luxquanta

merqury cybersecurity

White Paper

Quantum Safe Solutions: Real World CV-QKD and KMS Deployments

National Deployments of QKD Networks Across Research Institutions, Data Centers, and Government

A Luxquanta & Merqury Cybersecurity Quantum Security Whitepaper

1. Table of Contents

2. Executive Summary

Across Europe, nations are currently rolling out quantum communication infrastructure that provides provable, hardware-based protection against current and future decryption threats. At its core is Quantum Key Distribution (QKD). **This technology generates and exchanges symmetric encryption keys exploiting the fundamental laws of quantum mechanics**, with its security guaranteed by the laws of physics rather than computational complexity.

This white paper provides an operational view of one such real-world deployment: PRISM, Malta's national quantum communications initiative under the European Union's European Quantum Communication Infrastructure programme (EuroQCI).

EuroQCI was conceived to deploy a pan-European quantum-secure communications network, linking national terrestrial fibre segments and a space component. The deployment integrates QKD-based key exchange into existing telecoms to add a physics-based security layer for governments, critical infrastructure, data centres, and public services.

PRISM brings together Luxquanta's continuous-variable QKD (CV-QKD) technology and Merqury's expertise in orchestration and integration of quantum-safe networks, alongside contributions from national stakeholders such as Melita, MITA, and the University of Malta. The result is a live demonstration of how quantum-safe communications can be deployed on real fibre networks.

Rather than presenting abstract concepts, **the paper focuses on how deployments occur in practice: what infrastructure is required**, how QKD devices are integrated into existing environments, and the organizational roles necessary to make it work.

Specifically, this white paper aims to:

- Share a deployment flow and clear roadmap based on PRISM's live use case.
- Demonstrate how complementary expertise accelerates and de-risks implementation.
- Provide sector-relevant insights for governments, telecom operators, and enterprises.

By drawing on lessons from PRISM Malta, this white paper offers a practical roadmap for decision-makers, CEOs, CISOs, and policymakers seeking to understand how to bring quantum-safe communications from planning to operation.

3. The Quantum Threat Landscape

Last century, the development of quantum mechanics led to the First Quantum Revolution, a period of unprecedented technological advancement built on newly discovered quantum physics principles. The technologies developed during this era now form the foundation of modern society, embedded in semiconductors, lasers, medical imaging devices, and countless other systems we depend on daily.

But the discoveries of the past were only the beginning. **A new chapter is already unfolding, one that is reshaping industries, economies, and even our understanding of information itself that promise to set humanity towards a giant technology leap.**

3.1 The Second Quantum Revolution: A Paradigm Shift

Today, we are experiencing the Second Quantum Revolution. Where previous technologies applied general quantum principles through engineering solutions, current advances enable direct control and manipulation of individual quantum states. This capability unlocks performance levels and technology potential previously thought impossible.

Among second-revolution technologies, quantum computers stand out as the most ambitious and potentially transformative development. **In recent years, they have attracted massive investments from both governments and the private sector, accelerating their maturity in a global race for quantum supremacy**, which occurs when quantum processors surpass even the most advanced supercomputers.
This leap will unlock unprecedented advances in science, industry, medicine, and beyond, expanding computational capabilities to levels once unimaginable. Yet, with this progress comes a profound challenge: the vulnerability of today's cryptographic systems, which form the backbone of our digital security, and modern society.

3.2 Current Cryptographic Vulnerabilities

Modern digital security relies on public-key cryptography, particularly RSA and Elliptic Curve Cryptography (ECC). These algorithms secure most digital communications worldwide, from online banking and electronic signatures to government services and critical infrastructure.

Their resilience is based on the difficulty of solving specific mathematical problems:

- RSA depends on the hardness of factoring very large numbers.
- ECC relies on the difficulty of solving the elliptic curve discrete logarithm problem.

For classical computers, solving these problems is intractable; it would take thousands of years. This is why RSA and ECC have provided trusted protection for decades. But the arrival of quantum computing fundamentally changes this equation. **Once sufficiently powerful quantum computers capable of running algorithms (such as Shor's) emerge, this would break RSA and ECC entirely, shaking the foundations of today's digital security.** Such quantum computers are referred to as Cryptographically Relevant Quantum Computers (QRQC).

3.3 The Attacks

When quantum computers reach a sufficient scale, they will break cryptographic protections in real time. Attackers could forge digital identities, bypass secure connections, and compromise systems across every sector, from online banking to defence communications. Direct quantum attacks will undermine the future dependability of all systems built on classical cryptography.

Quantum Computing development is rapidly advancing worldwide, but the threat is already here. A new type of attack is already compromising critical data from the past and present.

