WHITEPAPER

Quantum-Safe Connectivity: How Sparkle's NaaS Services Future-Proof Today's Enterprises

Published by

MOBILE WORLD LIVE

In partnership with

SPARKLE ARQIT

Key Takeaways

- Quantum-safe connectivity is already deployable at scale across IP, optical, cloud and AI layers.
- Symmetric Key Agreement (SKA) provides deterministic, scalable and standards-aligned protection.
- Sparkle's QSI integrates quantum-safe capabilities directly into a NaaS orchestration model.
- Sparkle STLS-AI (patent-pending) extends quantum-safe communication to AI-to-AI and machine-to-machine sessions.

Introduction

The quantum race is on. Across the globe, some of the world's finest minds are helping governments and corporations to achieve the kind of technological dominance that will reshape human history. That future might still be some way off. But it gets closer with each new breakthrough.

In 2025 alone, we've seen advances in qubit stability, low-error quantum logic operation, and new chips, algorithms and computers which could help to scale projects and accelerate progress.

Yet while quantum may unlock untold advances for humanity, it also opens the door to a darker future. The advent of cryptographically relevant quantum computers (CRQCs) will herald the beginning of the end for public key cryptography as we know it. CRQCs will be able to solve the mathematical puzzles on which asymmetric encryption relies - enabling threat actors to unscramble some of our most sensitive information. Telcos and backbone operators are particularly at risk, as their networks carry sensitive interconnect and signalling data.

For critical infrastructure providers like telcos, financial services firms and defence contractors, there's no time to wait. Harvest now, decrypt later (HNDL) already represent a real and present threat. That's why Sparkle is taking concrete steps towards quantum safety. Governments and regulators are already issuing mandates for post-quantum systems to protect data at rest and in transit.

Faced with these challenges, enterprises need robust, easy to manage, quantum-safe connectivity and solutions. This is where Sparkle's cutting-edge Network as a Service (NaaS) platform comes in. The following whitepaper will explore the benefits of this platform, Sparkle Quantum Safe over Internet (QSI), which offers protection from CRQCs across optical, IP, cloud and AI layers.

The time is now: what's driving quantum safety?

CRQCs might still be some years away. But HNDL - also known as "store now, decrypt later" (SNDL) - represents a pressing threat. It posits that well-resourced threat actors, especially nation states, may already be stealing asymmetrically encrypted data with a view to unscrambling it once CRQCs become available.

This is a particularly insidious threat, as it will only become clear in years to come whether such efforts were successful. But attacks are already taking place, government security officials have warned. Although the targeted information would have to still be relevant in 10-15 years, it should be enough to give IT and security leaders sleepless nights. The compromise of highly sensitive military intelligence and corporate trade secrets could have a catastrophic impact.

HNDL aside, enterprises should already be planning their journey to quantum safety.

Some executives might dismiss it as a long-term business risk that doesn't require immediate attention. But it is precisely because there is no exact timeframe for the emergence of CRQCs that work must start now. Unfortunately, the lack of a "quantum-ready baseline" in current security frameworks complicates these efforts. It's why NaaS-delivered solutions like QSI are gaining traction as a way to reduce complexity and accelerate the journey.

Digital transformation fuels complexity and risk

The task is made more urgent still due to the sheer complexity of modern IT environments. The average enterprise runs hundreds of applications, usually spread across multiple cloud providers and on-premises servers. In fact, an estimated 86% are running multi-cloud operations and 70% have hybrid setups. Edge computing and Internet of Things (IoT) deployments further expand the corporate IT footprint, and exacerbate certificate and identity fragmentation

The promise of AI-powered business enhancements is encouraging ever more CIOs to double-down on digital transformation. According to McKinsey, global datacentres will require a staggering $6.7 trillion in capital outlays to keep pace with the sheer demand for compute power by 2030.

The concern is that the more data pipelines there are for enterprises to manage, the greater the potential attack surface for threat actors to target. A GSMA Intelligence report reveals that a majority (57%) of global telco leaders cite "signalling and interconnect" as one of the top three cyber threats affecting mobile networks. Nearly half (46%) predict a considerable net rise in such threats to network assets over the coming three years. This speaks to the dangers of sensitive data flows being targeted by HNDL attackers today, and CRQCs tomorrow.

Governments take action

All of which explains why governments and regulators are already gearing up for a post-quantum world, with various roadmaps and deadlines. They include:

The EU's Coordinated Roadmap for Post-Quantum Cryptography (PQC), which recommends that all member states have a PQC strategy in place by the end of 2026. High-risk systems must be fully migrated by the end of 2030 and medium and low-risk systems by 2035.

The US government mandates full migration to PQC for federal systems by 2035, with large enterprises encouraged to follow suit. The SEC has published its own roadmap, which is aligned to the same timelines.

