implementation plan of the EstQCI consists of six work packages. The targeted objectives are introduced in Section 4. The cross-participation and collaboration of the consortium members in the EstQCI Work Packages ensure efficient usage of resources and knowledge sharing.

The first phase of the project is a thorough planning of different aspects of the project, including its management and coordination, procurement specifications and procurement coordination. Discussions will be held with EU-27 producers and other Member States to specify which kind of equipment is the most suitable solution for next phases of the project. The planning process, including the consultations, will ensure that two criteria are met: the devices used in the network fit EstQCI project needs and resources are effectively used.

After the planning phase, three testbeds will be implemented for QCI experimentation:

1. The QCI metropolitan testbed

The QCI Metropolitan Testbed is used to test commercial QCI systems at first in a laboratory network environment, to allow faster and cost-effective benchmarking of different devices in different network configurations and conditions, but also to efficiently learn how to use and interface the devices before starting their actual on-field deployment.

With the QCI Metropolitan Testbed it is planned to test commercially available QCI devices. From the discussions with the providers so far, the understanding is that QKD they support can include Point-to-Point links and Point-to-Multipoint links based on optical switching, but most commercial QKD systems operate best with Point-to-Point links. This will be taken into account when establishing QCI metropolitan testbed.

The testbed can be metrologically facilitated by using freshly obtained Time-Correlated-Single Photon Counting system which includes both, a transmitter and a receiver testing capability. The system includes

two SPAD detectors in Hanbury-Twiss interferometer configuration allowing sources to be measured. In case of measurements of detectors, each SPAD can be used separately. For the purpose of the present project, the measurement system may need to be modified and enhanced in terms of wavelength range, as the QKD commercial devices use O- and C-bands.

The advantage of using existing system using openly available materials facilitates accumulating expertise in quantum communication technologies and experimenting different QKD aspects without depending on so-called black-box technologies. The possibility of familiarizing researchers with all aspects of QKD is an additional benefit of the system design and its further open use, e.g. for academia.

After testing in the lab, the Testbed will be deployed in the field between two institutions (approximately 10 kilometres apart). Its primary purpose is to gain a complete hands-on experience on all layers of the QCI (hardware and software aspects, security requirements and resilience against attacks).

2. The QCI long-distance testbed

This will be the first step toward the possible future backbone QCI network. A long-distance network is also needed for eventual cross-border connections. In this phase, different products of EU-27 producers are considered to ensure minimal signal loss. Tests and execution of the long-distance network in laboratory conditions will follow. Additionally, the long-distance network in the field is planned (also taking into account the future cross-border connections for EuroQCI). Different possible routes are analysed, depending on the discussions with neighbouring countries. Different considerations are taken into account, for example the existing fibre and network infrastructure, possible secure locations for the nodes and management conditions of these nodes.

In these two testbeds, a wide range of specifications must be tested. In addition to QCI devices also external detectors, encryptors and KMS. (Metrological) evaluation of the devices and the two testbeds is an integral part of the project to add an additional layer of trust to these systems. In addition, several aspects must be tested in both testbeds: QCI key performance indicators for metropolitan and long-distance networks; Network Line interfaces; physical environment and security requirements and network reliability. A control and management plan must be set up and general requirements for the network management need to be defined.

The key parameters to be tested and used for benchmarking purposes (both in the lab and on-field) of the QCI systems are:

- long-term stability
- key-rate at typical loss levels
- maximum tolerable loss
- KMS support and functionalities supported

At first, the QCI devices and their possible integration with the classical security infrastructure will be tested in the laboratory environment. The existing Metroserf facility described above is used for network testing in the laboratory conditions. After the needed performance and stability are reached in laboratory conditions, the works with long distance network can be started.

First of all, the backbone route across Estonia starting from Tallinn should be discussed and possibly decided. The QKD link between Estonia and Finland will be located in (or nearby) Tallinn, but the link with Latvia has not been finally decided. Efficient way to deploy long-distance QKDN is by using existing optical fibre infrastructure, which is currently located along railway. Future options accompanying with establishing railway connection Rail Baltic have to be cleared (see Figure below). Either direction of backbone can set some limits to the number of QKD nodes along the routes.



The present commercial QKD system are capable of covering up to 50 km (70 km-80 km upon special request) because of typical tolerable loss of about 20 dB being different for O- and C-band. For example, 70 km (distance from Tallinn to Tapa) long fibre loss is 26 dB at the wavelength of 1310 nm and 16 dB at the wavelength of 1550 nm. Promising MDI-QKD systems can reach 40 dB (and possibly beyond), not only allowing to avoid several trusted nodes, but it would lead to some advantages and more cost-effective solutions. Firstly, the same untrusted node can be used not only to connect just two users, but also to possibly build a star network connecting several users. In addition, by definition, the untrusted node does not require the same level of security of a trusted node. It must be secured to avoid denial-of-service (DoS) attacks but there is no risk that critical information is leaked to an eavesdropper. Furthermore, two MDI-QKD star networks can be connected via a shared node acting as a trusted node. Such configurations is very efficient, because a single trusted node can connect all the users of the two-star networks and may be useful for Estonian users in the future.

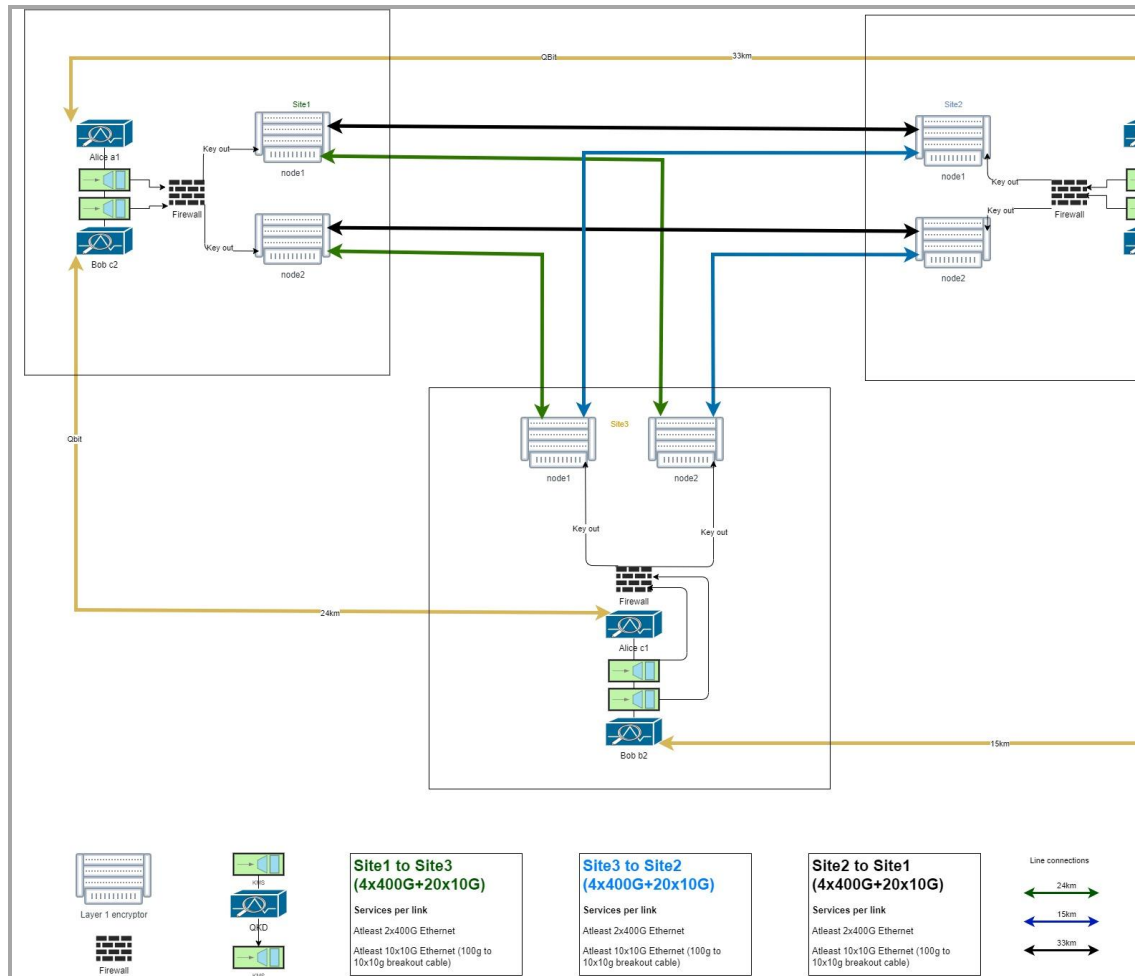
For key distribution, we might consider to develop QKD network (QKDN) components with basic core functionality including key-manager, QKDN controller, and management/orchestration components. The design and implementation will be based on exiting ETSI and ITU-T specifications, and high-level microservice oriented software frameworks. The main goals would be to support our testbed implementation by providing the required key management functions, like access control and key relaying, for testing and demonstrations, and to provide a platform for enhancing national capabilities for evaluating QKDN solutions. Furthermore, integration with universities simulating and evaluating QKDN performance would be an option.

The physical fibre route implementation of the project separates the fibres needed for quantum channels all the way through the planned connections. Due to security reasons, and in order to get lower attenuation for the quantum channel, the fibres can be connected to each other by fibre splicing instead of using ODF panels (Optical Distribution Frames). The site infrastructure construction work, if needed, will cover the required implementation of footprint, electricity, and cooling inside a trusted site location with high-security surveillance.

Also, tests for environmental conditions of QKD devices should be carried out to ensure proper operation in-the-field. Installations, joints and connections of optical fibre may depend on ambient conditions.

3. The QCI round network testbed for e-Government services

The Estonian State IT Centre and the Estonian Information Systems Authority are currently building up a new round network of data centers that will house the Estonian Government Cloud services. This gives the EstQCI project an opportunity to demonstrate the QKD functionality in real life high speed and low latency data center environment.

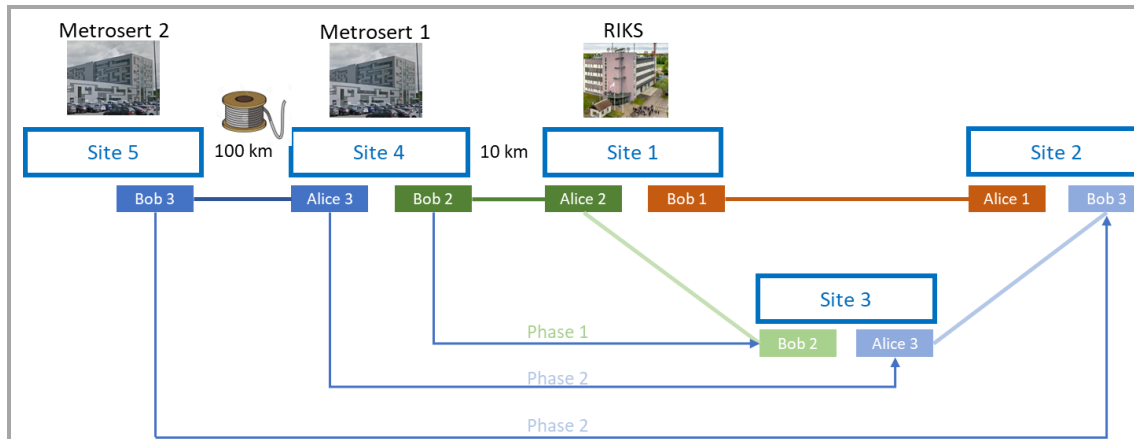


The testing of QKD within this network will be conducted in three phases to optimize project time efficiency and evaluate various solutions.

- In the first phase, two QKD systems will be integrated into the network for initial functionality and integration tests, utilizing lower 10G ports. Solutions for supporting three sites with two pairs of QKD devices will be established.
- In the second phase, the third QKD pair will be transitioned from Metrology tests to the round network. Initial functionality and stability tests will be conducted at lower speeds
- The third phase will involve the implementation of QKD for 400 G connections with low latency.

During the first stage, we will install and configure 2 QKD device pairs to work with 10 G Ports in the network. This setup is designed to thoroughly test functionality, key distribution, and network management. Close cooperation between the project team and the manufacturers of the QKD and network devices is essential during this phase to gain valuable insights into how QCI systems should be constructed and configured.

Throughout these tests, we will also explore the feasibility of supporting three sites with just two QKD device pairs. This investigation aims to develop strategies for failure management in the event of the loss of one QKD device in the round network. Additionally, we will assess the potential for reducing investment costs in future networks that may require fewer QKD devices. By focusing on moving only one device paid, we can conduct fundamental metrological tests and network integration concurrently, maximizing the efficiency of project time utilization.



In the second phase, the third QKD device pair will be introduced to the round network, and a comprehensive circular solution will undergo initial testing, starting with lower speeds on 10G ports. During this phase, rigorous operational, management, and monitoring tests will be conducted. This stage is crucial to ensure the stability of both the QKD and network devices, guaranteeing their reliable integration and operation before implementing the technology for high-speed connections.

In the third phase, the QKD devices will be integrated with high-speed, low-latency 400G connections. Testing at these higher speeds will provide valuable insights into the real-world requirements for QKD systems between data centers.

