NetworkSecure™

Arqit's quantum-safe encryption protects VPN data communications

Data is at **risk today**

Data is not safe. Legacy encryption is obsolete. The problem is big today, but quantum computers will soon defeat all legacy encryption. Alternative solutions (co-ordinated by NIST in the USA) have failed to demonstrate a rapid, mature and suitable solution.

SKA (Platform)™; Arqit's symmetric key agreement platform makes the communications links of any networked device or cloud machine secure against both current and future forms of attack on encryption.

All industries have an obligation to keep data secure - Arqit's focus is to protect key sectors:

- **Government and defence**
- **Telecoms**
- **IoT platforms and vendors**
- **Financial services**

Introducing **NetworkSecure**

Arqit NetworkSecure Adaptor is a lightweight software application that hardens traditional VPN communications against both traditional man-in-the-middle attacks and *Store Now, Decrypt Later*[1] quantum attacks.

Through a simple integration with existing network infrastructure, NetworkSecure allows organisations to easily and cost-effectively adopt a defence-in-depth approach, complying with the latest cybersecurity recommendations from standards bodies like NIST and protecting themselves from devastating future breaches.

[1]*SNDL attacks – Encrypted data is harvested today and stored by adversaries with the intent to decrypt it in the future when quantum computers reach sufficient maturity.*

Challenges

01

Quantum threat to data-in-transit

02

Time, skills and effort to migrate to most quantum-safe cryptography

03

High cost and management burden of many solutions

04

Compliance with industry standards and regulations

Arqit has the **solution**

NetworkSecure Adaptor is an easy to deploy and manage application that seamlessly integrates with a customer's network infrastructure to provide on-demand quantum-safe shared symmetric keys brokered by SKA (Platform).

Organisations can benefit from the core features of Arqit NetworkSecure Adaptor without having to integrate Arqit SDKs into customer applications. Keys are requested in real-time using the standard ETSI 014 API interface and consumed by network devices to provide an additional layer of encryption security, protecting data-in-transit traffic against PKI related attacks and the quantum threat, both of which exploit weaknesses in public key cryptography.

The solution improves efficiency, flexibility, and scalability at a lower cost compared to alternative solutions relying on Quantum Key Distribution (QKD) or Post Quantum Algorithms (PQA).

Giving you the **advantage**

Immediately hardens network communications and keeps data secure, preventing devastating SNDL attacks that carry significant financial, compliance, and reputational risk

Simple, small-footprint overlay to existing infrastructure, avoiding rip-and-replace by integrating seamlessly with PKI and IPsec

