



NordicQCI

Nordic Quantum
Communication Infrastructure

NordicQCI – networking with the stars

Timothy Gibbon

33rd NORDUnet Conference

8-10 Sept 2026, Luleå, Sweden

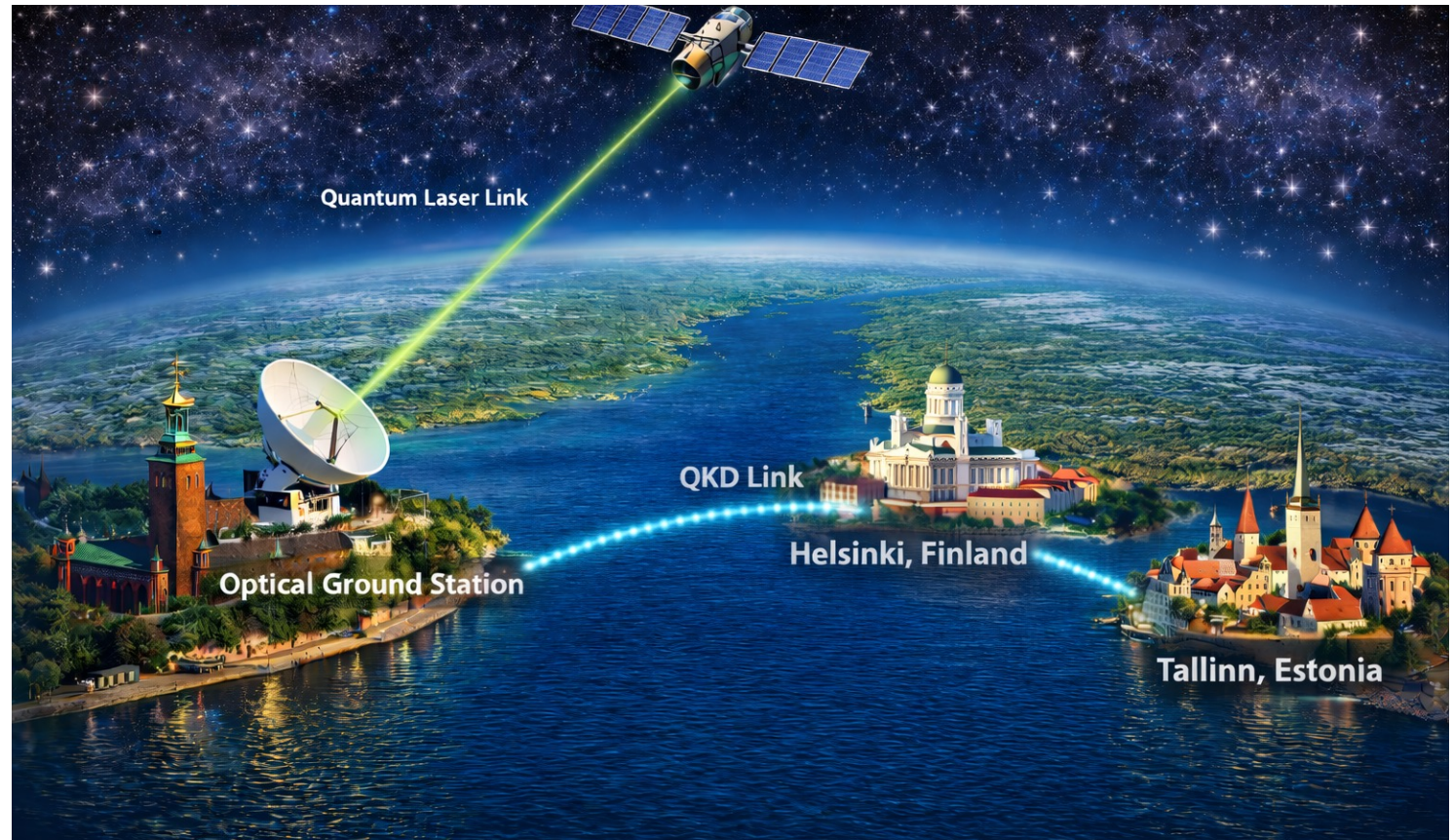
timothy.gibbon@ri.se



Co-funded by
the European Union

Project summary

- NordicQCI project is an important step to implement **Quantum communication capabilities over the national borders in Nordic countries**.
- Aim is to protect **critical public infrastructures** by securing their communications and data, especially those that cross-national borders and serve more than one Member State.
- The goal of the project is to provide **cross-border** connections between **Estonia-Finland and Finland-Sweden** in order to enable reliable and resilient transmission of sensitive communications and data between public authorities, research organisations and critical infrastructures in Member States.
- Implementation of the **terrestrial cross-border links** will take place over the submarine cables in Tallinn, Helsinki, Åland Islands and Stockholm metropolitan area.
- Also, an **interconnection with the EuroQCI's Space Segment** will be established in Stockholm via the optical ground station and related ground equipment to demonstrate the Eagle1 capabilities in the Nordic environment.
- This **NordicQCI project will benefit and utilize** all the work and implementations done in **DEP EuroQCI National projects** in 2023-2025 for national domains in Estonia, Finland and Sweden.



Overview of planned NordicQCI infrastructure linking the national QCIs of Sweden, Finland and Estonia and developing an optical ground station (OGS) for satellite connection in Stockholm.

Project structure

Consortium composition:

Number	Role	Short name	Legal name	Country
1	COO	RISE	RISE RESEARCH INSTITUTES OF SWEDEN AB	SE
2	BEN	METROSERT	AKTSIASELTS METROSERT	EE
3	BEN	CSC	CSC-TIETEEN TIETOTEKNIKAN KESKUS OY	FI
4	BEN	EAB	ERICSSON AB	SE
5	BEN	RIKS	STATE INFOCOMMUNICATION FOUNDATION	EE
6	BEN	SU	STOCKHOLMS UNIVERSITET	SE
7	BEN	ERVE	SUOMEN ERILLISVERKOT OY	FI
8	BEN	VTT	TEKNOLOGIAN TUTKIMUSKESKUS VTT OY	FI
9	BEN	KTH	KUNGLIGA TEKNISKA HOEGSKOLAN	SE
10	BEN	LIU	LINKOPINGS UNIVERSITET	SE

Contacts

WP1: timothy.gibbon@ri.se
laia.gines@ri.se
WP2: dushko.kuzmanovski@ericsson.com
WP3: Mohamed Bourennane <boure@fysik.su.se>
WP4: johan.laxen@erillisverkot.fi
WP5: ingrid.linnas@riks.ee

Activities:

WP1 Project coordination (Lead: RISE)

- T1.1 NordicQCI & EuroQCI coordination and reporting
- T1.2 Procurement coordination
- T1.3 Alignment with the Security Baseline
- T1.4 Dissemination and participation in EuroQCI initiative and dissemination of the study results

WP2 Studies (Lead EAB)

- T2.1 Study, design and specs for cross-border KME and network orchestration
- T2.2 Study, design and specs for cross-border Trusted Border nodes and site requirements
- T2.3 Study, design and specs of QKD OGS and terrestrial interfaces
- T2.4 Study and analysis of secure communications over long distance links
- T2.5 Study and analysis of QKD coexistence with classical transmission and PQC
- T2.6 Study and analysis of QKD system, equipment and link testing

WP3 Works Space Segment (Lead SU)

