WHITEPAPER

Delivering Secure Connectivity for the Future: Sparkle Launches Quantum-Safe over Internet (QSI)

In collaboration with Arqit, Adtran, and Intel – Pioneering Scalable, Quantum Secure Connectivity for Telecoms Networks

Published by

MOBILE WORLD LIVE

In partnership with

ARQIT Adtran intel SPARKLE

Executive summary

Cyber threats in the telco sector are projected to increase significantly worldwide over the next three years, with signalling and interconnect security becoming top concerns. The rapid digital transformation and vast amounts of data flowing through networks make telcos prime targets for cybercriminals. For example the cyberattack in October 2024[1] on major Telcos, labelled as “the worst telecom hack in our nation’s history - by far” by US Senate Intelligence Committee Chairman Mark Warner. While quantum computing offers transformative potential, it also introduces new risks. Malicious actors are already employing a “Harvest Now, Decrypt Later” strategy, collecting encrypted data now to decrypt once quantum computing can break existing encryption methods. This makes it crucial to prepare for the future of cybersecurity today.

With the rise of quantum-powered cyberattacks, telcos face the risk of compromised networks resulting in malicious data harvesting, regulatory fines, customer compensation and ultimately the erosion of customer trust, resulting in churn. It’s vital for telecommunication operators to strengthen their cybersecurity measures to protect sensitive data, critical infrastructure, and their reputation.

This whitepaper is your guide to making your network quantum-safe today.

Inside, you'll find:

- Understanding quantum threats: Learn how rapid advancements in quantum computing are creating future vulnerabilities in encryption and why "Harvest Now, Decrypt Later" is a real concern.
- Current solutions you can implement and scale now: Explore practical steps, like Symmetric Key Agreement (SKA), to safeguard communications today while preparing for tomorrow.
- Quantum-Safe technologies: Gain insights into the National Institute of Standards and Technology (NIST) post-quantum encryption standards and how organisations can transition to these solutions.
- Innovative approaches to security: Discover the world's first commercial Quantum-Safe Network-as-a-Service (NaaS), developed by Sparkle in partnership with Arqit, Adtran and Intel, which provides secure global communications without compromising VPN performance.

This whitepaper isn't just about understanding the risks; it's a practical guide to protecting your network now. By following these steps, you can ensure your infrastructure and communications are not only enhanced today but are resilient against quantum-powered cyberattacks, securing both your operations and your customers' trust.

The telco cyber threat landscape continues to evolve at rapid pace

New technologies bring new risks

In today's digital world, the threat landscape is evolving at an unprecedented pace. The increasing attack surfaces driven by consumer and enterprise digital transformation, combined with the vast volume of data that transits and is stored in the network, create fertile ground for cyber threats.

The emergence of quantum computing technology offers significant opportunities for advancements; however, it also poses unprecedented risks. As technology advances, so do the tactics and techniques employed by malicious actors, making it imperative for telecommunication operators to stay proactive in their cybersecurity measures.

Understanding the threat landscape and its evolution is crucial for developing robust defence strategies, ensuring the protection of sensitive data and critical network infrastructure. According to a GSMA Intelligence survey (Figure 1) of information and security senior executives within telcos, 65% of European operators surveyed have faced security breaches in the past three years. Of those, 53% reported data loss and theft as the main impact on their organisations, suggesting that long-lived encrypted stolen data may be already at risk. This issue could also affect regions with less stringent data requirements, making data theft and loss harder to detect.

Globally, most operators believe that mobile networks, devices, and cloud network assets are the most susceptible to cyber threats. As edge compute becomes more widespread, the cyber threat risks associated with this asset will increase. Therefore, it is crucial for both operators and enterprises to implement robust security measures to protect network assets, ensure data safety and mitigate potential risks associated with cyber threats.

As shown in Figure 2, the top three cyber threats impacting mobile networks globally are phishing/ smishing for 88% of operators, ransomware for 78% of operators and a bit down the list but still concerning, signalling and interconnect attacks. These threats not only compromise the confidentiality and integrity of sensitive data but also disrupt critical communications services.

Figure 1: More than a half of operators surveyed globally rated the threat level across mobile networks, devices and cloud as either very high or high

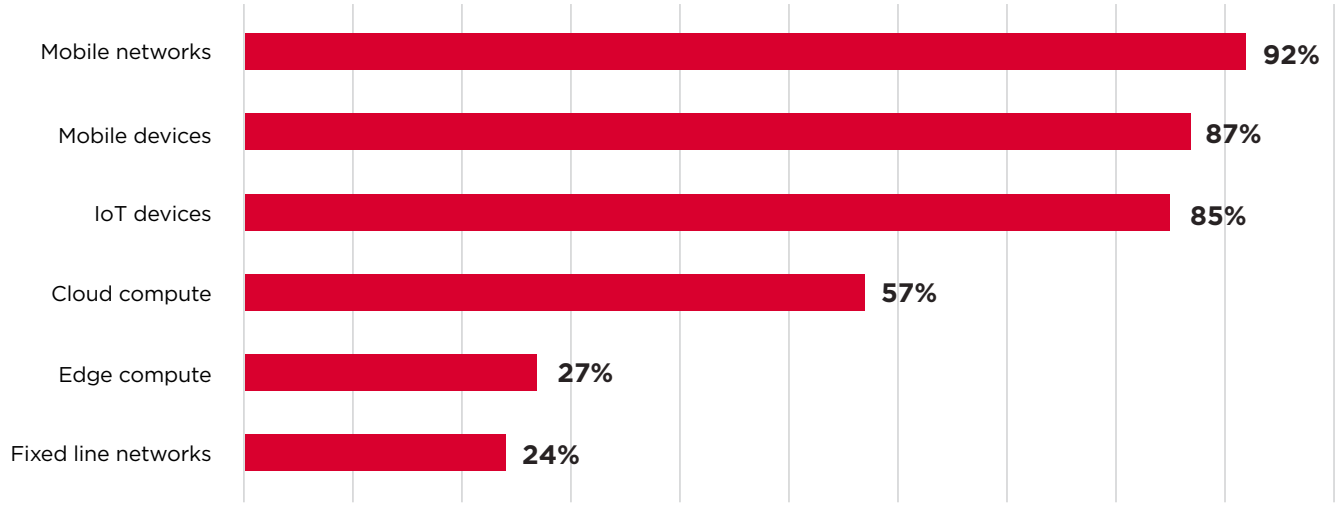


Figure 1: Source: GSMA Intelligence

Over the next three years, the landscape of cyber threats targeting network assets is expected to become increasingly challenging. Phishing/Smishing and Distributed-Denial-of-service attacks (DDoS) will be of major concern.