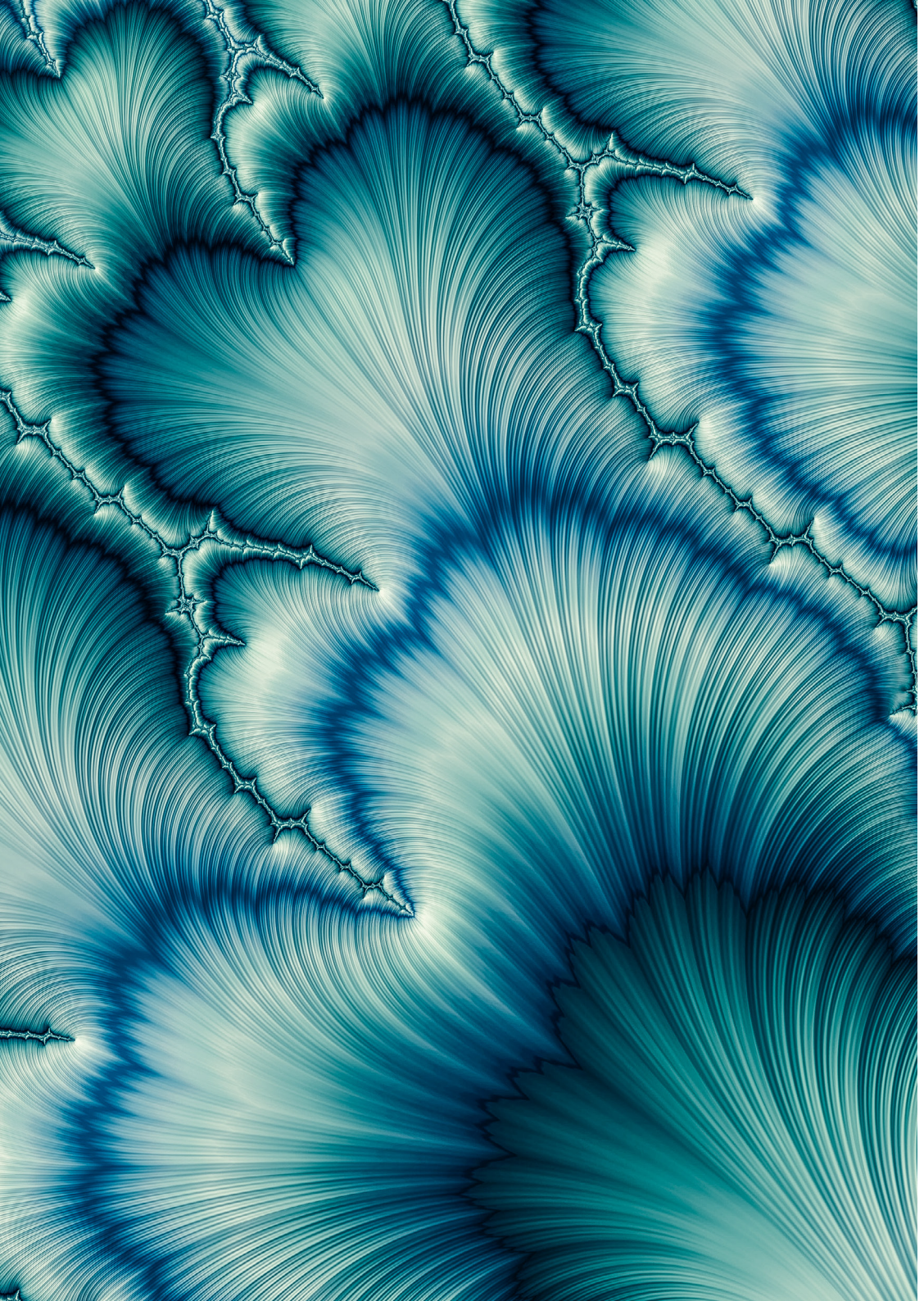
Minimal management overhead, with data easily exportable to existing SIEMs/XDR solutions

Enables compliance with National Security Memorandum NSM-10 and NSA CSfC Symmetric Key Management Requirements Annex 2.1

Conforms to NIST standards for cryptography e.g. AES-256, as well as NSA's recommended use of pre-shared keys to protect against the quantum threat

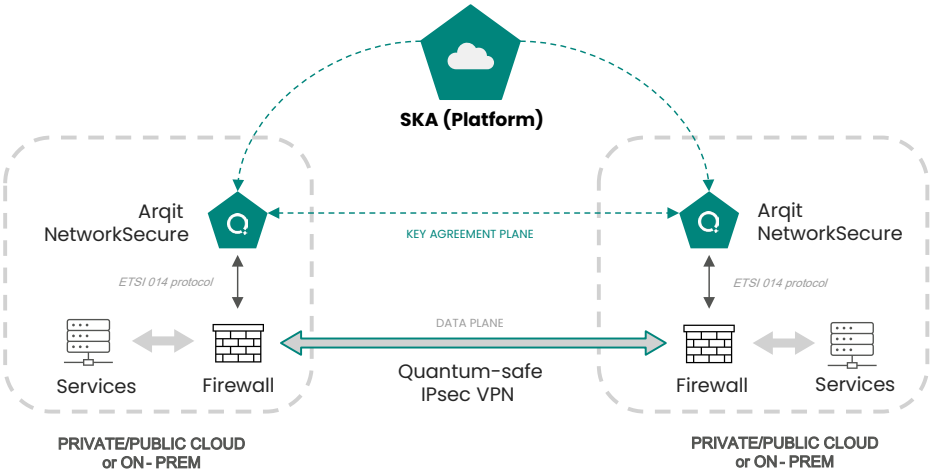
Easy-to-use Arqit Cloud console for advanced adaptor configuration management e.g. endpoint logical grouping and endpoint policies