The UK's National Cyber Security Centre (NCSC) has guidelines urging post-quantum plans begin in earnest in 2028 and complete migration to PQC for "all systems, services and products" by 2031-35.

Whether individual organisations are mandated by regulators/governments or not, the commercial imperative alone should be enough to kick start PQC plans. It goes without saying that a breach of sensitive encrypted data, such as IP or customer/employee personally identifiable information (PII), could lead to:

- Significant financial costs (legal fees, notification costs, forensics and incident response etc)
- Major reputational damage leading to customer churn, diminished share price, and a potential impact on future talent acquisition
- Legal and regulatory action which can amplify financial and reputational damage, including class-action lawsuits and possible fines (GDPR, HIPAA, CCPA etc)

Quantum-safe communications: scalability and security

Fortunately, there are several approaches that businesses can take to PQC, depending on the specific use case and their circumstances:

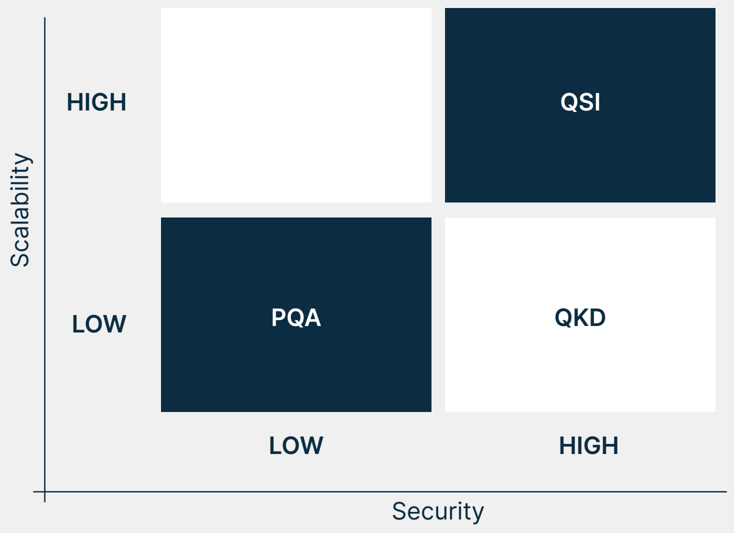
Quantum key distribution (QKD): Leverages the laws of quantum mechanics to create a secure quantum-safe method of exchanging cryptographic keys over regular, high capacity fibre links. It does so by sending photons encoded with data. If a threat actor tries to intercept the quantum-encoded key, it will disturb the particles, immediately flagging malicious activity. The sender and/or receiver can then immediately ditch the compromised key and abort communications.

Post-quantum algorithms (PQAs): New mathematical algorithms are currently undergoing standardization work by the US National Institute of Standards and Technology (NIST) and other bodies. These upgrade asymmetric algorithms to make them "quantum safe". Although relatively quick and easy to deploy at scale, and on existing infrastructure, there are some question marks over their long-term viability. PQAs could be broken in the future, as they derive their security from the same mathematical processes as current asymmetric encryption. And the larger key sizes involved may increase overheads and degrade performance.

Symmetric Key Agreement (SKA): While asymmetric algorithms work on public and private key pairs, SKA uses just one key. This is known by sender and recipient but not exchanged during communication, meaning even CRQCs cannot decipher it. The technology is available today and relatively quick, easy and cost-effective to deploy with no rip and replace needed. It also works with existing infrastructure and popular IPSec/TLS protocols and is perfect for fast, bulky data transfers.

Sparkle's QSI NaaS platform leverages an SKA engine from partner Arqit to deliver robust post-quantum encryption in an easy-to-deploy solution. It adds up to an end-to-end, quantum-safe communications solution that can be deployed today.

Although some enterprises will want to take a hybrid approach to their post-quantum planning, there are some considerations to bear in mind before selecting a solution. As this matrix shows, SKA (as per Sparkle QSI) offers the best combination of scalability and security.



Introducing QSI

Sparkle is the first global operator in the world to offer a commercial, quantum-safe NaaS solution, tested successfully across a number of commercial networks and use cases. QSI was initially designed to enhance traditional IPsec virtual private network (VPN) technologies so that communications travelling down these encrypted pipelines are safe from CRQCs and HNDL attacks. Since then, it has been expanded to other layers: optical and AI so far and validated through multiple international PoCs.

QSI does not require any hardware replacement or dedicated optical infrastructure. It leverages existing customer CPEs, uCPEs, virtual machines and cloud environments, enabling rapid adoption without disruptive upgrades.

QSI can be layered on L1, L2-ready and L3 connectivity and deployed on any kind of endpoint. Symmetric key endpoints can be connected to any existing CPE or universal CPE/virtual machine, or in the cloud. Symmetric encryption is controlled and orchestrated by Arqit's SKA platform and keys can be consumed by any existing protocols (IPsec, TLS, MQTT, MACsec). The SKA solution is also compatible with the main VPN providers like Fortinet.

