September 5, 2023

Arqit launches the world's first integrated solution for quantum-safe VPN connectivity using Symmetric Key Agreement

Juniper Networks provides secure networking technology for the quantum-safe VPN connectivity solution through a technology alliance with Arqit

LONDON, Sept. 5, 2023 /PRNewswire/ -- Arqit Quantum Inc. (Nasdaq: ARQQ, ARQQW) ("Arqit"), a leader in quantum-safe encryption, today announces the availability of the world's first integrated solution for quantum-safe VPN communications.

Arqit's QuantumCloud™ is the world's first fully scalable cloud-based symmetric key agreement platform, capable of creating zero trust quantum-safe encryption keys at any device. By integrating QuantumCloud™ with Juniper Networks® vSRX Virtual Firewall, the resulting solution enables quantum-safe encrypted connectivity between customer locations, keeping data safe both at rest and in transit. Arqit's QuantumCloud uses unique symmetric key agreement software to provide quantum-safe keys which are used by Juniper SRX devices during the formation of secure tunnels.

Juniper's vSRX Virtual Firewall supports the ETSI 014 standard and RFC8784 for IPsec, resulting in the first GA product supporting flexibility and scalability in generating and using symmetric keys from various sources, including Arqit's symmetric keys.

David Williams, Arqit Founder, Chairman and CEO said, "It is an honour to work with Juniper. We're excited to leverage our integration to deliver enhanced protection against sophisticated cyber attacks of today and tomorrow. In conjunction with Juniper's vSRX Virtual Firewall, our strong, simple encryption enables governments and enterprises to realise enhanced protection against cyber threats and to take a major step forward in significantly reducing the quantum threat from their risk registers."

Samantha Madrid, Group Vice President, Security Business and Strategy at Juniper Networks said, "Juniper is thrilled to be working with Arqit through our technology alliance to enable quantum-safe encrypted connectivity using the QuantumCloud Platform. It is imperative that innovation efforts continue in cybersecurity as threats continue to proliferate in tandem with the pace of digitalisation. Juniper and Arqit are paving the way for safe and reliable cybersecurity solutions to deliver the best experience for organisations and businesses."

Notes to Editors

"Store-now, decrypt-later" is a known threat:

- **UK National Cyber Security Centre (NCSC):** "The threat to key agreement is that an adversary collecting encrypted data today would be able to decrypt it in future, should

they have access to a CRQC [Cryptographically Relevant Quantum Computer]" (NCSC, Preparing for Quantum-Safe Cryptography whitepaper, 11 November 2020, link).
- **US Congress:** "The rapid progress of quantum computing suggests the potential for adversaries of the United States to steal sensitive encrypted data today using classical computers and wait until sufficiently powerful quantum systems are available to decrypt it" (Congress, Quantum Computing Cybersecurity Preparedness Act, 21 December 2022, link).
- **GSM Association (GSMA):** "The quantum threat presents multiple high-impact risks for the telecom industry and its users. Prior to the availability of a Cryptographically Relevant Quantum Computer (CRQC), motivated bad actors may harvest data and store it to decrypt it once quantum computing capabilities become available. This attack undermines data security with long-lived confidentiality needs, such as corporate IP, state secrets or individual bio-data. It is widely believed that some actors are already engaging in this type of attack" (GSMA, Post Quantum Telco Network Impact Assessment Whitepaper, 17 February 2023, link).

Symmetric cryptography is a solution that can be implemented right now and can be used for both encryption and key exchange:

- **UK National Cyber Security Centre (NCSC):** "In contrast with PKC [public-key cryptography], the security of symmetric cryptography is not significantly impacted by quantum computers, and with suitable key sizes, existing symmetric algorithms - such as AES - can continue to be used" (NCSC, Preparing for Quantum-Safe Cryptography, 11 November 2020, link).

The US Government has already directed their agencies to implement symmetric-key protections for National Security Systems (NSS):

- **The White House:** "By December 31, 2023, agencies maintaining NSS shall implement symmetric-key protections (e.g., High Assurance Internet Protocol Encryptor (HAIPE) exclusion keys or VPN symmetric key solutions) to provide additional protection for quantum-vulnerable key exchanges" (The White House, National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, 4 May 2022, link).

About Arqit

Arqit supplies a unique Symmetric Key Agreement 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. 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. 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 but also works in a standards compliant manner which does not oblige customers to make a disruptive rip and replace of their technology. Arqit was recently awarded the

Innovation in Cyber award at the UK National Cyber Awards and Cyber Security Software Company of the Year Award at the UK Cyber Security Awards. www.arqit.uk

Media relations enquiries:
Arqit: pr@arqit.uk
Gateway: arqit@gateway-grp.com

Investor relations enquiries:
Arqit: investorrelations@arqit.uk
Gateway: arqit@gateway-grp.com

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 the Arqit related to the business combination, (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 convert its pipeline into contracts or orders in backlog into revenue, (vi) the potential inability of Arqit to successfully deliver its operational technology, (vii) the risk of interruption or failure of Arqit's information technology and communications system, (viii) the enforceability of Arqit's intellectual property, 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 14 December 2022 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.

View original content:https://www.prnewswire.co.uk/news-releases/arqit-launches-the-worlds-first-integrated-solution-for-quantum-safe-vpn-connectivity-using-symmetric-key-agreement-301917780.html