Negligible performance and latency impact



Solution overview

Quantum-safe VPN tunnel enabled by **SKA (Platform)**

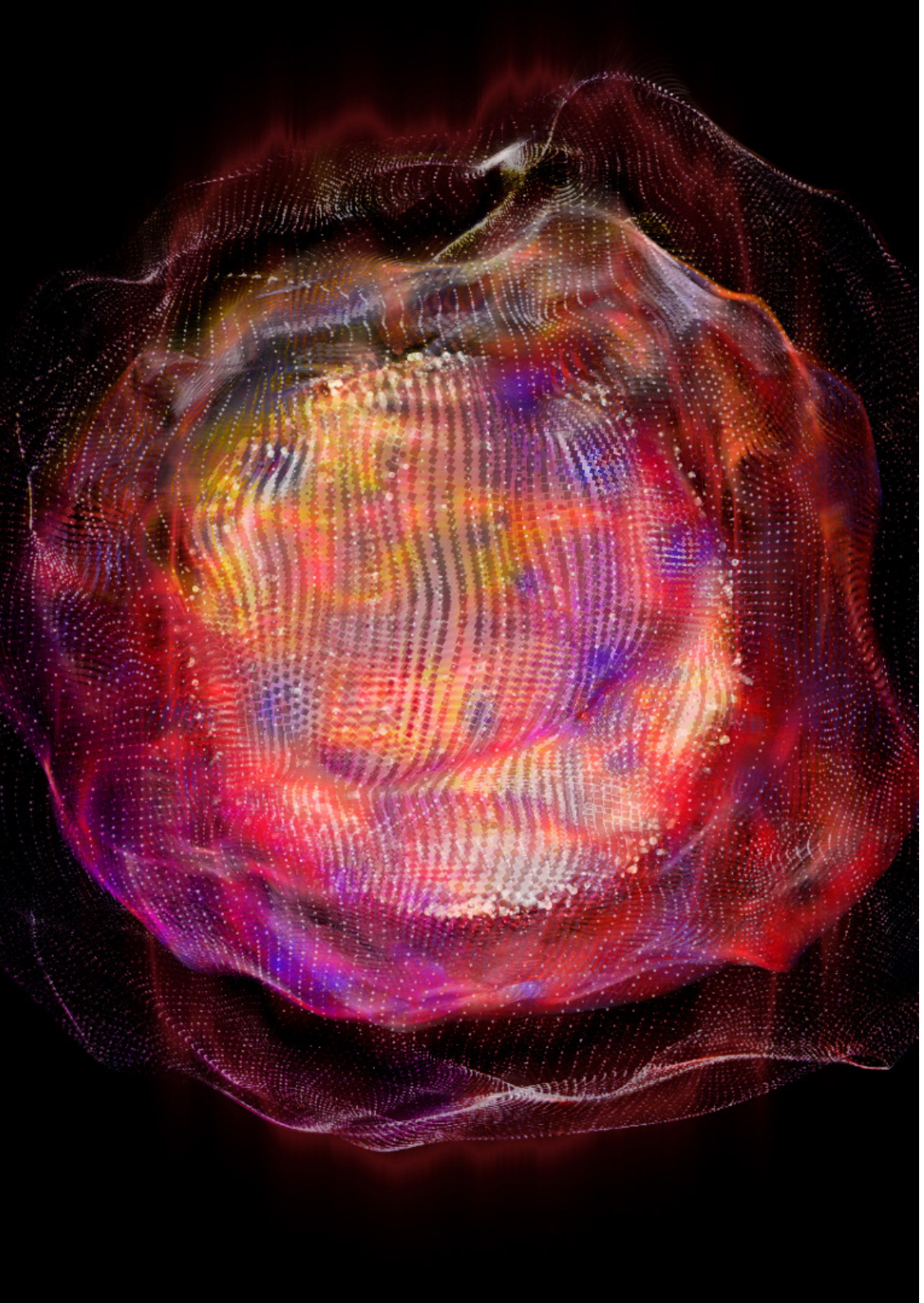


Each firewall (physical or virtual) securely connects to its designated NetworkSecure Adaptor over the secure, private local network using mutually authenticated and encrypted TLS sessions. When point-to-point IPsec VPN sessions are initiated or re-keying of existing tunnels are triggered by Firewalls, each participating firewall requests a shared quantum-safe key from its respective local NetworkSecure Adaptor server using the standardised ETSI 014 network protocol. The Adaptors agree a shared symmetric key with each other, using Arqit's SKA (Platform) as the key broker, and the keys are delivered in near real-time to the requesting firewalls over the ETSI interface.

The keys are used by the Firewalls, specifically the IKE key agreement protocol, in the construction of the IPsec VPN tunnel to deliver enhanced data protection.

Available with our **partners**

	FORTINET	JUNIPER NETWORKS	CISCO	HPE aruba networking