In the attack known as "Harvest Now, Decrypt Later" (HNDL), adversaries intercept and store encrypted data today, even though they cannot read it. Once QRQC comes to fruition, they will be able to decrypt these archives, exposing sensitive financial transactions, medical records, intellectual property, and government communications.

The decryption will happen years after the data was first collected. However, the danger lies in the time lag, as what appears secure now may be catastrophically vulnerable in the future. If there is data today that must remain secure for the years to come, the transition to quantum-safe alternatives to protect the data link must be a priority.

The window of vulnerability is already open, and the transition to quantum-safe solutions must begin immediately, before attackers exploit it.

3.4 The Need for Quantum-Safe Solutions

International agencies such as NIST in the United States and National Security Agencies (NSA's) around the world have already called for an urgent migration to quantum-safe solutions. Two complementary approaches lead the way.

- **Post-Quantum Cryptography (PQC):** Based on new mathematical algorithms assumed resistant to quantum attacks, PQC can be deployed through software and hardware upgrades at scale. PQC is the immediate solution to establish the first layer of quantum defence.

- **Quantum Key Distribution (QKD):** QKD uses quantum states of light to create and share encryption keys between two endpoints. These keys are inherently random, cannot be copied, and cannot be broken, even by the most powerful quantum computer. This technology provides a future-proof layer of security for the most critical nodes in a network.

After two decades of research and standardization, QKD is already being deployed across Europe and beyond, with projects like EuroQCI and national initiatives such as PRISM in Malta.

The technology has matured into a reliable, scalable tool that offers a future-proof layer of security for governments, operators, and enterprises that cannot risk their most valuable data.

4. The European Response: EUROQCI

Europe has positioned itself to lead this transition. In 2019, the European Union launched the European Quantum Communication Infrastructure (EuroQCI) project, an ambitious initiative to interconnect all EU member states through a secure backbone network utilizing quantum-safe communication.

The mission is to deploy a pan-European network of Quantum Key Distribution (QKD) nodes that establish quantum-secure communication channels, ensuring data privacy in the quantum era.
By 2023, EuroQCI moved from planning to action. Funded through the DIGITAL Europe Programme (DEP), the implementation strategy focuses on two critical tracks.

- **Technology Acceleration:** Advancing quantum communication systems to higher Technology Readiness Levels (TRLs)
- **National Network Deployment:** Building sovereign quantum-safe infrastructure within each member state

"There is a clear difference between promising quantum security and delivering it in operational networks. This deployment in Malta is a tangible proof of what it takes: telco-grade plug and play devices, scalable P2MP architectures, coexistence in DWDM, and systems that can be installed and operated reliably. At Luxquanta, we have focused for years on making CV-QKD deployable, not just demonstrable, delivering quantum security that behaves like true network infrastructure. The success of this project reflects that commitment. "

Vanesa Diaz
CEO.
Luxquanta.

5. EUROQCI, Prism & Maltese National Deployment

5.1 EuroQCI in Context

This White Paper presents the deployment of Luxquanta's Continuous-Variable QKD within Malta's PRISM initiative, showing how theoretical advances and market-ready products translate into operational security infrastructure. Far from being an isolated pilot, PRISM is part of the European Quantum Communication Infrastructure (EuroQCI), the EU's coordinated programme to establish a pan-European network for quantum-safe communications.

The collaboration with Merqury Cybersecurity, alongside national partners such as Melita, MITA, and the University of Malta, provides a blueprint for integrating quantum hardware with enterprise-grade security management. As one of the early national segments under EuroQCI, PRISM demonstrates a model that is both scalable and reproducible, relevant not only to Malta but also to deployments worldwide.

5.2 Malta's Strategic Role: The PRISM initiative

Malta's national deployment initiative, PRISM, exemplifies how Member States are translating the EU-level quantum communication strategy into operational reality. **Despite being a small nation, Malta's strategic geographic position and ambitious digital agenda make the country a strategic location for early deployment and implementation**. PRISM is one of the earliest national deployments moving from pilot to pre-production on live operator fibre, placing Malta at the forefront of EuroQCI's rollout. **PRISM is co-funded by the European Union under the Digital Europe Programme**, which reinforces its credibility, ensures oversight, and aligns the project with the broader EuroQCI roadmap. This EU backing transforms Malta's deployment into a blueprint for other Member States, demonstrating how European strategy can be implemented locally while maintaining cross-border interoperability.

It serves as a real-world example of practical National quantum-safe deployments. A consortium of national stakeholders drives the project, including:

- **Melita** provides the live fibre footprint and operational support.
- **MITA (Malta Information Technology Agency)** anchors government use cases and governance.
- **The Critical Infrastructure Protection Department** within the Ministry for Home Affairs ensures alignment with national risk management and resilience priorities.
- **Merqury Cybersecurity**, which provides orchestration and key management.