- T3.1 Designing, deploying and testing of OGS
- T3.2 Testing, investigation, and deployment of the interoperability between OGS and terrestrial segments
- T3.3 Testing, investigation, and deployment of specs of QKD OGS with European satellites
- T3.4 Cross project space segment activities

WP4 Works Terrestrial SWE-FIN (Lead ERVE)

- T4.1 Deployment and testing of cross-border links with interoperability methods
- T4.2 Testing secure cross-border quantum communication services with Ericsson use cases (SWE-FIN)
- T4.3 Testing secure cross-border quantum communication services with CSC use (SWE-FIN)
- T4.4 Implementation of ETSI-QKD-020 standard (Ericsson use case)
- T4.5 Implementing and Integrating PQC Algorithms for Enhanced QKD Coexistence (Ericsson use case)

WP5 Works Terrestrial EST-FIN (lead RIKS)

- T5.1 Deployment and testing of cross-border links with interoperability methods
- T5.2 Testing secure quantum communication services on EST-FIN link
- T5.3 Testing of secure key transfer through multiple MS and Space connection



Co-funded by
the European Union

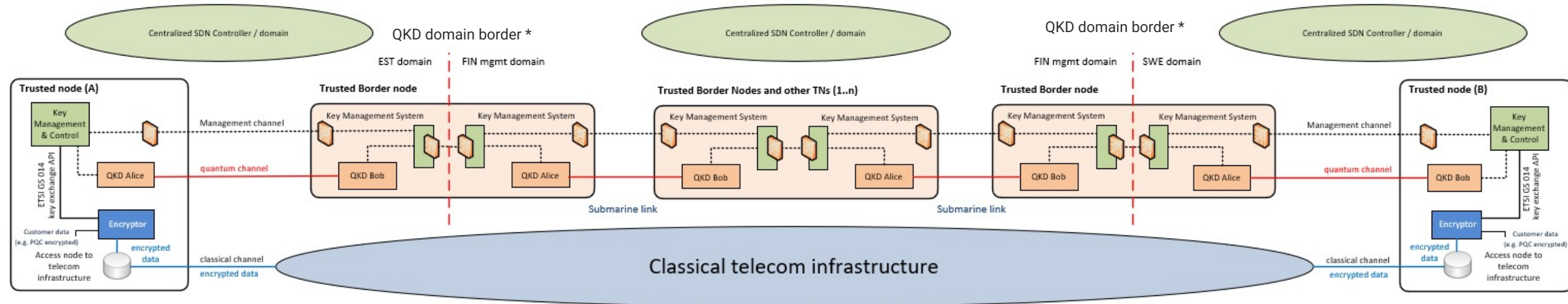
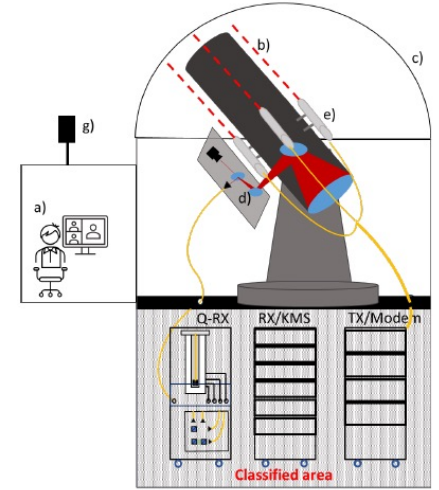


CEF cross-border setup visualization

To provide Cross-Border QKD Key forwarding connections and Use case demonstrations

- Target to have EST-FIN-SWE national QKD domains interconnected.
- National QKD domains (based on DEP projects) may need to be upgraded to meet CEF requirements
- Each quantum channel link, being either national or cross-border, need to be operated by one entity (= one QKD domain)
- Trusted border nodes terminating cross-border quantum channel links need to have a responsible operator and be managed by a single entity. This entity shall provide required resources and hosting for a cross-border quantum link equipment so that inter-domain QKD KMS connectivity can be established.

- Key Management Systems shall support interdomain connectivity e.g. virtual link discovery & routing, SLA and other possible requirements.
- No Security Certifications are in place for Quantum based Key Delivery yet.
- Encryption of the classical connections is handled separately from the cross-border Quantum channel.
- One SpaceQCI system shared with several MS use. Cross-border activities
- Space QKD connectivity to some other MSs? Cross-project activities



Co-funded by
the European Union



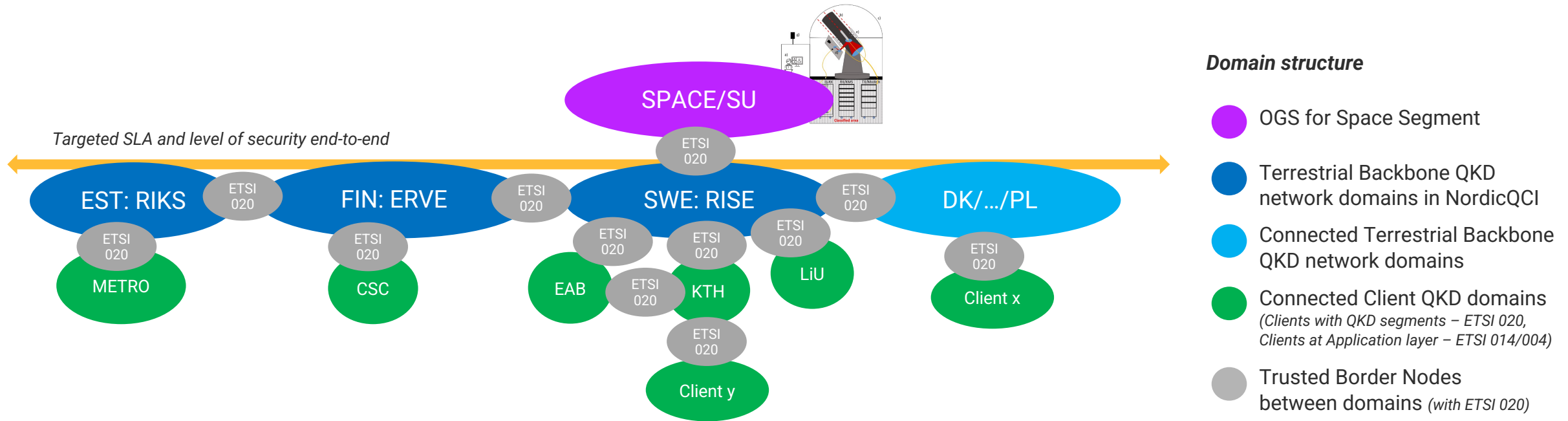
Estonia

Finland

Sweden

* Each QKD domain may contain
several Trusted nodes w/o encryptions

NordicQCI: QKD domain architecture



Domain responsibility

- Each QKDN provider and Connected QKD User is responsible of the management layer, control layer and security perimeters for all QKDN components located in his domain.
- Each QKDN provider is responsible to provide Key Forwarding service at the QKD layer with a decent availability/SLA and in secure manner as agreed between connected QKDN providers and Users.
- ETSI specified interfaces shall be applied for interoperation between connected QKDN providers / Users.

Reachability

- The Key Forwarding service will cover at least Tallinn, Helsinki to Åland and Stockholm with terrestrial connectivity and also EuroQCI Space Segment in Stockholm towards OGSs of the EuroQCI CEF partners.
- Target is also to implement cross-project terrestrial interconnectivity of the Key Forwarding service with the Danish CEF project and to get reachability to their QKDN domains in Denmark, Germany and Poland.