The advent of quantum computing will exacerbate these threats as it has the potential to break current encryption algorithms, making it easier for malicious actors to intercept and decrypt information stored and/or transferred in the network.

With quantum computers, vast amounts of data, including currently encrypted data, will be at risk. Some malicious actors are using a 'Harvest Now, Decrypt Later' strategy, where they collect, and store encrypted data now with the intent to decrypt it when cryptographically relevant quantum computers will become available.

As telecommunications operators deliver to enterprise verticals and support their business operations, the risk of being exposed to quantum-powered cyberattacks should matter to them. Beyond their operations, telcos should think about the security dynamics of their customers, in particular enterprise verticals and B2B end-users, which even before 5G, have proven to be a great source of business growth and profitability.

Figure 2: Top three cybersecurity threats affecting mobile networks globally

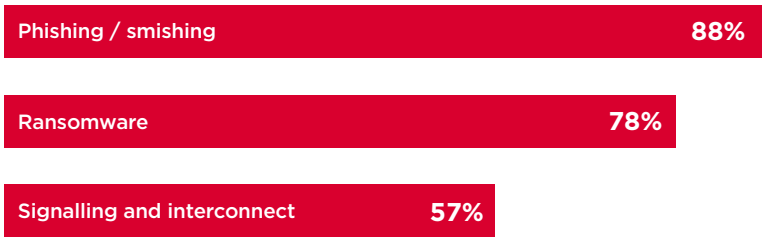
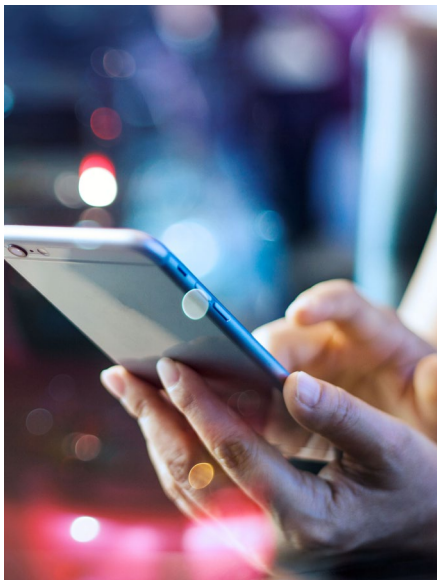


Figure 2: Source: GSMA Intelligence



Recent advancements in quantum computing

In a recent survey of quantum computing industry experts, over 50% of respondents indicated that the pace of development is faster (41.2%) or much faster (10.2%) than they expected[2].

Figure 3: Over the next three years, there will be a considerable net rise in cyber threats impacting network assets

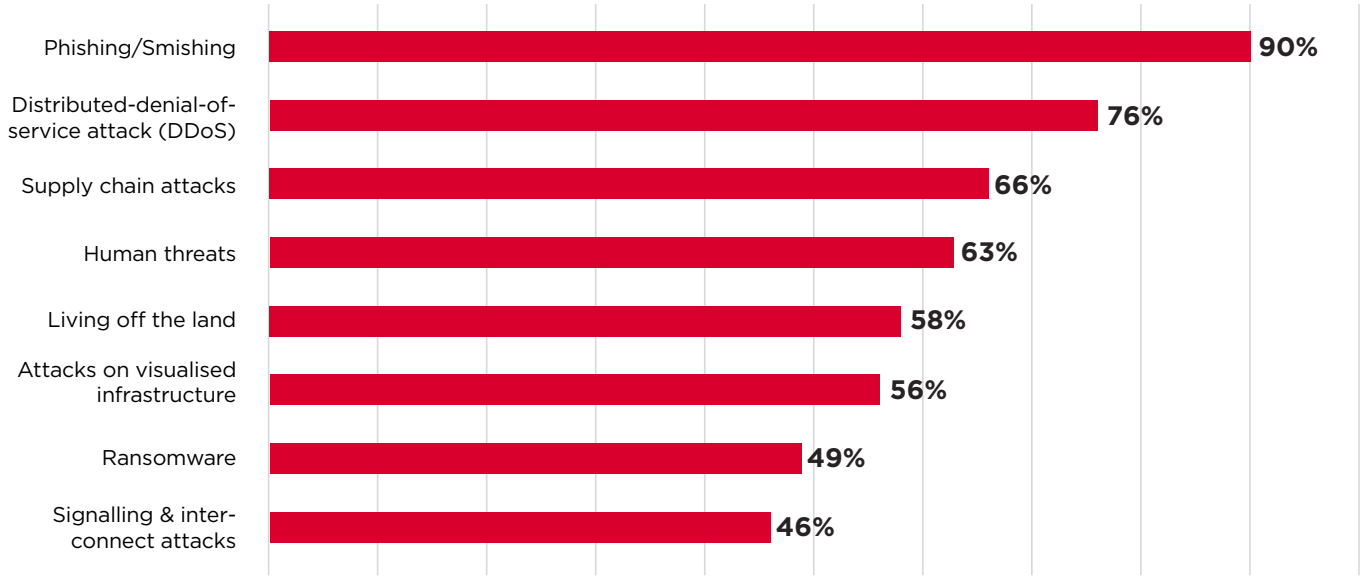


Figure 3: Source: GSMA Intelligence

Assessing the quantum computing security threat

As shown in Figure 4, the number of qubits, the basic unit of information in a quantum computer, that can be supported by quantum hardware is growing exponentially. This is thanks to significant investment by several major countries. For example, the US has invested over $3.5 billion in quantum computing research and development since 2020[3]. At the same time, China has also made significant advances lately that raised fears that it was close to breaking RSA-2048 encryption[4]. However, a closer look at the research reveals that this is less of an immediate threat.

Nevertheless, as rapid progress is being made in the field of quantum computing, it is becoming increasingly clear that current encryption algorithms that were previously thought unbreakable will be under threat. It is expected that quantum computers will become stable, affordable, and powerful enough to decrypt communications using current encryption technology. According to USAID, the most likely scenario is a breakthrough in the next decade with the possibility that a breakthrough could occur faster within the next 3 to 5 years[6].

The quantum security threat posed by Harvest Now, Decrypt Later strategies

While it might be comforting for some that the potential threat from quantum computing can be a decade away, it ignores the fact that malicious actors are already harvesting in anticipation of the availability of quantum computing.

