April 28, 2025

Arqit delivers quantum-safe protection enhanced by confidential computing

Changing the rules of trust in cloud computing

LONDON, April 28, 2025 (GLOBE NEWSWIRE) -- Arqit Quantum Inc. (Nasdaq: ARQQ, ARQQW), a leader in quantum-safe encryption, has announced the delivery of quantum-safe protection enhanced by confidential computing; data protection that helps ensure no third party, not even the cloud provider, can access a customer's encryption keys or workloads, even when distributed across multiple hosts. Powered by Intel Trust Domain Extensions (Intel TDX) and Arqit NetworkSecure™, this solution strengthens the security of Arqit's quantum-resistant crypto key delivery system.

With the right approach, organisations can now overcome long-standing cloud security challenges: gaining full control over encryption keys, securing data in transit, enabling trusted collaboration, and reducing the cost and complexity of additional hardware.

Protecting sensitive data in the cloud has always depended on placing trust in infrastructure providers despite the theoretical risk that they could access encryption keys or data as it moved between environments. This risk is now addressed.

With Arqit NetworkSecure running inside a Trusted Domain (TD) created by Intel TDX, encryption keys are:

- Generated inside the Intel TDX enclave
- Visible only to the TD owner
- Rotated frequently
- Protected with quantum-safe symmetric encryption between enclaves

Even Arqit and Intel are outside the trust boundary. This architecture provides advanced data sovereignty by design.

How It Works

In the Intel TDX environment, each TD is encrypted and isolated from other software, the hypervisor, and the infrastructure host. Arqit's software operates inside this confidential VM, generating and managing encryption keys that never leave the TD. Keys are used to secure communications between TDs across hosts, enabling safe, quantum-secure data flows without exposing any secrets to the infrastructure.

Use Cases

1. **Network Security for Telcos**
   Telcos deploying Network-as-a-Service (NaaS) or virtual RAN (vRAN) on white-box hardware face new security demands. Arqit NetworkSecure can now run inside an Intel TDX **trust domain** on these platforms, designed to keep traffic encryption and key

management isolated and quantum-safe. Remote attestation helps verify the environment hasn't been tampered with.

2. **Enterprise Edge & AI Workloads**
   Large enterprises moving sensitive workloads between on-prem environments and the cloud need strong isolation and secure communication. Arqit and Intel TDX isolate the workload and secure the channel using symmetric keys, all without exposing processes inside TD to the cloud or the infrastructure provider.
3. **Virtual Hardware Security Modules (HSMs) for Critical Infrastructure**
   Instead of costly physical Hardware Security Modules (HSMs), organisations can now deploy Arqit's symmetric key platform inside TDs as a "virtual HSM" – cutting costs while meeting the highest security standards for cryptographic operations.
4. **Secure Collaboration Across Domains**
   In sectors like defence, finance, and public services, data collaboration often involves multiple parties. Using secure enclaves and Arqit's ephemeral key model, organisations **can now enable secure, privacy-preserving analytics across trusted domains.**

Looking Ahead

Confidential computing can elevate security to the next level. Security enhancements include:

- Infrastructure that meets the highest bar
- Zero key access for operators
- Quantum-safe encryption as standard
- Hardware-based trust anchors
- Attestation independent of the provider's infrastructure
- Verified isolation through TD attestation

This level of assurance is especially vital in regulated industries like finance, defence, and national infrastructure.

Andy Leaver, CEO of Arqit:
"This collaboration with Intel delivers a powerful enhanced model for securing data in the cloud. By combining Intel's trusted hardware with Arqit's quantum-safe encryption, we're giving customers full control of their security, removing infrastructure providers from the trust equation entirely. It's a significant step forward for digital sovereignty, and demonstrates the future of confidential computing can be both stronger and simpler."

Bob Ghaffari, Vice President, Network and Edge Group, Intel Corporation:
"Arqit's quantum-safe encryption technology running in Intel TDX creates a powerful addition to confidential computing where data sovereignty and protection of the information you process are ever more important to organizations of any size and form."

Further information here:

https://arqit.uk/resources/data-sovereignty-with-confidential-computing-and-networking

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 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 Defence 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.

Source: Arqit