The PRISM project is not developed in isolation but is deeply embedded within Malta's broader digital and security ecosystem, while maintaining close collaboration and continuous alignment with the overall EuroQCI deployment, the involved member states, and the critical partners.

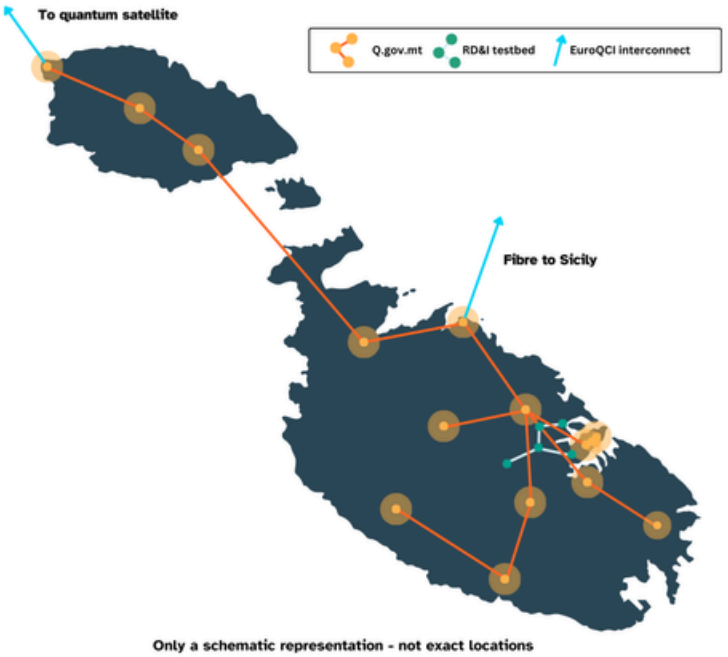
5.3 National Deployment: Malta's QCI Network

The Maltese deployment has been executed across the country, securing different links from diverse sectors and use cases. Malta's goal within the EuroQCI initiative is to secure the country's critical links using QKD, combining vendors and approaches to build a diverse, adaptable network.

The links span across the country, as seen in Figure X, with exit links to satellite and direct connections to Sicily (Italy), also following the pan-European secure communication efforts of the EuroQCI to interconnect member states. **A total of 5 Luxquanta's Continuous Variable QKD links have already been deployed across the country, together with the Merqury Cybersecurity KMS/Orchestration solution and in close collaboration with PRISM EuroQCI members Melita and MITA. More links are expected to be deployed as part of Malta's QCI Network.**

→ "With our extensive deployment in Malta, Merqury and Luxquanta demonstrated the two most essential ingredients for commercial QKD: excellent quantum hardware that can operate on existing telecommunication networks, together with a software stack to manage the quantum network."

André Xuereb.
CEO & Co-founder.
Mercury Cybersecurity.



6. Luxquanta–Merqury QKD Links in Malta's EuroQCI Network

No national quantum deployment succeeds on technology alone. Deploying quantum-safe communication infrastructure requires trusted partnerships that combine cutting-edge science with practical integration expertise, backed by demonstrated, seamless interoperability among technologies. In the deployments described in this whitepaper under the PRISM context, **the collaboration between Luxquanta and Merqury Cybersecurity illustrates this balance.**

Luxquanta provides the quantum backbone through its Continuous-Variable Quantum Key Distribution (CV-QKD) systems, which generate and distribute quantum-derived keys. In parallel, Merqury Cybersecurity delivers a quantum network management suite, including the Quantum Key Management System (QKMS) and network monitoring and control. This suite enables seamless integration of QKD nodes within existing telecom infrastructure.

While Merqury Cybersecurity is actively involved in the PRISM EuroQCI project, part of the EU-funded national initiatives aimed at enabling national deployments, Luxquanta also leads an EU-funded consortium focused on increasing the technology's TRL for practical deployment. The QUARTER consortium operates under the Digital Europe Programme and includes SMEs, established industry operators, and academic institutions.

By integrating Luxquanta's CV-QKD technology with Merqury Cybersecurity's advanced quantum network management suite, the Malta national deployments ensure quantum-grade security through seamless integration within telecom infrastructures.

6.1 Deployment Scope and Links

The deployed QKD network spans multiple operational sectors. Five links are protected with Nova Iq®, Luxquanta's CV-QKD system.

In the PRISM testbed, these QKD links interconnect a small set of national nodes, enabling resilient backup and secure communications between critical government sites.

