November 11, 2025

Arqit launches SKA Central Controller to simplify quantum-safe network deployments for Managed Service Providers

LONDON, Nov. 11, 2025 (GLOBE NEWSWIRE) -- Arqit Quantum Inc. (NASDAQ: ARQQ, “Arqit”), a global leader in quantum-safe encryption, today announced the launch of SKA Central Controller (SKA-CC), an innovative software platform that future-proofs network security against current and post-quantum threats.

SKA-CC is a crypto-agile, low-footprint product that enables Telco and Defense Managed Service Providers to deliver quantum-safe network services without the cost and complexity of traditional key management. The platform generates dynamic symmetric keys for both endpoint authentication and encrypted VPN tunnels, removing reliance on long-lived pre-shared keys or PKI-based infrastructures.

SKA-CC ensures that data moving over virtual private networks across wireline, mobile, cloud and AI-enabled environments is protected by strong, lightweight and scalable cryptography that is quantum-safe by design.

Enabling new high-growth security services for telecom operators

SKA-CC supports a wide range of telecom and communication infrastructure use cases, allowing service providers to deploy advance security capabilities for existing and new offerings, including:

- **Secure Network-as-a-Service (NaaS):** Quantum-safe, multi-layer VPN services with multi-tenant key usage policy controls. Securing use cases for virtual network functions, Universal CPE and Virtual Private Cloud interconnections for highly automated management and orchestration (MANO) environments.
- **Optical (OSI Layer 1):** Integrates quantum-safe symmetric keys with OEM transport equipment that utilises OTNsec.
- **Carrier Ethernet (OSI Layer 2):** Enables high-throughput, quantum-safe MACsec point-to-point links.
- **Internet Protocol (OSI Layer 3):** Mixing in symmetric keys to IPsec VPNs, making them quantum-safe.
- **Application Programming Interfaces (OSI Layer 4-7):** Fortifying TLS-based APIs to a quantum-safe standard.
- **Mobile VPNs:** Delivers post-quantum secure VPN services for mobile and remote users.
- **Private 5G:** Secures infrastructure connectivity between radio base stations and the core network.

- **IoT / OT security:** Protects communication between edge gateways, IoT hubs and cloud services, ideal for energy, oil and gas and critical infrastructure applications.

By integrating SKA-CC, Telcos can differentiate their services and build new revenue streams while meeting the rising demand for post-quantum security across connected industries.

“Quantum computing will change the threat landscape,” **said Scott Alexander, Chief Product Officer at Arqit.** “SKA-CC gives our partners a practical way to secure their networks today, and stay ahead of tomorrow’s risks. It extends Arqit’s mission to make strong encryption simple and scalable, enabling the telecom ecosystem to deliver trusted, quantum-safe connectivity at global scale.”

Notes to Editors

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 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.arqitgroup.com

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.

ARQIT

Source: Arqit