The "Harvest Now, Decrypt Later" strategy means communication data can be stored today with a view to decrypting it later using quantum computing. While not all communication holds its value for a long time, there is a great deal

Figure 4: Number of qubits supported by quantum hardware growing exponentially[5].

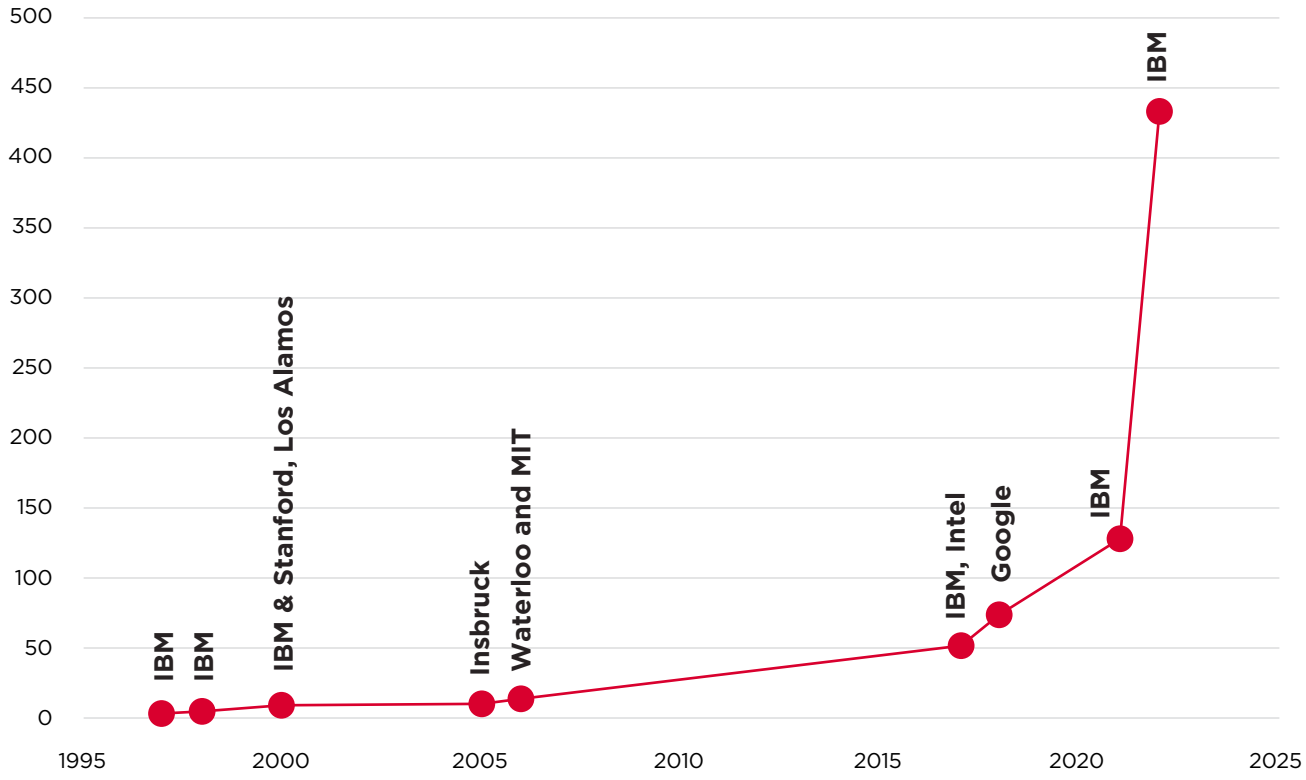


Figure 4: Source: Number of qubits supported by quantum hardware growing exponentially

of information exchanged by organisations that is highly sensitive and valuable, sometimes connected to national security or a significant financial implication, for many years. It is for this reason that several major governments are investing heavily in quantum computing initiatives and understanding the impact of quantum computing in general.

Recent advances in quantum-proof solutions

Since 2016, the National Institute for Science and Technology (NIST) has been engaging with experts from around the globe to identify public key encryption algorithms that can withstand cyberattacks from quantum computers. In August 2024, NIST standards for three of four targeted algorithms were announced and the final algorithm was expected to be standardised in the following months.

The four targeted algorithms were selected from a list of 82 algorithms proposed from 25 countries.

The availability of these new standards is a significant contribution in securing asymmetric public key algorithms, which today are vital to secure Internet communication, finance transactions, cryptocurrencies and more.

In December 2024, Australia announced their commitment to drop some cryptographic standards such as SHA-256, RSA, ECDSA and ECDH by 2030. This plan emerged over fears as stated by the Australian Signals Directorate (ASD) of the "projected technological advances in quantum computing".

New algorithms take time to deploy

It should also be noted that deprecation and replacement of incumbent algorithms in commercial solutions can take much longer than a decade and pose a security threat for many years. For example, the digital signature verification algorithm MD5 was first broken in 2005 but has been exploited several times since then and is still part of solutions, such as content management systems, today.

A similar scenario involves SHA-1, which was also shown to be cryptographically weak in 2005, deprecated by NIST in 2011, but continued to be part of Microsoft solutions until 2020. NIST have noted that complex systems need more migration time and have set a deadline of 2030 to phase out use of SHA-1.

Important things to keep in mind when assessing the threat from quantum computing and the availability of new quantum-safe asymmetric key algorithms:

- MD5 and SHA-1 were both believed to be cryptographically strong when introduced, but were subsequently proven to be vulnerable, which shows that any public key algorithm can potentially be broken
- Once broken, it can take several decades before the algorithms are replaced, leading to significant vulnerabilities that can be exploited
- One of the reasons why algorithms persist even after they are proven to no longer be trustworthy is because migrating to a new algorithm is costly and time consuming

Quantum-proof solutions that can be deployed today

Public Key Infrastructure (PKI) is both important and widespread, which is why NIST has focused on establishing consensus on quantum-proof algorithm standards that can be widely adopted and deployed. A complementary solution that is also accepted by NIST and many other cybersecurity experts as being quantum-safe is Symmetric Key Agreement (SKA). While asymmetric public key algorithms, like those used in PKI, rely on a public and private key mechanism, SKA uses one secret key that is known to each party but not exchanged during communication. This makes communication in theory impossible to decipher, even for quantum computers.

In addition, SKA is relatively cost-effective to implement and deploy and is available today. Arqit is the first vendor to provide a proven, commercial, quantum-proof SKA solution that can be deployed quickly on Intel-based network infrastructure. Together with partner Intel, Arqit has enabled Sparkle to deliver the first quantum-proof Network-as-a-Service (NaaS) offering that can provide future-proof security for public and private communications both effectively and cost-efficiently.