The key parameters to be evaluated:

- Collaboration and cooperation between QKD and network devices
- Configuration and monitoring requirements for key exchange
- Performance and stability of key management at high speeds.
- Key rate requirements in real-life environments
- Strategies for handling failure modes.

In preparation for the EuroQCI, the knowledge gained from these tests will provide valuable insights into the requirements for international connections. Once the EuroQCI connection is established with Finland, our ambition is to leverage the Government Cloud for cross-border communication and connect to the Quantum Computer LUMI in Finland. This connection to LUMI will grant Estonian state institutions, academia, and industry access to secure quantum computing power, fostering collaboration and innovation across various sectors.

An integral part of the project is the involvement of different stakeholders in all work packages. Governmental entities must be involved to ensure that possible future regulatory conditions are in place for actual network deployment and usage. In addition, different governmental entities will be responsible for later deployment of a backbone network. Thus, an active knowledge transfer through different workshops must be ensured to guarantee the trained personnel necessary for possible next steps. Additionally, industry, academia and future service providers must be involved to identify possible use cases. During the project, future support measures for product and service development for the industry are defined (financial support measures and various staff training possibilities).

The goal is to reach 75% of relevant representatives of academia (the target audience are two largest universities of Estonia: Tartu University and Tallinn University of Technology and other relevant technical research institutions). Because of the relatively low number of possible relevant representatives of academia in Estonia, it is likely to reach most of the target audience with the dissemination activities.

In terms of engaging service providers and industry, the approach will be based on relevant industry associations (for example: Estonian Electronics Industries Association, Estonian Defence and Aerospace Industry Association). Active involvement of 5 to 10 companies (based in Estonia) in workshops is realistic, taking into account the number of relevant industry representatives in Estonia.

Project management, quality assurance and monitoring and evaluation strategy

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 is described in Section 2.3 and its detailed description will follow in the consortium agreement (including quality assurance). For each Work Package, milestones are described in Section 4.2. These milestones allow one to monitor the progress of each Work Package towards the objectives of the project.

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 procurements of the project will be carried out in accordance with the Estonian Public Procurement Law, one of the leading principles of which is to ensure resource-efficient use of public funds. Instead of purchasing the devices, the possibility of renting them is explored to ensure that during the project only those devices are purchased that can later be used for further development of the EuroQCI project. During the preparation of technical specifications for the procurements, discussions with regional partners are held to exchange experiences and best practices and procure devices that are interoperable. The field demonstrations will be conducted using a fibre that has already been deployed to avoid additional cost in infrastructure.

All consortium members will report the financial aspects to the project manager/coordinator (MKM), who will be responsible for the cost-efficient use of all financial resources and report to the European Commission.

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 includes two leading ministries (Ministry of Economic Affairs and Communications and Ministry of Defence), which indicates the importance of the project for the Estonian government. In addition, State Infocommunication Foundation brings in the expert knowledge in the field of infrastructures and infocommunication services. Metrosert's role as a research and development institution is to provide expertise in the field of quantum communication and testing experimental solutions.

Ministry of Economic Affairs and Communications (MKM) - The objectives of the Ministry of Economic Affairs and Communications is to create overall conditions for the growth of the competitiveness of the Estonian economy and its balanced and vital development by drafting and implementing Estonian economic policy and evaluating its outcomes. The Ministry develops national development plans in the spheres within its area of government and will ensure their coordination with various transnational development plans, organises the funding, implementation and performance evaluation of such plans. Co-operation with the European Union and international organisation is organised within the Ministry's area of government. The Ministry of Economic Affairs and Communications elaborates and implements the state's economic policy and economic development plans, including in the field of information society. <https://www.mkm.ee/en>

Ministry of Defence - The Ministry of Defence is responsible for organising national defence, including the roles of National Security Authority and National Classified Communication and Information System Security Authorities with responsibilities in management and control of the procedures and measures for

protecting classified information. One of the tasks of the MoD is to ensure that Estonia is capable for defending itself against cross-domain external threats. <https://kaitseministeerium.ee/en>

State Infocommunication Foundation (RIKS) - Created at the end of 2000, RIKS (State Infocommunication Foundation) is a non-commercial foundation administered by the Ministry of Economic Affairs and Communications. RIKS provides communication-related services for public institutions and other state-budgeted institutions and operative communication. RIKS provides operative, radio and maritime communications, and telephone services. The mission of RIKS is to provide public institutions, local municipalities and other state budgeted institutions with cohesive, high quality, secure and cost-effective communication-related services, including communications for specific purposes through its own infrastructures and infocommunication services delivered from the free market. <https://riks.ee/>

Metrosert AS – Metrosert is a state-owned company, an evaluated research and development institution and an accredited calibration laboratory. Pursuant to a long-term agreement with the Estonian Ministry of Economic Affairs and Communications, Metrosert fulfils the functions of the Central Office of Metrology in Estonia (equivalent to a National Metrology Institute). Metrosert has 20 years of international experience with research projects in the field of optical metrology. <https://metrosert.ee/en/company/>

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	Organization	Role/tasks/professional profile and expertise
Kaido Tee	MKM	Project coordination / 5 years of cyber security management and cyber exercises experience
Erik Janson	MKM	General coordination (WP3)/ 20 years of experience in ICT, security, infrastructure and Greentech areas both business and technology management role
Ingrid Linnas	RIKS	Primary Coordinator Contact, Project manager / 12 years of project management experience
Priit Kollo	RIKS	General coordination (WP2)/ WP4/ 20 years of IT and network solutions management experience.
Raimo Kure	RIKS	WP 5/ 21 years of experience in satellite solutions.
Kristo Gumbälis	RIKS	WP 2, WP3; WP4/ 7 years of network administrator experience. Cisco certified associate.
Raido Raidma	RIKS	WP2, WP3, WP4/ 7 years of network administration and implementation experience.
Andres Kuusk	RIKS	WP2; WP3; WP4/ 8 years of experience in system integrations.
Mari Aru	Metrosert	General coordination (WP1- WP4)/ Head of R&D at Metrosert
Aigar Vaigu	Metrosert	WP2, WP3, WP4, advisory role/ Research experience in quantum optics (low photon flux optics)
Toomas Kübarsepp	Metrosert	WP2; WP3; WP4/ Professor of Metrology, PhD in optics. Over 20 years of research experience
Meelis-Mait Sildoja	Metrosert	WP2, WP3, WP4/ PhD in measurement science (optics). 17 years of research experience.

Mihkel Rähn	Metrosert	WP2-WP4, Research scientist, PhD in physics (optics)
Miiko Peris	MoD	Head of Department of Innovation
Greta Elva-Jõemaa	MoD	Cyber Policy Advisor, Department of Innovation
Marek Lehtsalu	MoD	NSA, NCSA representative

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.

For specific questions concerning devices and technology, scientists from the University of Tartu could be involved in advisory roles. Collaboration with network providers (rent of fiber) and providers of QCI systems and subsystems is necessary. Close cooperation with the Estonian State IT Centre and the Estonian Information Systems Authority to successfully implement and manage the QKD devices in real data centre environment. Additionally, we will collaborate with neighbouring countries to exchange experiences and learn from each other. We will also work in close contact with the European Commission to ensure that our project is in synergy with other initiatives from the Digital Europe Programme.

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.

Consortium management will ensure the management of the project in terms of KPIs, financial plan and results in accordance with the Grant Agreement.

The project coordinator is responsible for the overall coordination of the project. The project coordinator is the representative of the project.

On 1. of March 2023, it was decided to reorganise the roles, with Mrs Ingrid Linnas acting as the Project manager and taking the role over from MKM. In the portal definition Mrs Ingrid Linnas is taking the role of Primary Coordinator Contact, and Mr Kaido Tee keeping an unofficial supporting role. This was registered and agreed from the Commission side on the 4 of April 2023.

The project official Coordination and ownership will remain in MKM in terms of strategic coordination, the allocation and distribution of financial contributions received from the European Commission. The project manager role is transferred to RIKS's and assigned to Mrs Ingrid Linnas.

The project manager is responsible for the management of the project and for the communication between different members of the consortium. The project manager will also coordinate the communication with partners (other countries, European Commission). The project coordinator ensures that the project is in line with the Grant Agreement. Project manager deals with all administrative and financial issues.

The project manager will set up regular meetings within the consortium to ensure information exchange and progress. Work Package meetings are organised by Work Package leaders. In addition, the project coordinator will organise review meetings with the European Commission. All meetings will be held in a hybrid format.

A detailed description of the responsibilities of each partner will be included in the Consortium Agreement. This agreement will also define mechanisms for dealing with possible conflicts between the members of the consortium. Consortium agreement will determine the decision-making process between the members of the consortium. The consortium agreement will also describe a quality management plan to ensure the management of project related documentation; monitoring/quality control of the KPIs and management of potential risks.

The role of the project coordinator will also be to manage the allocation and distribution of financial contributions received from the European Commission. The project coordinator will be responsible for meeting the requirements and rules of the Digital Europe Program.

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.

During the project, advanced experimental quantum systems and networks are deployed in Estonia using pilot devices and systems produced by EU-27 companies where possible. This will contribute to further standardization and development of these systems towards maturity and help to define the needs of EuroQCI.

The EstQCI project will make the systems and networks available for testing to prepare relevant stakeholders for the large-scale uptake and use of such systems and technologies. The project aims to involve different national stakeholders to demonstrate the first use of QCI systems in different application scenarios. Quantum networks will be made available to industries contributing to developing national-based products and services. This will contribute to preparation for the future large-scale deployment of EuroQCI. An open-access testbed and trainings provide tools for training potential future users of the network. Hands-on experience with the network will help to formulate new business ideas and design services, which will create new opportunities for Estonian companies. These new services and products will contribute to a competitive European quantum communication industry.

Quantum systems will be made available for educational purposes providing a training environment for technical and research staff as well as national users from public authorities or other organisations. This will ensure that there are enough trained personnel to deploy a larger scale quantum communication network in Estonia in the future. It will also contribute to the success of further projects in the same field in cooperation with the European Commission and other Member States.

During the project, the first long-distance quantum communication network in Estonia will be demonstrated in laboratory conditions to prepare for the large-scale deployment of a QCI in the region. A round QKD network will be demonstrated and tested in real life data center environment. This will open up the possibility to test the integration and cooperation of QKD, PQC and traditional cybersecurity systems. Deploying the experimental QKD systems with advanced high speed and low latency connections aims to prepare for the large-scale uptake and use of such systems and technologies for State communication, Private sector and the EuroQCI connections. The experience gained from the EstQCI activities will enable to lay the foundation for securing the Government Cloud services and gain inputs to State and commercial cyber security strategies and policies.


Cross-border deployment is prepared in cooperation with neighboring countries. This will contribute to regional deployment of the EuroQCI network to ensure that no country in Northern-Europe stays isolated from a terrestrial connection to Central Europe.

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.*

Dissemination and communication are key activities for the EstQCI project. The purpose of these activities is to explain the project to different stakeholders as well as to general public so that a broader understanding of the benefits of quantum communication is achieved. It is important to define the target groups for different communication activities. The most important target group consists of the key stakeholders – cybersecurity industry and R&D institutions. It is important that these institutions have an opportunity for exchange to identify potential new products and services. Communication message to this group is targeted to availability of a new network and the opportunity to use this network for testing purposes. Another important target group comprises the potential end users of new products and

services. These can be different governmental institutions or companies that provide services for the end user (healthcare or financial institutions). The communication activities for this group will be aimed at creating awareness of potential new services and map the needs of the customers. Third target group consists of regulators and policy makers, as well as media representatives and general public. Communication messages to this group are aimed at raising general awareness and justifying the public investment to the project.

The channels to reach the three above mentioned target groups are different. We will involve different industrial associations and organise events to bring together potential service providers and customers. Whenever possible, these events will be organised for an international audience because of the limited size of Estonian industry. In this way we can broaden the circle of potential collaborations between stakeholders. We will also organise several project workshops to promote the access to the network as a testbed and bring together academia and industry. The broader public will be informed through media coverage and social media channels of the members of the consortium. During the project we will define KPIs for dissemination and communication activities.

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

EstQCI project will strengthen the competitiveness of Estonia's cyber security industry by offering an opportunity to develop and test new products in the field of quantum communication. This will result in creation of new jobs and additional tax income. In addition, the project will contribute to the enhancement of national competences in preparation for the full EuroQCI deployment. These competences can be used to create new services for EU's market.

Securing the network of servers with Quantum Technologies will facilitate the secure transition of Estonian public institutions to a new Government Cloud solution. Centralizing all databases and information in one location presents opportunities to advance e-services, ultimately achieving the desired one-point access to all governmental services and information securely. This ensures that Estonian residents and e-residents can benefit from the protective capabilities of digitalization, ensuring the safety of our digital lives.

Through these measures, we are making significant strides in digital development by bringing the government closer to its people and simplifying the process of accomplishing our needs and desires. Most importantly, if the common infrastructure of quantum communication has been built up in Europe, our society can benefit from standardized and secure information exchange, may it be information exchanged between security institutions, protection of personal data or flawless functioning of a digital state.

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)).

WP1 Project management and procurement coordination

WP2 Development of trustworthy quantum communication network topology in metropolitan area.

