ARQIT | SPARKLE

Case study

Telecommunications

Confronting high-stakes security risks across fiber networks amid the quantum threat

Overview

Leading global service provider Telecom Italia Sparkle SpA operates an extensive Tier 1 fiber network that forms the backbone of the TIM Group, providing international routing infrastructure and global connectivity services. As a major player in the submarine cable industry, Sparkle owns and manages a global and technologically advanced proprietary network spanning 600,000 kilometers across 33 countries, connecting Europe, the Americas, and Asia. Their network facilitates the global transmission of vast amounts of internet data, including sensitive information.

Sparkle prides itself on exceptional customer care, delivering customized solutions with top performance and cost efficiency in the international telecommunications market, consistently providing value through credibility. However, in the wake of recent threats, the company faces significant challenges as customers demand enhanced security following high-profile cyber-attacks. The urgency to stay at the technological forefront is greater than ever, particularly as governments and businesses increasingly view underwater cables as vulnerable to espionage.

This vulnerability was starkly highlighted by a series of severances including after Houthi rebels in Yemen sank a ship in the Red Sea. Telecom providers are increasingly concerned about the risk of data transmissions being intercepted and decoded by the imminent threat of powerful quantum computers, raising the specter of "Harvest Now, Decrypt Later" attacks. These issues underscore the critical importance of fortifying the security of global telecommunications infrastructure.

At a glance

Telecom Italia Sparkle SpA

Submarine cable industry.

Global transmission of IP data.

600,000 km Tier 1 fiber network infrastructure across 33 countries worldwide.

International routing infrastructure and global connectivity services for TIM Group.

Challenges

Operates in a technologically advanced and complex environment.

Underwater cables are vulnerable to interception by state-sponsored actors

Increased threat to customer's sensitive data through sophisticated cyber threat including from a quantum computer.

Risk of harvest now, decrypt later attacks.

Sparkle customers requesting an increased level of security following a series of high-profile cyber-attacks.

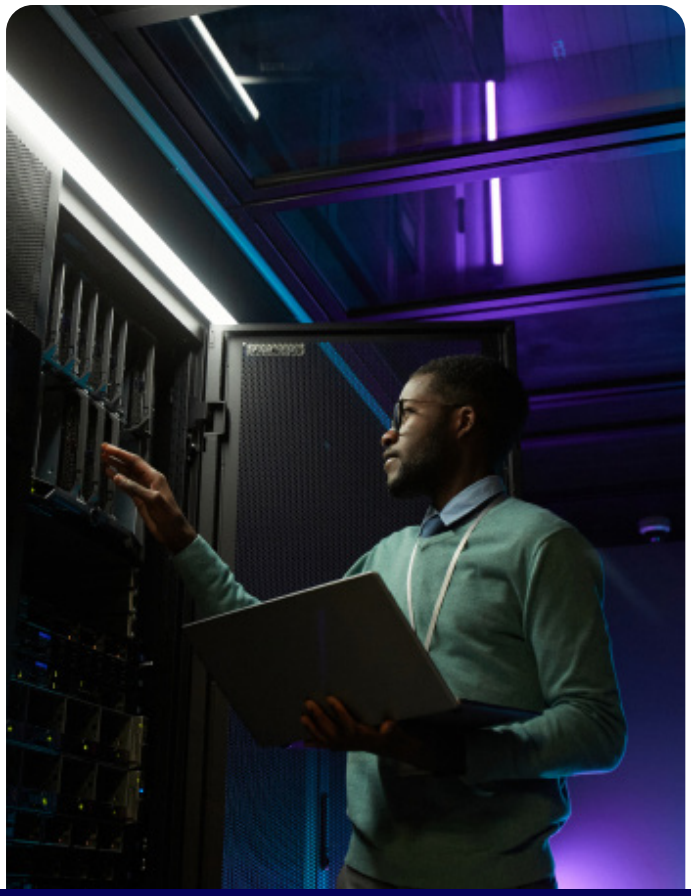
> **Our state-of-the-art global network provides critical services to carriers, institutions, and enterprises who choose and trust Sparkle's leading secure connectivity services to keep their data safe. The successful completion of the quantum-safe VPN POC, preliminary to a large-scale commercial launch, anticipates the potential threat of quantum decryption and confirms our market-leading commitment to continuously elevating the security and resilience of Sparkles infrastructure.**
>
> – Daniele Mancuso, Chief Marketing & Product Management Officer, TI Sparkle

Securing tomorrow: Sparkle's quest for quantumsafe encryption

As a critical infrastructure provider, Sparkle recognized the necessity of preventing any intercepted information from being decoded by quantum computers in the future. They needed to adopt a robust, forward-secrecy approach using quantum-safe security systems to protect their customers' sensitive information from the threat of "Harvest Now, Decrypt Later" attacks.

To achieve this, Sparkle explored new encryption techniques, focusing on Post-Quantum Cryptography (PQC) technologies and potential vendors. Any proposed solution had to be reliable and scalable, with the ability to mediate key exchange in various environments, including challenging ones.

