WHITEPAPER

Accelerating the Journey to Data Sovereignty and Quantum-Safe Networks with Arqit and Intel

Published by

MOBILE WORLD LIVE

In partnership with

ARQIT intel.

Introduction

In the digital world, trust is the bedrock on which business success is built. Customers must trust the companies they interact with to keep their data safe. And business leaders must have confidence that transformative new services can be introduced without increasing the risk of breaches, disruption and compliance failures. But achieving this kind of assurance is getting harder as the cyber-attack surface grows.

Organisations as diverse as telcos, retailers and financial institutions are looking to technology to give them an advantage. In a world beset by geopolitical and economic uncertainty, investments in cloud infrastructure, IoT, cloud-hosted AI services and flexible working are not just preferable – they're increasingly essential to deliver the resilience and agility modern organisations need.

But with digital transformation comes potential risk.

It's creating new data sovereignty challenges as organisations look for solutions to guarantee the confidentiality, portability and availability of data stored across distributed environments. Many are starting to realise that residency alone isn't enough to satisfy regulators and their own resilience requirements.

Then there's the rapidly approaching era of cryptographically relevant quantum computers (CRQCs). Governments have set timelines for the transition to post-quantum cryptography (PQC), with most wanting migration to be completed by 2035. With around a decade to go, this might seem like plenty of time. But the scale and complexity of the challenge means that, for many large businesses such as telcos, these efforts need to start now. The emergence of harvest-now-decrypt-later (HNDL) and trust-now-forge-later (TNFL) attacks makes the process even more urgent.

A recent Bain & Company study reveals a significant gap in cybersecurity readiness. Some 90% of responding organisations say they are not prepared to defend against quantum computing-related threats. Only 10% have a roadmap to quantum-safety. That's despite nearly three-quarters (71%) expecting quantum-powered attacks within five years and almost a third claiming it could be as soon as three.

This whitepaper will light the way to data sovereignty and quantum safety. We'll explain what's at stake, and how to overcome some common cost, complexity and scalability challenges with Arqit NetworkSecure™.

The coming quantum threat

Threats to data in transit are nothing new. Successful man-in-the-middle MITM attacks can stem from weak cryptographic algorithms, mismanaged certificates, compromised Certificate Authorities (CAs) and much more. But an even bigger challenge lies ahead.

When CRQCs finally emerge, entities with the finances and skill to operate them will be able to run Shor's Algorithm. Doing so means they'll be able to solve the problems on which asymmetric encryption derives its security within just hours or minutes, as opposed to the millions or billions of years it takes conventional computers. It will be the end for public key cryptography as we know it.

However, CRQC threats also present in more insidious ways:

HNDL: It is likely that state actors are already sweeping up large quantities of data encrypted via public-key cryptography, with a view to unmasking it once CRQCs become available. Long-lived data like pharma secrets, financial information and healthcare records are particularly at risk. The threat exists today, not in five years' time. And the only way to mitigate it is by beginning the transition to quantum-safety immediately.

TNFL: This is like HNDL but for digital signatures. It posits that threat actors will be able to crack and then forge the signatures and certificates we trust today, once CRQCs arrive. Thus, the foundational mechanisms we use today to ensure data integrity, authenticity and security will no longer be trustworthy.

There are arguably even starker implications for digital security. Signatures are used to form the root of trust for software updates, device identities and communication protocols. If they can be forged at will in the future, threat actors could silently push malicious software updates, forge commands on critical systems and alter records. The trust on which the digital world is built will collapse, with potentially catastrophic impacts.

If signatures on firmware or software need to be valid for an entire device lifecycle, planning may need to begin now - especially for long-lived kit.

Beyond security: what else matters

Finding a way to mitigate such threats today should therefore be a priority for global organisations. But there are other considerations. These include:

Form factor: Workloads are getting pushed out to the edge in ever-greater volumes to support AI-powered apps and services. While this might offer speed, cost efficiency and even sovereignty benefits, it reduces the space and power available for quantum security solutions. Size and power efficiency can therefore be important.

Scalability: No two organisations are the same. But some, including telcos, will require quantum-safe communications that scale to thousands of endpoint devices. Organisations managing large numbers of AI agents will also be looking to scale their efforts. Many may struggle to generate encryption keys over a network and will need to do so locally.