WP3 Testing of deployed QCI in metropolitan area

WP4 Demonstration of long-distance quantum communication network

WP5 Regional coordination and EuroQCI integration

WP6 Creating impact and dissemination

4.2 Timetable

Project extension
<p>The project consortium is formally requesting an extension of the project duration by six months, until the end of 2025. This request is due to delays encountered during the testing and deployment phases of the project, specifically related to the Quantum Key Distribution (QKD) devices.</p> <p>The procurement of the QKD and encryption systems was completed at the end of 2023, with testing initiated in Q1 2024. However, evaluation testing has revealed multiple instabilities and software issues within the QKD systems, significantly affecting the progress of both the test plan and the deployment of the metropolitan network. The software modifications required to resolve these issues have led to notable behavioral changes in the QKD devices. As a result, the testing conducted before and after the software updates is no longer comparable.</p> <p>Furthermore, the software releases for the encryption devices, enabling the use of QKD (ETSI 014 standard) on 400G connections has been postponed to Q1 2024. This delays the start of high speed testing on the ring network.</p> <p>To ensure accurate and consistent results, many of the test plan activities will need to be repeated, causing an estimated delay of at least four months. Additionally, given the delayed software release for encryption devices and ongoing instability of the QKD devices, we anticipate further challenges during the ring network testbed phase. Therefore, we foresee the need for an additional six months to complete the project effectively and ensure that all objectives are met.</p> <p>This extension will allow the consortium to address the existing issues thoroughly and deliver reliable outcomes within the extended timeframe.</p>

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	Q 3	Q 4
T1.1 - Project management												
T1.2 - Procurement coordination												
T1.3 - Alignment with the security baseline												
T2.1 – Preparation for the networks												
T2.2 – Testing of the devices												
T2.3.1 – Deployment of the metropolitan network												
T2.3.2 – Deployment of the round network												
T3.1.1 – Evaluation of the metropolitan network												
T3.1.2 – Evaluation of the round network												
T3.2 – Identification of use cases												
T3.3.1 – First use cases in the metropolitan network												
T3.3.2 – First use cases in the round network												
T3.4 – Knowledge dissemination												
T4.1 – Evaluation of technologies												
T4.2 – Test planning and execution of long-distance network												
T4.3 – Demonstration of the network												
T4.4 – Planning of the long-distance network in the field												
T5.1 – Planning of cross-border connections												
T5.2 – Planning of international testing												
T5.3 – Discussions on possible satellite interconnection												
T5.4 – International stakeholder events												
T5.5 - Participation in the EuroQCI initiative and collaboration with the DIGITAL topic 3 project (co-ordination and support action CSA) and with other EuroQCI projects.												
T6.1 – Implementation of the communication plan												

[illegible]

Color legend:

	Original plan		Amendment new plan
			Amendment removed time

4.3 Subcontracting

No subcontracting

5. OTHER

5.1 Ethics

<p>Ethics</p> <p><i>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 .</i></p>
<p>See annex</p>

5.2 Security

INFORMATION ON SECURITY ISSUES (SECURITY SECTION)

Table of content:

1. *Summary of the project security issues*
2. *Sensitive information with security recommendation*
3. *Classified information*
 - 3.1 *Security aspects letter (SAL)*
 - 3.2 *The security classification guide (SCG) (appendix B of the SAL) NB: There is no appendix A.*
 - 3.3 *Request for visit (appendix C of the SAL)*
 - 3.4 *Facility Security Clearance Information Sheet (FSCIS) (appendix D of the SAL)*
 - 3.5 *Minimum requirements for protection of EUCI in electronic form at RESTREINT UE/EU RESTRICTED level handled in the beneficiary's CIS (appendix E of the SAL)*
4. *Security staff*
 - 4.1 *Project security officer (PSO)*
 - 4.2 *Security advisory board (SAB)*
5. *Other project-specific security measures*

Appendix C

Appendix D

1. SUMMARY OF THE PROJECT SECURITY ISSUES

Possible security issues in the project concern potential future uses of the new quantum communication network. If the network will be used for exchanging classified information, the planning of the future network and its operational details could be considered classified as well. In addition, the Commission plans to define a security baseline for EUQCI projects by 2024. As a result, a gap analysis and roadmap on how to reach this baseline has to be created as a part of the EstQCI project. The dissemination level of these documents will be RESISTENT UE/EU RESTRICTED

2. SENSITIVE INFORMATION WITH SECURITY RECOMMENDATION

Sensitive information with security recommendation

Number and name of the deliverable	Name of lead participant	Date of production	Name of entity authorised for access
1.3 Gap analysis and roadmap for alignment with the security baseline	MKM	M30	MKM EE MoD

3. CLASSIFIED INFORMATION

3.1 Security aspects letter (SAL)

SECURITY ASPECTS LETTER (SAL) — SECURITY REQUIREMENTS	
GENERAL CONDITIONS	
1.	This security aspects letter (SAL) is an integral part of the classified grant agreement [or subcontract] and describes grant agreement-specific security requirements. Failure to meet these requirements may constitute sufficient grounds to terminate the grant agreement.
2.	Grant beneficiaries are subject to all obligations set out in Decision 2015/444 ² and its implementing rules (Decision 2021/259 ³). If the grant beneficiary faces a problem of application of the applicable legal framework in a Member State, it must refer to the Commission security authority and the national security authority (NSA) or designated security authority (DSA).
3.	Classified information generated when performing the grant agreement must be marked as EU classified information (EUCI) at security classification level, as determined in the security classification guide (SCG) in Appendix B to this letter. Deviation from the security classification level stipulated by the SCG is permissible only with the written authorisation of the granting authority.
4.	The rights of the originator of any EUCI created and handled for the performance of the classified grant agreement are exercised by the European Commission, as the granting authority.
5.	Without the written consent of the granting authority, the beneficiary or subcontractor must not make use of any information or material furnished by the granting authority or produced on behalf of that authority for any purpose other than that of the grant agreement.
6.	Where a facility security clearance (FSC) is required for the performance of a grant agreement, the beneficiary must ask the granting authority to proceed with the FSC request. For the performance of this grant agreement, at least the below beneficiaries must obtain the FSC: <ul style="list-style-type: none"> – Ministry of Economic Affairs and Communications – Ministry of Defence – State Infocommunication Foundation
7.	The beneficiary must investigate all security breaches related to EUCI and report them to the granting authority as soon as is practicable. The beneficiary or subcontractor must immediately report to its NSA or DSA, and, where national laws and regulations so permit, to the Commission security authority, all cases in which it is known or there is reason to suspect that EUCI provided or generated pursuant to the grant agreement has been lost or disclosed to unauthorised persons.
8.	After the end of the grant agreement, the beneficiary or subcontractor must return any EUCI it holds to the granting authority as soon as possible. Where practicable, the beneficiary or subcontractor may destroy EUCI instead of returning it. This must be done in accordance with the national laws and regulations of the country where the beneficiary is based, with the prior agreement of the Commission security authority, and under the latter's instruction. EUCI must be destroyed in such a way that it cannot be reconstructed, either wholly or in part.

² Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

³ Commission Decision (EU, Euratom) 2021/259 of 10 February 2021 laying down implementing rules on industrial security with regard to classified grants (OJ L 58, 19.2.2021, p. 55).

9. Where the beneficiary or subcontractor is authorised to retain EUCI after termination or conclusion of the grant agreement, the EUCI must continue to be protected in accordance with Decision 2015/444 and with Decision [2021/259](#).
10. Any electronic handling, processing and transmission of EUCI must abide by the provisions laid down in Chapters 5 and 6 of Decision 2015/444. These include, *inter alia*, the requirement that communication and information systems owned by the beneficiary and used to handle EUCI for the purpose of the grant agreement (hereinafter 'beneficiary CIS') must be subject to accreditation⁴; that any electronic transmission of EUCI must be protected by cryptographic products approved in accordance with Article 36(4) of Decision 2015/444, and that TEMPEST security measures must be implemented in accordance with Article 36(6) of Decision 2015/444.
11. The beneficiary or subcontractor must have business contingency plans (BCPs) to protect any EUCI handled in the performance of the classified grant agreement in emergency situations and must put in place preventive and recovery measures to minimise the impact of incidents associated with the handling and storage of EUCI. The beneficiary or subcontractor must inform the granting authority of its BCP.

GRANT AGREEMENTS REQUIRING ACCESS TO INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED

12. In principle, personnel security clearance (PSC) is not required for compliance with the grant agreement⁵. However, information or material classified RESTREINT UE/EU RESTRICTED must be accessible only to beneficiary personnel who require such information to perform the grant agreement (*need-to-know principle*), who have been briefed by the beneficiary's security officer on their responsibilities and on the consequences of any compromise or breach of security of such information, and who have acknowledged in writing the consequences of a failure to protect EUCI.
13. Except where the granting authority has given its written consent, the beneficiary or subcontractor must not provide access to information or material classified RESTREINT UE/EU RESTRICTED to any entity or person other than those of its personnel who have a need-to-know.
14. The beneficiary or subcontractor must maintain the security classification markings of classified information generated by or provided during the performance of a grant agreement and must not declassify information without written consent from the granting authority.
15. Information or material classified RESTREINT UE/EU RESTRICTED must be stored in locked office furniture when not in use. When in transit, documents must be carried inside an opaque envelope. The documents must not leave the possession of the bearer and they must not be opened *en route*.
16. The beneficiary or subcontractor may transmit documents classified RESTREINT UE/EU RESTRICTED to the granting authority using commercial courier companies, postal services, hand carriage or electronic means. To this end, the beneficiary or subcontractor must follow the programme (or project) security instruction (PSI) issued by the Commission and/or Decision [2021/259](#).
17. When no longer required, documents classified RESTREINT UE/EU RESTRICTED must be destroyed in such a way that they cannot be reconstructed, either wholly or in part.
18. The security accreditation of beneficiary CIS handling EUCI at RESTREINT UE/EU RESTRICTED level and any interconnection thereof may be delegated to the beneficiary's security officer if national laws and regulations so permit. Where accreditation is thus delegated, the NSAs, DSAs or security accreditation authorities (SAAs) retain responsibility for protecting any RESTREINT UE/EU RESTRICTED information that is handled by the beneficiary and the right to inspect the security measures taken by the beneficiary. In addition, the beneficiary must provide the granting authority and, where required by national laws and regulations, the competent national SAA with a statement of compliance certifying that the beneficiary CIS and the related interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level.

HANDLING OF INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)

⁴ The party undertaking the accreditation will have to provide the granting authority with a statement of compliance, through the Commission security authority, and in co-ordination with the relevant national security accreditation authority (SAA).

⁵ Where beneficiaries are from Member States requiring PSCs and/or FSCs for grants classified RESTREINT UE/EU RESTRICTED, the granting authority lists in the SAL these PSC and FSC requirements for the beneficiaries in question.

19. Minimum requirements for CIS handling information classified RESTREINT UE/EU RESTRICTED are laid down in Appendix E to this SAL.

CONDITIONS UNDER WHICH THE BENEFICIARY MAY SUBCONTRACT

20. The beneficiary must obtain permission from the granting authority before subcontracting any part of a classified grant agreement.
21. No subcontract may be awarded to an entity registered in a non-EU country or to an entity belonging to an international organisation, if that non-EU country or international organisation has not concluded a security of information agreement with the EU or an administrative arrangement with the Commission.
22. Where the beneficiary has let a subcontract, the security provisions of the grant agreement apply *mutatis mutandis* to the subcontractor(s) and its (their) personnel. In such a case, it is the beneficiary's responsibility to ensure that all subcontractors apply these principles to their own subcontracting arrangements. To ensure appropriate security oversight, the beneficiary's and subcontractor's NSAs and/or DSAs will be notified by the Commission security authority of the letting of all related classified subcontracts at the levels of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET. Where appropriate, the beneficiary's and subcontractor's NSAs and/or DSAs will be provided with a copy of the subcontract-specific security provisions. NSAs and DSAs requiring notification about the security provisions of classified grant agreements at RESTREINT UE/EU RESTRICTED level are listed in the annex to Decision [2021/259](#).
23. The beneficiary may not release any EUCI to a subcontractor without the prior written approval of the granting authority. If EUCI to subcontractors is to be sent frequently or as a matter of routine, then the granting authority may give its approval for a specified length of time (e.g. 12 months) or for the duration of the subcontract.

VISITS

24. Visits involving access or potential access to information classified RESTREINT UE/EU RESTRICTED will be arranged directly between the sending and receiving establishments without the need to follow the procedure described in paragraphs 25 to 27 below.
25. Visits involving access or potential access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET will be arranged directly between the sending and receiving establishments (an example of the form that may be used for this purpose is provided in Appendix C).
26. Visitors must prove their identity on arrival at the host facility by presenting a valid ID card or passport.
27. The facility hosting the visit must ensure that records are kept of all visitors. These must include their names, the organisation they represent, the date of expiry of the PSC (if applicable), the date of the visit and the name(s) of the person(s) visited. Without prejudice to European data protection rules, such records are to be retained for a period of no less than five years or in accordance with national rules and regulations, as appropriate.

ASSESSMENT VISITS

28. The Commission security authority may, in cooperation with the relevant NSAs or DSAs, conduct visits to beneficiaries' or subcontractors' facilities to check that the security requirements for handling EUCI are being complied with.