Vendor Products	• FortiGate firewalls	• SRX firewalls • vSRX on NFX platform	• Cisco 1000 Series Integrated Services Routers • Cisco ASR 1000 Series Aggregation Services Routers • Catalyst 8300 Series Edge Platforms • Catalyst 8500 Series Edge Platforms • Catalyst 8000V Edge Software	• HPE Aruba Mobility Controller Virtual Appliance (VMC) • HPE Aruba VIA VPN Client
Key Interface Protocol *(protocol to request external quantum safe encryption keys)*	• ETSI 014	• ETSI 014	• Cisco SKIP	• RFC 8784
Network Protocol *(data communications protocol secured by quantum safe keys)*	• IPSec / IKEv2	• IPSec / IKEv2	• IPSec / IKEv2	• IPsec / IKEv2



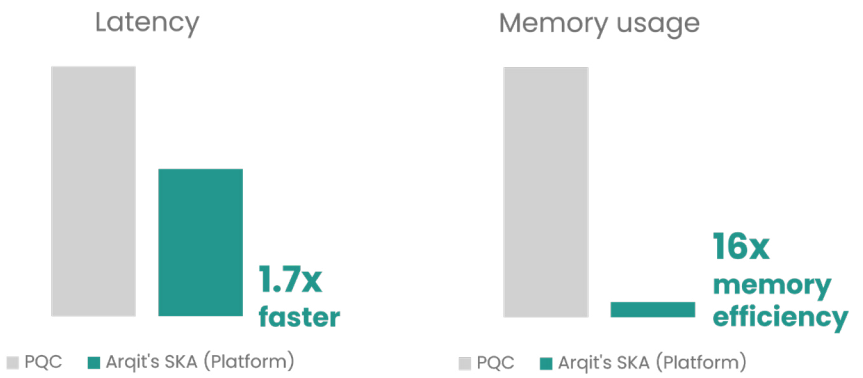
Compatible with current industry cryptographic recommendations

Name	Use	Approved	Conforms to Guidance[1]	CNSA 2.0
SKA Platform Hardware	SKA Blueprint	✓		
AES256-GCM	Block cipher	✓		✓
SHA-256	Hash Function	✓		
SHA-384	Hash Function	✓		✓
HMAC	Message Authentication	✓		
Key establishment protocol	Symmetric key agreement and authentication		✓	
Protocol interfaces	Using keys in transport protocols like TLS and IPsec		✓	

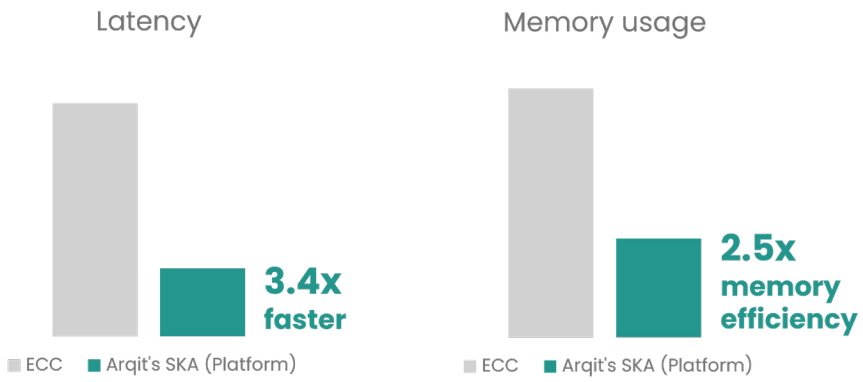
[1]NIST do not approve protocols, but in some instances provide guidance recommending how protocols should be implemented data