Among the benefits of QSI are:

- Compatible with diverse range of customer networking equipment, VPNs and security protocols
- Avoids the overheads and certificate lifecycle management headaches associated with PKI
- Ensures quantum-safe communications in multiple use cases (DC to DC, IoT, edge computing, customer sites to cloud)
- Simple deployment and management thanks to NaaS model
- Continuous key rotation for optimized security
- High performance at scale
- Zero trust architecture
- Crypto agility future-proofs system against new threats, changing standards, or emerging vulnerabilities

The NaaS advantage

Sparkle's NaaS platform leverages software-defined networking to offer customers performance, control and scalability on demand. Everything can be managed through a dedicated centralized portal or API in an agile, automated manner. Unlike isolated quantum-safe point solutions, QSI is delivered through Sparkle's NaaS orchestration layer, which unifies provisioning, lifecycle management, policy control and multi-layer integration across network, cloud and edge domains. With QSI, end users get:

- Optimised, VPN-based and quantum-safe connections
- Cost-optimised compute based on Intel technology
- Zero-touch provisioning enabled by Adtran

Sparkle secures across diverse network environments:

L3: IPsec

Protects critical communications between datacenters, customer sites, and from customer locations to the cloud. Sparkle's QSI IPsec offering uses Arqit SKA technology (SKA Platform and NetworkSecure Adaptor) to generate and manage post-quantum, pre-shared keys at VPN endpoints. StrongSwan (or alternative VPN vendors) then integrate these keys to make the IPsec tunnel quantum safe. PCIe accelerator cards based on the Intel NetSec Accelerator Reference Design provide a powerful, compact server-on-a-card for hosting the lightweight Arqit NetworkSecure Adaptor. Adtran enables zero-touch deployment through the Ensemble MANO management platform.

Quantum Safe to Cloud:

Leverages quantum-safe IPsec connectivity (as above) to ensure data in transit to AWS is protected from CRQCs. Available via Sparkle or the AWS Marketplace, it is designed to protect business-critical workloads like AI inference pipelines, with no additional infrastructure required. Also supports edge computing and IoT use cases. Sparkle is proud to be one the first global operators to offer quantum-safe networking on AWS Marketplace.

L1: Quantum Safe Over Optical:

Extends QSI framework to optical transport for quantum-safe encryption reaching 400 Gb/s. Symmetric encryption keys delivered by QSI are directly injected into a third-party vendor's optical modules, enabling line-rate optical encryption. The solution works dynamically thanks to the Sparkle NaaS platform, with no loss of performance.

The future of QSI – Symmetric TLS for Agentic AI

While QSI secures connectivity between locations, STLS-AI provides quantum secures communication sessions and crypto-identity between autonomous software entities. The two are complementary: QSI protects the network layer, and STLS-AI protects the conversation layer.

Agentic AI represents the next wave of technology innovation, set to usher in a new era of business productivity and efficiency. These autonomous AI systems are forecast to explode in number, as businesses set them to work, planning, reasoning and acting to complete tasks autonomously. According to McKinsey, 62% of global organizations are in the experimental stage, or more advanced phases of development.

The challenge is that traditional certificate and public key cryptography-based security approaches are no longer fit for purpose in this new era of agentic AI. The client-server model and static, pre-issued certificates simply aren't designed to support the dynamic way AI agents interact with each other and third-party systems.

This is where Sparkle STLS-AI comes in. The patent-pending solution extends SparkleQSI NaaS service into the AI domain, replacing asymmetric handshakes with a fully symmetric, quantum-safe and orchestrated identity layer for machine-to-machine and agent-to-agent communications. With STLS-AI, every AI session dynamically establishes a verifiable crypto-identity, enabling trust, authentication, and encryption natively between AI entities.

Securing connectivity anywhere

Sparkle QSI ensures quantum-safe connectivity between any kind of location:

DC to DC: IPsec VPN tunnels secure business-critical traffic between datacentres and customer locations, ensuring organisations in highly regulated sectors like government, finance and military achieve quantum safety.

DC/customer site to public cloud: QSI's quantum-safe IPsec connectivity ensures data flowing to business-critical, cloud-hosted apps remains secure.

DC to edge: Quantum-safe VPN tunnels between on-premises edge datacenters and AWS VPCs for optimised security. Enabled by lightweight Arqit/Intel hardware.

IoT: Sparkle's Quantum Safe to Cloud allows customers to protect traffic directly from the IoT gateway or edge node into the cloud region. Since QSI is based on symmetric keys, it scales easily to environments with lots of small devices without the complexity of heavy PKI management.

How it works

STLS-AI features three components:

Network Secure Adapter (NSA): An endpoint module that enables agents to establish symmetric session keys and manage their crypto identity.

