Case Study

Communications Service Providers

Arqit Quantum-Safe VPN for Sparkle NaaS

Sparkle conducts POC of Arqit Quantum Safe VPN on Intel® NetSec Accelerator Reference Design with orchestration provided by Adtran Ensemble MANO software

Network as a Service (NaaS) offerings are gaining market traction as organizations seek flexible, scalable, and cost-effective networking solutions that can be deployed without heavy capital investments in hardware.

With NaaS, organizations can provision and manage networking services on-demand, making it an attractive option for navigating digital transformation, remote work, and cloud migration. The ability to scale bandwidth, ensure performance, and adapt to changing connectivity needs in real-time has led to increasing adoption of NaaS.

Securing this data has always been paramount. Virtual private networks (VPNs) help safeguard sensitive information by establishing encrypted tunnels between users and their destinations. For NaaS customers, VPNs offer an additional layer of security, ensuring that data transmitted remains confidential and protected from cyber threats.

Even though today's VPNs provide advanced encryption that protects data in transit, future quantum computers can break the encryption, revealing the data. For its popular NaaS services, Sparkle has trialed a quantum-safe VPN solution based on technology from Arqit, an Intel® Industry Solution Builders member.

Sparkle is NaaS Leader

Leading global service provider Sparkle offers a comprehensive suite of services tailored to a diverse range of customers including OTTs, carriers, service providers, and enterprises. Its offerings span from secure global IP transit for accessing internet content to high-performance international network bandwidth. Additionally, Sparkle provides a unique array of infrastructure solutions and proprietary colocation services, ensuring top-tier connectivity and security for all its customers.

Sparkle has expressed its ambition to be the world's first quantum-safe internet service provider, facing the challenge of ensuring secure communication between data centers and customer branch offices and sites over the open internet with forward-secrecy. This ambitious plan sets a new standard for security in the face of emerging quantum computing threats.

To address the challenge, Sparkle collaborated with Arqit on a proof of concept (POC) for a sophisticated solution using Intel-based Network Accelerator cards, installed in Supermicro IoT SuperServer with Intel® Xeon® Scalable processors. The project aimed to establish IPsec traffic between both servers such that the data remains quantum-safe from end-to-end, regardless of the route taken over the open internet.

Defending Against Store Now, Decrypt Later (SNDL) Attacks

Quantum computers are not yet sufficiently powerful to break encryption but the threat of store now, decrypt later (SNDL) is real and is here today. It is crucial for Sparkle's customers to start mitigating the risk by transitioning to quantum-safe connectivity.

Expanding its partnership with Arqit, Sparkle is pioneering the exploration of quantum-safe IPsec connectivity between data centers. The focal point of this groundbreaking initiative is its one of the most advanced data centers in Europe, the Metamorphosis II site in Athens, Greece.

This state-of-the-art facility was the perfect choice to host the world's first quantum-safe POC of encrypted internet links utilizing Arqit's cutting-edge technology.

Metamorphosis II, an open-hub facility, provides an unparalleled and advanced NaaS platform for the most sophisticated customers. It is designed to deliver a fast, open, and resilient configuration, tailored to the needs of carriers, OTTs, and enterprises. This facility ensures direct interconnection for corporate and institutional entities, enhancing its operational efficiency and security.

By leveraging this advanced infrastructure, Sparkle aims to lead the industry in implementing quantum-safe solutions, setting a new benchmark for data security and high-speed connectivity. This initiative underscores its commitment to innovation and excellence, paving the way for a more secure and reliable internet for all.

The Future of Secure Internet Pioneering Quantum-Safe Connectivity

The solution for Sparkle involved Arqit, Intel, and Adtran who combined to deploy the quantum-safe VPN solution with Arqit's NetworkSecure Adapter, executed on a NetSec accelerator card based on Intel® NetSec Accelerator Reference Design. This collaboration marks a significant leap forward in the quest for robust and future-proof internet security.