The innovations provided by Arqit, Intel and Sparkle provide a viable path forward for quantum-proof communications that can be deployed today. The collaboration between Arqit, Intel and Sparkle is leveraging the unique expertise and technology of each party to deliver a ground-breaking commercial solution that can be deployed at scale.

How Sparkle developed a Quantum-Safe Network-as-a-Service

Sparkle is the first connectivity provider in the world to offer a commercial, quantum-safe solution according to the Network-as-a-Service (NaaS) model. The solution, already tested in commercial networks on a number of different use cases.

Key advantages of NaaS:

- It is the first commercial quantum-safe connectivity solution to be deployed at scale
- There is no performance degradation to highly optimized VPN connections while enabling quantum-safe encryption
- It is based on cost optimized compute platforms based on Intel technologies
- Zero-touch provisioning has been enabled by Adtran

In short, the solution provides all the benefits of quantum-safe encryption at the touch of a button for Sparkle customers with no trade-off in performance or convenience.

Sparkle's first IPsec-based VPN service with quantum-safe encryption offers an additional feature for customers who need to communicate sensitive data globally, but more use cases are on Sparkle's radar including quantum-safe Cloud Connect, capacity and IoT. All Sparkle quantum-safe solutions are offered on-demand through Sparkle NaaS platform in order to optimise the network cryptography agility and observability, minimising the upgrade time towards a quantum- safe network.

The Sparkle quantum-safe NaaS solution is made possible by unique solutions from partners Arqit, Adtran and Intel. Arqit provides an enterprise-grade solution for post-quantum symmetric cryptographic key generation for secure authentication and data encryption. Intel provides CPU, Ethernet controller/adapters, tuned IPsec libraries, and other accelerator technologies, including the unique NetSec Accelerator card (based on Intel® NetSec Accelerator Reference Design), which is a high-performance server on a PCIe card that hosts Virtual Network Functions (VNFs) in the Sparkle NaaS solution.

Sparkle, Arqit, Adtran and Intel have been collaborating for some time on validating the feasibility of quantum-safe VPN connectivity with several successful trials and Proof-of-Concepts. However, the goal of the collaboration was not just to show that quantum-safe connectivity is possible. Sparkle had the ambition from the beginning to offer the first commercial quantum-safe connectivity service globally.

This has resulted in a commercial offering that is reliable, easy to deploy and does not affect highly optimized VPN performance.

It is the perfect example of a NaaS ecosystem, where service providers and technology companies work in synergy to deliver on-demand end-to-end services that are future-proof.

The Quantum-Safe NaaS solution

The Sparkle quantum-safe NaaS solution today provides secure IPsec-based VPN connectivity between global end-points as a service that can be adopted quickly and easily by customers. The NaaS solution addresses use cases in the following areas

1. End-to-end private connectivity: from customer site to customer site. VPN customers can upgrade their existing (and already robust) encryption level, to protect highly sensitive data.
2. Data Centre-to Cloud: securing the transfer of sensitive data from a Data Centre (DC) to a Public Cloud Providers (PCP) through the Sparkle Cloud Connect offering. As many sensitive applications are hosted by PCPs, there is a need for securing not only the transfer of the exchanged data, but also the data inside the DC and PCP environments. This requirement will be important in networking for AI use cases, as the training of AI engines requires massive amounts of data to be transferred to AI regions, necessitating absolute integrity. As a result, securing AI source of information before AI training will be critical.
3. POP-to-POP: connectivity between DCs and edge locations over the Internet or VPNs to secure any transfer of data within the enterprise network.
4. IoT: the deployment of symmetric post-quantum safe encryption for termination points of the Sparkle IoT Solution.
5. Capacity: for highly regulated verticals including government, finance and military customers deploying full capacity services and even dark fibres.

In its initial release, quantum-safe connectivity is provided as an add-on option to IPsec VPN connectivity for customers who need to protect critical communications both today and in the future. The high throughput IPsec VPN solution is based on a strongSwan or vendor specific VPN implementation delivered on Intel platforms. Arqit provides an overlay encryption solution taking advantage of strongSwan VPN support for upgrading existing cryptography algorithms to post-quantum cryptography. This allows a Post-quantum, Pre-shared Key (PPK) to be generated at VPN endpoints in addition to authentication methods provided by IKEv2.

The PCIe accelerator cards based on Intel® NetSec Accelerator Reference Design provides a powerful, compact server-on-a-card for hosting various Virtual Network Functions (VNFs). This includes the lightweight Arqit NetworkSecure™ Adaptor, which is responsible for seamless integration of quantum-safe pre-shared keys with existing infrastructure. The accelerator also hosts FD.io Vector Packet Processing (VPP) accelerated network functions for high throughput, efficient data plane operations supporting the establishment of strongSwan VPN tunnels. This ensures that there is zero performance degradation for VPN services supporting Arqit quantum-safe encryption.