- Government infrastructure
- Telecom operators
- Healthcare and research
- Academia

From a deployment perspective, this architecture translates into the following QKD links:

- Madliena (Melita Data Centre) → MITA Sta Venera (~12 km)
- Madliena (Melita Data Centre) → MITA Mater Dei Hospital (~10 km)
- Madliena (Melita Data Centre) → Critical Infrastructure Protection Department (~15 km)
- Madliena (Melita Data Centre) → Armed Forces of Malta (~14 km)
- UM Faculty of ICT → MITA Mater Dei Hospital (~1 km)

6. Luxquanta–Merqury QKD Links in Malta's EuroQCI Network

Of the five deployed links, four originate from Melita's ISO 27001-certified Madliena Data Centre and follow a point-to-multipoint (P2MP) topology. In this configuration, a single QKD transmitter distributes quantum-derived keys to four receiver nodes over commercial lit fibre from Melita, reducing the number of transmitters required and optimising total deployment cost.

The single link from the UM Faculty to Mater Dei Hospital, spanning only 1km, is deployed using dedicated dark fibre.

In addition, the following links are being prepared for deployment:

- Enemalta Marsa → MITA Mater Dei Hospital (~9 km)
- Enemalta Marsa → Enemalta Delimara (~17 km)
- Police HQ → Critical Infrastructure Protection Department (~1 km)

Taken together, this set of verticals remains a small sample of the broader quantum-safe migration landscape. However, it demonstrates a key point: QKD can be applied where it matters most across different operational contexts without requiring a single, uniform network model. Interoperability between nodes and specific use cases is critical for foundational quantum-safe networks.

6.2 Network Topology

When assessing a QKD deployment, the primary considerations are the network particularities, its topology, and the infrastructure in which the system will operate.

The evaluation should focus on the aspects that materially influence performance and integration:

- How nodes are interconnected
- How quantum and classical channels coexist
- How QKD links are orchestrated to secure the required endpoints.

Point-to-point (P2P)QKD connections

Point-to-multipoint (P2MP) QKD connections

6. Luxquanta–Merqury QKD Links in Malta's EuroQCI Network

These design choices depend on the nodes to be protected and the operational constraints of the underlying network. **The QKD deployment in Malta integrates multiple link types and fibre scenarios to form a flexible, scalable, and cost-optimised quantum-secure architecture.** The topology is characterised by:

- A combination of **point-to-point (P2P) and point-to-multipoint (P2MP)** configurations
- Four links operating over Melita's commercially lit **DWDM fibre**, where quantum and classical channels coexist
- One link deployed on dedicated dark fibre reserved exclusively for **QKD**

This hybrid design enables the network to meet diverse connectivity requirements while maintaining a coherent, robust security framework. In the lit-fibre segments, the quantum channel used to generate and distribute keys coexists with classical traffic on the same optical infrastructure. **This coexistence is enabled through wavelength-division multiplexing (DWDM), which allows the quantum signal to operate in parallel with classical channels within the same fibre plant.** Continuous-variable QKD is well suited to this environment due to its resilience and adaptability in dense spectral conditions, enabling operators to reuse existing fibre assets and reduce deployment effort.

The dedicated dark-fibre link complements the DWDM-based approach in an overall network by providing an isolated transmission path when possible. **This offers a second integration model for environments where segregation of quantum channels is preferred, or an available empty fibre can be used.** Together, these configurations highlight the practical versatility of QKD within an operational telecom network. Supporting multiple topologies is also key to cost optimisation. In particular, **the P2MP architecture allows a single transmitter to serve multiple receivers, reducing the number of transmitters required and enabling a more efficient scale-up of quantum-secure communications.**

To summarize these concepts:

- **Point-to-multipoint architecture.** Keys are generated and distributed from a single QKD transmitter to multiple QKD receivers. This configuration can reduce deployment costs by eliminating the need for a dedicated transmitter for each additional node.
- **Coexistence in lit fibre.** QKD links can be incorporated into existing optical fibre without deploying dark, dedicated fibre for the quantum channel. Systems that properly adapt to network and fibre conditions are needed to scale the quantum-safe migration across a network while easing deployment.

7. Technologies Involved: CV-QKD & KMS Orchestrator

→ In Malta's deployment, Luxquanta's Continuous-Variable QKD (CV-QKD) system provides a quantum-safe security layer for data communications, working in tandem with Merqury Cybersecurity's Key Management System (KMS). The KMS serves as the operational interface between QKD links and encryption applications, ensuring that quantum-derived keys are managed and delivered to authorised consumers.

This combination is representative of a real-world deployment. The technologies are introduced below.