However, current key exchange methods rely heavily on Public Key Infrastructure (PKI) utilizing Elliptic-curve Diffie–Hellman (ECDH), which face a significant vulnerability to decryption by quantum computers. While efforts are underway to develop New Post-Quantum Algorithms (PQAs) to address this threat, they are not yet readily available for implementation. Moreover, the process of standardizing these algorithms is lengthy, and their quantum security remains unproven. In addition, PQAs are expected to be slower and more memory-intensive with complex computational cryptography, particularly challenging in industries like telecommunications with intricate operational environments. Moreover, as these cryptographic keys are increasingly relied upon for prolonged periods, the duration of security risk exposure escalates significantly.



> **Sparkle's quantum-safe rollout is a first mover, but this will become table stakes.**
>
> – Kevin Bocek, CIO, Venafi Inc.

Solving the problem

Requirements

Quantum-safe VPN for data in transit.

Reliable and scalable solution available today.

Ability to mediate key exchange in challenging, and complex environments.

Fast key rotation over-the-air (OTA).

Solution

Arqit SKA-Platform™

Arqit NetworkSecure™ Adaptor for Fortinet Fortigate Next Generation Firewall (NGFW)

2-site POC between Catania, Sicily and Frankfurt, Germany. A 2,000 kilometer stretch of fiber between datacenters.

Supported by Telsy, a TIM Group cybersecurity company.

Benefits

- Quantum-safe VPN with perfect forward secrecy.
- Zero-trust architecture.
- No loss of performance on the IPsec tunnel.
- Strong authentication.
- Zero downtime, continuous running of IPsec tunnel.
- Configurable re-keying frequency.
- Fast and frequent key rotation – every 3 minutes.

Next Steps

Implementation across the rest of the global fiber network over the next year, starting in Europe Mid-2024.

Quantum-Safe Revolution: Sparkle's Partnership with Arqit

Sparkle recognized the need for a fresh perspective in addressing their security concerns and turned to Arqit for assistance in developing a post-quantum transition plan, after seeing the announcement on Arqit's integration with Fortinet and BT in late 2023 for a commercially available quantum-safe VPN.

As a key member of the GSMA Post-Quantum Telco Network (PQTN) Taskforce, Arqit has been supporting the global mobile ecosystem for the advanced protection of telecommunications in a future of advanced quantum computing.

Addressing many of the challenges and uncertainty surrounding modern encryption techniques and post-quantum algorithms (PQA), Arqit is at the forefront of revolutionizing the post-quantum cybersecurity landscape, offering a highly scalable and proven quantum-safe cryptography solution that is both reliable and readily deployable today.

Through the creation of a software-based quantum-safe virtual private network (VPN), Arqit has marked a significant milestone in network security. By leveraging Arqit's SKA-Platform™ (Symmetric Key Agreement), alongside Arqit's NetworkSecure Adaptor for Fortinet, Sparkle has the ability to facilitate key exchange between VPN endpoints in a quantum-safe manner, ensuring robust authentication, perfect forward secrecy, zero-trust architecture, and configurable re-keying, thus solidifying its position as the preferred solution.

> **Sparkle's establishment of the first quantum-safe VPN between Catania and Frankfurt signifies a key milestone in telecoms cybersecurity. By leveraging Arqit's SKA-Platform, Sparkle is pioneering a new era of secure communication, ensuring the resilience of critical networks against the looming threat of quantum adversaries.**
>
> - David Williams, CEO, Arqit

Introducing Arqit NetworkSecure Adaptor for Fortinet

To fortify Sparkle's defenses against complex VPN vulnerabilities, the combined strengths of Fortinet and Arqit's VPN Encryption Solution, NetworkSecure, proved to be the perfect combination. This cuttingedge-solution introduces quantum-safe symmetric keys, providing robust protection against potential threats across VPN channels.

NetworkSecure seamlessly integrates Fortinet FortiGate Next-Generation Firewalls with Arqit's SKA-Platform, delivering automated, on-demand quantum-safe protection for VPN data communications. Each FortiGate firewall securely connects to its NetworkSecure Adaptor over the local network, facilitating the generation and rotation of keys over-the-air (OTA) as needed. This ensures continuous, adaptable encryption, offering utmost protection for sensitive data transmitted across VPN links.

By integrating quantum-safe symmetric keys, NetworkSecure effectively mitigates vulnerabilities inherent in traditional VPN protocols such as IPsec, enhancing the security of communication links and addressing evolving cyber threats. Its intelligent encryption mechanism simplifies the process, setting a new standard for VPN security.

To validate the solution against their intricate requirements, Sparkle conducted a Proof-of-Concept (POC) between key sites—Catania in Sicily and Frankfurt in Germany. This 2,000-kilometer stretch of fiber between datacenters provided an ideal testbed to evaluate the platform's capabilities, performance, and security level.

During the POC, exploratory test cases were executed to establish a quantum-safe IPsec tunnel between the two sites using key creation and rotation enabled by Arqit's SKA-Platform. An initial IPsec tunnel was established and once operational, Arqit was integrated to fortify the tunnel with quantum-safe capabilities, including frequent key rotations managed by the firewall. During the process, Sparkle's technical team gained familiarity with the solution.

The POC produced promising results, demonstrating rapid key rotation every three minutes without compromising the performance of the IPsec tunnel. Additionally, the tunnel operated continuously with zero downtime, underscoring the reliability and effectiveness of the solution.

Delighted by the successful POC, Sparkle plans to deploy the solution across other parts of their global fiber network over the next year, starting with expansion in Europe by mid-2024.