Sparkle PoC at a Glance

Situation

- Athens Data Center 'Metamorphosis II,' Greece.
- Global transmission of IP data.
- International routing infrastructure and global connectivity services for TIM Group.

Challenges

- Increased threat to sensitive customer data through sophisticated cyber risk including from quantum computers.
- Risk of store now, decrypt later attacks.
- Minimal changes to the data centers and edge location hardware infrastructure.

Arqit Solution Provides

- Secure communication between data centers in an open-source environment.
- Quantum-safe VPN for data in transit.
- Reliable and scalable solution available today.
- Fast key rotation over-the-air (OTA).

Intel® NetSec Accelerator Reference Design

This reference design combines an Intel® Ethernet Network Controller with an Intel® Xeon® D processor, packaged in a PCIe add-in card. Designed for network security workloads, the card features the functionality of a server with the capability to support security workload orchestration and real time and out-of-band management capabilities.

It is designed for network security workloads such as data plane packet processing, IPsec, SSL/TLS, firewall, SASE. The Intel Xeon D processor also enables analytics and inferencing

"Our NaaS vision is rooted in the belief that connectivity should be seamless, ubiquitous, secure and adaptable. We envision a world where businesses can effortlessly scale their wide area networks, adapting to changing demands with agility and precision. NaaS enables this by offering flexible, on- demand network services that are easily customizable to meet the unique needs of each customer. Whether it's expanding bandwidth during peak times, ensuring low latency for critical applications, or providing secure connections for sensitive data, Sparkle's NaaS solutions are designed to deliver unparalleled performance and reliability."

- Daniele Mancuso, Chief Marketing & Product Management Officer, Sparkle

for network security on the edge without the deployment of expensive and power hungry GPUs. The add-in cards based on the reference design allows flexible augmentation and scale to the compute resources network security infrastructure requires.

It's unique form factor allows deployment of additional network security optimized compute in space- and power-constrained data centers and edge locations. By plugging in the NetSec Accelerator into an existing host platform you can significantly improve the total cost of ownership in deploying premium NaaS workloads in existing datacenter infrastructure with minimal impact on space and power consumption.

Arqit SKA and strongSwan Combine for Quantum Safe VPN

Arqit's NetworkSecure Adapter integrates seamlessly with strongSwan, a widely used open-source VPN library, to create an out-the-box quantum-safe VPN. Leveraging Arqit's SKA Platform, this setup generates post-quantum, symmetric pre-shared keys (PPK), which are then passed into the strongSwan configuration. StrongSwan integrates these keys with IPSec using the RFC 8784 standard, making the IPsec tunnel quantum-safe. These keys can be refreshed as often as required.

The NetworkSecure Adapter plays a crucial role in this VPN setup, providing IPsec offloading capability through a process called Vector Packet Processing (VPP), which is fully compatible with Arqit's solution. This compatibility enables the establishment of a quantum-safe IPsec connection without compromising network performance.

Adtran then enabled zero-touch deployment of the solution through Ensemble MANO, a management platform for the creation and deployment of virtualized services, and the Ensemble Connector, a high- performance switching and virtualization platform that hosts multi- vendor VNFs. Since the NetSec Accelerator is managed independent of the host, the Ensemble solution makes management of the NaaS environment seamless. The entire solution can be templated and automatically deployed, allowing the infrastructure to be scaled without the overhead of manual deployment.

This architecture is ideally suited for a quantum-secure point of presence (PoP) server, delivering a high-throughput, quantum-safe VPN connection. For the POC, this advanced system is deployed at Sparkle's Metamorphosis II site – a strategic location serving as the central hub to receive secure connections from other locations, demonstrating the feasibility and efficiency of the solution.