Continuous-Variable Quantum Key Distribution (CV-QKD)

Quantum Key Distribution (QKD) is a quantum communication technology that harness the laws of physics, rather than mathematical assumptions, to generate and distribute symmetric encryption keys between two endpoints. **Continuous-Variable QKD generates these keys by encoding information in the continuous properties of highly attenuated ligh**t, transmitted as quantum states over standard ptical fibre. Any attempt to intercept the quantum exchange introduces a measurable disturbance. This allows the legitimate nodes to bound an eavesdropper's information and preserve key confidentiality.

Key Management System (KMS)

Quantum-derived keys must be securely managed, distributed, and consumed by network services. This orchestration is provided by **Merqury Cybersecurity's Key Management System (KMS), which bridges the QKD layer and the encryption applications that use the keys.**

At the Hand-off, the KMS:

- Ingests the keys produced by the Luxquanta QKD link at each site
- Verifies key origin and records the associated events
- Exposes a controlled key service, making keys available to authorised consumers under defined access policies and link scoping

Using the Keys

Approved encryptors request keys through this interface and receive the correct key material for the specified endpoint pair. The KMS maintains service continuity as paths or devices change, while providing operational visibility by correlating quantum-link status with key-service health.

Every request and delivery is logged with timestamps and identity context to support troubleshooting and compliance. **This hand-off enables quantum-derived keys to integrate into standard network services without disrupting existing architectures.**

7. Technologies Involved: CV-QKD & KMS Orchestrator

7.1 Luxquanta's Solution: Nova Iq® CV-QKD System

Luxquanta's systems are based on **Continuous-Variable QKD (CV-QKD)**, a modern approach that addresses key deployment barriers faced by earlier quantum communication systems. Whereas **Discrete-Variable QKD (DV-QKD)** typically relies on highly specialised detectors and sensitive components and often requires **dedicated fibre infrastructure, CV-QKD** uses standard telecom components that are mature and widely deployed in production networks.

CV-QKD is therefore well suited to telecom environments: it is compatible with standard optical equipment and can be engineered to coexist with classical traffic, enabling quantum-safe key generation without requiring a dedicated quantum-only fibre in many scenarios.

This same class of equipment already operates across optical fibre networks worldwide. With the commercially available **Nova Iq® CV-QKD system**, operators can accelerate deployment and integrate more easily into existing infrastructures. This shift towards continuous-variable technology delivers four strategic advantages for deployment at national and European scale:

Infrastructure compatibility

CV-QKD signals can coexist with conventional data traffic on the same fibre under DWDM. The quantum channel used to distribute keys can be integrated within the same C-band as existing telecom wavelengths, avoiding the cost and disruption of deploying dedicated quantum-only fibre.

Flexibility

Luxquanta systems can operate over links **exceeding 100 km (up to ~20 dB channel loss)** and support point-to-multipoint network topologies. Compared with **DV-QKD, CV-QKD** achieves similar reachable distances, while **CV-QKD** can be implemented entirely with telecom-grade components. This flexibility supports scalability and practical integration in existing networks without disrupting current network operation.

7. Technologies Involved: CV-QKD & KMS Orchestrator

Key generation at scale

Key generation remains stable across a range of link distances and supports multiple secure services over a **single quantum-secure link**, meeting the needs of governments, telecom operators, and enterprises with diverse security requirements.

Enabling deployment in production networks

By leveraging existing network infrastructure and components, **CV-QKD reduces integration barriers** and makes quantum-safe communications practical across national and cross-border networks. It does not require additional infrastructure or complex engineering to allocate the quantum channel.

Technical Requirements and Considerations

From a technical perspective, a **QKD system requires only an optical fiber connection**, using a single wavelength λ as the quantum channel. In other words, if the locations to be secured are already connected by optical fiber, CV-QKD systems can be easily integrated using the same fiber, even when operating alongside classical data channels in the same C-band used in telecommunications. With no additional setup or infrastructure investment.

In Luxquanta's CV-QKD implementation, the transmitter "encodes" the 0s and 1s of the cryptographic keys in light by sending coherent pulses with small, random modulations of amplitude and phase (continuous variables), and the receiver measures them using coherent detection.

The endpoints then run post-processing on the classical channel, including error correction and privacy amplification, to mitigate noise and distill shared secret keys. These keys are then handed off to the key-management layer for distribution to encryptors.

Luxquanta brings a proven, commercially deployed CV-QKD technology validated across dozens of real-world operator environments worldwide. From landmark projects such as PRISM in Malta to the wider EuroQCI program, Luxquanta is actively advancing Europe's objectives in digital sovereignty, cybersecurity resilience, and technological independence.