SECURITY CLASSIFICATION GUIDE

29. A list of all the elements in the grant agreement which are classified or to be classified in the course of the performance of the grant agreement, the rules for so doing and the specification of the applicable security classification levels are contained in the security classification guide (SCG). The SCG is an integral part of this grant agreement and can be found in Appendix B to this Annex.

3.2 The security classification guide (SCG) (appendix B of the SAL)

Security classification guide (SCG)

Use of classified background information

Reference and name of document	Classification level	Originator (EU institution, EU Member State, non-EU country or IO under whose authority the information was created and classified)	Reference number of originator authorisation for use
Security baseline	R-UE/EU-R	European Commission	To be communicated later

Security classification guide (SCG)					
Production of EU classified <u>foreground</u> information					
Number and name of deliverable	Classification level (R-UE/EU-R, C-UE/EU-C, S-UE/EU-S)	Beneficiaries involved in production / entities authorised for access			
		Name	Responsibility (security manager/main contributor, contributor, blind contributor, reader only)	Date of production	Comments (need-to-know, purpose of access and planned use for 'Reader only' role)
Gap analysis	R-UE/EU-R	MKM	Security manager / main contributor	M30	
		EE MoD	Main contributor	M30	

3.3 Request for visit (appendix C of the SAL)

The rules and templates for requests for visits can be found at the end of this section.

3.4 Facility Security Clearance Information Sheet (FSCIS) (appendix D of the SAL)

The rules and templates for the facility security clearance information sheet can be found at the end of this section.

3.5 Minimum requirements for protection of EUCI in electronic form at RESTREINT UE/EU RESTRICTED level handled in the beneficiary's CIS (appendix E of the SAL)

MINIMUM REQUIREMENTS FOR CIS	
General	
1.	The beneficiary must be responsible for ensuring that the protection of RESTREINT UE/EU RESTRICTED information complies with the minimum security requirements as laid down in this security clause and with any other additional requirements advised by the granting authority or, if applicable, by the national security authority (NSA) or designated security authority (DSA).
2.	It is the beneficiary's responsibility to implement the security requirements identified in this document.
3.	For the purpose of this document, a communication and information system (CIS) covers all equipment used to handle, store and transmit EUCI, including workstations, printers, copiers, fax machines, servers, network management systems, network controllers and communications

controllers, laptops, notebooks, tablet PCs, smart phones and removable storage devices such as USB-sticks, CDs, SD-cards, etc.

4. Special equipment, such as cryptographic products, must be protected in accordance with its dedicated security operating procedures (SecOps).
5. Beneficiary must establish a structure responsible for the security management of the CIS handling information classified RESTREINT UE/EU RESTRICTED and appoint a security officer responsible for the facility concerned.
6. The use of IT solutions (hardware, software or services) privately owned by beneficiary staff for storing or processing RESTREINT UE/EU RESTRICTED information is not permitted.
7. Accreditation of the beneficiary's CIS handling information classified RESTREINT UE/EU RESTRICTED must be approved by the security accreditation authority (SAA) of the Member State concerned or delegated to the beneficiary's security officer as permitted by national laws and regulations.
8. Only information classified RESTREINT UE/EU RESTRICTED that is encrypted using approved cryptographic products may be handled, stored or transmitted (by wired or wireless means) as any other unclassified information under the grant agreement. Such cryptographic products must be approved by the EU or a Member State.
9. External facilities involved in maintenance/repair work must be contractually obliged to comply with the applicable provisions for handling of information classified RESTREINT UE/EU RESTRICTED, as set out in this document.
10. At the request of the granting authority or relevant NSA, DSA, or SAA, the beneficiary must provide evidence of compliance with the security clause of the grant agreement. If an audit and inspection of the beneficiary's processes and facilities are also requested, to ensure compliance with these requirements, beneficiaries must permit representatives of the granting authority, the NSA, DSA and/or SAA, or the relevant EU security authority to conduct such an audit and inspection.

Physical security

11. Areas in which CIS are used to display, store, process or transmit RESTREINT UE/EU RESTRICTED information or areas housing servers, network management systems, network controllers and communications controllers for such CIS should be established as separate and controlled areas with an appropriate access control system. Access to these separate and controlled areas should be restricted to individuals with specific authorisation. Without prejudice to paragraph 8, equipment as described in paragraph 3 must be stored in such separate and controlled areas.
12. Security mechanisms and/or procedures must be implemented to regulate the introduction or connection of removable computer storage media (such as USBs, mass storage devices or CD-RWs) to components on the CIS.

Access to CIS

13. Access to a beneficiary's CIS handling EUCI is allowed on a basis of strict need-to-know and authorisation of personnel.
14. All CIS must have up-to-date lists of authorised users. All users must be authenticated at the start of each processing session.
15. Passwords, which are part of most identification and authentication security measures, must be at least nine characters long and must include numeric and 'special' characters (if permitted by the system) as well as alphabetic characters. Passwords must be changed at least every 180 days. They must be changed as soon as possible if they have been compromised or disclosed to an unauthorised person, or if such compromise or disclosure is suspected.
16. All CIS must have internal access controls to prevent unauthorised users from accessing or modifying information classified RESTREINT UE/EU RESTRICTED and from modifying system and security controls. Users are to be automatically logged off the CIS if their terminals have been inactive for some predetermined period of time, or the CIS must activate a password-protected screen saver after 15 minutes of inactivity.
17. Each user of the CIS is allocated a unique user account and ID. User accounts must be automatically locked once at least five successive incorrect login attempts have been made.
18. All users of the CIS must be made aware of their responsibilities and the procedures to be followed to protect information classified RESTREINT UE/EU RESTRICTED on the CIS. The responsibilities and procedures to be followed must be documented and acknowledged by users in writing.

19. SecOPs must be available for the users and administrators and must include descriptions of security roles and associated list of tasks, instructions and plans.

Accounting, audit and incident response

20. Any access to the CIS must be logged.
21. The following events must be recorded:
- a) all attempts to log on, whether successful or failed;
 - b) logging off (including being timed out, where applicable);
 - c) creation, deletion or alteration of access rights and privileges;
 - d) creation, deletion or alteration of passwords.
22. For all of the events listed above, the following information must be communicated as a minimum:
- a) type of event;
 - b) user ID;
 - c) date and time;
 - d) device ID.
23. The accounting records should provide help to a security officer to examine the potential security incidents. They can also be used to support any legal investigations in the event of a security incident. All security records should be regularly checked to identify potential security incidents. The accounting records must be protected from unauthorised deletion or modification.
24. The beneficiary must have an established response strategy to deal with security incidents. Users and administrators must be instructed on how to respond to incidents, how to report them and what to do in the event of emergency.
25. The compromise or suspected compromise of information classified RESTREINT UE/EU RESTRICTED must be reported to the granting authority. The report must contain a description of the information involved and a description of the circumstances of the compromise or suspected compromise. All users of the CIS must be made aware of how to report any actual or suspected security incident to the security officer.

Networking and interconnection

26. When a beneficiary CIS that handles information classified RESTREINT UE/EU RESTRICTED is interconnected to a CIS that is not accredited, this significantly increases the threat to both the security of the CIS and the RESTREINT UE/EU RESTRICTED information that is handled by that CIS. This includes the internet and other public or private CIS, such as other CIS owned by the beneficiary or subcontractor. In this case, the beneficiary must perform a risk assessment to identify the additional security requirements that need to be implemented as part of the security accreditation process. The beneficiary must provide to the granting authority, and where required by national laws and regulations, the competent SAA, a statement of compliance certifying that the beneficiary CIS and the related interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level.
27. Remote access from other systems to LAN services (e.g. remote access to email and remote SYSTEM support) is prohibited unless special security measures are implemented and agreed by the granting authority, and where required by national laws and regulations, approved by the competent SAA.

Configuration management

28. A detailed hardware and software configuration, as reflected in the accreditation/approval documentation (including system and network diagrams), must be available and regularly maintained.
29. The beneficiary's security officer must conduct configuration checks on hardware and software to ensure that no unauthorised hardware or software has been introduced.
30. Changes to the beneficiary CIS configuration must be assessed for their security implications and must be approved by the security officer, and where required by national laws and regulations, the SAA.
31. The system must be scanned for any security vulnerabilities at least once a quarter. Software to detect malware must be installed and kept up-to-date. If possible, such software should have a national or recognised international approval, otherwise it should be a widely accepted industry standard.

32. The beneficiary must develop a business continuity plan. Back-up procedures must be established to address the following:
- a) frequency of back-ups;
 - b) storage requirements on-site (fireproof containers) or off-site;
 - c) control of authorised access to back-up copies.

Sanitisation and destruction

33. For CIS or data storage media that have at any time held RESTREINT UE/EU RESTRICTED information the following sanitisation must be performed to the entire system or to storage media before its disposal:
- a) flash memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives) must be overwritten at least three times and then verified to ensure that the original content cannot be recovered, or be deleted using approved deletion software;
 - b) magnetic media (e.g. hard disks) must be overwritten or degaussed;
 - c) optical media (e.g. CDs and DVDs) must be shredded or disintegrated;
 - d) for any other storage media, the granting authority or, if appropriate, the NSA, DSA or SAA should be consulted on the security requirements to be met.
34. Information classified RESTREINT UE/EU RESTRICTED must be sanitised on any data storage media before it is given to any entity that is not authorised to access information classified RESTREINT UE/EU RESTRICTED (e.g. for maintenance work).

4. SECURITY STAFF

4.1 Project security officer (PSO)

Project security officer (PSO)		
Name	Nationality	Profession
Marve Kaljumäe	Estonian	Advisor, Ministry of Economic Affairs and Communications

4.2 Security advisory board (SAB)

Security advisory board (SAB)			
Member's name	Nationality	Profession	Areas of competence
Marve Kaljumäe	Estonian	Advisor, Ministry of Economic Affairs and Communications	
Kersti Piilma	Estonian	Estonian Foreign Intelligence Service	
Marek Lehtsalu	Estonian	Estonian Foreign Intelligence Service	
Kalev Karu	Estonian	Estonian Foreign Intelligence Service	

5. OTHER PROJECT-SPECIFIC SECURITY MEASURES

APPENDIX C

REQUEST FOR VISIT**(MODEL)**

DETAILED INSTRUCTIONS FOR COMPLETION OF REQUEST FOR VISIT

(The application must be submitted in English only)

HEADING	Check boxes for visit type, information type, and indicate how many sites are to be visited and the number of visitors.
4. ADMINISTRATIVE DATA	To be completed by requesting NSA/DSA.
5. REQUESTING ORGANISATION OR INDUSTRIAL FACILITY	Give full name and postal address. Include city, state and post code as applicable.
6. ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED	Give full name and postal address. Include city, state, post code, telex or fax number (if applicable), telephone number and e-mail. Give the name and telephone/fax numbers and e-mail of your main point of contact or the person with whom you have made the appointment for the visit. <u>Remarks:</u> 1) Giving the correct post code (zip code) is important because a company may have various different facilities. 2) When applying manually, Annex 1 can be used when two or more facilities have to be visited in connection with the same subject. When an Annex is used, item 3 should state: "SEE ANNEX 1, NUMBER OF FAC:..." (state number of facilities).
7. DATES OF VISIT	Give the actual date or period (date-to-date) of the visit in the format 'day - month - year'. Where applicable, give an alternate date or period in brackets.
8. TYPE OF INITIATIVE	Specify whether the visit has been initiated by the requesting organisation or facility or by invitation of the facility to be visited.
9. THE VISIT RELATES TO:	Specify the full name of the project, contract or call for tender using commonly used abbreviations only.
10. SUBJECT TO BE DISCUSSED/ JUSTIFICATION	Give a brief description of the reason(s) for the visit. Do not use unexplained abbreviations. <u>Remarks:</u> In the case of recurring visits this item should state 'Recurring visits' as the first words in the data element (e.g. Recurring visits to discuss_____).
11. ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED	State SECRET UE/EU SECRET (S-UE/EU-S) or CONFIDENTIAL UE/EU CONFIDENTIAL (C-UE/EU-C), as appropriate.
12. PARTICULARS OF VISITOR	<u>Remark:</u> when more than two visitors are involved in the visit, Annex 2 should be used.