Co-funded by
the European Union



WP4 Works Terrestrial SWE-FIN

Deployment of the QKDN with interoperability

- T4.1 Deployment and testing of cross-border links with interoperability methods (SWE-FIN)
- includes preparation of the FIN and SWE QKD domains and interoperability towards Space Segment domain
 - utilises Study task results for purchase process of QKDN and implementation of the Border Trusted Nodes
 - implement interoperability between terrestrial and Space Segment domains (FIN-SWE, SWE-DAN, SWE-Space)

Use case demonstrations

- T4.2 Testing secure cross-border quantum communication services with Ericsson use cases (SWE-FIN)
- T4.3 Testing secure cross-border quantum communication services with CSC use (SWE-FIN)
- T4.4 Implementation of ETSI-QKD-020 standard (Ericsson use case)
- T4.5 Implementing and Integrating PQC Algorithms for Enhanced QKD Coexistence (Ericsson use case)

Preparation of C-B TN & connections and national infras (fibres, TNs, QKD, KMS, Encryptors, mgmt)

Purchasing process of QKD, KMS, SDN Controller & Orchestration based on study results. Deliveries.

Testing of QKD, KMS, SDN Controller & Orchestration systems. Implementation, Use Cases demonstrations.

2026												2027												2028												2029					
Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42



Co-funded by
the European Union



Quantum secure cross-border EuroHPC collaboration

Why it matters: EuroHPC supercomputers are shared across countries, so moving data and workloads between sites needs strong protection.

What QKD adds: Quantum key distribution gives a way to generate and exchange encryption keys with very high security guarantees. It protects the classical network carrying HPC traffic.

Why high capacity is important: HPC traffic is large and continuous, so the protected link must support real operational data rates, not just a demo.

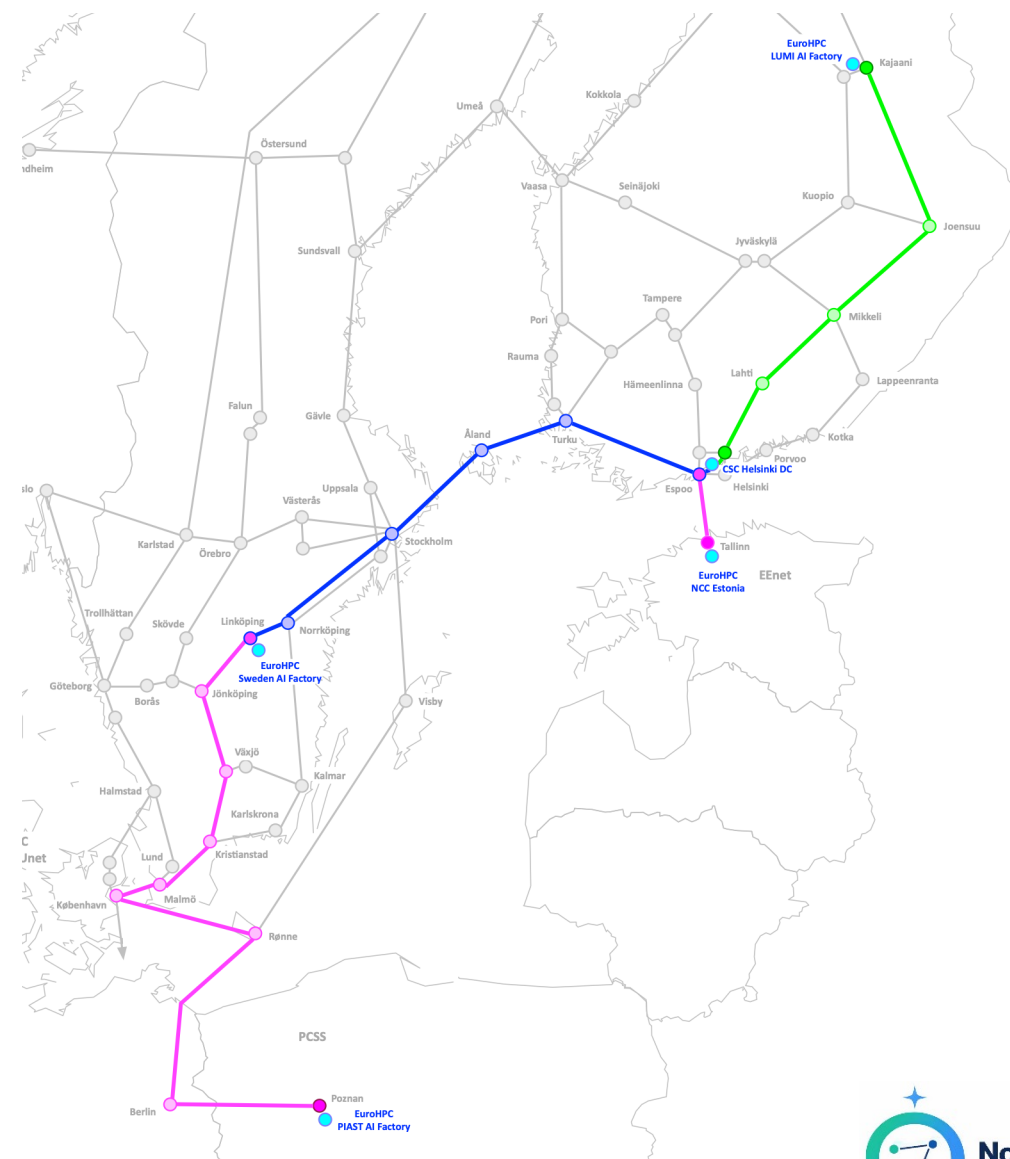
Use case: Secure transfer of sensitive scientific datasets, checkpoints, and inter-site workflows between supercomputing centres.

Value for users: Enables collaboration HPC workloads without weakening security.

Value for Europe: Builds trusted digital infrastructure and supports technological sovereignty.

Key challenge solved: Combining ultra-fast networking with cryptographic key renewal across long distances and multiple national sites.

Outcome: A model for future federated supercomputing and secure data spaces.



Co-funded by
the European Union



T2.5 QKD coexistence with classical transmission and PQC

- Evaluating and hardening the cryptographic components of existing QKD system
- Hybrid QKD-PQC solutions
- QKD coexistence with classical transmission

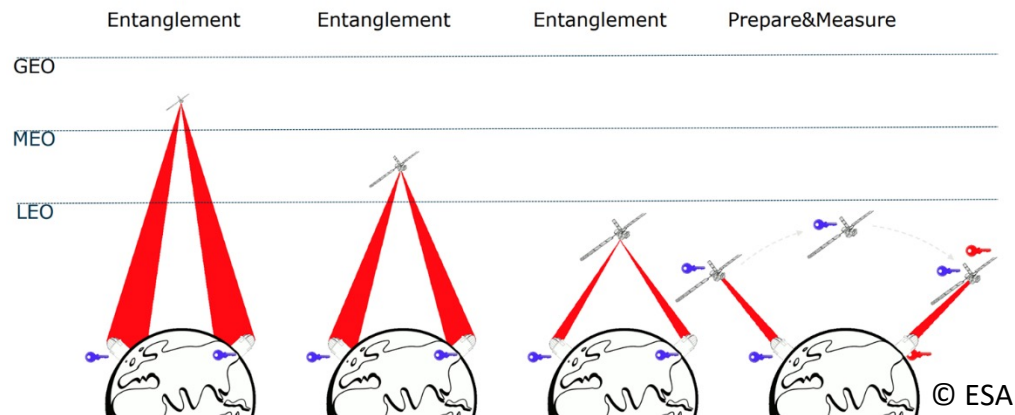
Topics covered/work in progress:

- Overall security of QKD systems
- QKD KMS authentication
- Research on hybrid key solutions
- Compilation of relevant terminology and standards (ETSI, ISO/IEC, IETF)
- Evaluation of Quantum and Classical Random Number Generators
- QKD integration with existing systems (optical, data and control planes)

WP3 – Space segment

- T3.1 Designing, deploying and testing of OGS
- T3.2 Testing, investigation, and deployment of the interoperability between OGS and terrestrial segments
- T3.3 Testing, investigation, and deployment of specs of QKD OGS with European satellites
- T3.4 Cross project space segment activities

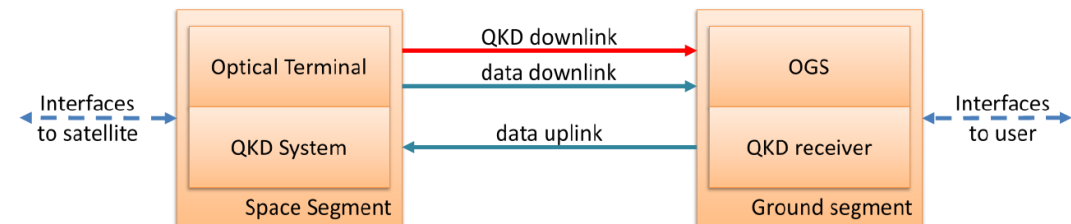
Different QKD space systems



Satellite-based solution for communication for long distances



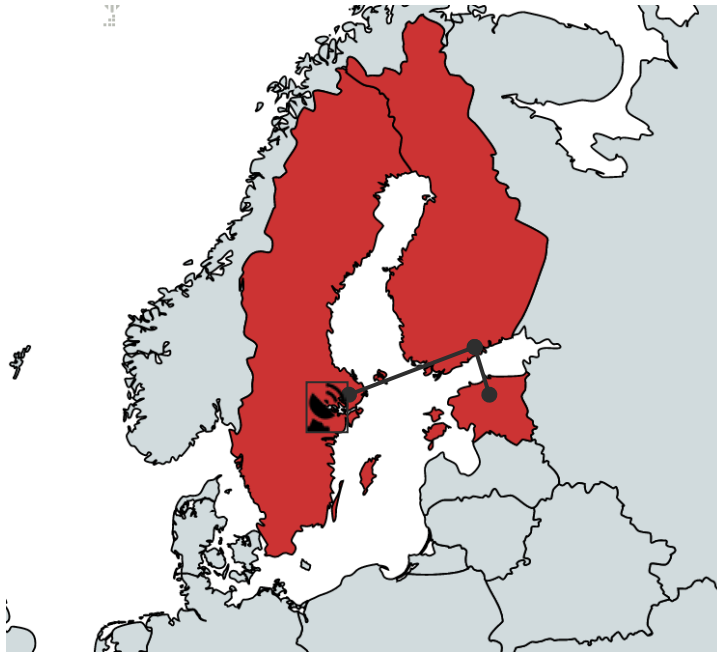
Albanova Optical Ground Station (OGS)



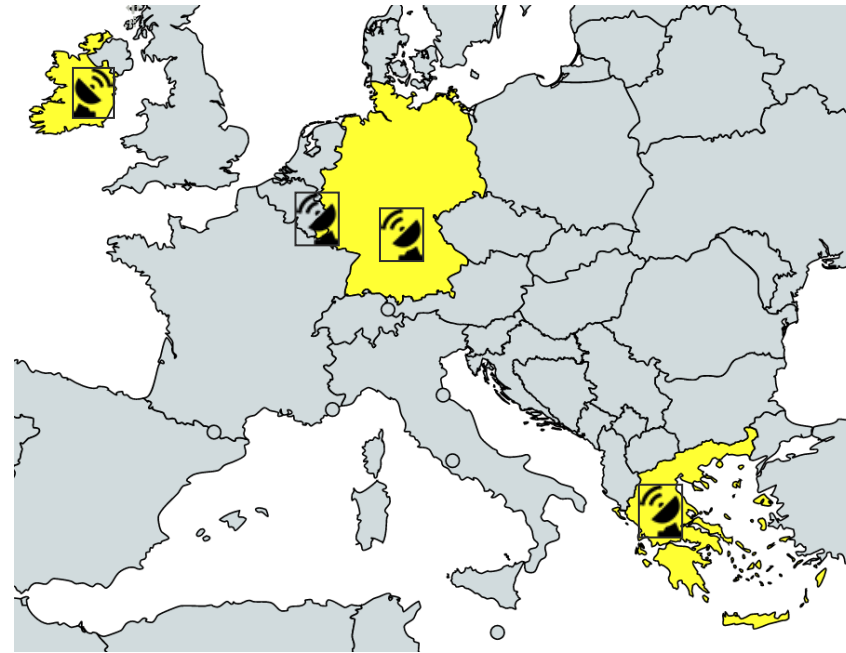
BB84 decoy protocol with relative phase encoding in C-Band
Tentative EAGLE-1 launch date is Q3 2027

Connecting to cross-border EuroQCI

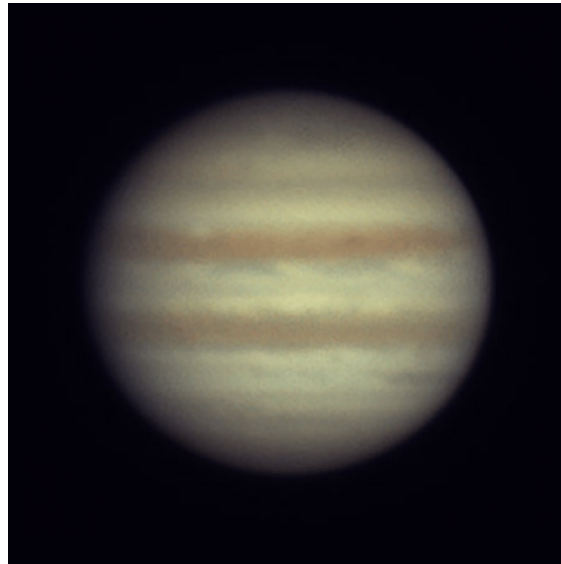
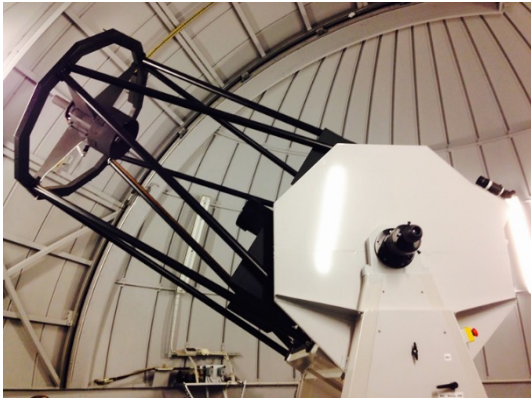
NordicQCI
Sweden, Finland and Estonia



TransEuroOGS
Ireland, Luxemburg, Germany, Greece



Albanova Optical Ground Station (OGS)