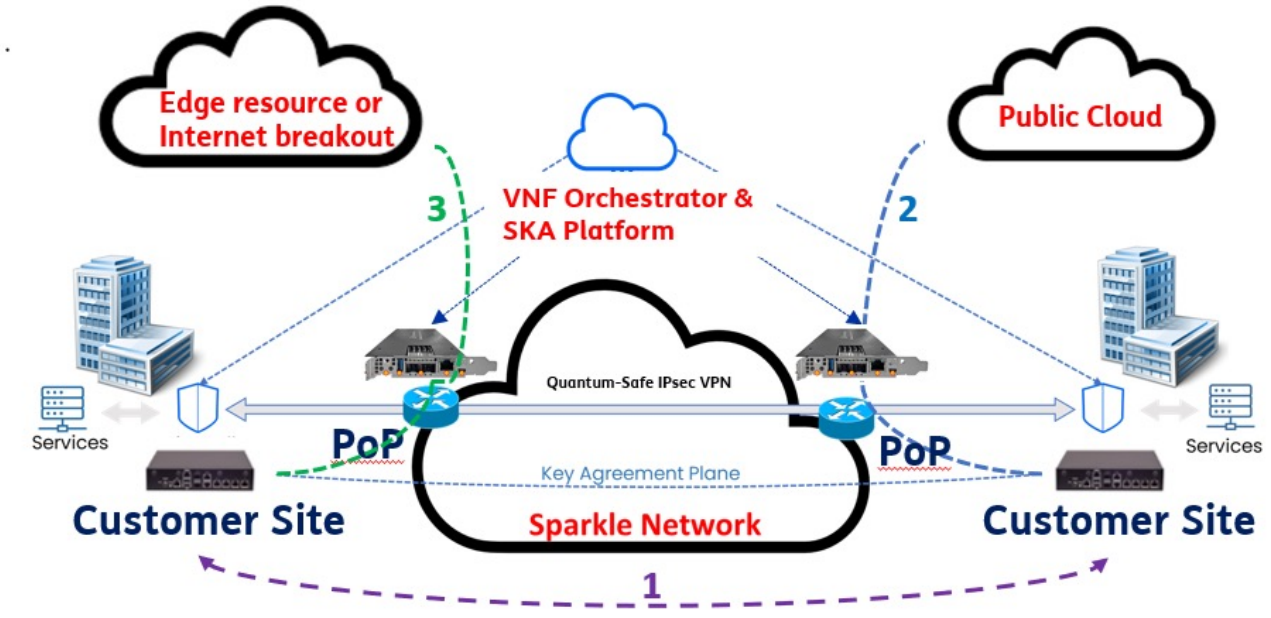
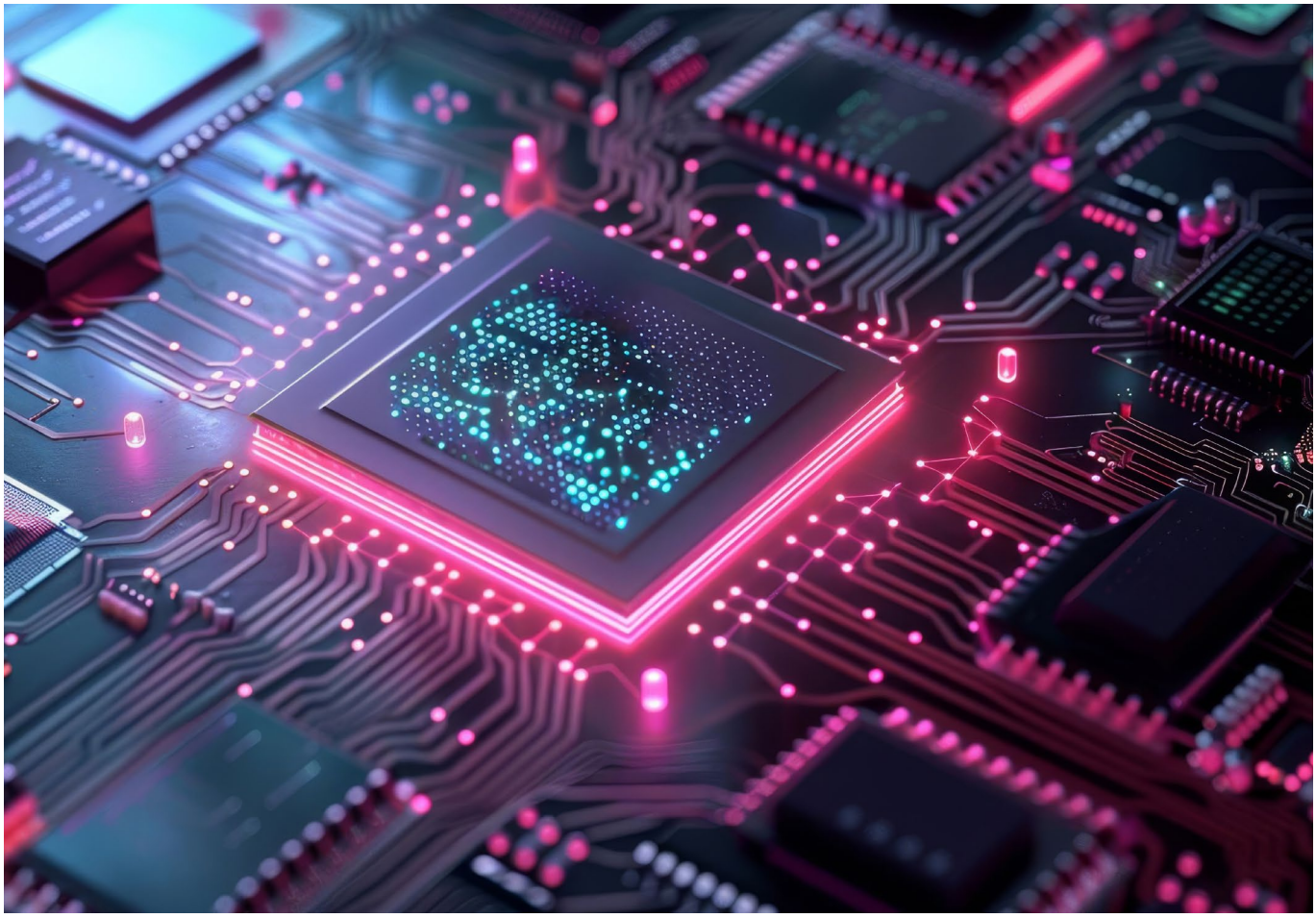


Figure 5: NaaS Quantum-Safe over Internet Intial Use Cases



The deployment and management of virtual network functions with zero-touch automation is provided by a MANO management and orchestration software.

The advantage of this approach is that post-quantum cryptography can be deployed quickly, easily, and at scale as an add-on function operating on TCO optimized PCIe accelerator card. An additional advantage is that the performance overhead is non-existent to highly optimized VPN data plane performance delivered by Intel.

Post-quantum encryption at scale

The Arqit solution is the first post-quantum cryptography solution to be deployed effectively and cost-efficiently at scale. While there are a number of SKA solutions and technology available, Arqit is unique in focusing on ease of deployment at scale with a now proven technology and approach.

The Arqit post-quantum cryptography solution consists of two major entities:

- Arqit SKA-Platform™
- Arqit NetworkSecure™ Adaptor

Arqit SKA-Platform

Arqit SKA-Platform manages permissions for endpoints in the network. In essence, the platform controls which devices and users are allowed to communicate with each other. Endpoints in the network that use Arqit post-quantum cryptography first register with Arqit SKA-Platform and every endpoint is regularly authenticated thereafter. Communication between endpoints and the platform is performed over an out-of-band secure channel separating user communication from encryption key administration. Unlike conventional encryption methods, Arqit's SKA-Platform enables rapid deployment across diverse environments without disrupting existing workflows.

Arqit NetworkSecure Adaptor

Arqit NetworkSecure Adaptor is lightweight software that is easy to deploy in any environment. In the Sparkle NaaS solution, the Arqit NetworkSecure Adaptor is running as a VNF on an Intel-based NetSec accelerator card configured in an Intel-based standard server.