Cost: Persistent economic uncertainty means many organisations are looking to achieve quantum-safety as cost-efficiently as possible. Some will not need to support more than a small number of devices, and will therefore prefer smaller form factors which require less upfront investment and power.

Compliance: Organisations should ensure any approach aligns with recommended best practices for quantum safety, including NSA, NIST, CSNA 2.0 and FIPS 140-3 standards.

Speed and simplicity: Quantum-safety is the goal for all data flows. But solutions that end up worsening latency may end up doing more harm than good. IT leaders want to support the business not just by making encrypted streams unhackable, but by ensuring that network performance is relatively unaffected.

They also need solutions that integrate neatly with existing infrastructure, particularly endpoint devices, and are simple to configure and deploy. Most organisations have little appetite or capacity to manage the cost and disruption associated with rip and replace.

Timelines:

Many governments have set a deadline of 2035 for complete migration to PQC. In the UK, the National Cyber Security Centre (NCSC) wants organisations to start executing high-priority upgrades from

2028

Just two years away. The European Commission urges organisations to fully transition high-risk systems and critical infrastructure to PQC by the end of 2030. In the US, all federal agencies will need to move off legacy algorithms by 2030.

2035

Will be an ambitious target for many given the complexity of their digital infrastructure, the proliferation of legacy devices and the ubiquity of public-key cryptography. Organisations concerned about HNDL need solutions they can deploy today.