Installation of OGS Satellite tracking system
at Albanova, Sweden



RI
SE



VINNOVA
Sweden's Innovation Agency



Co-funded by
the European Union

(click for video)



Co-funded by
the European Union



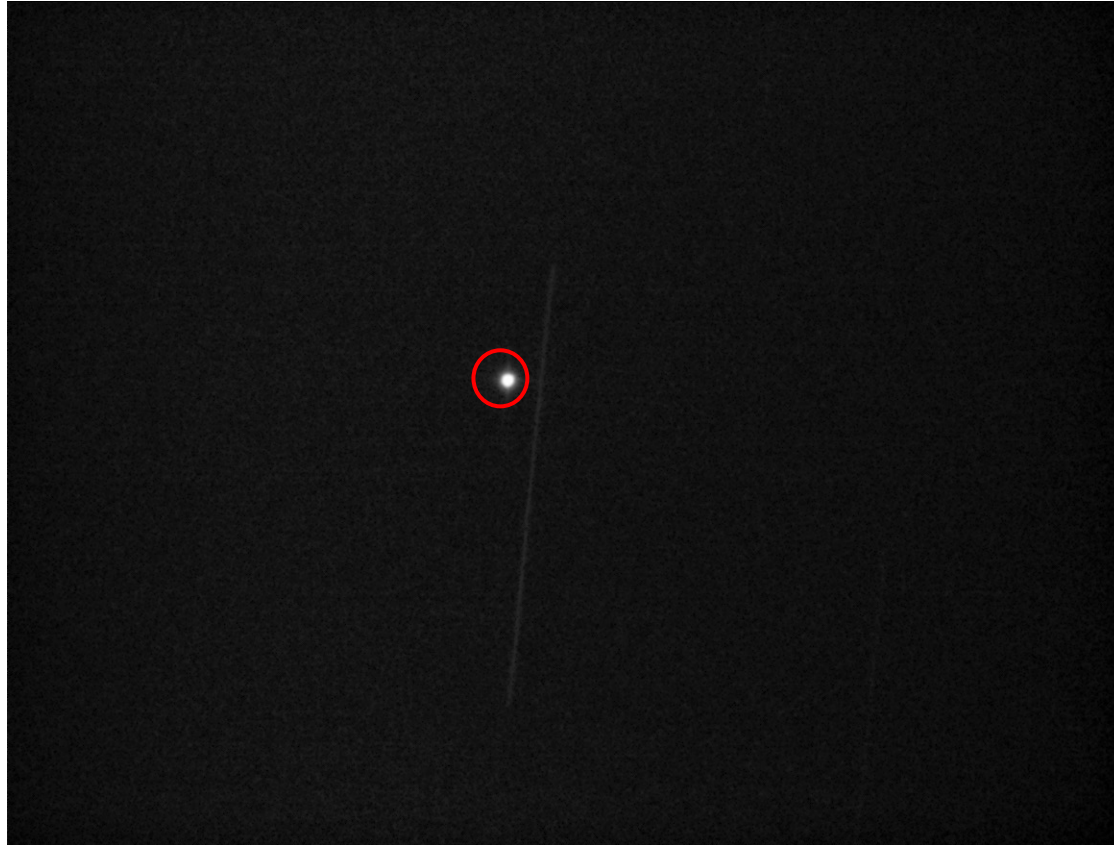
Tracking capabilities of telescope

The tracking was performed in a fully “blind” mode, relying solely on the predicted satellite ephemeris. No active guiding was applied,.

A mechanism is available to accept guiding commands from external software, indicating that near-perfect tracking performance can be achieved in future experiments.

The observed residual drift is slow and low-frequency, making it well-suited to correction via closed-loop guiding.

CHEOPS (CHaracterising ExOPla
nets Satellite) at an Altitude of
715 km



(click for video)

WP5 – Works EST-FIN and EST-LUX

KMS studies

Study for KMS to determine the technical and operational requirements

EST-FIN connection

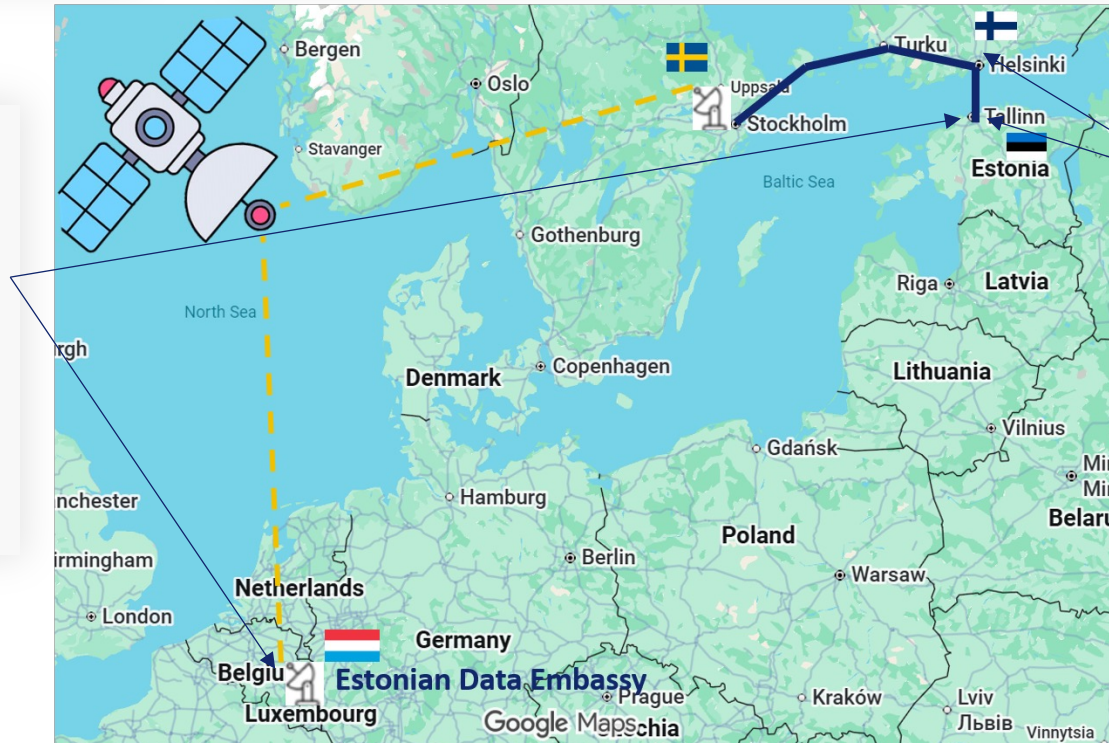
Buildup of QKD link between Estonia and Finland

KMS implementation and validation

Implementation and validation of the KMS solution

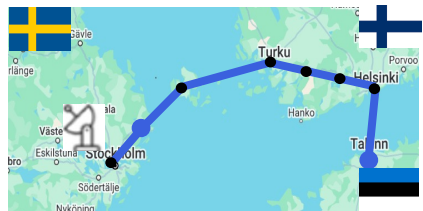
Use-case EST to Data embassy in LUX

Key forwarding from Estonia through Finland to Swedish OGS with the final destination to Estonian Data Embassy in Luxembourg.