13. THE SECURITY OFFICER OF THE REQUESTING ENTITY	This item requires the name, telephone number, fax number and e-mail of the requesting facility's Security Officer.
14. CERTIFICATION OF SECURITY CLEARANCE	<p>This field is to be completed by the certifying authority.</p> <p>Notes for the certifying authority:</p> <p>a. Give name, address, telephone number, fax number and e-mail (can be pre-printed).</p> <p>b. This item should be signed and stamped (if applicable).</p>
15. REQUESTING SECURITY AUTHORITY	<p>This field is to be completed by the NSA/DSA.</p> <p>Note for the NSA/DSA:</p> <p>a. Give name, address, telephone number, fax number and e-mail (can be pre-printed).</p> <p>b. This item should be signed and stamped (if applicable).</p>

<p align="center">REQUEST FOR VISIT</p> <p align="center">(MODEL)</p> <p align="center">TO: _____</p>		
1. TYPE OF VISIT REQUEST	2. TYPE OF INFORMATION	3. SUMMARY
<input type="checkbox"/> Single <input type="checkbox"/> Recurring <input type="checkbox"/> Emergency <input type="checkbox"/> Amendment <input type="checkbox"/> Dates <input type="checkbox"/> Visitors <input type="checkbox"/> Facility <p>For an amendment, insert the NSA/DSA original RFV Reference No_____</p>	<input type="checkbox"/> C-UE/EU-C <input type="checkbox"/> S-UE/EU-S	<p>No of sites: _____</p> <p>No of visitors: _____</p>
4. ADMINISTRATIVE DATA:		

Requester:	NSA/DSA RFV Reference No _____
To:	Date (dd/mm/yyyy): ____/____/____
5. REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:	
NAME:	
POSTAL ADDRESS:	
E-MAIL ADDRESS:	
FAX NO:	TELEPHONE NO:
6. ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED (<i>Annex 1 to be completed</i>)	
7. DATE OF VISIT (dd/mm/yyyy): FROM ____/____/____ TO ____/____/____	
8. TYPE OF INITIATIVE:	
<input type="checkbox"/> Initiated by requesting organisation or facility	
<input type="checkbox"/> By invitation of the facility to be visited	
9. THE VISIT RELATES TO CONTRACT:	
10. SUBJECT TO BE DISCUSSED/REASONS/PURPOSE (Include details of host entity and any other relevant information. Abbreviations should be avoided):	
11. ANTICIPATED HIGHEST CLASSIFICATION LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:	
12. PARTICULARS OF VISITOR(S) (<i>Annex 2 to be completed</i>)	

13. THE SECURITY OFFICER OF THE REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

DATE (dd/mm/yyyy): ____/____/____

STAMP

15. REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

DATE (dd/mm/yyyy): ____/____/____

STAMP

16. REMARKS (Mandatory justification required in the case of an emergency visit):

<Placeholder for reference to applicable personal data legislation and link to mandatory information for the data subject, e.g. how Article 13 of the General Data Protection Regulation⁶ is implemented.>

⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

ANNEX 1 to RFV FORM

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
<p>1.</p> <p>NAME:</p> <p>ADDRESS:</p> <p>TELEPHONE NO:</p> <p>FAX NO:</p> <p>NAME OF POINT OF CONTACT:</p> <p>E-MAIL:</p> <p>TELEPHONE NO:</p> <p>NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT:</p> <p>E-MAIL:</p> <p>TELEPHONE NO:</p>
<p>2.</p> <p>NAME:</p> <p>ADDRESS:</p> <p>TELEPHONE NO:</p> <p>FAX NO:</p> <p>NAME OF POINT OF CONTACT:</p> <p>E-MAIL:</p> <p>TELEPHONE NO:</p> <p>NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT:</p> <p>E-MAIL:</p> <p>TELEPHONE NO:</p> <p>(Continue as required)</p>

<Placeholder for reference to applicable personal data legislation and link to mandatory information for the data subject, e.g. how Article 13 of the General Data Protection Regulation⁷ is implemented.>

⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

ANNEX 2 to RFV FORM**PARTICULARS OF VISITOR(S)**

1.

SURNAME:

FIRST NAMES *(as per passport)*:DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

2.

SURNAME:

FIRST NAMES *(as per passport)*:DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

(Continue as required)

<Placeholder for reference to applicable personal data legislation and link to mandatory information for the data subject, e.g. how Article 13 of the General Data Protection Regulation⁸ is implemented.>

⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

APPENDIX D

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS) **(MODEL)**

INTRODUCTION

1.1 Attached is a sample Facility Security Clearance Information Sheet (FSCIS) for the rapid exchange of information between the National Security Authority (NSA) or Designated Security Authority (DSA), other competent national security authorities and the Commission Security Authority (acting on behalf of granting authorities) with regard to the Facility Security Clearance (FSC) of a facility involved in application for, and implementation of, classified grants or subcontracts.

1.2 The FSCIS is valid only if stamped by the relevant NSA, DSA or other competent authority.

1.3 The FSCIS is divided into a request and reply section and can be used for the purposes identified above or for any other purposes for which the FSC status of a particular facility is required. The reason for the enquiry must be identified by the requesting NSA or DSA in field 7 of the request section.

1.4 The details contained in the FSCIS are not normally classified; accordingly, when an FSCIS is to be sent between the respective NSAs/DSAs/Commission this should preferably be done by electronic means.

1.5 NSAs/DSAs should make every effort to respond to an FSCIS request within ten working days.

1.6 Should any classified information be transferred or a grant or subcontract awarded in relation to this assurance, the issuing NSA or DSA must be informed.

**Procedures and Instructions for the
use of the Facility Security Clearance Information Sheet (FSCIS)**

These detailed instructions are for the NSA or DSA, or the granting authority and the Commission Security Authority that complete the FSCIS. The request should preferably be typed in capital letters.

HEADER	The requester inserts full NSA/DSA and country name.
1. REQUEST TYPE	<p>The requesting granting authority selects the appropriate checkbox for the type of FSCIS request. Include the level of security clearance requested. The following abbreviations should be used:</p> <p>SECRET UE/EU SECRET = S-UE/EU-S</p> <p>CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C</p> <p>CIS = Communication and information systems for processing classified information.</p>
2. SUBJECT DETAILS	<p>Fields 1 to 6 are self-evident.</p> <p>In field 4 the standard two-letter country code should be used. Field 5 is optional.</p>
3. REASON FOR REQUEST	<p>Give the specific reason for the request, provide project indicators, number of the call or grant. Please specify the need for storage capability, CIS classification level, etc.</p> <p>Any deadline/expiry/award dates which may have a bearing on the completion of an FSC should be included.</p>
4. REQUESTING NSA/DSA	State the name of the actual requester (on behalf of the NSA/DSA) and the date of the request in number format (dd/mm/yyyy).
5. REPLY SECTION	<p>Fields 1-5: select appropriate fields.</p> <p>Field 2: if an FSC is in progress, it is recommended to give the requester an indication of the required processing time (if known).</p> <p>Field 6:</p> <p>a) Although validation differs by country or even by facility, it is recommended that the expiry date of the FSC be given.</p> <p>b) In cases where the expiry date of the FSC assurance is indefinite, this field may be crossed out.</p> <p>c) In compliance with respective national rules and regulations, the requester or either the beneficiary or subcontractor is responsible for applying for a renewal of the FSC.</p>
6. REMARKS	May be used for additional information with regard to the FSC, the facility or the foregoing items.
7. ISSUING NSA/DSA	State the name of the providing authority (on behalf of the NSA/DSA) and the date of the reply in number format (dd/mm/yyyy).

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS)**(MODEL)**

All fields must be completed and the form communicated via Government-to-Government or Government-to-international organisation channels.

REQUEST FOR A FACILITY SECURITY CLEARANCE ASSURANCE

TO: _____

(NSA/DSA Country name)

Please complete the reply boxes, where applicable:

[] Provide an FSC assurance at the level of: [] S-UE/EU-S [] C-UE/EU-C

for the facility listed below

[] Including safeguarding of classified material/information

[] Including Communication and Information Systems (CIS) for processing classified information

[] Initiate, directly or upon a corresponding request of a beneficiary or subcontractor, the process of obtaining an FSC up to and including the level of withlevel of safeguarding andlevel of CIS, if the facility does not currently hold these levels of capabilities.

Confirm accuracy of the details of the facility listed below and provide corrections/additions as required.

1. Full facility name:

Corrections/Additions:

.....

.....

2. Full facility address:

.....

.....

3. Postal address (if different from 2)

.....

.....

4. Zip/post code/city/country

.....

.....

5. Name of the Security Officer

.....

.....

6. Telephone/Fax/E-mail of the Security Officer

.....

.....

7. This request is made for the following reason(s): (provide details of the pre-contractual (proposal selection) stage, grant or subcontract, programme/project, etc.)

.....

Requesting NSA/DSA/granting authority: Name: Date: (dd/mm/yyyy).....

REPLY (within ten working days)

This is to certify that:

1. ☐ the abovementioned facility holds an FSC up to and including the level of ☐ S-UE/EU-S

☐ C-UE/EU-C.

2. The abovementioned facility has the capability to safeguard classified information/material:

☐ yes, level: ☐ no.

3. the abovementioned facility has accredited/authorised CIS:

☐ yes, level: ☐ no.

4. ☐ in relation to the abovementioned request, the FSC process has been initiated. You will be informed when the FSC has been established or refused.

5. ☐ the abovementioned facility does not hold an FSC.

6. This FSC assurance expires on: (dd/mm/yyyy), or as advised otherwise by the NSA/DSA. In the case of earlier invalidation or any changes to the information listed above, you will be informed.

7. Remarks:

Issuing NSA/DSA Name: Date:(dd/mm/yyyy).....

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.
-

ANNEXES**LIST OF PREVIOUS PROJECTS**

List of previous projects <i>Please provide a list of your previous projects for the last 4 years.</i>					
Participant	Project Reference No and Title, Funding programme	Period (start and end date)	Role (COO, BEN, AE, OTHER)	Amount (EUR)	Website (if any)
Metrosert	17FUN06 Single-photon sources as new quantum standards, European Metrology Programme for Research and Innovation, Horizon2020	Start: 01/06/2018 End: 31/05/2021	BEN		https://www.siqust.eu/
Metrosert	19NRM06 Metrology for Testing the Implementation Security of Quantum Key Distribution Hardware, European Metrology Programme for Research and Innovation, Horizon2020	Start: 01/09/2020 End: 28/02/2024	BEN		http://empir.npl.co.uk/metisq/
Metrosert	20FUN05 ingle- and entangled photon sources for quantum metrology, European Metrology Programme for Research and Innovation, Horizon2020	Start: 01/06/2021 End: 31/05/2024	BEN		https://seume.cmi.cz/

PURCHASES AND EQUIPMENT

Purchase costs (travel and subsistence, equipment and other goods works and services) <i>Details for major cost items (needed if costs declared under 'purchase costs' are higher than 15% of the claimed personnel costs). Start with the most expensive cost items, down to the 15% threshold.</i>				
Coordinator:	MKM			
Cost item name	Category	WP(s)	Explanations	Costs (EUR)
PR costs	Other goods and services	WP3	Costs for PR-services to inform stakeholders about the events (social media coverage, media coverage). MKM	1 000
Media and PR costs	Other goods and services	WP6	Communication services for execution of the communication plan, such as media and social media coverage, creation of a visual identity of the project, promotion of events. Costs covered by MKM	16 000

Travel costs	Travel and Subsistence	WP1, WP3	6 trips: 2x2 people Central- Europe	6 000
Travel costs	Travel and Subsistence	WP5	Regional coordination, participation in events, participation in EuroQCI. Around 6 trips, 4x2 people Central-Europe, 2 trips to the neighbors (FI, SE, LT, LV, PL)	10 000
Travel costs	Travel and Subsistence	WP4, WP6	Participation in stakeholder events, Central-Europe, 3x2 persons.	5 500

Purchase costs (travel and subsistence, equipment and other goods works and services)

Details for major cost items (needed if costs declared under 'purchase costs' are higher than 15% of the claimed personnel costs).

Start with the most expensive cost items, down to the 15% threshold.

Participant 2:	Metrosert			
Cost item name	Category	WP(s)	Explanations	Costs (EUR)
Training costs	Other goods and services	WP3	Metrosert will organize 2 training sessions each for potential users of the network. Organizational costs of events.	10 000
Travel costs	Travel and Subsistence	WP1, WP2; WP5	Visitation of potential suppliers and cooperation with other NatQCI projects. Participation in relevant conferences and lab visits. Around 6 trips, 4x2 people Central-Europe, 2 trips to the neighbors (FI, SE, LT, LV, PL)	10 000
Construction services costs	Other goods and services	WP4	Construction services to set up the long-distance network test lab at Metrosert	30 900
SPAD	Equipment	WP2, WP3, WP4	For evaluation of the networks and components, specially for this project, Metrosert	20 000
Optical delay lines	Equipment	WP2, WP3, WP4	For evaluation of the networks and components, specially for this project, Metrosert	12 000
Two White Rabbit low-jitter switches	Equipment	WP2, WP3, WP4	For evaluation of the networks and components, specially for this project, Metrosert	14 000
Entangled photon pair source at telecom wavelengths	Equipment	WP2, WP3, WP4	For evaluation of the networks and components, specially for this project, Metrosert	60 000
Pulsed laser	Equipment	WP2, WP3, WP4	For evaluation of the networks and components, specially for this project, Metrosert	12 000
Fast optical modulators	Equipment	WP2, WP3, WP4	For evaluation of the networks and components, specially for this project, Metrosert	30 000
Optical fibre	Equipment	WP4	100 km of optical fiber for laboratory testing, WP4, Metrosert	8 000
Two Optical Time Domain Reflectometers	Equipment	WP3, WP4	For evaluation of the networks and components, specially for this project, WP3. WP4	12 000

Optical Wavelength Meter	Equipment	WP3, WP4	For evaluation of the networks and components, specially for this project. WP3, WP4	35 000
Polarization Controller/Scrambler	Equipment	WP3, WP4	For evaluation of the networks and components, specially for this project. WP3, WP4	7 000

Purchase costs (travel and subsistence, equipment and other goods works and services)

Details for major cost items (needed if costs declared under 'purchase costs' are higher than 15% of the claimed personnel costs).