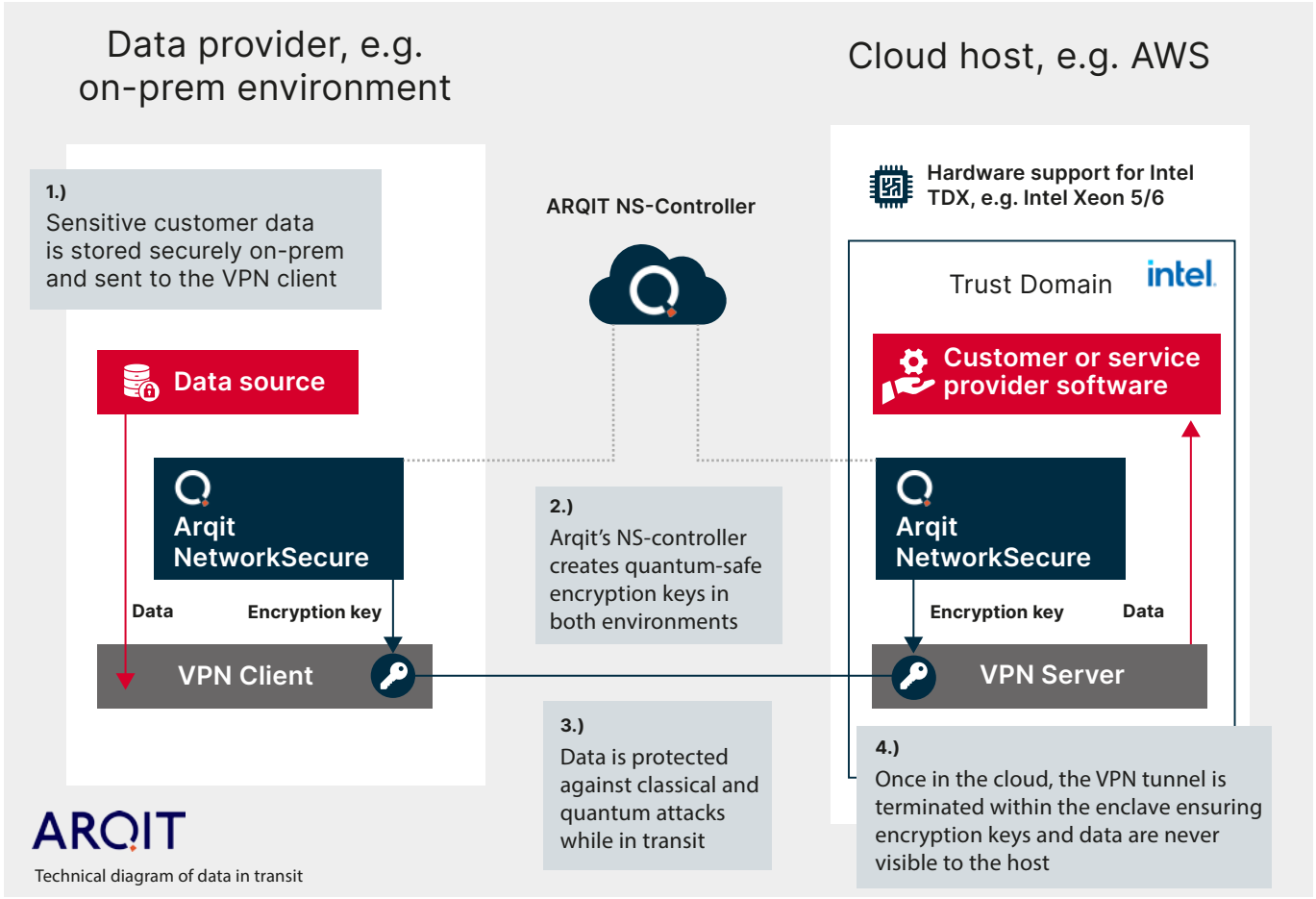
Protecting data in transit

Arqit NetworkSecure is a lightweight, easy-to-deploy solution designed for use at the network edge to future-proof networks against quantum attack. Rather than use public key infrastructure (PKI) which could be broken by CRQCs, it relies on symmetric key agreement (SKA), for protecting quantum-resistant symmetric keys (eg AES-256). The product is also designed in compliance with NSA, NIST, CSNA 2.0 and FIPS 140-3 standards.

Here's how it protects data in transit.

1) **Mutual authentication:** Each virtual/physical endpoint device is authenticated with NetworkSecure using an authentication key unique to each device. This aligns with Zero Trust principles as devices must be continuously authenticated, rotating the unique key to a new value. Device compromises and spoofing can be detected in near real time and any endpoints at risk can be automatically quarantined to eliminate risks to the network.

2) **Encrypted tunnelling:** NetworkSecure enables endpoint devices to agree a shared quantum-safe symmetric key that only the devices themselves know. They use a split-trust model, meaning Network Secure helps the two endpoints agree on a key, without any other entity (e.g., a CSP) knowing what the final key is. The key can be rotated for every new session to achieve perfect forward secrecy (PFS). Once a shared symmetric key is agreed upon, it is used to harden a standard tunnel (eg, an IPsec VPN), encrypting the data with AES-256 before it is sent across the network.



Technical diagram of data in transit

Three ways Arqit NetworkSecure can be deployed

Consider the following use cases:

Telcos: NetworkSecure enables telcos and service providers to offer quantum-safe VPNs via a simple-to-deploy and deliver Network as a Service (NaaS) model. Scalable to thousands of endpoints - including mobile devices, uCPE and Private 5G base stations - it offers protection for data in transit across untrusted networks. High availability and disaster recovery features support resilient network architectures and telco-grade SLAs.

Enterprise: NetworkSecure is designed for deployment at the edge, making it ideal for branch offices, restaurants, hotels and even remote locations like oil rigs and offshore wind farms.
As more of these locations process sensitive information (from point-of-sale machines, IoT sensors and office-based edge devices) it needs to be protected as it's sent to centralised locations for further processing.

Military: Modern military operations require the ability to rapidly deploy mobile, scalable and agile command-and-control (C2) infrastructure in a range of diverse scenarios. Solutions must be efficient, with low OpEx/CapEx, and support a range of hardware, software and network bearers — while maintaining robust security today and in the future. However, existing pre-shared symmetric key (PSK)-based networks are saddled with deployment, cost, interoperability and mobility challenges.

NetworkSecure offers a highly secure and more scalable option for agile C2 to ensure mission success. It delivers improved flexibility, assurance and manoeuvrability, with low overheads, a small form factor and low power requirements.

Working with Intel

Arqit has built NetworkSecure in collaboration with Intel. One of the platforms Intel developed, Intel Netsec Accelerator Reference Design, provides an exceptional and unique advantage in deploying NetworkSecure . Here's how:

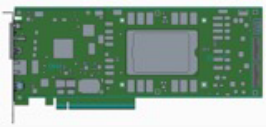
NetworkSecure is a lightweight software application that provides a key management solution. Deployed on small form-factor Intel-based servers or lightweight virtual machines, the solution enables data sovereignty and quantum-safe networking from the core and the cloud to the edge. NetworkSecure integrates with Intel-based Netsec Accelerator cards, leveraging the scalable architecture and network acceleration capability to enable a plug-and-play device that can be added to an existing server infrastructure with no impact on space and with minimal power and cooling. Whether you're deploying secure AI acceleration at the edge or high-performance quantum-safe networking in the cloud, Arqit and Intel can meet your requirements today.