In addition to the robust infrastructure at the PoP, the initiative also leverages universal customer premise equipment (uCPE). These lightweight and inexpensive hardware devices act as the enterprise entry point for the secured VPN tunnel and can be easily deployed at customer sites. With Arqit's software integrated, the uCPE can consume Arqit's encryption keys and connect back to the PoP, enabling a quantum-safe internet link directly at the customer premises. The main share of the security workloads run in the PoP, thus alleviating the need for an expensive server at the enterprise location.

The POC results validated the architecture before its rollout in a production environment. By demonstrating the effectiveness of this quantum-safe VPN solution, Sparkle, Arqit, Intel and Adtran are setting new standards in internet security, ensuring that businesses and consumers alike are protected against evolving quantum threats.

Successful POC Establishes Quantum-safe VPN for Sparkle

Sparkle's implementation of a quantum-safe IPsec VPN solution (see Figure 1) is now a live service, yet it marks a significant advancement in secure internet connectivity. By leveraging the combined strengths of Intel, Adtran, and Arqit,

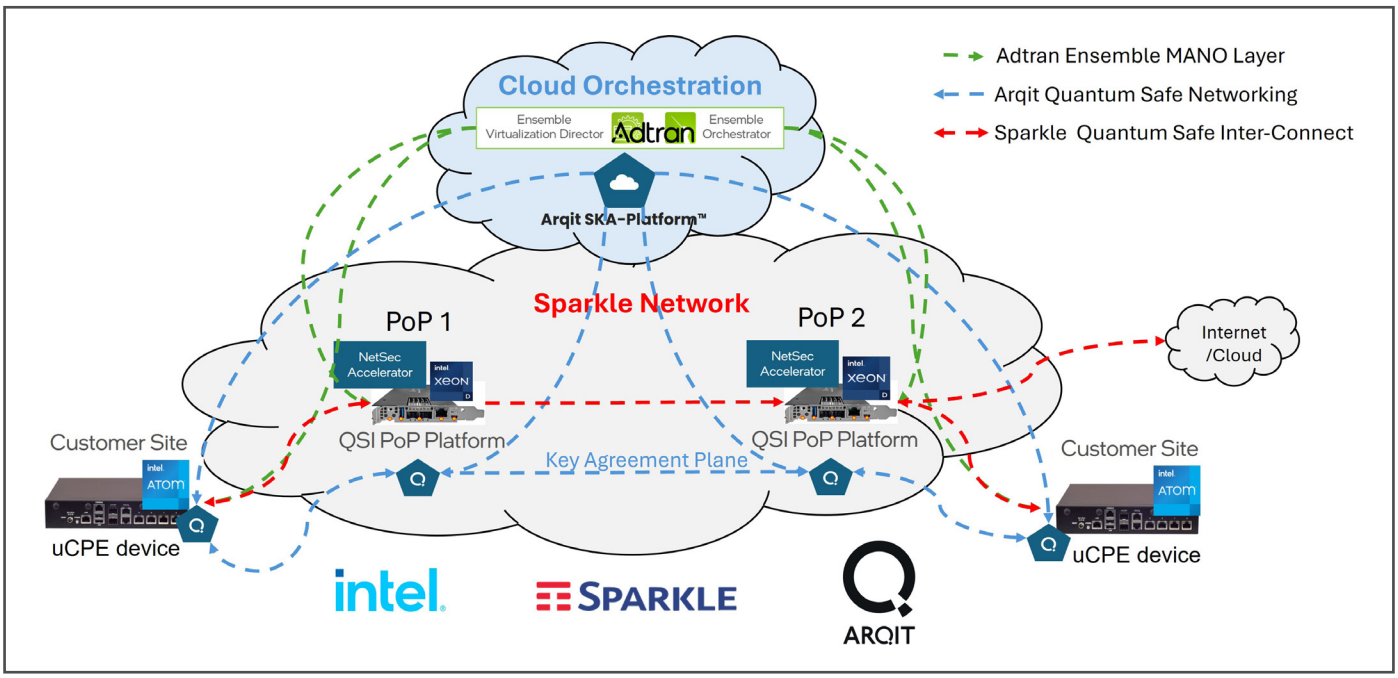

Figure 1. This diagram shows the complete quantum-safe VPN for Sparkle.

