



THE WORLD'S COMMUNICATION PLATFORM

SPARKLE | CLOUD & DATA CENTER
PLATFORM

SPARKLE | CORPORATE
PLATFORM



ANTONELLA SANGUINETI

Head of Marketing & Product
Management Networking, Cloud,
Security & Identity Solutions





Quantum Safe Interconnect: bringing quantum-safe security into the era of programmable connectivity

The digital infrastructure ecosystem is entering a new phase. The rapid evolution of artificial intelligence, distributed cloud architectures and quantum computing is transforming the way data, applications and systems interact. In this scenario, cybersecurity can no longer rely only on stronger defenses or faster threat detection. It must evolve toward a programmable, scalable and crypto-agile security model capable of protecting data, services and machine-to-machine interactions against both current cyber risks and emerging cryptographic threats.

One of the most significant challenges is the risk known as "store now, decrypt later": sensitive encrypted data can be collected today and decrypted in the future once quantum computing capabilities become sufficiently mature. This scenario is accelerating the transition toward Post-Quantum Cryptography (PQC) and quantum-resilient architectures. In 2024, the U.S. National Institute of Standards and Technology (NIST) finalized its first post-quantum cryptography standards, marking a major milestone in the global migration toward quantum-safe security.

The urgency is also reflected in market forecasts. According to McKinsey, the global quantum technology market could reach up to \$97 billion by 2035, while quantum computing revenues alone are expected to exceed \$1 billion in 2025, following rapid growth from an estimated \$650–750 million in 2024. At the same time, replacing today's public-key cryptography across global digital infrastructures

is expected to take 10 to 20 years, making early adoption of quantum-safe strategies increasingly critical.

However, organizations cannot replace their networks, security architectures and cloud connectivity models overnight. They need a gradual, interoperable and operationally sustainable path toward quantum-safe protection.

This is the challenge addressed by Quantum Safe Interconnect (QSI), Sparkle's solution designed to bring quantum-safe protection into real-world interconnection services, enabling enterprises, carriers and cloud ecosystems to secure critical data against both today's cyber threats and tomorrow's cryptographic risks.

QSI introduces a software-based quantum-safe cryptographic overlay that can be deployed across existing network and security infrastructures, strengthening protection without requiring a complete redesign. Unlike approaches based on dedicated encryption appliances or Quantum Key Distribution (QKD) deployments, QSI is designed to operate seamlessly within existing IPsec, VPN and hybrid-cloud environments.

A key differentiator of QSI is its integration into a Network-as-a-Service (NaaS) model. Quantum-safe connectivity becomes a service that can be activated, managed and scaled across distributed environments, combining advanced cryptographic protection with automation, operational simplicity and service agility.



"The quantum threat is often associated with a future Q-Day, but in reality the transition has already begun," says Antonella Sanguineti, Head of Networking, Cloud, Security & Identity Solutions at Sparkle. "Organizations need to start building crypto-agility today because migrating critical infrastructures will take years. The challenge is to make quantum-safe security practical, interoperable and deployable without disrupting existing networks."

The solution has been designed to extend quantum-safe protection across multiple domains and interconnection points through a single end-to-end approach. QSI has been successfully validated in AWS multi-region cloud environments and is available through AWS Marketplace, allowing organizations to integrate quantum-safe connectivity into hybrid-cloud scenarios with minimal operational impact.

Sparkle has also expanded the commercial availability of QSI across 20 Equinix IBX data centers spanning Europe, the Americas and Asia, enabling enterprises and service providers to introduce quantum-safe protection within global interconnection ecosystems. This positions QSI among the first operator-led commercial quantum-safe interconnection services capable of delivering consistent protection across heterogeneous international infrastructures.

Beyond its immediate benefits, QSI is designed as a foundation for Sparkle's broader trust architecture. Its software-based, NaaS-enabled approach makes quantum-safe protection deployable across existing infrastructures while preparing customers for the next evolution of secure digital communications. This vision extends beyond network and cloud connectivity to STLS-AI (Symmetric TLS for Agentic AI), Sparkle's patent-pending transport-layer protocol designed for autonomous AI systems. By replacing certificate-based trust with a symmetric, certificate-less and quantum-resilient model, STLS-AI aims to enable scalable, low-latency trust between AI agents, applications and digital services.

QSI has also received significant industry recognition. Following the "Best Security Solution Provider" award at the CC Global Awards 2025, Sparkle's quantum-safe strategy was further acknowledged in Berlin this year receiving the "Best NaaS Platform Provider" award for

"SECURITY CAN NO LONGER BE TREATED AS A SEPARATE LAYER ADDED TO THE NETWORK,"

combining on-demand connectivity, orchestration, cloud integration and quantum security within a single programmable environment.

The solution has already progressed from innovation to commercial deployment, with early adoption by customers in the financial sector, demonstrating the growing demand for quantum-resilient security in highly regulated environments where confidentiality, integrity and long-term protection of sensitive data are business-critical requirements.

"Security can no longer be treated as a separate layer added to the network," concludes Sanguineti. "It needs to become an intrinsic capability of digital connectivity itself. By combining programmable networking, cloud integration and quantum-safe cryptography, we are enabling customers to prepare for the next generation of trusted digital infrastructures."

Quantum Safe Interconnect ultimately reflects a broader transformation taking place across the telecommunications industry. As quantum computing, AI and cloud-native architectures reshape digital infrastructure, security is evolving from a perimeter function into a programmable service embedded directly within connectivity. By enabling a gradual transition toward quantum resilience without disrupting existing infrastructures, QSI demonstrates how operators can turn one of the industry's most complex future challenges into a practical capability available today.