Maltese SME specialising in the real-world deployment of developed quantum-safe communication technologies seeks R&D partners to work on a proposal for EU funding such as Horizon Europe, EUREKA or EUROSTARS building on the existing PRISM EuroQCI project.

Summary

Profile type	Company's country	POD reference
Research & Development Request	**Malta**	**RDRMT20251229003**
Profile status	**Type of partnership**	**Targeted countries**
PUBLISHED	**Research and development cooperation agreement**	**• World**
Contact Person	**Term of validity**	**Last update**
Alexia PACE KIOMALL	**7 Jan 2026** **7 Jan 2027**	**7 Jan 2026**

General Information

Short summary

The Maltese company seeks financial institutions, telecommunication operators, supervisory or policy bodies, universities and research institutes that would like to join their consortium seeking EU funding to further build on the work already carried out under the quantum communication initiative PRISM.

Full description

The Maltese company is the technical lead behind the EuroQCI project co-funded by the European Union under the Digital Europe Programme. Through this project, the Maltese company has designed and developed a quantum secured testbed network across the Maltese Islands. It has also deployed Malta's first quantum key distribution link on live telecom fibre, and run multi-site trials combining commercial QKD devices, optical transport equipment and classical encryption systems.
The company's contribution is a vendor-agnostic, standards-aligned software stack for integrating PQC and QKD into networks, combined with operational lessons from PRISM and from international demonstrations with networking and quantum-technology vendors. In those demonstrations, quantum-secured connectivity was established between on-premises data centres and cloud infrastructure using QKD systems, backbone fibre and commercial routing and encryption equipment. Within PRISM, they have also worked with local partners on QKD-assisted links and quantum-secured VPNs. Together, these activities provide a foundation for new research that is ambitious but grounded in what has already been shown to work.

They now would like to extend this experience into applied research and demonstration projects in sectors where long-term confidentiality and resilience are critical, especially in the finance and healthcare sectors.
Quantum-era threats and “store now, decrypt later” attacks are increasingly recognised, but there is little empirical data on how post-quantum cryptography (PQC) and QKD behave when used on backbone links between data centres or across borders. Thus the objective of the next project is to create collaborative testbeds that generate such data under realistic conditions, using infrastructure contributed by partners. Thus they are seeking financial institutions such as banks, or healthcare institutions to create a quantum-safe backbone testbed connecting at least 2 financial or critical infrastructure sites via one or more telecom operators. Over this testbed, partners would deploy PQC-based protections at suitable layers and, where feasible, overlay QKD to supply additional keying material, then measure how these approaches affect performance, availability, operational effort and the ability to produce evidence for compliance compared with current practice based solely on classical cryptography.
Academic partners would help define measurement and analysis methods; financial and regulatory stakeholders would map technical metrics to risk indicators and assurance artefacts that are meaningful for supervisors, auditors and internal governance.
Expected outputs include reference architectures for quantum-safe backbones, deployment and operations guidance, and case studies showing where PQC alone is sufficient and where QKD may add measurable value.
Depending on the funding call, projects could also include training and outreach activities, using Malta's PRISM network and related demonstrations as visible showcases of quantum communication in operation. All work would build on the company's existing activities rather than on hypothetical future capabilities, so that results can be translated quickly into practical guidance and, where appropriate, commercial offerings.

Advantages and innovations

The company has already been leading the PRISM EuroQCI project co-funded by the European Union under the Digital Europe Programme. It can act as Lead once again and is experienced in writing and submitting proposals for EU funding.
The Lead expert is a professor and academic with connections to other Universities and research centres.

Technical specification or expertise sought

Depending on the expertise and experience of the collaborating partner, the entity is expected to work on established work packages as part of a consortium via an EU funded project agreement.

Stage of development

Already on the market

Sustainable Development goals

- **Goal 8: Decent Work and Economic Growth**
- **Goal 9: Industry, Innovation and Infrastructure**

IPR Status

Secret know-how

IPR Notes

Partner Sought

Expected role of the partner

Ideal partners would be financial institutions, telecom operators, universities and research institutes, and, where relevant, supervisory or policy bodies willing to enter into research and development cooperation agreements via application to EU funding, such as Horizon Europe, EUREKA and EUROSTARS calls. The main interest is in consortia that combine domain expertise in finance or critical infrastructure with access to suitable fibre and data-centre resources and experience in EU-funded collaborative R&D.

Type of partnership

Type and size of the partner

Research and development cooperation agreement

- **R&D Institution**
- **SME 11-49**
- **Big company**
- **University**
- **SME 50 - 249**

Call Details

Framework program

Horizon Europe

Call title and identifier

Depends on the call

Submission and evaluation scheme

Anticipated project budget

Coordinator required

No

Deadline for EoI

31 Dec 2026

Deadline of the call

30 Sep 2026

Project duration in weeks

Web link to the call

Project title and acronym

Dissemination

Technology keywords

- **01006005 - Network Technology, Network Security**
- **01006007 - Research Networking, GRID**
- **01004005 - e-Government**

Market keywords

- **01006001 - Defence communications**
- **02007013 - Banks/financial institutions software**
- **02007012 - Medical/health software**
- **01006004 - Communications services**

Targeted countries

- **World**

Sector groups involved