March 5, 2024

# Arqit announces reseller agreement with Total Computers

LONDON, March 05, 2024 (GLOBE NEWSWIRE) -- Arqit Quantum Inc. (Nasdaq: ARQQ, ARQQW) (Arqit), a leader in quantum-safe encryption, today announced a reseller agreement with Total Computers (Total), the digital transformation experts, for Arqit's Symmetric Key Agreement Platform and NetworkSecure™ Adaptor.

In an ever-connected world, enterprises need to take urgent action to strengthen their encryption to counter the growing threats from cyber adversaries. Compliant with NSA standards, Arqit's Platform as a Service makes symmetric encryption keys which cannot be broken even by quantum attack. Easily integrated at modest cost with dynamic rotating authentication, Arqit's groundbreaking technology is now available to Total customers as part of their comprehensive suite of services.

At Total Computers, the extensive range of services and solutions encompasses Cloud, Cyber Security, Infrastructure, Managed Services, and Workspace. Total's approach is consultative, and they are dedicated to ensuring customer success. It is this commitment that has earned them the trust of both our customers and partners, as they consistently provide the superior levels of service they require.

**David Williams, Arqit Founder, Chairman and CEO said:**

"We are thrilled to partner with Total to offer our encryption technology to their customers, who can now easily harden their networks for enhanced protection against current and future cyber threats. Enterprises need to be able to secure their data against both current and future cyber threats and with Arqit's unique products, they have off-the-shelf solutions that can be easily deployed today."

**Kevin Goodall, Managing Director, Total Computers said:**

"In today's increasingly interconnected and cyber-threat prone world, enterprises need to ensure that cyber security is a core part of their strategy. We are delighted to offer Arqit's groundbreaking encryption technology as part of our comprehensive suite of services for our customers."

**Notes to Editors**

**The UK Government acknowledges the quantum threat:**

- **UK National Cyber Security Centre (NCSC):** "A quantum computer will allow the attacker to read information that has been encrypted in the past, and forge information in the future" (NCSC, Preparing for Quantum-Safe Cryptography whitepaper, 11 November 2020, link).

**"Store-now, decrypt-later" is a known threat and concerning for data with a long-time value:**

- **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).

**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 existing symmetric algorithms with at least 128-bit keys (such as AES) can continue to be used” (NCSC, Next steps in preparing for post-quantum cryptography, 3 November 2023, link).

- **US National Security Agency (NSA):** “NSA considers using pre-shared symmetric keys in a standards-compliant fashion a better near-term post-quantum solution than implementing experimental post-quantum asymmetric algorithms” (NSA, The Commercial National Security Algorithm Suite 2.0 and Quantum Computing, 7 September 2022, 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 Quantum Inc. (Nasdaq: ARQQ, ARQQW) (Arqit) supplies a unique encryption 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. Compliant with NSA standards, 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. It also works in a standards compliant manner which does not oblige customers to make a disruptive rip and replace of their technology. Recognised for groundbreaking innovation at the Institution of

Engineering and Technology awards in 2023, Arqit has also won the Innovation in Cyber Award at the National Cyber Awards and Cyber Security Software Company of the Year Award at the Cyber Security Awards. Arqit is ISO 27001 Standard certified. 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

**About the acquisition**

boxxe, a UK-based IT Services and Solutions provider, announced the acquisition of Total Computers, **effective 31*st* January 2024**, in a move that accelerates boxxe's strategy in the corporate market. boxxe owner Phil Doye had previously acquired a minority stake in Total Computers in November 2022. Total has a rich heritage as a partner of choice for many of the UK's most successful and recognised companies, and through its own acquisition of Overbright in 2022, it added deep digital transformation expertise. This acquisition creates one of the UK's largest providers of software, solutions and services to both the public and private sector.

**About boxxe**

boxxe is a leading provider of software, solutions, and services to the public and private sectors. For over thirty-five years, boxxe has used its deep expertise, practical know-how and collaborative approach, to implement flexible tech solutions to help organisations accelerate growth, increasing productivity and reducing downtime for customers. Our range of services empowers organisations and gives people the confidence to use tech to be their best and better – commercially, socially, and sustainably.

**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, (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, and (viii) 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 21 November 2023 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