The Adaptor is the platform for generating the symmetric keys for authentication and encryption and is coordinated by the Arqit SKA-Platform. It injects keys into the strongSwan VPN over an existing IP network, offering a post-quantum overlay for customers who need to protect critical data.

How post-quantum symmetric key encryption is established

The process for establishing post-quantum symmetric key encryption, is as follows:

1. The Arqit NetworkSecure Adaptor is deployed to endpoints as a VNF running on Intel-based NetSec accelerator cards using Adtran zero-touch provisioning.
2. Arqit NetworkSecure Adaptor then registers with Arqit SKA-Platform where it is provisioned with the correct permissions to use the post-quantum encryption service.
3. A root key, known as a "bootstrap key", is delivered to each Adaptor over a secure, out-of-band communication channel, which is then used in API calls to register the endpoint and authenticate subsequent interactions. This supports a zero-trust security model. Each time the endpoint authenticates with Arqit SKA-Platform the key is transformed offering an additional level of protection.
4. When two endpoints want to communicate, they must first authenticate and establish a quantum-safe tunnel with Arqit SKA-Platform. Each endpoint then receives key material from the platform, which is used by the endpoints to synthesise the final symmetric key for communication. This approach ensures that the final key is not known to the Arqit SKA-Platform.
5. The symmetric keys are then used to encrypt data communication over the VPN where a variety of cyphers can be used, such as AES-256.

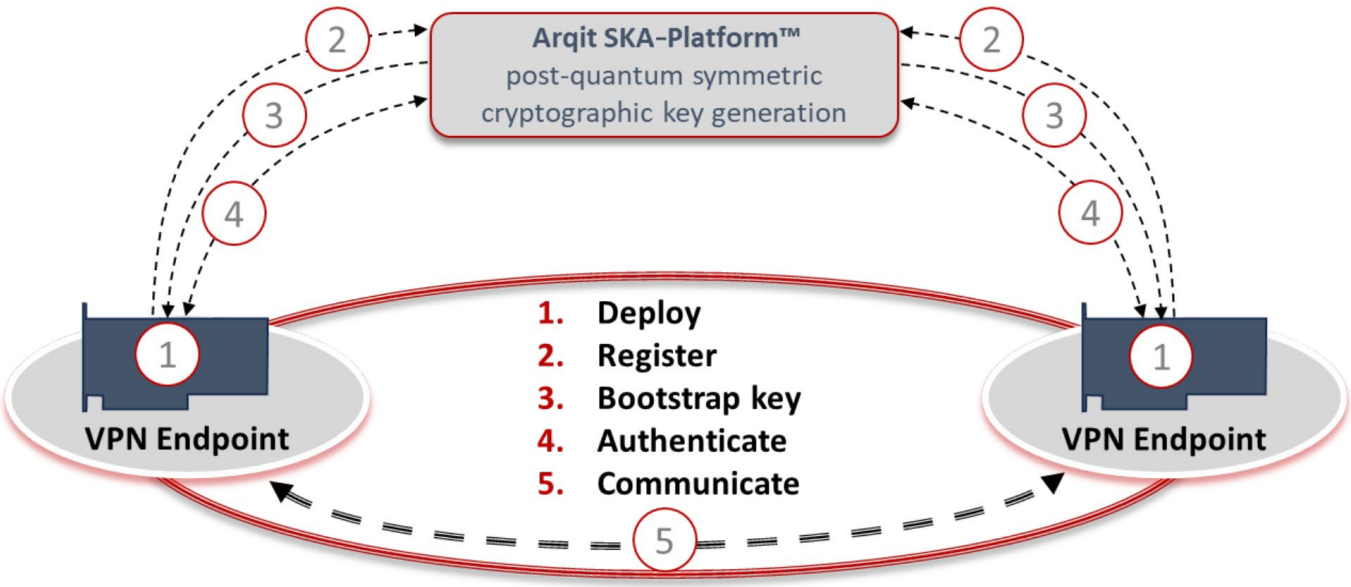


Figure 6: Establishing post-quantum symmetric key encryption

Powerful yet compact edge computing

While Arqit NetworkSecure Adaptor is lightweight, it still requires hardware that is powerful enough to ensure minimal impact on VPN performance. The Intel NetSec Accelerator Reference Design provides a compact, yet powerful compute platform for this purpose with proven performance.

The NetSec accelerator card is based on the Intel NetSec Accelerator Reference Design[7], which provides a blueprint for PCIe cards with the compute resource and capability to support full orchestration and management of network and security workloads. This includes IPsec, SSL/TLS, firewall, SASE, analytics and inferencing for network security.

The NetSec accelerator card is based on an Intel® Xeon® D SOC with 32GB memory and 100GB SSD on-board storage. The 100 Gigabit Ethernet is provided by Intel® Ethernet Controller E810.

This provides a complete server-on-a-card compute platform that can be deployed in any COTS server, especially effective in edge deployments when space, power, and management resources become scarce.

The NetSec accelerator card can support a virtualized environment with several VNFs making it a cost-efficient and reliable augmentation to existing compute platforms running VNFs.

The combination of VPP and strongSwan hosted on NetSec accelerator cards provides a high-performance networking software stack that can ensure full duplex throughput up to 50 Gigabit per second performance even when supporting quantum-safe encryption.

Sparkle, Arqit, Adtran and Intel have performed extensive testing of the combined solution during 2023 and 2024 to ensure that there is no performance impact for VPNs. In these tests[8], performance was compared for VPNs using PKI, the current method for VPN encryption, and performance using Arqit PPK.

Using the Intel-based NetSec accelerator card for Arqit NetworkSecure Adaptor, there is no impact on the performance of the IPsec tunnel. Thus quantum-safe networking on Intel-based infrastructure can be achieved without performance degradation and without modifying the infrastructure in place.

Quantum-Safe over Internet service from Sparkle

The Quantum-Safe over Internet (QSI) service is now available to Sparkle customers. Launched in October 2024[9], the new service enables Sparkle customers to upgrade their Internet Access VPN connectivity with quantum-safe encryption. This is the first product in Sparkle's NaaS suite, which soon will include all other use cases.

With QSI and NaaS, Sparkle has achieved its goal of becoming the first connectivity provider to offer a quantum-safe VPN commercial service at scale and in a flexibly consumable way. This provides Sparkle with a significant head-start over competitors with a platform that can support additional quantum-safe use cases.

QSI provides real value for Sparkle's ecosystem

Sparkle, while innovating the approach to quantum-safe encryption through NaaS, is committed to developing the quantum security ecosystem through top vendor engagement and standardization activities.

