July 30, 2025

# Arqit launches quantum-safe SKA Edge Controller to secure deployed military operations

LONDON, July 30, 2025 (GLOBE NEWSWIRE) -- Arqit Quantum Inc. (Nasdaq: ARQQ, ARQQW) ("Arqit"), a global leader in quantum-safe encryption, today announced the launch of **SKA Edge Controller (SKA-EC)**, a ruggedised, quantum-safe Symmetric Key Agreement (SKA) communications platform designed to meet the needs of forward-deployed defense operations. The system enables rapid setup of secure, scalable command and control (C2) nodes in contested, disconnected and high-threat environments without the constraints of traditional encryption infrastructure.

SKA-EC extends Arqit's SKA-Platform™ to the tactical edge. It enables distributed and mobile force elements to operate securely and independently using small form-factor hardware appliances including BioDigitalPC® cards, COTS servers or virtualised cloud nodes.

By dynamically generating symmetric encryption keys across trusted endpoints, SKA-EC eliminates the operational risks of pre-shared keys (PSKs) and the complexity of Public Key Infrastructure (PKI), offering a crypto-agile, zero trust ready solution built for high-tempo environments.

Designed specifically to support modern defense operations, SKA-EC enables:

- **Quantum-safe security** at the edge, ensuring future-proof protection against nation-state and quantum threats.
- **Rapid deployment** of secure force elements across remote, mobile or cloud environments.
- **Distributed, scalable architecture** supporting independent or interconnected C2 nodes.
- **Resilience in contested environments**, including disconnected or bandwidth-constrained operations.
- **SWaP efficiency**, reducing the cost, size, weight and logistics overhead of traditional cryptographic systems.
- **Compliance with NSA, NIST, CSNA 2.0 and FIPS 140-3 standards**, ensuring readiness for mission-critical deployments.

SKA-EC supports a wide range of military use cases from mobile HQs and deployed force elements, to command links for autonomous platforms and unmanned aerial or ground vehicles enabling agile mission architectures without compromising on security or performance.

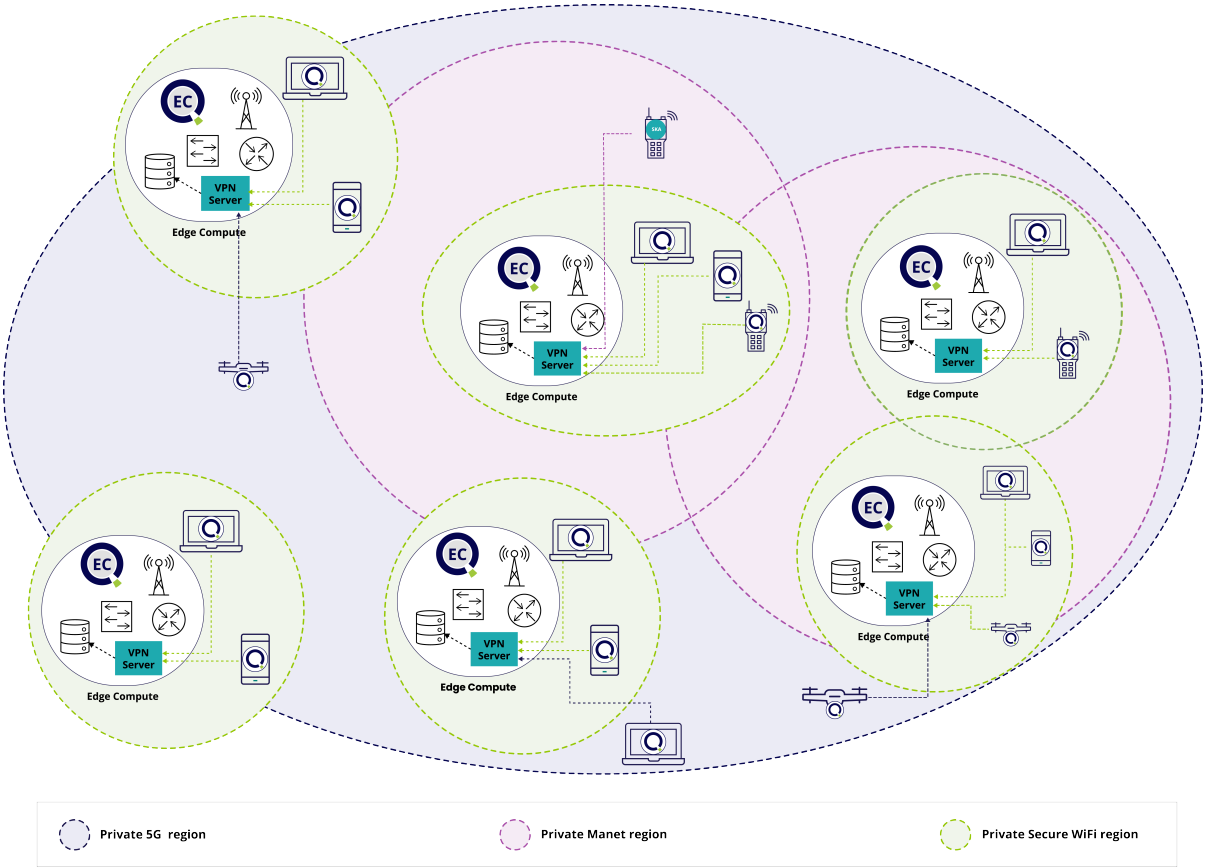
"Defense operations demand more than just connectivity, they require quantum-safe, resilient communications that can be deployed fast and operate under pressure," **said Paul**

**Feenan, Chief Commercial Officer at Arqit.** “SKA-EC delivers that capability as a secure-by-design, crypto-agile solution ready for the modern defense operating environment.”