Arqit's SKA (Platform) outperforms both ECC and PQC for latency and memory consumption

Latency and memory use compared with **PQC**



Latency and memory use compared with **ECC**



Case study

Secure drone data

> “Integrating Arqit’s technology onto our Smart Connect™ avionics gives our customers an operational advantage in multi-domain operations and beyond. With authentication on a continuous basis, even if an asset becomes compromised it can be deactivated in real time. This has not been seen before. Our demonstration with Arqit represents a milestone development in the security of crewed and uncrewed applications.”
>
> **Dr Yoge Patel, Blue Bear CEO**

Blue Bear is an agile Systems Integrator and a pioneer in Autonomous Systems. With the proliferating use of autonomous drones or UAVS by military forces globally, BlueBear recognise that issues of data security and encryption are ever more crucial. Traditionally, communications between UAVs and ground stations have been fraught with security risks, operational limitations and a lack of scalability.

Arqit’s SKA technology was integrated into Blue Bear’s Smart Connect™ device to deliver collaborative multi-domain missions for defence and civil applications.

This scalable solution can be applied to any data transmission path between operators, mission systems and crewed/uncrewed vehicles. The solution can be used on any open or closed network in C2 of air, land or sea borne systems and is agnostic of the communication bearers.

Using full symmetric encryption of task and target data secured by SKA (Platform), image data of potential targets was encrypted and relayed securely. Additionally, through active authorisation of endpoints and frequent rotation of symmetric keys, the attack surface area was limited, and perfect secrecy of the data was achieved.

Case study

Network manager for sensitive research data

> "The recent feature launches from leading network equipment vendors combined with Arqit's technology gives Jisc and its members the opportunity to test new features that harden encryption on data links to a quantum-safe level. We are pleased to be at the forefront of piloting quantum safe cryptography within the academic and research sector to safeguard IP and innovation data."
>
> **Simon Farr, Director of Innovation & IT, Jisc**

Jisc manages the UK's national research and education network ("JANET") which is part of UK CNI. It serves hundreds of education customers including top universities, academic and research institutions, as well as major global research institutions like CERN and MIT.

Jisc is highly aware of SNDL threat to sensitive research data traffic on the JANET network.

Jisc deployed NetworkSecure on Fortinet to secure point-to-point connection between Fortinet firewalls."