→ "Telco-grade approach means QKD fits into existing networks with ease. We've built our operational model so that network teams can deploy with confidence, knowing that support, maintenance, and troubleshooting are handled by the people who built the system."

Sebastian Etcheverry.
CTO & Co-founder.
Luxquanta.

7.2 Merqury Cybersecurity: Quantum Network Suite

Merqury provides the components required to extend the reach of multiple pairs of Luxquanta's CV-QKD across brownfield networks with minimal operational friction. The quantum network suite delivers three core capabilities.

Secure quantum key lifecycle management

Merqury's KMS turns quantum-generated keys into a managed service: request, deliver, account, monitor, and fail over. It is network-aware, supports multi-hop topologies, and is designed for redundancy, so key delivery continues as paths change. The result is consumable, auditable keying without application rewrites.

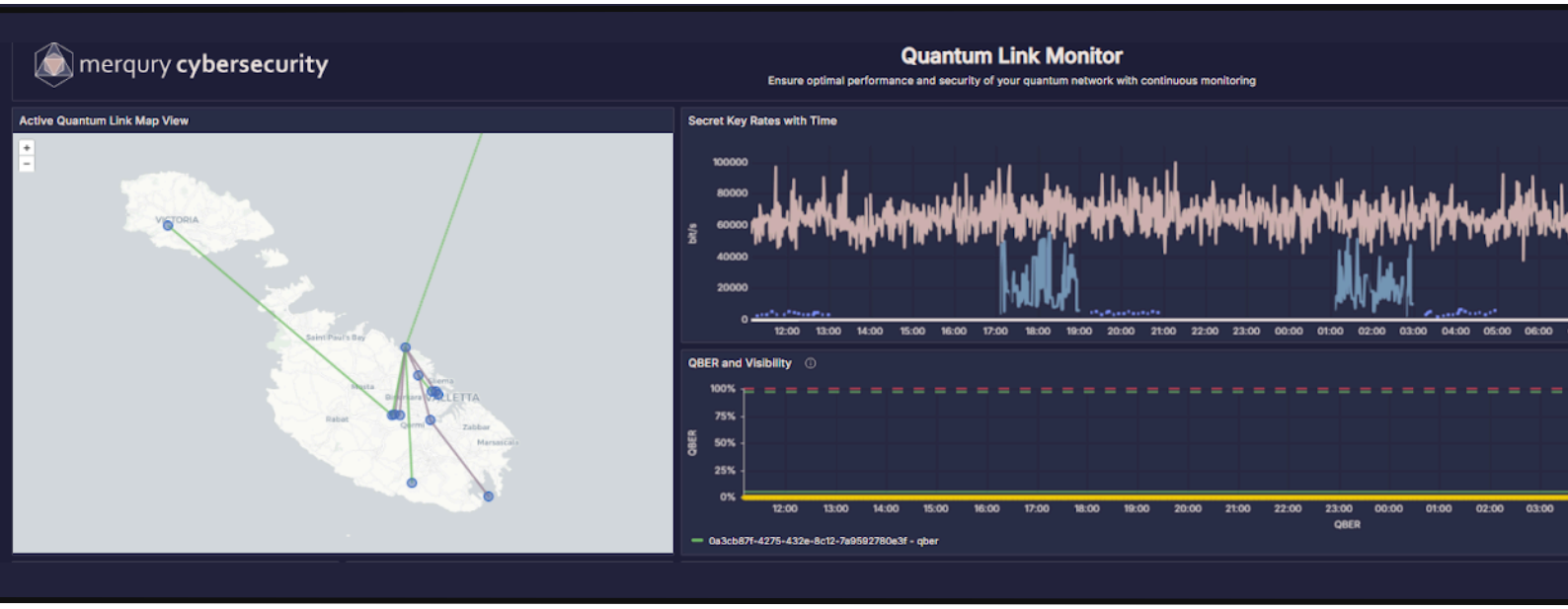
Integration into telecom and IT systems

The suite is built for minimal disruption. It integrates at gateway points such as inter-data-center links, government WAN edges, and cloud perimeters, using existing interfaces and fitting alongside established IPsec, MPLS, TLS, and MACsec workflows. This model has been demonstrated in carrier and cloud settings where QKD at the transport layer is combined with classical controls at the edge.int-to-point pilots to metro rings and mesh topologies.

Orchestration across multiple vendors and technologies

A vendor-agnostic stack, combined with monitoring and control, supports interoperability across mixed estates typical of national segments, including government, NREN, and carrier networks. This is the enabler for scale: consistent behaviour, continuous telemetry, and a straightforward path from point-to-point pilots to metro rings and mesh topologies.