SKA-EC is available now to government and defense partners. Find out more and arrange a deployment trial, demonstration or briefing here: https://arqit.uk/products/ska-ec

## Notes to Editors

**Figure 1: Interconnected Multi-Node Network** *(The image shows how SKA-EC enables symmetric encryption for a modern deployed headquarters made up of multiple scalable nodes that can operate independently or collectively, creating a dispersed and disaggregated environment.)*




## About Arqit

Arqit Quantum Inc. (Nasdaq: ARQQ, ARQQW) supplies a unique encryption software 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. Compatible with NSA CSfC Components and meeting the demands of NSA CSfC Symmetric Key Management Requirements Annexe 1.2. and RFC 8784, Arqit’s Symmetric Key Agreement Platform uses a lightweight software agent that allows end point devices to create encryption keys locally in partnership with any number of other devices. The keys are computationally secure and facilitate Zero Trust Network Access. It can create limitless volumes of keys with any group size and refresh rate and can regulate the secure entrance and exit of a device in a group. The agent is lightweight and will thus run on the smallest of end point devices. The product sits within a growing portfolio of granted patents. It also works in a standards compliant manner which does not oblige customers to make a

disruptive rip and replace of their technology. In September 2024, Arqit was named as an IDC Innovator for Post-Quantum Cryptography, 2024. Arqit is winner of two GSMA Global Mobile Awards, The Best Mobile Security Solution and The CTO Choice Award for Outstanding Mobile Technology, at Mobile World Congress 2024, recognised for groundbreaking innovation at the 2023 Institution of Engineering and Technology Awards and winner of the National Cyber Awards' Cyber Defense Product of the Year 2024 and Innovation in Cyber Award 2022, as well as the Cyber Security Awards' Cyber Security Software Company of the Year Award 2022. Arqit is ISO 27001 Standard certified. www.arqit.uk

**Media relations enquiries:**
**Arqit:** pr@arqit.uk

**Investor relations enquiries:**
**Arqit:** investorrelations@arqit.uk

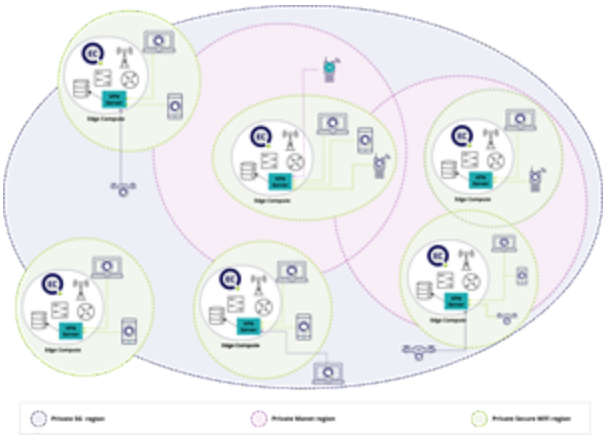
**Caution About Forward-Looking Statements**

This communication includes forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995. All statements, other than statements of historical facts, may be forward-looking statements. These forward-looking statements are based on Arqit's expectations and beliefs concerning future events and involve risks and uncertainties that may cause actual results to differ materially from current expectations. These factors are difficult to predict accurately and may be beyond Arqit's control. Forward-looking statements in this communication or elsewhere speak only as of the date made. New uncertainties and risks arise from time to time, and it is impossible for Arqit to predict these events or how they may affect it. Except as required by law, Arqit does not have any duty to, and does not intend to, update or revise the forward-looking statements in this communication or elsewhere after the date this communication is issued. In light of these risks and uncertainties, investors should keep in mind that results, events or developments discussed in any forward-looking statement made in this communication may not occur. Uncertainties and risk factors that could affect Arqit's future performance and cause results to differ from the forward-looking statements in this release include, but are not limited to: (i) the outcome of any legal proceedings that may be instituted against Arqit, (ii) the ability to maintain the listing of Arqit's securities on a national securities exchange, (iii) changes in the competitive and regulated industries in which Arqit operates, variations in operating performance across competitors and changes in laws and regulations affecting Arqit's business, (iv) the ability to implement business plans, forecasts, and other expectations, and identify and realise additional opportunities, (v) the potential inability of Arqit to successfully deliver its operational technology, (vi) the risk of interruption or failure of Arqit's information technology and communications system, (vii) the enforceability of Arqit's intellectual property, (viii) market and other conditions, and (ix) other risks and uncertainties set forth in the sections entitled "Risk Factors" and "Cautionary Note Regarding Forward-Looking Statements" in Arqit's annual report on Form 20-F (the "Form 20-F"), filed with the U.S. Securities and Exchange Commission (the "SEC") on 5 December 2024 and in subsequent filings with the SEC. While the list of factors discussed above and in the Form 20-F and other SEC filings are considered representative, no such list should be considered to be a complete statement of all potential risks and uncertainties. Unlisted factors may present significant additional obstacles to the realisation of forward-looking statements.

A photo accompanying this announcement is available at
https://www.globenewswire.com/NewsRoom/AttachmentNg/bc035e9e-9815-4d43-9ca2-

9071e2467856

**An Interconnected Multi-Node Network**



**The image shows how SKA-EC enables symmetric encryption for a modern deployed headquarters made up of multiple scalable nodes that can operate independently or collectively, creating a dispersed and disaggregated environment.**

Source: Arqit