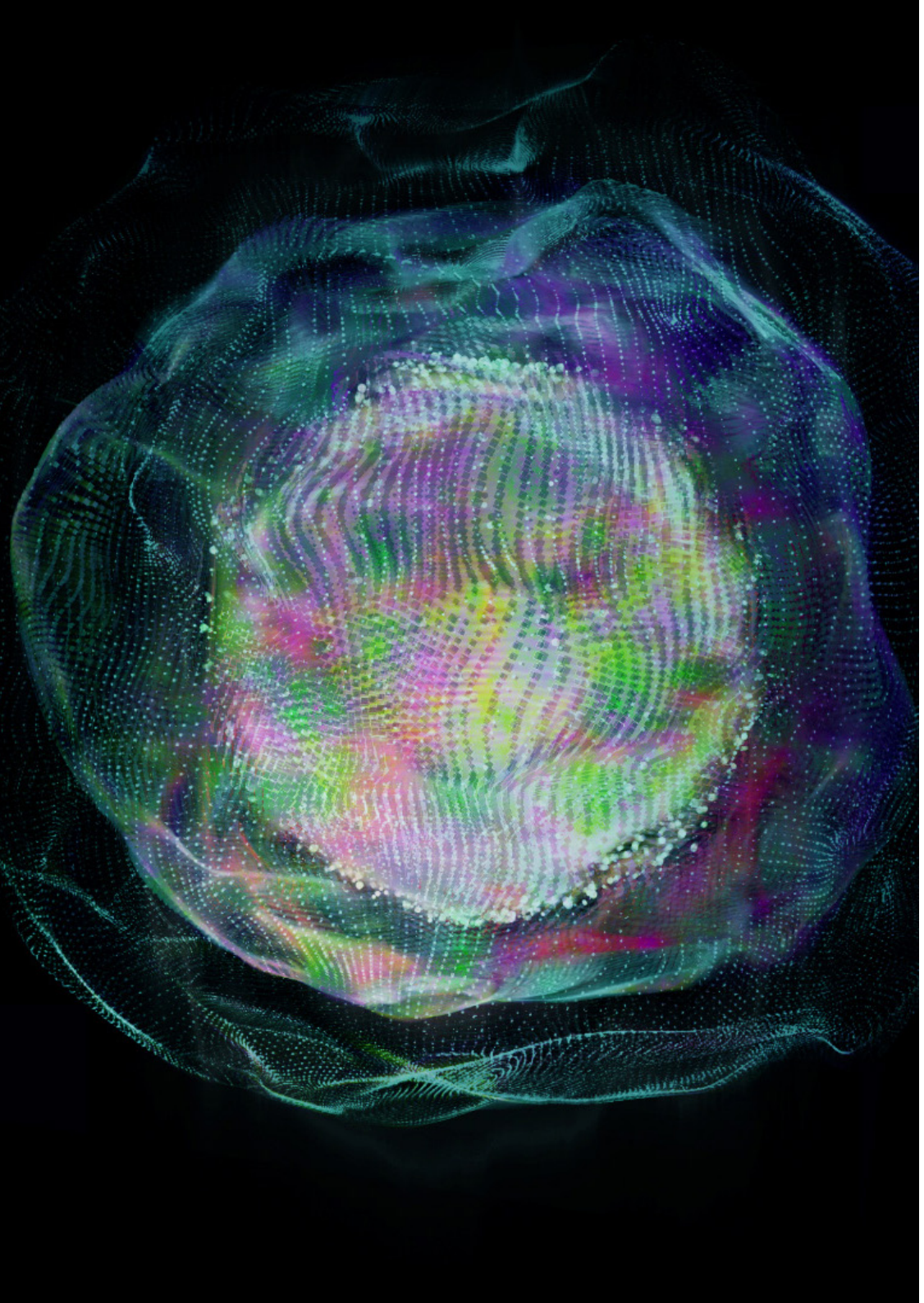
Case study

Quantum-safe security for private 5G networks

Private enterprise networks based on 5G cellular technology are accelerating digital transformation across industries Private 5G gives enterprises access to high-speed, massively scalable, and ultra-reliable wireless connectivity, allowing them to implement innovative IoT and mobile solutions that enhance productivity, drive automation and improve customer engagement.

Arqit's lightweight software agent was integrated with Athonet's RAN equipment and AWS cloud core to enable secure registration with Arqit's SKA (Platform). The RAN and core connect to each other via an IPsec VPN tunnel and symmetric keys are generated directly on the endpoints to establish the tunnel and encrypt the data.

Due to Arqit's SKA (Platform), data passing between the RAN and core is now verifiably secure even against quantum attack, future-proofing the 5G network.



Awards and Recognition

IET Excellence and Innovation Award

- **CTO Choice: Outstanding Mobile Technology Award**
- **Best Mobile Security Solution**

Cyber Security Software of the Year

The Innovation in Cyber Award

> "The work of Arqit is important to ensuring that the UK continues to be a world leader in cyber security."
>
> The Rt Hon Oliver Dowden CBE MP, *Deputy Prime Minister*

> "Companies such as Arqit are leading the way in demonstrating how the UK's cyber expertise can enhance cyber capabilities, helping to further strengthen security across the Kingdom's cyberspace."
>
> Juliette Wilcox, *Cybersecurity Ambassador, UK's Department for International Trade*

arqit.uk

Learn more now