Sparkle, Arqit, Adtran and Intel collaboration establishes new era in secure communications

The successful collaboration of Sparkle, Arqit, Adtran and Intel in delivering Sparkle QSI and NaaS commercial services at scale has delivered a number of industry firsts:

- The first commercial quantum-safe connectivity solution
- The first scale deployment of a quantum-safe encryption solution
- The first scale deployment of PCIe server-on-a-card solution capable of supporting quantum-safe encryption without affecting VPN performance
- A successful collaboration of a connectivity provider and technology vendors delivering a quantum-safe encryption solution at scale

The collaborative effort proves that a commercially viable, quantum-safe encryption solution can be delivered at scale today based on symmetric key algorithms. It provides a blueprint for other connectivity providers and technology vendors in how to bring new secure communications solutions based on post-quantum cryptography to market quickly and effectively.

Connectivity providers and other telcos can use the Sparkle case as inspiration for new value-adding services that address both cybersecurity challenges of today and tomorrow.

Implications for telecom operators and their enterprise customers

The best time to prepare is now

Any network component utilising a protocol that is susceptible to future quantum attacks and deemed sufficiently exposed must be made quantum-safe. This includes network components using protocols such as IPsec, TLS, HTTPS, authentication mechanisms based on public/private keys, PKI and digital certificates.

Governments are already planning and advising businesses to transition to Post-Quantum-Cryptography (PQC). In the United States, the 2023 national cybersecurity strategy[10] advises the private sector to ready its own networks and systems for a post-quantum future. Likewise, the European Union has issued recommendations urging member states to develop a comprehensive strategy for the adoption of post-quantum cryptography[11].

According to the GSMA Intelligence operator survey, 69% of operators surveyed globally believe that in the next three years government regulations for network security will become either more stringent or significantly more stringent.

This suggests that an increasing number of governments will eventually mandate that both operators and enterprises comply with specific quantum-safe requirements.

Cyber attacks have the potential to inflict disastrous consequences across every sector. The urgency of this threat is underscored by a GSMA Intelligence survey, which reveals that the public sector, financial services and healthcare are currently the most vulnerable to cyber threats, and in addition, they could be already vulnerable to quantum-powered attacks[12].

Figure 7: In the next three years government regulation for network security will become either more stringent or significantly more stringent for 69% of operators globally

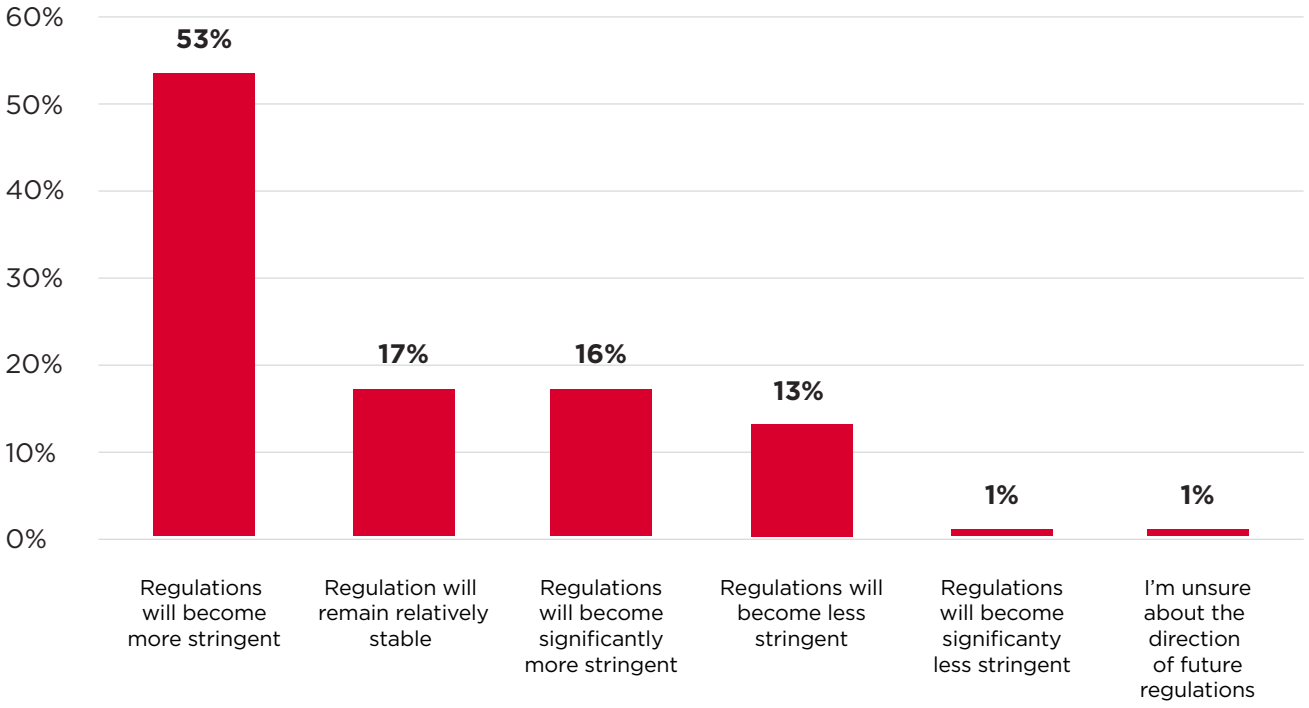


Figure 7: Source: GSMA Intelligence

In response, enterprises recognize the importance of cybersecurity now and in the future, making it a top priority in their digital transformation spending[13]. This prioritisation is evident in critical sectors such as financial services, healthcare, manufacturing, retail, transportation and energy and utilities.

Adopting next-gen quantum-safe encryption solutions, such as the Sparkle quantum-safe connectivity solutions, can greatly enable enterprise digital transformation through its seamless network integration, ensuring both cost-efficiency and long-term data security.

Telecommunications companies must address the security dynamics facing their enterprise customers and B2B end-users. Since before the arrival of 5G, operators understood that enterprises represented the best opportunity for business growth and profitability.

To meet the security demands of early adopters, service providers delivering private mobile networks to enterprise customers should ensure their network equipment is quantum-ready. This is especially vital for sectors handling long-term encrypted data, such as banking, healthcare, insurance and the public sector.

In instances where enterprise customers, particularly SMEs, are slow to take proactive measures against quantum threats, initial demand for quantum-safe solutions may be limited. During this transitional phase, service providers can offer early quantum-safe service proposition to those customer groups, who for certain reasons, would welcome a 'premium level of protection 'until the level of protection becomes 'standard' for all[14].