Start with the most expensive cost items, down to the 15% threshold.

Participant 3:	RIKS			
Cost item name	Category	WP(s)	Explanations	Costs (EUR)
Workshop costs	Other goods and services	WP3	RIKS will organise two (international) workshops for stakeholders to identify potential use cases. Organisational costs of events such as technical support, room rent, catering.	20 000
PR costs	Other goods and services	WP3	Costs for PR-services to inform stakeholders about the events (social media coverage, media coverage). RIKS	4 000
Event costs	Other goods and services	WP5	Two international stakeholder events, 31 100 EUR each, RIKS. Costs include rent, technical support, catering.	62 200
Media and PR costs	Other goods and services	WP6	Communication services for execution of the communication plan, such as media and social media coverage, creation of a visual identity of the project, promotion of events. Costs covered by RIKS	73 800
Travel costs	Travel and Subsistence	WP1, WP3	2 to 3 trips to other countries (1 conference/workshop on the topic, 2 trips to neighboring countries)	6 000
Travel costs	Travel and Subsistence	WP5	Regional coordination, participation in events, participation in EuroQCI. Around 7 trips, 4x2 people Central Europe, 3 trips to the neighbors (FI, SE, LT, LV, PL)	10 000
Travel costs	Travel and Subsistence	WP4, WP6	Participation in stakeholder events, Central-Europe, 2x2 persons.	5 500
Travel costs	Travel and Subsistence	WP1, WP2; WP5	Visitation of potential suppliers and cooperation with other NatQCI projects. Participation in relevant conferences. Around 3 trips, 1x2 people Conferences, 2x2 people Central Europe	5 000
Training costs	Other goods and services	WP3	RIKS will organize 2 training sessions for potential users of the network. Organizational costs of events.	10 000
QKD Systems	Equipment	WP2, WP4	For metro network and testing of the long-distance network, specially for this project, RIKS	644 000
Required management	Equipment	WP2, WP4	For metro network and testing of the long-distance network, specially for this project, RIKS	220 000

systems for all equipment				
Multichannel SNSPD detection unit	Equipment	WP2, WP3, WP4	For evaluation of the networks and components, specially for this project, RIKS	200 000
QKD compatible encryption devices	Equipment	WP2, WP4	For metro network and testing of the round network, specially for this project, RIKS	610 000

Purchase costs (travel and subsistence, equipment and other goods works and services)

Details for major cost items (needed if costs declared under 'purchase costs' are higher than 15% of the claimed personnel costs).

Start with the most expensive cost items, down to the 15% threshold.

Participant 4:	Ministry of Defence			
Cost item name	Category	WP(s)	Explanations	Costs (EUR)
Travel costs	Travel and Subsistence	WP1	Alignment with security baseline will probably require a trip to Brussels	2 000
Travel costs	Travel and Subsistence	WP3	Participation in stakeholder events for the security sector. 2 events	4 000
Travel costs	Travel and Subsistence	WP5	Cooperation with relevant bodies of neighbouring countries (FI, SE, LT, LV, PL), 5000 EUR, 3 to 4 trips	5 000
Travel costs	Travel and Subsistence	WP6	Participation in stakeholder events, 1 event, 1 person.	2 000

Equipment with full-cost option

For calls where full-capitalised costs are exceptionally eligible for listed equipment (see Call document), indicate below the equipment items for which you request the full cost option, and justify your request. Ensure consistency with the budget details provided in the previous table

Equipment Name	Description (including WP, task number and BEN/AE to which it is linked)	Estimated Costs (EUR)	Justification (why is reimbursement at full-cost needed?)	Best-Value-for-Money (how do you intend to ensure it?)
QKD Systems	QKD systems with DV-QKD, 2 pcs standard pairs – 408 000 EUR, 1 pcs R&D device pair 216 000 EUR, Tech. support 20 000 EUR, WP2 and WP4, RIKS	644 000	For metro and round network, testing of the long-distance network, specially for this project	Public procurement procedure
QKD compatible encryption devices	Total cost of equipment 1,2 M EUR, 50% dedicated to this project WP2, WP4	610 000	For round network, testing integration of QKD to optical networks. 50% of equipment specially for this project	Public procurement procedure

Required management systems for all equipment	WP2, WP4	220 000	For metro network and testing of the long-distance network, specially for this project, RIKS	Public procurement procedure
Multichannel SNSPD detection unit	WP2, WP3 and WP4, RIKS	200 000	For evaluation of the networks and components, specially for this project	Public procurement procedure
SPAD	WP2, WP3 and WP4, Metrosert	20 000	For evaluation of the networks and components, specially for this project	Comparison of at least three offers
Optical delay lines	WP2, WP3 and WP4, Metrosert	12 000	For evaluation of the networks and components, specially for this project	Comparison of at least three offers
Two White Rabbit low-jitter switches	WP2, WP3 and WP4, Metrosert	14 000	For evaluation of the networks and components, specially for this project	Comparison of at least three offers
Entangled photon pair source at telecom wavelengths	WP2, WP3 and WP4, Metrosert	60 000	For evaluation of the networks and components, specially for this project	Public procurement procedure
Pulsed laser	WP2, WP3 and WP4, Metrosert	12 000	For evaluation of the networks and components, specially for this project	Comparison of at least three offers
Fast optical modulators	WP2, WP3 and WP4, Metrosert	30 000	For evaluation of the networks and components, specially for this project	Public procurement procedure
Optical fiber	100 km of optical fiber for laboratory testing, WP4, Metrosert	8 000	For testing of the long-distance network, specially for this project	Comparison of at least three offers
Two Optical Time Domain Reflectometers	WP3, WP4, Metrosert	12 000	For evaluation of the networks and components, specially for this project	Comparison of at least three offers
Optical Wavelength Meter	WP3, WP4, Metrosert	35 000	For evaluation of the networks and components, specially for this project	Public procurement procedure
Polarization Controller/Scrambler	WP3, WP4, Metrosert	7 000	For evaluation of the networks and components, specially for this project. WP3, WP4	Comparison of at least three offers

*Basis for calculation; One trip, 1 person, 2 nights + daily allowances is around 1500 EUR (Estonia is at the border of EU, flying is expensive). Project period is almost three years.

MKM support letter for round network



REPUBLIC OF ESTONIA
MINISTRY OF ECONOMIC AFFAIRS
AND COMMUNICATIONS

European Commission
Digital Europe program
Call: DIGITAL-2022-QCI-02

Our Ref: 08.09.2023 No 1.1-7/23-543

Letter of support
for the

EstQCI project activities

This letter is to confirm that the Estonian Ministry of Economic Affairs and Communication (MKM), represented by Vice Chancellor of Digital Development Luukas Kristian Ilves, is committed to supporting the Estonian Quantum Infrastructure Project (EstQCI) in developing the Quantum secure network between data centers that will house the governmental cloud services. Securing the round network of data centers towards the threats of the developing Quantum computer is a significant step in achieving the targets set in the Estonia's Digital Agenda 2030. Implementation of Quantum Key Distribution (QKD) and developed competences will enable to fulfill the following objectives:

- ***Directions which enable us to take a leap in development and ensure the sustainability of digital government***

Future-proof digital government platforms are sustainable and change flexibly according to the changing needs of users and technological possibilities. All public services are human-centric – designed and provided on the basis of users and their needs and preferences, while guaranteeing their fundamental rights and privacy.

One of the foundations and success factors of the Estonian digital government has been development based on strong platforms, i.e. central infrastructure components and services. This has sped up the development and introduction of digital services throughout the country and society. Implementation of QKD will allow the users to be secure of the privacy of their data and enable the development of one point access to all governmental services and information in a secure way.

- ***Improve the cybersecurity***

The cyber security objective makes a direct contribution to the implementation of the vision of digital society 2030, since the aim is to guarantee the protection of our digital government, economy and digital way of life more broadly. The current cyber security capacity of the state is insufficient for preventing risks. Implementation of QKD will allow Estonia to be a trailblazing and leading country in specific prioritized fields of cyber security in the EU and at a broader international level.

In a safe environment, we can make bold advances in our digital development: the development of services, the digital transformation in the economy and the creation of future solutions. The implementation of QKD to increase the cyber security thus

Suur-Ameerika 1 / 10122 Tallinn / ESTONIA
Phone: +372 625 6342 / Fax: +372 631 3660 / E-mail: info@mkm.ee / <http://www.mkm.ee>

consistently supports the entire vision, also keeping in mind and promoting national security interests.

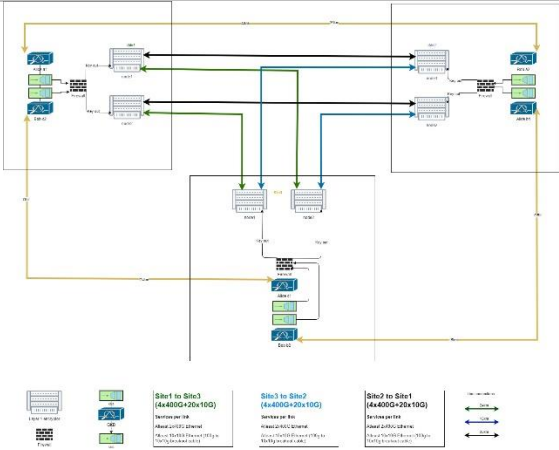
With best regards,

(signed digitally)

Luukas Kristian Ilves
Vice Chancellor of Digital Development
Republic of Estonia Ministry of Economic Affairs and Communication

HISTORY OF CHANGES		
VERSION	PUBLICATION DATE	CHANGE
2.0	02.12.22	Implementation plan – changes made according to the Evaluation Summary Report – More detailed description of the planned action added.
2.0	2.12.22	Implementation plan – target numbers of dissemination activities added
2.0	2.12.22	Project team – recruitment time of project coordinator added. One research scientist added (Mihkel Rähn, Metrosert)
2.0	2.12.22	Detailed budget added for other goods and services
2.0	2.12.22	Detailed budget added for equipment
2.0	2.12.22	Changes in the budget for beneficiaries and coordinator – more pm added, less goods/services. Increases for pm for work packages.
2.0	5.12.22	5.2 Security information added
3.0	8.12.22	Two tables of costs updated – added explanation for PR-costs and removed 2 items from equipment list according to the list from the Commission
3.0	8.12.22	Appendixes for the security part added.
3.0	8.12.22	Section 4 added
3.0	8.12.22	MS18 added to WP 1
3.0	8.12.22	D12-D15 dissemination level changed from sensitive to public
3.0	8.12.22	Changes in the costs table – duplicated the equipment to purchase costs.
4.0	8.12.22	Travel costs explanation added.
5.0	9.12.22	Costs per participant tables added. 4.2 deleted.
6.0	12.12.22	Travel costs added for MoD and MKM
6.0	12.12.22	Equipment added for Metrosert
7.0	24.04.23	Transfer of Project manager responsibilities and budget from MKM to RIKS. Due date correction for Deliverable 6.3 from M6 to M30.
7.1	02.05.2023	Adding Kalev Karu to Security advisory board
7.2	25.05.2023	Correction from Feedback from EU Commission: Deliverable 6.3 back to M6 as this is meant as the Dissemination and exploitation plan and not the final report. Rephrasing “Consortium management and decision-making risk(if applicable)”
8.0	7.10.23	<p>Amendment no. 2: AMD-101113143-3</p> <p>• Point 1.1 Objectives and activities – Added:</p> <p>Estonia has been a pioneer in converting public services into flexible e-solutions for its citizens and e-residents. Thus, it is important to ensure that there are no major cyber incidents that would compel citizens to abandon the online services that have been developed since the early 2000s and are an integral part of the Estonian governance structure. There is a profound understanding in Estonia that creation and development of a successful digital state requires strategic coherence between developing information society and ensuring cyber security.</p> <p>The implementation of the Government Cloud solution provides an excellent foundation for public e-services and solutions, making Estonia the most digital</p>