Sparkle has set a new benchmark for data security, paving the way for a secure and resilient network infrastructure capable of withstanding the evolving threats posed by quantum computing.

The primary objective of the project was to construct an architecture with a hub-and-spoke topology, validating it through a proof of concept before expanding the network. Exploratory test cases on key creation and policy options driven by strongSwan and Arqit SKA Platform were conducted to ensure the solution's effectiveness.

The outcomes of the POC were significant and multifaceted. Sparkle successfully established quantum-safe IPsec VPN tunnels, ensuring robust, secure communication between data centers. The team became well versed in Arqit's SKA Platform and NetworkSecure solutions, gaining valuable hands-on-experience.

Conclusion

The project demonstrated the effective deployment of quantum-safe IPsec VPN using strongSwan and VPP on Intel NetSec Accelerator Reference Design-based accelerator cards, highlighting its flexible deployment capability in space and power constrained network infrastructure. High-frequency key rotation was enabled, providing forward secrecy without compromising the IPsec tunnel stability. Zero-touch deployment via the Adtran orchestration and management software delivered effective scalability.

The measurable results included secure encrypted tunnels configured between servers at the Athens site, validating the project's core objective. Additionally, the project evaluated Arqit's enhanced quantum-safe encryption alongside existing VPN products, ensuring comprehensive security integration.

The successful zero-touch deployment and configuration via Adtran Ensemble of the Arqit SKA Platform for an open-source VPN scenario using strongSwan and VPP underscored the feasibility of the solution. Finally, the validation of strongSwan's ability to frequently rotate symmetric keys, facilitated by Arqit, demonstrated the project's effectiveness in maintaining continuous, secure communication.

A Quantum-Safe Solution

- Arqit SKA Platform* - post-quantum symmetric cryptographic key generation.
- Arqit NetworkSecure* Adapter – seamless integration of quantum-safe pre- shared keys with existing infrastructure.
- Supermicro IoT SuperServer SYS-211HE-FTNR - VM-ready server powered by Intel® Xeon® processors.
- Intel-based NetSec Accelerator Cards– offload network and security applications to improve throughput and reduce CPU load.
- FD.io VPP (Vector Packet Processing) – accelerated network functions for fast, efficient data plane operations.
- Adtran Ensemble MANO - management platform for virtualized services.
- Adtran Ensemble Connector – high performance switching and virtualization for multi-vendor VNFs.
- strongSwan IPsec VPN – secure VPN tunnel creation with encryption and authentication, supporting post-quantum pre-shared keys (PPK) for quantum safe IPsec connections.

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.
- Optimized TCO using a plug-in acceleration card.

Learn More

Sparkle Launches Its Network as a Service (NaaS) Product Suite with Quantum-Safe over Internet

Arqit SKA Platform*

Arqit NetworkSecure* Adapter

Supermicro IoT SuperServer SYS-211HE-FTNR

FD.io VPP (Vector Packet Processing)

Adtran Ensemble MANO

Adtran Ensemble Connector

StrongSwan IPsec VPN

Intel® NetSec Accelerator Reference Design

Intel® Industry Solution Builders

Notices & Disclaimers

Performance varies by use, configuration and other factors.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See configuration disclosure for details. No product or component can be absolutely secure.

Intel optimizations, for Intel compilers or other products, may not optimize to the same degree for non-Intel products.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

See our complete legal Notices and Disclaimers.

Intel is committed to respecting human rights and avoiding causing or contributing to adverse impacts on human rights. See Intel's Global Human Rights Principles. Intel's products and software are intended only to be used in applications that do not cause or contribute to adverse impacts on human rights.

0125/AL/DJA/PDF Please Recycle 363751-001US