Introducing the Intel®NetSec Accelerator Reference Design Resource Augmentation Card

- Intel® Ethernet Controller + Intel SoC
- Intel scalable architecture
  - Crypto/Compression
  - AI Acceleration
  - Network Function Acceleration
- Plug and Play Architecture
- Ease of Integration into existing provisioning and orchestration
  - OpenStack
  - Kubernetes

Version 1
Intel Atom® P5700: 8C, 16C
Intel® Ethernet Controller E810

Version 2
Intel® Xeon® D: 4C, 8C, 10C
Intel® Ethernet Controller E810



Version 3
Intel® Xeon® 6 SoC,
Intel Atom® P6900 SoC
Intel® Ethernet E830 Controller

Deployment Scenarios	Use Cases and Workloads
CPU Augmentation Card	**Adding Compute to an existing host** No Impact on Space Minimal Power Minimal Cooling
Full Application Offload Aka Distributed Appliance	**Disaggregated Security Functions** Firewall SD WAN
Partial Application Offload	**Network Accelerator** IPSec Intrusion Protection

Three generations of Intel-based NetSec Accelerator Cards

Key advantages to accelerate your quantum-safe journey

Let's recap the benefits of NetworkSecure for your business:

Eliminates the risk of a damaging data breach or HNDL attack and reduces the risk associated with TNFL attacks, and helps the journey towards data sovereignty by ensuring that encryption keys are only visible to the devices that need them.

Cost efficiency and reduced complexity: integrates with COTS endpoint technology, is compatible with current encryption algorithms/industry standards, and removes the need for expensive PSKs

Provides peace of mind to accelerate digital transformation projects/AI (for enhanced CX, trust, operational efficiency and revenue), helping customers achieve data sovereignty and supporting zero trust architectures

Flexibility to scale with the business, up or down, with tiered annual licence subscriptions provide the flexibility to start with a small number of endpoints and scale over time

Rest APIs enable integration with remote monitoring and management NOC and SOC systems (e.g., SIEM)

Minimal infrastructure to deploy and maintain with resilience options for telco grade SLAs

Cryptographic agility, adapting to any future key size without impacting speed and performance, and independent of any hardware requirements

Conforms to NIST SP 800-71 and CSNA 2.0 standards for cryptography (e.g., AES-256, hashing algorithms), complies with National Security Memorandum NSM-10 and NSA CSfC Symmetric Key Management Requirements Annex 2.1, FIPS 140-3 Inside, and is ISO 27001 and Cyber Essentials certified

What to do next

If you're keen to get started on your journey to quantum safety, here are some best next steps:

1) Check where you use public key crypto by running an accredited Automated Cryptography, Discovery & Inventory tool such as Encryption Intelligence Check if existing systems can handle a change in encryption standards
2) Work out if your use cases match the ones above
3) Get board-level buy in by piloting NetworkSecure

Find us at MWC Barcelona 2026 to find out how Arqit can streamline your journey to quantum safety. Drop by the Arqit stand 7C11, Hall 7.

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

Arqit secures the world's most critical data with quantum-safe encryption software. Simple, scalable, and compliant, its products integrate with existing infrastructure, and requires no rip and replace of hardware.

Arqit provides a complete "Detect, Protect,Comply" solution for governments and enterprises that detects and inventories cryptographic assets, protects data, ensures compliance, and safeguards transition to the post-quantum era.

Arqit's primary product offerings are Encryption Intelligence and NetworkSecure™. Encryption Intelligence detects cryptographic exposure, identifies vulnerabilities, and maps dependencies NetworkSecure™ protects data in transit with provably secure post-quantum cryptography and contributes to establishment of confidential compute environments for complete data sovereignty.

Arqit is an IDC Innovator for Post-Quantum Cryptography (2024) and a multi-award-winner in quantum-safe security.

For more information, visit www.arqitgroup.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