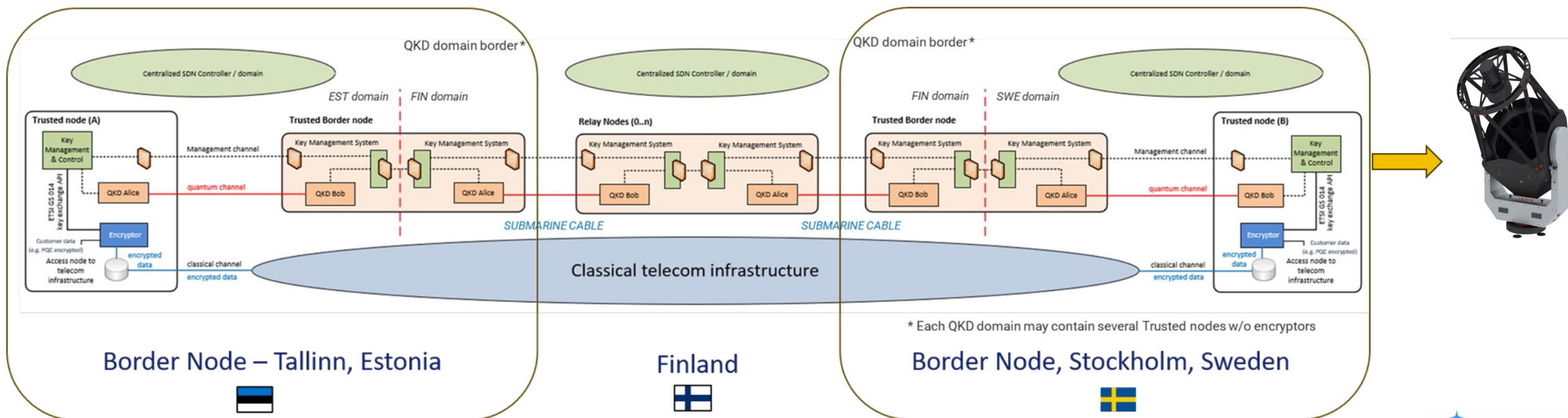
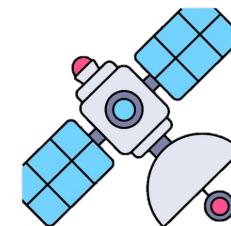
Use-case EST-FIN

Research network use-case between Estonian and Finnish Academic networks

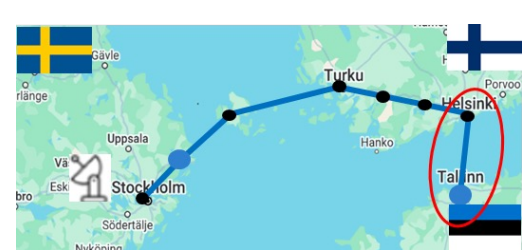


WP5 - Tasks

- T5.1 Deployment and testing of cross-border links with interoperability methods
- T5.2 Testing secure quantum communication services on EST-FIN link
- T5.3 Testing of secure key transfer through multiple MS and Space connection

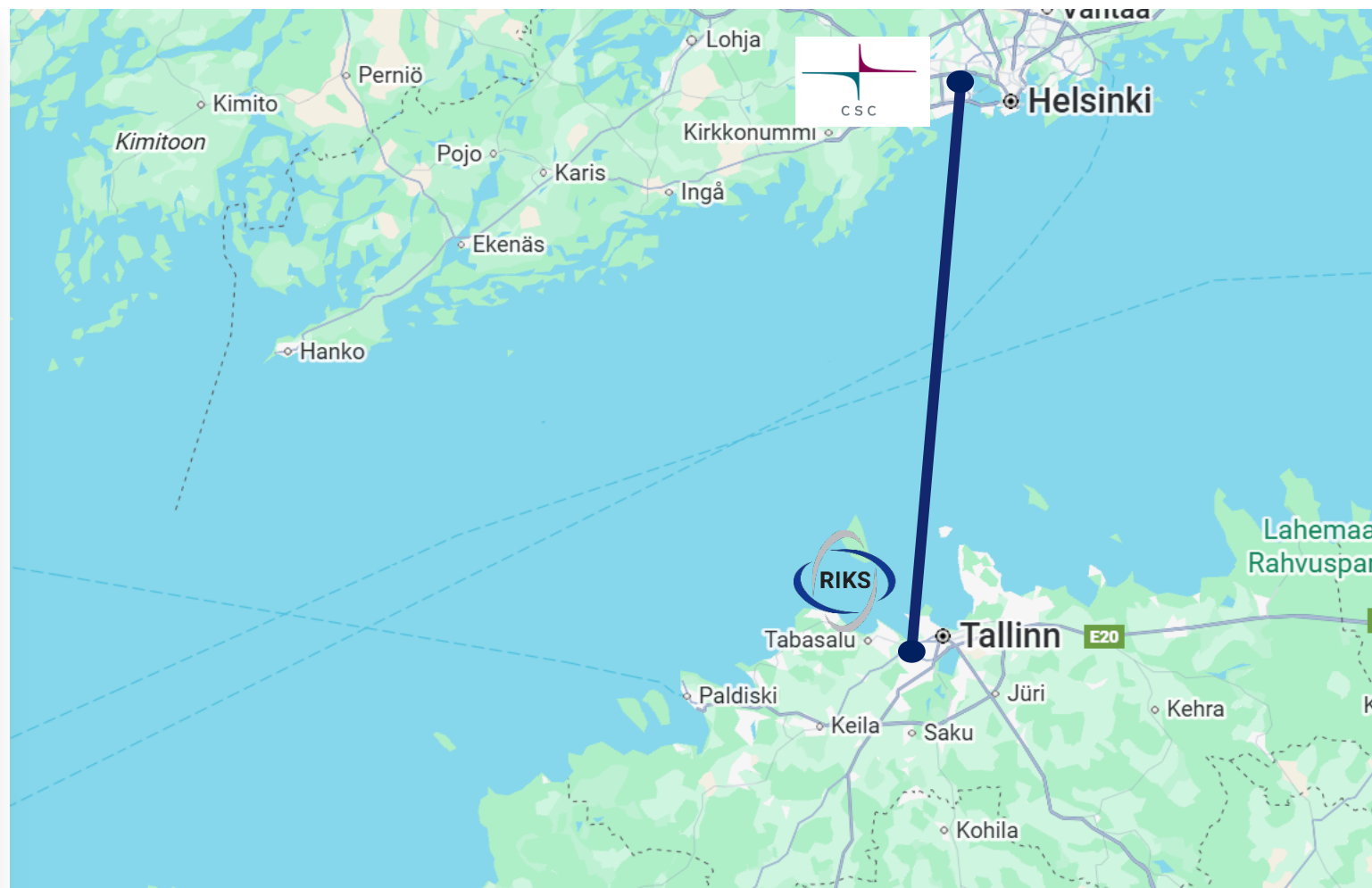


Co-funded by
the European Union



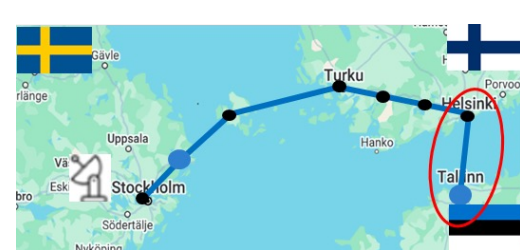
T 5.1: Est – FIN QKD connection

- **Physical connection between CSC and RIKS using a submarine cable**
- Preparation of the Trusted Node in Estonia
- Fibre measurements
- **Test the links with existing QKD devices to confirm operation**
- Build virtual testbed to test KMS functionality
Evaluate open source solutions
- Define and procure KMS solution
- **Build the network with final QKD devices**
- **Implement the final KMS and develop the functionality for inter-domain key transfer**