		<p>country in the world. With the Government Cloud solution, Estonia is taking the next step in its digital evolution to expand its ICT society. The Estonian Government Cloud will lead to the modernization and renewal of existing information systems, to embrace the opportunities offered by cloud technology and allow more agility in provision of e-services by the Estonian government agencies and critical service providers to residents and e-residents. Estonian public institutions will gradually transition from existing legacy systems to the new Government Cloud solution. Therefore, Estonia's cybersecurity strategy aims to become the most secure digital state to protect government data and ensure the state's longevity. With the advancement of quantum computing, this vision requires an understanding of possible uses of quantum technology for cybersecurity, the development of competences and infrastructure while supporting the relevant industry.</p> <p>The Estonian State is currently constructing a new round network between data centers that will house the Government Cloud. The EstQCI project has the opportunity to enable Estonia to be the first state to secure its Government Cloud with Quantum Communication Technology. The Estonian QCI project aims to lay the foundation for scaling up the respective competence in Estonia and providing infrastructure for the industry to secure e-Government services. Implementing QKD technology in the round network of data centers will enable us to enhance the privacy and cybersecurity of our citizens' data, which is currently stored and managed by existing legacy systems, including state registries, healthcare, social benefits, vehicle and transportation systems, to name a few.</p> <p>Added goal</p> <p>f: Demonstration of QKD implementation and usage on low latency and high-capacity connections between servers in a round network, securing the Estonian Government cloud services.</p>
8.0	7.10.23	<p>• Point 1.2 Contribution to long-term policy objectives – added:</p> <p>Estonian is advanced in their e-Government services from which many are already running on our Government Cloud servers. In cooperation with the Estonian State IT Centre and the Estonian Information Systems Authority, the EstQCI project will test the QKD systems on real life low latency and high speed connections between data centers that house the Government Cloud. The experience obtained through these demonstrations is valuable input for further developments in the area of quantum communication implementation for securing large capacity networks. In addition, the results from these tests will lay the foundation of future National Cyber Security policies and strategies.</p> <p>The implementation of QKD to the Government cloud will enable us to lay the foundation to start using the cloud services to share Classified information within the state and after the connections of EuroQCI also internationally.</p> <p>•</p>
8.0	7.10.23	<p>• Point 2.1 Maturity - Added:</p> <p>Estonia is advanced, with more than 20 years of experience, in securing a digital state and governmental e-services. The development and implementation of Governmental Cloud is bringing Estonia to the next step in its digital evolution to expand its ICT society. The long experience will contribute to developing and testing the QKD systems in real life environments and give valuable input to the development of Quantum technologies.</p>
8.0	7.10.23	<p>• Point 2.2 Maturity - Implementation plan and efficient use of resources – Added third testbed description:</p> <p>The QCI round network testbed for e-Government services</p> <p>The Estonian State IT Centre and the Estonian Information Systems Authority are currently building up a new round network of data centers that will house the Estonian Government Cloud services. This gives the EstQCI project an opportunity to demonstrate the QKD functionality in real life high speed and low latency data center environment.</p>

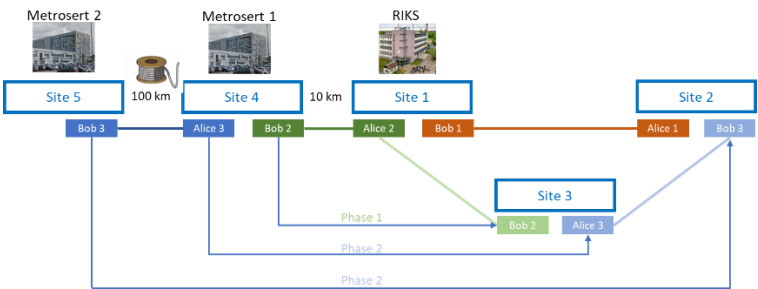


The testing of QKD within this network will be conducted in three phases to optimize project time efficiency and evaluate various solutions.

- In the first phase, two QKD systems will be integrated into the network for initial functionality and integration tests, utilizing lower 10G ports. Solutions for supporting three sites with two pairs of QKD devices will be established.
- In the second phase, the third QKD pair will be transitioned from Metrology tests to the round network. Initial functionality and stability tests will be conducted at lower speeds
- The third phase will involve the implementation of QKD for 400 G connections with low latency.

During the first stage, we will install and configure 2 QKD device pairs to work with 10 G Ports in the network. This setup is designed to thoroughly test functionality, key distribution, and network management. Close cooperation between the project team and the manufacturers of the QKD and network devices is essential during this phase to gain valuable insights into how QCI systems should be constructed and configured.

Throughout these tests, we will also explore the feasibility of supporting three sites with just two QKD device pairs. This investigation aims to develop strategies for failure management in the event of the loss of one QKD device in the round network. Additionally, we will assess the potential for reducing investment costs in future networks that may require fewer QKD devices. By focusing on moving only one device paid, we can conduct fundamental metrological tests and network integration concurrently, maximizing the efficiency of project time utilization.



In the second phase, the third QKD device pair will be introduced to the round network, and a comprehensive circular solution will undergo initial testing, starting with lower speeds on 10G ports. During this phase, rigorous operational, management, and monitoring tests will be conducted. This stage is crucial to ensure the stability of both the QKD and network devices, guaranteeing their reliable integration and operation before implementing the technology for high-speed connections.

In the third phase, the QKD devices will be integrated with high-speed, low-latency 400G connections. Testing at these higher speeds will provide valuable

		<p>insights into the real-world requirements for QKD systems between data centers.</p> <p>The key parameters to be evaluated:</p> <ul style="list-style-type: none"> • Collaboration and cooperation between QKD and network devices • Configuration and monitoring requirements for key exchange • Performance and stability of key management at high speeds. • Key rate requirements in real-life environments • Strategies for handling failure modes. <p>• In preparation for the EuroQCI, the knowledge gained from these tests will provide valuable insights into the requirements for international connections. Once the EuroQCI connection is established with Finland, our ambition is to leverage the Government Cloud for cross-border communication and connect to the Quantum Computer LUMI in Finland. This connection to LUMI will grant Estonian state institutions, academia, and industry access to secure quantum computing power, fostering collaboration and innovation across various sectors.</p>
8.0	7.10.23	<p>• Point 2.3 Outside resources - added RIA and RIT:</p> <p>Close cooperation with the Estonian State IT Centre and the Estonian Information Systems Authority to successfully implement and manage the QKD devices in real data center environment.</p> <ul style="list-style-type: none"> •
8.0	7.10.23	<p>• Point 3.1 Expected outcomes and deliverables – added:</p> <p>During the project, the first long-distance quantum communication network in Estonia will be demonstrated in laboratory conditions to prepare for the large-scale deployment of a QCI in the region. A round QKD network will be demonstrated and tested in real life data center environment. This will open up the possibility to test the integration and cooperation of QKD, PQC and traditional cybersecurity systems. Deploying the experimental QKD systems with advanced high speed and low latency connections aims to prepare for the large-scale uptake and use of such systems and technologies for State communication, Private sector and the EuroQCI connections. The experience gained from the EstQCI activities will enable to lay the foundation for securing the Government Cloud services and gain inputs to State and commercial cyber security strategies and policies.</p> <p>• Point 3.2 Competitiveness and benefits for society – Added:</p> <p>Securing the network of servers with Quantum Technologies will facilitate the secure transition of Estonian public institutions to a new Government Cloud solution. Centralizing all databases and information in one location presents opportunities to advance e-services, ultimately achieving the desired one-point access to all governmental services and information securely. This ensures that Estonian residents and e-residents can benefit from the protective capabilities of digitalization, ensuring the safety of our digital lives.</p>
8.2	9.10.23	<p>Point 4.2 Timetable - Added round network, metropolitan network timeline shifted earlier</p>
8.2	9.10.23	<p>Annexes: PURCHASES AND EQUIPMENT</p> <ul style="list-style-type: none"> • Defined traveling for RIKS (in line with original budget and to reduce undefined costs for RIKS) – 10 000 EUR • Reduced cost for QKD devices as a result of our tender outcomes plus one extra pair of QKD devices – 644 000 EUR • Added line for QKD compatible encryption devices in the amount of 610 000 EUR (50% of total equipment cost counted to this project, the other 50% is covered by RIKS) • Removed line for “External Key Management system for QKD key exchange” in the amount of 160 000 EUR

8.2	9.10.23	MKM support letter for round network use case added to Annexes for part B																																																																																																																																																																																																																																																																																																																																																														
9.0	8.10.24	<div><div>Point 4.2 Timeline</div><div><p>The project consortium is formally requesting an extension of the project duration by six months, until the end of 2025. This request is due to delays encountered during the testing and deployment phases of the project, specifically related to the Quantum Key Distribution (QKD) devices.</p><p>The procurement of the QKD and encryption systems was completed at the end of 2023, with testing initiated in Q1 2024. However, evaluation testing has revealed multiple instabilities and software issues within the QKD systems, significantly affecting the progress of both the test plan and the deployment of the metropolitan network. The software modifications required to resolve these issues have led to notable behavioral changes in the QKD devices. As a result, the testing conducted before and after the software updates is no longer comparable.</p><p>Furthermore, the software releases for the encryption devices, enabling the use of QKD (ETSI 014 standard) on 400G connections has been postponed to Q1 2024. This delays the start of testing high speeds on the ring network.</p><p>To ensure accurate and consistent results, many of the test plan activities will need to be repeated, causing an estimated delay of at least four months. Additionally, given the delayed software release for encryption devices and ongoing instability of the QKD devices, we anticipate further challenges during the ring network testbed phase. Therefore, we foresee the need for an additional six months to complete the project effectively and ensure that all objectives are met.</p><p>This extension will allow the consortium to address the existing issues thoroughly and deliver reliable outcomes within the extended timeframe.</p></div></div> <div><table><tr><th rowspan="2">ACTIVITY</th><th colspan="4">YEAR 1</th><th colspan="4">YEAR 2</th><th colspan="4">YEAR 3</th></tr><tr><th>Q 1</th><th>Q 2</th><th>Q 3</th><th>Q 4</th><th>Q 1</th><th>Q 2</th><th>Q 3</th><th>Q 4</th><th>Q 1</th><th>Q 2</th><th>Q 3</th><th>Q 4</th></tr><tr><td>T1.1 - Project management</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T1.2 - Procurement coordination</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T1.3 - Alignment with the security baseline</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T2.1 - Preparation for the networks</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T2.2 - Testing of the devices</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T2.3.1 - Deployment of the metropolitan network</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T2.3.2 - Deployment of the round network</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T3.1.1 - Evaluation of the metropolitan network</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T3.1.2 - Evaluation of the round network</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T3.2 - Identification of use cases</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T3.3.1 - First use cases in the metropolitan network</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T3.3.2 - First use cases in the round network</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T3.4 - Knowledge dissemination</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T4.1 - Evaluation of technologies</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T4.2 - Test planning and execution of long-distance network</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T4.3 - Demonstration of the network</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T4.4 - Planning of the long-distance network in the field</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T5.1 - Planning of cross-border connections</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T5.2 - Planning of international testing</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T5.3 - Discussions on possible satellite interconnection</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T5.4 - International stakeholder events</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T5.5 - Participation in the EuroQCI initiative and collaboration with the DIGITAL topic 3 project (co-ordination and support action CSA) and with other EuroQCI projects.</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T6.1 - Implementation of the communication plan</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T6.2 - Stakeholder events</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>T6.3 - Planning of support measures for the industry</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table><div><div></div>Original plan<div></div>Amendment new plan<div></div>Amendment removed time</div></div>	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	Q 3	Q 4	T1.1 - Project management													T1.2 - Procurement coordination													T1.3 - Alignment with the security baseline													T2.1 - Preparation for the networks													T2.2 - Testing of the devices													T2.3.1 - Deployment of the metropolitan network													T2.3.2 - Deployment of the round network													T3.1.1 - Evaluation of the metropolitan network													T3.1.2 - Evaluation of the round network													T3.2 - Identification of use cases													T3.3.1 - First use cases in the metropolitan network													T3.3.2 - First use cases in the round network													T3.4 - Knowledge dissemination													T4.1 - Evaluation of technologies													T4.2 - Test planning and execution of long-distance network													T4.3 - Demonstration of the network													T4.4 - Planning of the long-distance network in the field													T5.1 - Planning of cross-border connections													T5.2 - Planning of international testing													T5.3 - Discussions on possible satellite interconnection													T5.4 - International stakeholder events													T5.5 - Participation in the EuroQCI initiative and collaboration with the DIGITAL topic 3 project (co-ordination and support action CSA) and with other EuroQCI projects.													T6.1 - Implementation of the communication plan													T6.2 - Stakeholder events													T6.3 - Planning of support measures for the industry												
	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	Q 3	Q 4																																																																																																																																																																																																																																																																																																																																																				
T1.1 - Project management																																																																																																																																																																																																																																																																																																																																																																
T1.2 - Procurement coordination																																																																																																																																																																																																																																																																																																																																																																
T1.3 - Alignment with the security baseline																																																																																																																																																																																																																																																																																																																																																																
T2.1 - Preparation for the networks																																																																																																																																																																																																																																																																																																																																																																
T2.2 - Testing of the devices																																																																																																																																																																																																																																																																																																																																																																
T2.3.1 - Deployment of the metropolitan network																																																																																																																																																																																																																																																																																																																																																																
T2.3.2 - Deployment of the round network																																																																																																																																																																																																																																																																																																																																																																
T3.1.1 - Evaluation of the metropolitan network																																																																																																																																																																																																																																																																																																																																																																
T3.1.2 - Evaluation of the round network																																																																																																																																																																																																																																																																																																																																																																
T3.2 - Identification of use cases																																																																																																																																																																																																																																																																																																																																																																
T3.3.1 - First use cases in the metropolitan network																																																																																																																																																																																																																																																																																																																																																																
T3.3.2 - First use cases in the round network																																																																																																																																																																																																																																																																																																																																																																
T3.4 - Knowledge dissemination																																																																																																																																																																																																																																																																																																																																																																
T4.1 - Evaluation of technologies																																																																																																																																																																																																																																																																																																																																																																
T4.2 - Test planning and execution of long-distance network																																																																																																																																																																																																																																																																																																																																																																
T4.3 - Demonstration of the network																																																																																																																																																																																																																																																																																																																																																																
T4.4 - Planning of the long-distance network in the field																																																																																																																																																																																																																																																																																																																																																																
T5.1 - Planning of cross-border connections																																																																																																																																																																																																																																																																																																																																																																
T5.2 - Planning of international testing																																																																																																																																																																																																																																																																																																																																																																
T5.3 - Discussions on possible satellite interconnection																																																																																																																																																																																																																																																																																																																																																																
T5.4 - International stakeholder events																																																																																																																																																																																																																																																																																																																																																																
T5.5 - Participation in the EuroQCI initiative and collaboration with the DIGITAL topic 3 project (co-ordination and support action CSA) and with other EuroQCI projects.																																																																																																																																																																																																																																																																																																																																																																
T6.1 - Implementation of the communication plan																																																																																																																																																																																																																																																																																																																																																																
T6.2 - Stakeholder events																																																																																																																																																																																																																																																																																																																																																																
T6.3 - Planning of support measures for the industry																																																																																																																																																																																																																																																																																																																																																																
		<div><div>Changes to the list of purchased Equipment for Metroser</div><div><p>In the QKD-devices procured, the polarization 3 state efficient BB84 decoy encoding scheme is employed. The project tasks envisage measurement of the mean photon number statistics of a QKD transmitter in order to evaluate Poissonian nature of the source applied in the transmitter. This can be done with the measurement apparatus consisting of a Hanbury Brown-Twiss (HBT) interferometer, which is available at Metroser, however, needs some modifications. The need for modifications was foreseen in the EstQCI project description.</p><p>When measuring the mean photon number statistics of a QKD transmitter using the HBT setup, the polarization controller or scrambler plays a crucial role in</p></div></div>																																																																																																																																																																																																																																																																																																																																																														

ensuring accurate results. The polarization state of light can significantly affect the detection process, especially when using Superconducting Nanowire Single-Photon Detectors (SNSPDs), which are sensitive to the polarization of incoming signals. To avoid polarization-dependent bias in the measurement, the polarization controller/scrambler is employed to randomize the polarization state of the input signal. This randomization ensures that the polarization effects are averaged out, leading to more reliable and representative measurements of the photon statistics emitted by the QKD transmitter.