Symmetric Key Agreement (SKA) platform: A cloud or on-prem key orchestrator featured in Sparkle's QSI infrastructure (powered by Arqit), which ensures quantum-safe key lifecycle management. Sparkle operates and orchestrates the SKA infrastructure.

Modified TLS Runtime (STLS Engine): A secure transport layer adaptation of the standard TLS stack, redesigned to accept externally injected symmetric keys instead of generating them through public-key handshakes. This enables full compatibility with existing TCP/IP applications, while replacing certificate-based negotiation with direct symmetric key injection from the NSA. It ensures the entire session is quantum-safe, deterministic, and PKI-free.

STLS-AI Gateway Platform (coming soon): This will extend protection to the application layer, orchestrating trust among distributed agents and systems.

The underlying mechanism replaces public-key cryptography with bilocation key exchanges and symmetric ratcheting. This produces an evolving identity chain for every agent - continuously verifiable and immune to quantum decryption threats.

Demonstrating the power of STLS-AI

Sparkle staged a live demonstration of STLS-AI in action at the MEF Global NaaS Event 2025 in Dallas in November—showing two autonomous agents collaborating securely over a transatlantic connection.

In the demo, the agents interacted securely over a connection between London and Northern Virgina. They executed a telecom ordering workflow through the Model Context Protocol (MCP), comparing service quotes and validating transactions in real time. We ran two identical scenarios: one using standard HTTPS to secure the connection, and the other deploying STLS-AI's symmetric, quantum-safe session layer.

The results were impressive. STLS-AI reduced handshake traffic by up to 87%, while simultaneously establishing verifiable cryptographic identity and symmetric encryption across the Atlantic. The demo showed for the first time that autonomous AI systems can authenticate, negotiate, and exchange data in a quantum-safe way on a production network.

Pioneered by Sparkle, secure agentic communications at global scale are now within the grasp of enterprise customers across the planet.

Securing the future

No two organisations are alike. But no matter what your corporate risk appetite, it's time to take the CRQC threat seriously, and begin planning your transition to quantum safety. There are no shortcuts. But with Sparkle's QSI you have a readymade, technologically proven Network as a Service (NaaS) suite to secure connectivity, whatever your use case.

Consider it an essential companion on your journey to a post-quantum future. Start your plans today by:

- Running quantum risk assessments across critical systems
- Developing a clear post-quantum transition roadmap
- Piloting post-quantum solutions like Sparkle QSI
- Engaging senior business leadership and other key stakeholders
- Collaborating across industry to share best practices, such as via the Mplify W174 initiative in which Sparkle participating leading the editorial and coordination effort

The post-quantum transition has already begun. Operators, enterprises and cloud ecosystems will require quantum-safe connectivity that is deployable today, interoperable tomorrow and scalable over the next decade. Sparkle QSI and STLS-AI represent practical, standards-aligned building blocks for this transition.

Sparkle is TIM Group's global operator, first international service provider in Italy and among the top worldwide, offering a full range of infrastructure and global connectivity services – capacity, IP, SD-WAN, colocation, IoT connectivity, roaming and voice - to national and international Carriers, OTTs, ISPs, Media/Content Providers, and multinational enterprises. As a leading player in the submarine cable industry, Sparkle owns and manages a network of more than 600,000 km of fiber stretching across Europe, Africa, the Middle East, the Americas, and Asia. Sparkle's sales team has a global presence, with representatives in 32 countries.

Find out more about Sparkle following its X and LinkedIn profiles or visiting the website tisparkle.com

Mobile World Live is the premier destination for news, insight and intelligence for the global mobile industry. Armed with a dedicated team of experienced reporters from around the world, we are the industry's most trusted media outlet for breaking news, special features, investigative reporting, and expert analysis of today's biggest stories.

We are firmly committed to delivering accurate, quality journalism to our readers through news articles, video broadcasts, live and digital events, and more. Our engaged audience of mobile, tech and telecom professionals, including C-suite executives, business decision makers and influencers depend on the unrivalled content and analysis Mobile World Live provides to make informed business decisions every day.

Since 2016, Mobile World Live has also had a team of in-house media and marketing experts who work directly with our brand partners to produce bespoke content and deliver it to our audience in strategic yet innovative ways. Our portfolio of custom work - including whitepapers, webinars, live studio interviews, case studies, industry surveys and more – leverage the same level of industry knowledge and perspective that propels our newsroom.

Mobile World Live is published by, but editorially independent from, the GSMA, producing Show Daily publications for all GSMA events and Mobile World Live TV – the award-winning broadcast service of Mobile World Congress and home to GSMA event keynote presentations.

Find out more at www.mobileworldlive.com

Disclaimer: The views and opinions expressed in this report are those of the authors and do not necessarily reflect the official policy or position of the GSMA or its subsidiaries.