Co-funded by
the European Union

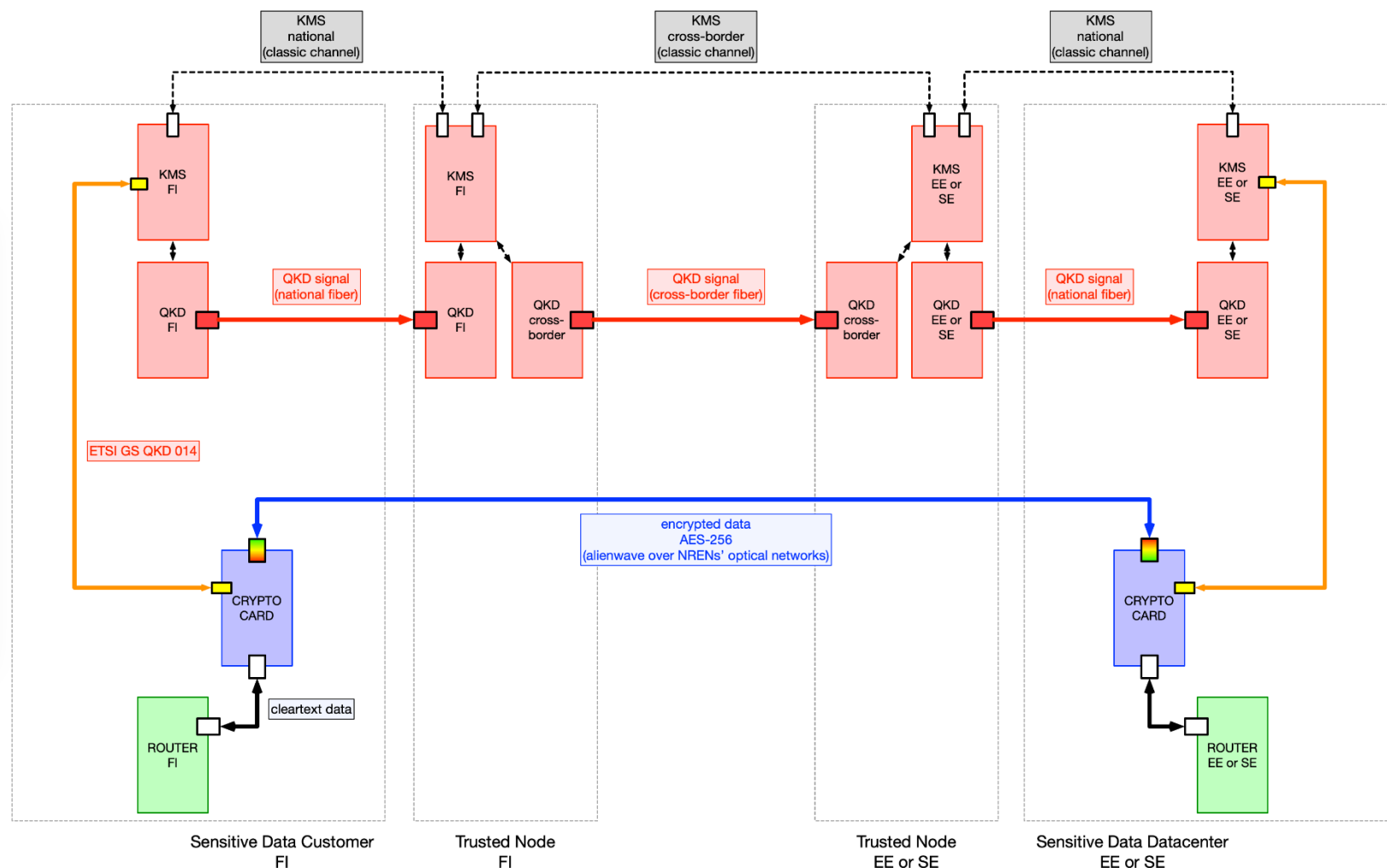




T5.2: Use-case 1 – Research network

Securing sensitive Research data between Estonian and Finnish Research network

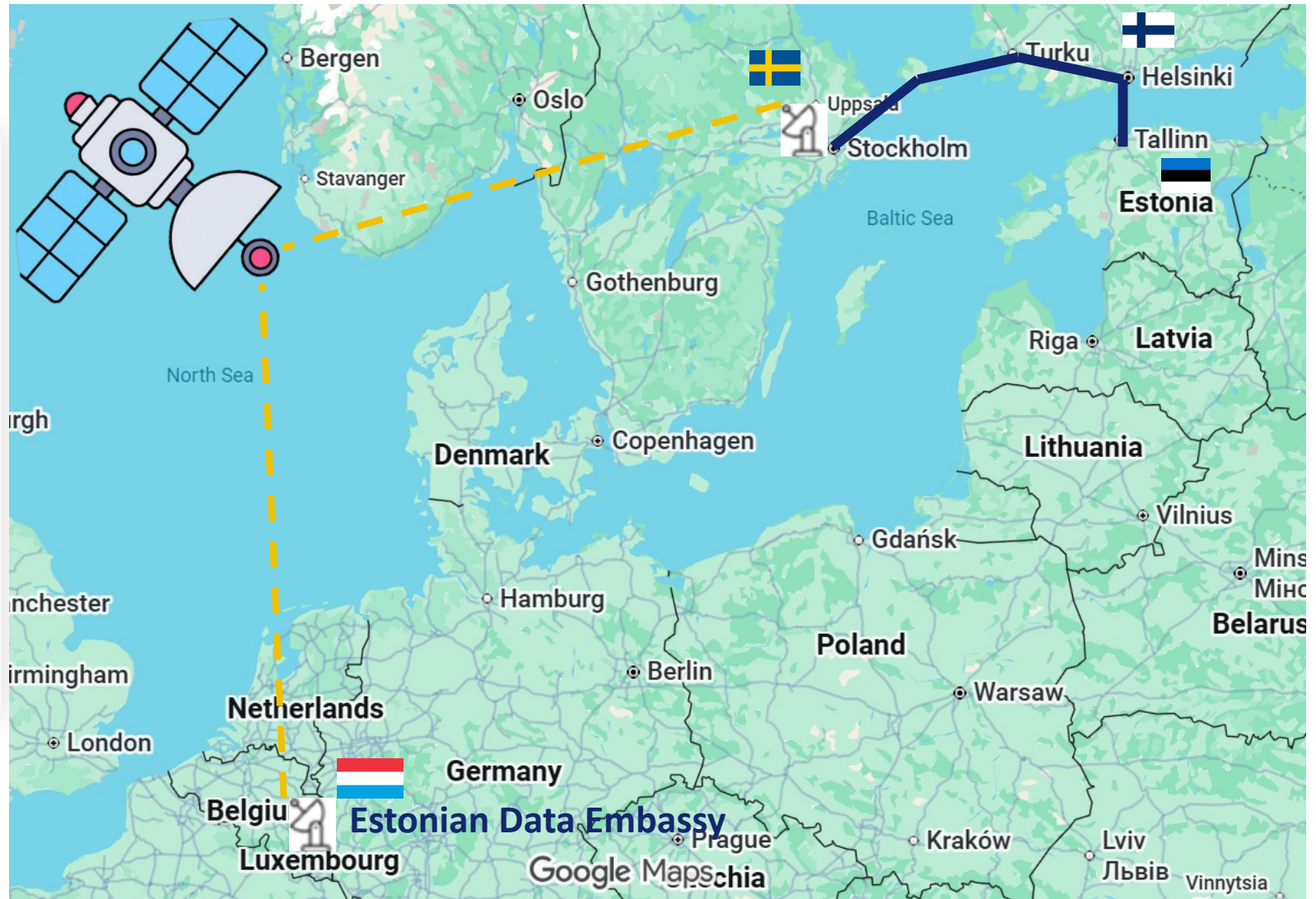
- Transfer key from Finnish domain to the final customer through the Estonian domain
- Test QKD encryption on connection up to 400G in the Research network