In addition, a polarization controller is also necessary to adjust the polarization of the input pulses at the QKD receiver (Bob). In practical QKD systems, the polarization of light can fluctuate due to various factors such as fiber bending, environmental changes, and other transmission-related variables. By using a polarization controller, it is possible to dynamically align and tune the polarization state of the incoming pulses to Bob's detection apparatus. This adjustment is critical for characterizing the impact of polarization variation on the overall efficiency of the QKD system.

The initial price investigation shows the purchase cost around 6 500 eur for the polarization controller or scrambler. However, the previous experience in procurement shows that the price can be higher in official procurement due to additional requirements on warranty and support. Therefore, the price is estimated to 7 000 eur.

Optical fibre	Equipment	WP4	100 km of optical fiber for laboratory testing, WP4, Metroser	45 000 8 000
Polarization Controller/Scrambler	Equipment	WP3, WP4	For evaluation of the networks and components, specially for this project. WP3, WP4	7 000

DATA SHEET

1. General data

Project summary:

Project summary
The purpose of the EstQCI project is to deploy the first experimental QKD network in Estonia in order to be prepared for the full deployment of the EuroQCI. EstQCI should provide the basis for the fast uptake and deployment of quantum security technology by building up the competence of relevant ministries, companies and other entities. In addition, the project would serve as a deployment model for the future deployment of QKD network in Estonia. The project aims to build up a metropolitan QKD network and test long-distance links to be ready for connections with neighbouring countries. In these networks, devices from EU-27 developers will be used, when possible. The main goals of the project are as follows: a) Building up the know-how and competence of relevant entities for future deployment of QKD networks and services b) Testing the readiness of devices from EU-27 producers to gain information about their suitability for the Estonian conditions and needs c) First demonstrations of the use of the network between metropolitan areas as well as for long-distance network in laboratory conditions d) Collaborating with neighbouring countries and preparation for cross-border links with Finland, Latvia and Sweden e) Sharing knowledge with relevant stakeholders, raise the awareness of companies and other relevant entities about the possibilities of the network to prepare for future secure connectivity/ cyber security applications. f) Demonstration of QKD implementation and usage on low latency and high-capacity connections between servers in a round network, securing the Estonian Government cloud services. One of the important elements of the EstQCI project is coordination with Finland, Latvia, Lithuania, Poland and Sweden to create a foundation for the future cooperation within the margins of EuroQCI project and to prepare for terrestrial cross-border connections between Member States. As a result of the project we will open our network for interested parties (for example cyber security industry, academia etc) and facilitate the exploration of further use cases of the network. We will build up a wide-scale competence among the relevant stakeholder

Keywords:

- Quantum Technologies (e.g. computing and communication)

Project number: 101113143

Project name: Estonian Quantum Communication Infrastructure

Project acronym: EstQCI

Call: DIGITAL-2022-QCI-02

Topic: DIGITAL-2022-QCI-02-DEPLOY-NATIONAL

Type of action: DIGITAL Simple Grants

Granting authority: European Commission-EU

Grant managed through EU Funding & Tenders Portal: Yes (eGrants)

Project starting date: fixed date: 1 January 2023

Project end date: 31 December 2025

Project duration: 36 months

Consortium agreement: Yes

2. Participants

List of participants:

N°	Role	Short name	Legal name	Ctry	PIC	Total eligible costs (BEN and AE)	Max grant amount	Entry date	Exit date
1	COO	MKM	MAJANDUS JA KOMMUNIKATSIOONIMINISTEERIUM	EE	963638450	285 048.00	142 524.00		
2	BEN	Metrosert	AKTSIASELTS METROSERT	EE	994104016	831 390.00	415 695.00		

N°	Role	Short name	Legal name	Ctry	PIC	Total eligible costs (BEN and AE)	Max grant amount	Entry date	Exit date
3	BEN	RIKS	STATE INFOCOMMUNICATION FOUNDATION	EE	911424126	2 729 035.00	1 364 517.50		
4	BEN	EE MoD	KAITSEMINISTEERIUM	EE	905124655	154 080.00	77 040.00		
Total						3 999 553.00	1 999 776.50		

Coordinator:

- MAJANDUS JA KOMMUNIKATSIOONIMINISTEERIUM (MKM): from 20 December 2022 to present

3. Grant

Maximum grant amount, total estimated eligible costs and contributions and funding rate:

Total eligible costs (BEN and AE)	Funding rate (%)	Maximum grant amount (Annex 2)	Maximum grant amount (award decision)
3 999 553.00	50	1 999 776.50	1 999 776.50

Grant form: Budget-based

Grant mode: Action grant

Budget categories/activity types:

- A. Personnel costs
 - A.1 Employees, A.2 Natural persons under direct contract, A.3 Seconded persons
 - A.4 SME owners and natural person beneficiaries
- B. Subcontracting costs
- C. Purchase costs
 - C.1 Travel and subsistence
 - C.2 Equipment
 - C.3 Other goods, works and services
- D. Other cost categories
 - D.1 Financial support to third parties
 - D.2 Internally invoiced goods and services
- E. Indirect costs

Cost eligibility options:

- Standard supplementary payments
- Average personnel costs (unit cost according to usual cost accounting practices)
- Country restrictions for subcontracting costs
- Limitation for subcontracting
- Travel and subsistence:
 - Travel: Actual costs
 - Accommodation: Actual costs
 - Subsistence: Actual costs

- Equipment: depreciation and full costs for listed equipment
- Costs for providing financial support to third parties (actual cost; max amount for each recipient: EUR 0.00)
- Indirect cost flat-rate: 7% of the eligible direct costs (categories A-D, except volunteers costs and exempted specific cost categories, if any)
- VAT: Yes
- Country restrictions for eligible costs
- Other ineligible costs

Budget flexibility: Yes (no flexibility cap)

4. Reporting, payments and recoveries

4.1 Continuous reporting (art 21)

Deliverables: see Funding & Tenders Portal Continuous Reporting tool

4.2 Periodic reporting and payments

Reporting and payment schedule (art 21, 22):

Reporting					Payments	
Reporting periods			Type	Deadline	Type	Deadline (time to pay)
RP No	Month from	Month to				
					Initial prefinancing	30 days from entry into force/10 days before starting date/ financial guarantee (if required) – whichever is the latest
1	1	12	Periodic report	60 days after end of reporting period	Interim payment	90 days from receiving periodic report
2	13	24	Periodic report	60 days after end of reporting period	Interim payment	90 days from receiving periodic report
3	25	36	Periodic report	60 days after end of reporting period	Final payment	90 days from receiving periodic report

Prefinancing payments and guarantees:

Prefinancing payment		Prefinancing guarantee		
Type	Amount	Guarantee amount	Division per participant	
Prefinancing 1 (initial)	1 299 854.73	n/a	1 - MKM	n/a
			2 - Metrosert	n/a
			3 - RIKS	n/a
			4 - EE MoD	n/a

Reporting and payment modalities (art 21, 22):

Mutual Insurance Mechanism (MIM): No

Restrictions on distribution of initial prefinancing: The prefinancing may be distributed only if the minimum number of beneficiaries set out in the call conditions (if any) have acceded to the Agreement and only to beneficiaries that have acceded.

Interim payment ceiling (if any): 90% of the maximum grant amount

No-profit rule: Yes

Late payment interest: ECB + 3.5%

Bank account for payments:

EE891010220034796011

Conversion into euros: Double conversion

Reporting language: Language of the Agreement

4.3 Certificates (art 24):

Certificates on the financial statements (CFS):

Conditions:

Schedule: only at final payment, if threshold is reached

Standard threshold (beneficiary-level):

- financial statement: requested EU contribution to costs \geq EUR 325 000.00

4.4 Recoveries (art 22)

First-line liability for recoveries:

Beneficiary termination: Beneficiary concerned

Final payment: Coordinator

After final payment: Beneficiary concerned

Joint and several liability for enforced recoveries (in case of non-payment):

Limited joint and several liability of other beneficiaries — up to the maximum grant amount of the beneficiary

Joint and several liability of affiliated entities — n/a

5. Consequences of non-compliance, applicable law & dispute settlement forum

Applicable law (art 43):

Standard applicable law regime: EU law + law of Belgium

Dispute settlement forum (art 43):

Standard dispute settlement forum:

EU beneficiaries: EU General Court + EU Court of Justice (on appeal)

Non-EU beneficiaries: Courts of Brussels, Belgium (unless an international agreement provides for the enforceability of EU court judgements)

6. Other

Specific rules (Annex 5): Yes

Standard time-limits after project end:

Confidentiality (for X years after final payment): 5

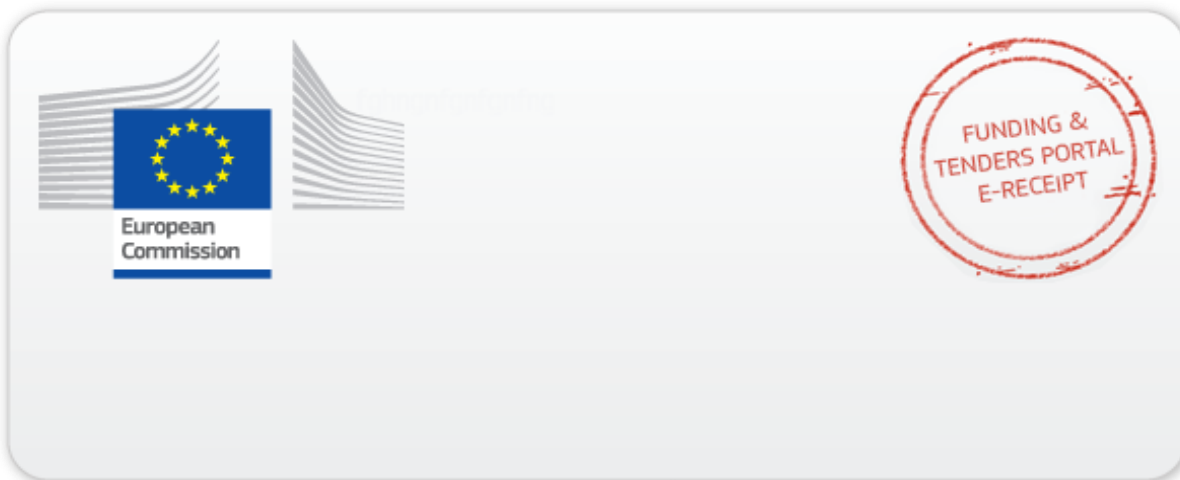
Record-keeping (for X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

Reviews (up to X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

Audits (up to X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

Extension of findings from other grants to this grant (no later than X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

Impact evaluation (up to X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)



This electronic receipt is a digitally signed version of the document submitted by your organisation. Both the content of the document and a set of metadata have been digitally sealed.

This digital signature mechanism, using a public-private key pair mechanism, uniquely binds this eReceipt to the modules of the Funding & Tenders Portal of the European Commission, to the transaction for which it was generated and ensures its full integrity. Therefore a complete digitally signed trail of the transaction is available both for your organisation and for the issuer of the eReceipt.

Any attempt to modify the content will lead to a break of the integrity of the electronic signature, which can be verified at any time by clicking on the eReceipt validation symbol.

More info about eReceipts can be found in the FAQ page of the Funding & Tenders Portal.

(<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/faq>)