Case Study: Sparkle

Quantum-Safe Connectivity and Zero Trust Encryption

August 2025

SPARKLE

Delivering Real-Time, Identity-Driven Security for the Post-Quantum Era

Challenge

The rapid advancement of quantum computing and AI-driven cyber threats has put traditional encryption models at risk. For critical infrastructure sectors such as finance, healthcare, government, and defense, the stakes are especially high. Sparkle sought to future-proof its global backbone by delivering an API-driven, on-demand network that provides quantum-safe encryption and Zero Trust security as a service.

Solution

Sparkle partnered with Arqit, Adtran, Intel and Lanner to build a Quantum-Safe over Internet (QSI) architecture that integrates post-quantum cryptography with Mplify Lifecycle Service Orchestration (LSO). At the edge of the network, Arqit's symmetric encryption engine generated quantum-safe keys on demand. These were deployed through Lanner's universal CPE generic devices, which handled key distribution and traffic protection at line rate. Intel provided a Zero Trust reference architecture to tie the solution into enterprise identity systems.

The solution was tested over a 4,000-kilometer span from Barcelona to Athens, demonstrating quantum-safe symmetric encryption over two IPsec tunnels, with configurable key rotation mechanisms. Sparkle is collaborating with Mplify and industry partners to standardize Mplify LSO APIs that enable real-time provisioning and assurance of encrypted services as defined in Mplify W174 Product Attributes and Use Cases for Quantum-Safe Services. The implementation also validated subject and target identities in alignment with Mplify's Zero Trust model, enabling end-to-end identity assurance and service-level access control.

This architecture allows providers to offer secure, zero-trust-based network overlays to customers requiring compliance with emerging global security mandates and country-based policies for the mandatory transitions to post-quantum solutions. By decoupling trust from physical infrastructure and integrating encryption policy enforcement at the edge, the Sparkle QSI model supports a scalable range of scenarios from sovereign cloud services and cross-border collaboration to AI data pipelines and IoT backhaul.

Furthermore, implementing the QSI solution through automation and a Network-as-a-Service (NaaS) approach makes the solution quick to deploy, easy to manage, and flexible enough to adapt to changing scenarios.

Results

Sparkle's QSI demonstration delivered the following advancements:

- First live demonstration of quantum-safe encryption aligned with Mplify Zero Trust architecture.
- Zero-touch Provisioning (ZTP) of end-to-end service fully orchestrated to provide on-demand activation/deactivation.
- Real-time symmetric key exchange across unlimited spans with configurable intervals and policy driven management of end-points allowed for key generation.
- Hardware-based enforcement of access control and identity validation.
- Integration with LSO APIs for dynamic provisioning and assurance.
- Showcases secure, API-driven connectivity built in line with emerging NaaS models and automation standards.

Key Takeaways

- Quantum-safe encryption is real, tested, and deployable at scale.
- Identity-first security is achievable via Zero Trust frameworks aligned to Mplify's LSO APIs.
- Real-time provisioning of secure services enables monetization of compliance and sovereignty demands.
- Cross-industry collaboration is essential to bring secure-by-design network services to market.

Get Involved

Sparkle's work demonstrates how secure, on-demand, identity-driven services can be operationalized today. If you're building sovereign, mission-critical, or AI-adjacent network services, partner with Sparkle and Mplify to co-develop and scale quantum-safe architectures.

Engage with Mplify now to shape the future of secure connectivity in the post-quantum era.

About Mplify

Mplify is a global alliance of network, cloud, cybersecurity, and enterprise organizations working together to accelerate the AI-powered digital economy through standardization, automation, certification, and collaboration. As the defining authority behind Carrier Ethernet, Lifecycle Service Orchestration (LSO) APIs, and certified SASE and SD-WAN, Mplify has developed the global blueprint for Network-as-a-Service (NaaS) that is empowering the industry to innovate, interoperate, and scale trusted network services across a global ecosystem. For more information, please visit mplify.net and follow us on LinkedIn, BlueSky, and YouTube @mplifyalliance