T5.3: Use-case 2 – EST-FIN-SWE-OGS

Transferring QKD key from Estonia through Finland to Swedish OGS to Connect to Luxembourg QCI and hopefully to the Estonian Data Embassy

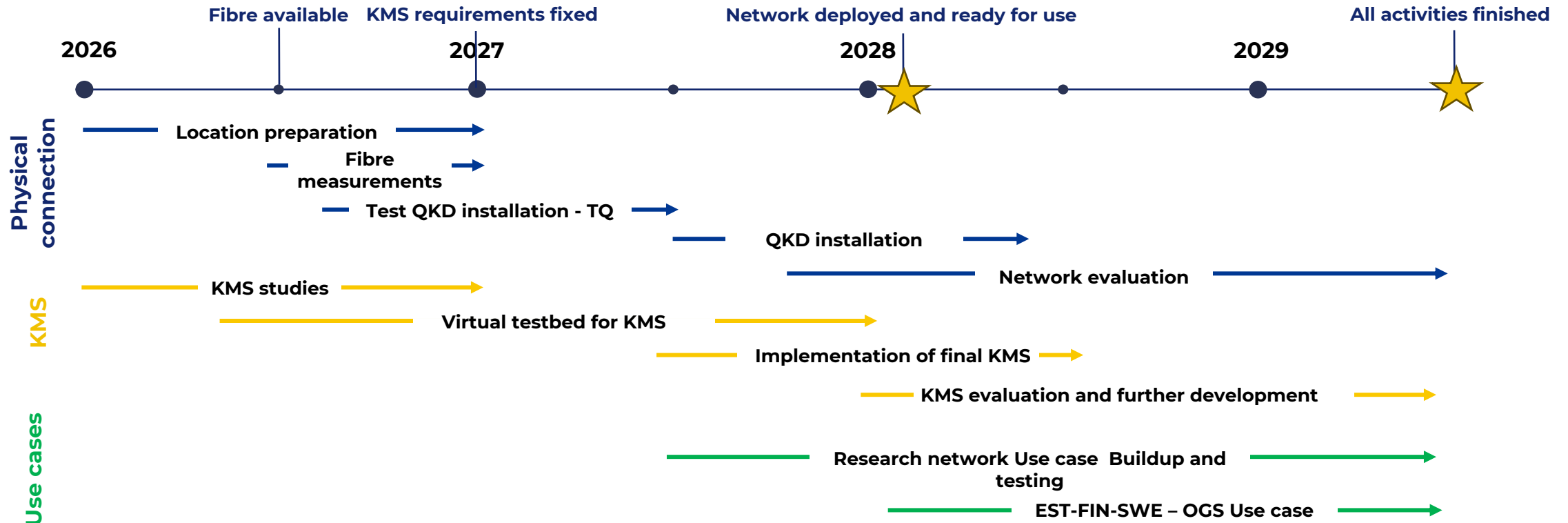
- KMS setup to allow key transfer from Estonia through Finnish domain to Swedish OGS
- Test connectivity and key transfer with Eagle 1 satellite
- Cooperation with Luxembourg QCI project for receiving the QKD Key
- If Possible - test connection to Estonian Data embassy in Luxembourg



Co-funded by
the European Union



WP5 – Timeline



First KMS workshop in May 2026

KMS solution was demonstrated in a workshop with Merqury and ThinkQuantum solutions with ETSI 020 interface between country domains. Network connections with Fortigate devices and use-case for video conference.

Estonia Workshop Plan 25/26/27 May 2026

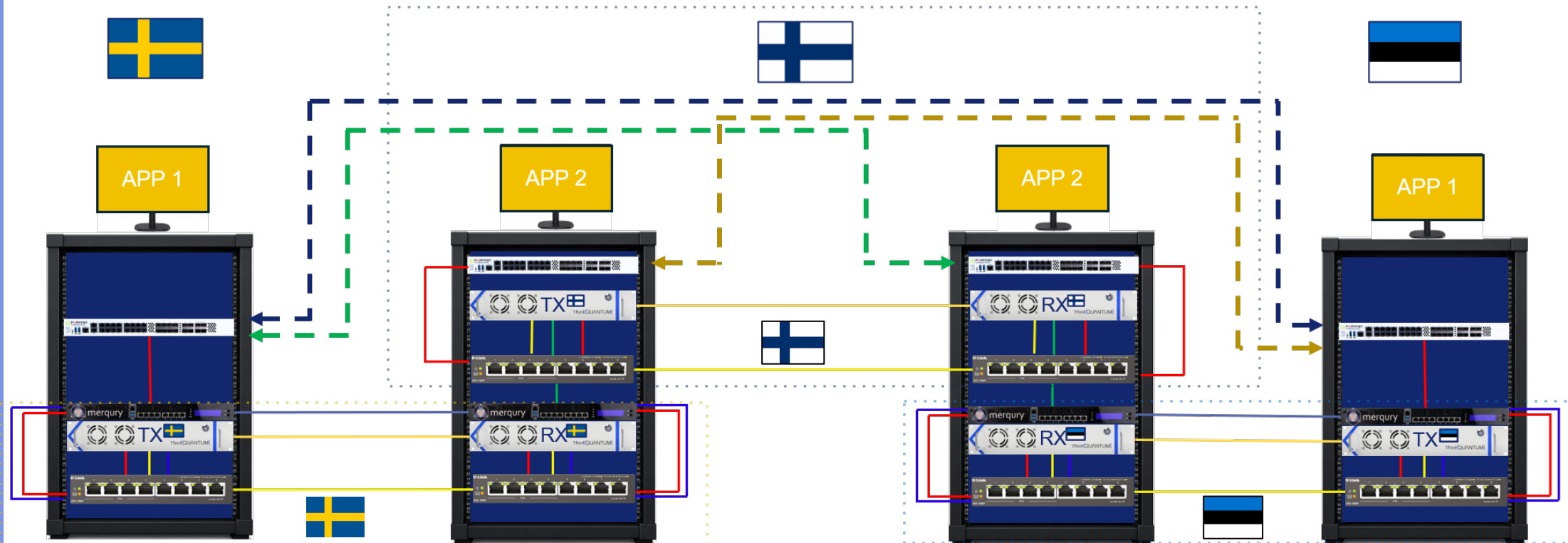


QKD
ThinkQuantum

Network
Fortigate

KMS
ThinkQuantum
Merqury

Use-case
Video conference



Merqury

ThinkQuantum

Merqury

First KMS workshop in May 2026

ETSI 020 demonstration between EST-FIN-SWE by Merqury and ThinkQuantum KMS solutions





Thank you!