With a slow ARPU growth in the connectivity business, revenue diversification remains an imperative for operators.

As demand expands for solutions across a range of technology areas the B2B segment offers significant growth opportunities.

According to GSMA Intelligence research, the total telcos enterprise addressable market beyond core telecom is estimated to reach almost $1 trillion by 2030[15] and security services strongly factor into this[16], with 73% of telcos surveyed claiming security services are either very or extremely important to their enterprise strategy.

By offering innovative scalable quantum-proof solutions to enterprise customers, telecommunications companies can unlock substantial revenue opportunities. Embracing post-quantum cryptography solutions now enables telcos to foresee the market demand for next-gen post-quantum encryption solutions, positioning telcos as leaders in compliance and innovation.

Figure 8: Enterprise service portfolio and importance rankings

How important are security services to the success of your enterprise strategy?

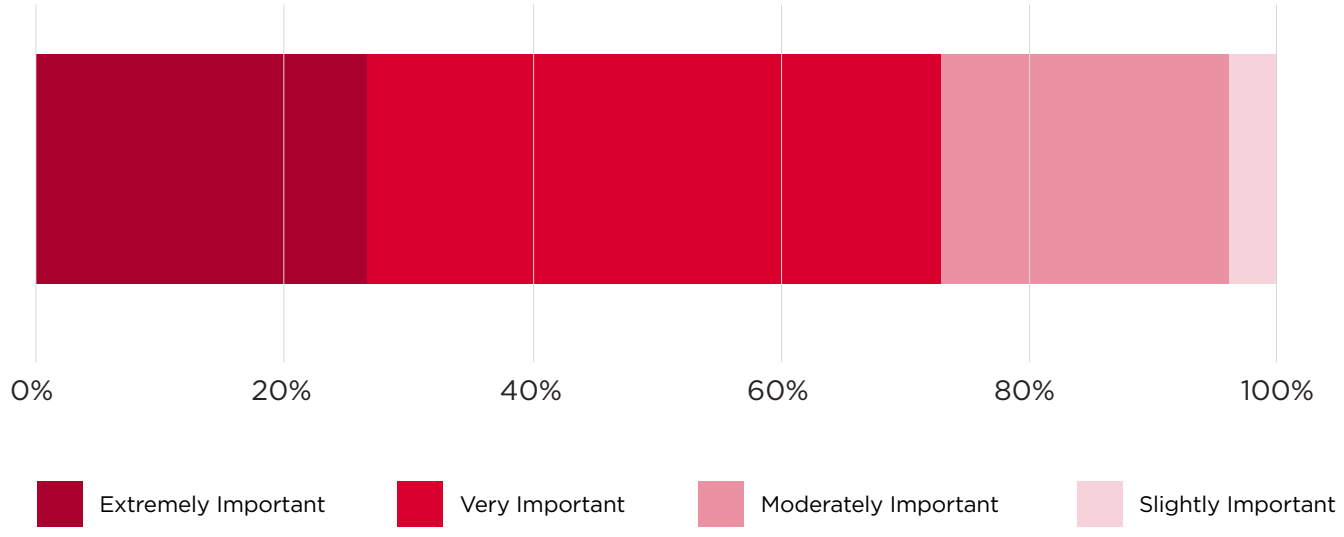


Figure 8: Source: GSMA Intelligence

Sources

[1] Source: Examining the 'Worst' Telco Cyber Attack in US History - https://cybermagazine.com/articles/examining-the-worst-telco-cyber-attack-in-us-history

[2] Source: 2024 Quantum Computing Report: The Current & Future State

[3] Source: Quantum Computing: Developments in the UK and US | Inside Privacy

[4] Source: Chinese Quantum Computing Advance Shows Progress, Innovation, But Not an Imminent Threat to Encryption

[5] Source: "Quantum Monte Carlo for Economics: Stress Testing and Macroeconomic Deep Learning", Vladimir Skavysh, Sofia Priazhkina, Diego Guala, Thomas R. Bromley, ResearchGate

[6] Source: Quantum Futures: International Development and the Quantum Computing Transition

[7] For more details see: Intel NetSec Accelerator Reference Design https://www.intel.com/content/www/us/en/products/docs/processors/atom/netsec-accelerator-reference-design-solution-brief.html

[8] For more details see: Arqit and Intel Test Post Quantum Cryptography (PQC) Solution https://networkbuilders.intel.com/solutionslibrary/arqit-intel-test-post-quantum-cryptography-pqc-solution

[9] Source: Sparkle Launches Its Network as a Service (NaaS) Product Suite with Quantum-Safe over Internet https://www.tisparkle.com/media/press-release/sparkle-pioneers-network-service-naas-quantum-safe-internet-use-case

[10] Source: National Cybersecurity Strategy March 2023, The White House https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[11] Source: Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

[12] Source: 'When and how to prepare for post-quantum cryptography', McKinsey, 2022

[13] Source: 'The rise of digital industries: navigating enterprise needs, investments and supplier decisions', GSMA Intelligence, 2024

[14] Source: Post Quantum Telco Network Impact Assessment Whitepaper https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/08/PQ.1-Post-Quantum-Telco-Network-Impact-Assessment-Whitepaper-Version1.0.pdf

[15] Source: The opportunity for operators in B2B technology services https://data.gsmaintelligence.com/research/research/research-2024/the-opportunity-for-operators-in-b2b-technology-services

[16] Source: The opportunity for operators in B2B technology services', GSMA Intelligence, 2024




Arqit Quantum Inc. supplies a unique encryption Platform as a Service which makes the communications links of any networked device, cloud machine or data at rest secure against both current and future forms of attack on encryption – even from a quantum computer. Compliant with NSA standards, Arqit's Symmetric Key Agreement Platform delivers a lightweight software agent that allows devices to create encryption keys locally in partnership with any number of other devices. The keys are computationally secure and operate over zero trust networks.

Find out more at www.arqit.uk

ADTRAN Holdings, Inc is the parent company of Adtran, Inc., a leading global provider of open, disaggregated networking and communications solutions that enable voice, data, video and internet communications across any network infrastructure. From the cloud edge to the subscriber edge, Adtran empowers communications service providers around the world to manage and scale services that connect people, places and things.

Find out more at www.adtran.com

Intel is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better.

Find out more at www.intel.com

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. A major player in the submarine cable industry, Sparkle owns and manages a network of more than 600,000 km of fiber spanning from Europe to Africa and the Middle East, the Americas and Asia.

Find out more at www.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.