Merqury adds another critical layer that supports the transition of advanced quantum technology into an operations-grade service: physics-anchored keys delivered through standardized interfaces to the equipment organizations already run. Integrating quantum-safe communications into existing networks starts with a clear assessment. QKD rollout must be planned as part of the organization's security roadmap, aligned with existing workflows and operational processes.



7.3 End-to-End Architecture

Before deployment begins, Merqury deploys the key management and orchestration layer. **This layer then bridges Luxquanta's CV-QKD devices with the organisation's live network.** Once quantum keys are generated on the fibre, approved encryptors can request, receive, and audit them without re-engineering existing systems.

Each site hosts a Merqury quantum network node connected to the Luxquanta QKD device and to the network's encryptors or gateways. T**hese appliances expose a controlled key service interface and enforce the organisation's authorisation and distribution policies defined by its security posture.** Operations teams use a monitoring and control console that correlates quantum-link status with key-service health, and all activity is logged to support compliance and audit requirements. In short, Luxquanta's CV-QKD provides physics-anchored key material.

Merqury makes it operational across production networks. The deployment integrates IPsec and MACsec encryptors alongside dense wavelength-division multiplexing (DWDM) transport, enabling quantum-secured encryption at the network layer while remaining compatible with existing telecommunications infrastructure.

7.4 Plug-and-Play Integration

QKD systems are masterpieces of modern engineering. Vendors, particularly Luxquanta, have invested heavily in the firmware and software layer for QKD to ensure devices adapt quickly to different network environments. As a result, users and technicians spend minimal time on deployment, with the process streamlined to reduce operational overhead. **Modern systems encapsulate the complex parts, such as timing, calibration, and alarms, behind a managed control plane.**

The device firmware and software negotiate operating parameters and maintain the link within a stable operating window. For operations teams, deployment becomes a repeatable workflow of patch, power, provision, and verify, rather than a bespoke optical project.

In practice, Luxquanta systems follow a plug-and-play approach: once connected to the fibre network, they automatically adapt to link conditions through in-house proprietary software. Integration with Merqury Cybersecurity is already established, so link bring-up and key management occur simultaneously through automated workflows.

Once the groundwork is in place, fieldwork is straightforward: rack the endpoints, patch the fibres, set the wavelength plan, equalise power, and run acceptance checks.

The QKD endpoints then handle link synchronization, clock recovery, and device self-tests. Coexistence with live DWDM traffic is managed through coherent detection, optical filtering, and channel isolation, so operators mainly confirm the optical budget and verify that alarms remain clean.

7.5 OSI Interoperability

QKD-derived keys can be used across multiple layers of the OSI stack, enabling encryption to be applied where it delivers the most operational value, from applications and IP tunnels down to Ethernet and optical transport.

This flexibility allows organisations to introduce quantum-safe key material without redesigning their network architecture and to select the most suitable integration point for each service, performance constraint, and security requirement.

The table below summarises how different OSI layers can consume QKD keys, the typical devices involved, and representative use cases.

Layer	Device Using QKD Keys	Function	Use Cases
Layer 4 to 7	Servers, virtual machines, and application-layer appliances (e.g., email, databases, cloud services)	Consume QKD keys for data encryption or secure session handling	Application-level encryption: databases, email, secure backups, cloud key usage
Layer 3	Routers / Firewalls / IP Gateways	Use QKD keys for IPsec encryption and authentication	Encrypted WAN communication between sites, secure VPN tunnels
Layer 2	Switches and Layer 2 encryptors	Use QKD keys for Ethernet frame encryption (e.g., MACsec)	Secure point-to-point Ethernet links, LAN/MAN security
Layer 1	Optical transport systems	Perform optical encryption using QKD keys (e.g., DWDM or 100G/400G line encryption)	Ideal for high-capacity point-to-point links between data centres

8. Practical Benefits of Integration

Building on the key hand-off, integrating Luxquanta's CV-QKD with Merqury's KMS turns quantum key generation into a network-consumable service. The benefits are operational and immediate.

Operational simplicity

The integration replaces bespoke, link-by-link work with a repeatable workflow: bring up the QKD link, attach the KMS, authorise consumers, and monitor. Keys are exposed at gateway points, so existing applications and routing can continue to operate without modification.

Continuity by design

Because the KMS is network-aware, it can maintain key delivery as paths or devices change, preserving service availability while providing live status and alarms for operations teams.

Auditability and control

Every key request and delivery is logged with timestamps and identity context, enabling traceability for governance and compliance. Access policies define which users or systems can obtain keys for specific site pairs, enforcing least-privilege key usage.

Interoperability in brownfield environments

Keys are delivered to approved encryptors via a controlled interface that integrates with existing encryption workflows (e.g., IPsec, TLS, or MACsec), avoiding code changes and reducing rollout risk.

Scalability from pilot to network

The same operational pattern extends from point-to-point pilots to larger topologies and national segments, with the KMS providing the policy control, monitoring, and logging that production environments require.

→ "By multiplexing QKD links on a live network, we drove down costs and improved resilience, resulting in an integrated, reliable, and cost-effective system for deployment in commercial environments."

André Xuereb.
CEO & Co-founder.
Merqury Cybersecurity.

9. Key Strategy: Added Value from Partnership

The partnership between Luxquanta and Merqury Cybersecurity, as demonstrated within PRISM, ensures that advanced quantum hardware is matched with enterprise-grade orchestration and integration. This combination enables operational efficiency, real-time monitoring, and secure key management aligned with national and European cybersecurity priorities.

Importantly, Malta's deployment is not limited to securing government institutions. The project also demonstrates the flexibility of QKD across diverse use cases and sectors. Demonstrations have included data centre interconnection and medical data transfer, showing that QKD can be deployed beyond traditional state-level applications and extended to critical industries. The examples presented in this report reflect real-world QKD deployments using mature, commercial-grade technologies already in operation. Rather than an R&D experiment, these national initiatives establish a practical foundation for quantum-safe migration across both public and private infrastructures, accelerating the deployment of QKD and its supporting ecosystem.

9.1 Key Takeaways

- **Operational integration is the differentiator:** Pairing CV-QKD with a KMS/orchestration layer turns quantum keys into a governed service that standard encryptors and applications can actually consume.
- **Coexistence is achievable in the real world:** Most links can run on commercially lit DWDM fibre, proving QKD can be introduced without requiring dedicated new fibre everywhere.
- **Hybrid deployment patterns scale better:** A pragmatic mix of point-to-point and point-to-multipoint approaches helps optimise cost, reach, and resilience as a network grows.
- **Interoperability reduces deployment friction:** Standards-aligned interfaces and clean integration paths allow quantum keys to slot into existing IPsec/MACsec security architectures with minimal disruption.
- **Security is as much "ops" as physics:** Monitoring, audit trails, policy controls, and lifecycle management are essential to preserve trust in keys over time, not only generate them.

QKD must run like infrastructure: Repeatable deployment patterns, operational monitoring, and key lifecycle processes matter as much as raw link performance.

9.2 Next Steps

If you are planning or operating EuroQCI/QCI deployments and want to assess CV-QKD integration, coexistence on commercially lit DWDM fibre, or operational key delivery into standard IPsec/MACsec environments, Luxquanta and Merqury can support feasibility assessments, pilot deployments, and integration planning. Get in touch to discuss your requirements and the most practical path to an operations-grade quantum-safe architecture.

→ About Luxquanta

At Luxquanta, we want to secure a brighter future. We believe in a future that is full of possibility, powered by innovation. The technologies emerging today will solve our greatest challenges, from climate change to disease, reshaping how we live, work, and connect. Yet, these very advancements carry the potential to shatter the digital security foundations we depend on.

For this future to truly flourish, it demands an unshakeable bedrock: quantum-grade security that innovates and evolves as rapidly as the world around it.

At LuxQuanta, we see beyond just protection. Security is an enabler. We see a world where advanced security unlocks boundless possibility, becoming the powerful platform for unprecedented progress. We build the trust that unlocks tomorrow's potential. We secure a brighter future, so you can build yours without limits.

https://www.luxquanta.com/

→ Contact

Email
sales@luxquanta.com
contact@merqury.eu

Phone Number
+34 692 35 87 23 - Luxquanta
+356 79944118 - Merqury

Address Luxquanta
Av. Joan Carles I, 30, 1º1ª, 08908
L'Hospitalet de Llobregat, Barcelona. Spain.

Address Merqury Cybersecurity
Takeoff Business Incubator. University of Malta
Msida, MSD 2080. Malta

Social Media
https://www.linkedin.com/company/luxquanta
https://www.linkedin.com/company/merqury

→ About Merqury

Quantum threats are no longer theoretical. Sensitive data is already being harvested under "store now, decrypt later" strategies, and global institutions such as NIST, the NSA, and the European Commission have issued clear warnings. Merqury addresses this urgency with a full-stack, vendor-agnostic platform that integrates post-quantum cryptography (PQC) and quantum key distribution (QKD). Merqury's solutions are drop-in compatible, built for scalability, and aligned with standards like ETSI GS QKD 014 — helping organisations adopt quantum-safe communication systems today, without disrupting existing infrastructure.

https://www.merqury.eu/