SOLUTION BRIEF

Arqit Symmetric Key Agreement for Quantum-Safe Security of Classified Solutions

A commercial solution that meets the demands of US National Security Memorandum-10 and CSfC Symmetric Key Management Requirements Annex 2.1

1 Executive Summary

- The White House National Security Memorandum 10 clearly mandates that Government agencies adopt symmetric key protections for NSS to meet the challenge of quantum computing by the end of 2023.
- Agencies like the NSA are updating their guidance to customers to help them achieve this goal, but it's challenging given the traditional difficulty of dynamically scaling symmetric key agreement mechanisms.
- Arqit's SKA™ platform is available today and allows endpoints to agree symmetric keys on-demand using highly secure standards-based mechanisms and conforms to the most recent requirements published by CSfC.

2 Symmetric key protection requirements

On May 4th, 2022, the White House published National Security Memorandum 10 (NSM-10)[1] in direct response to the emerging threat posed by powerful quantum computers, currently in development by all major global powers. Quantum computing can be used to break most public-key based cryptography widely used on public and private data networks. This risk posed is grave: as stated in NSM-10

> "When it becomes available, a [quantum computer] could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions."

NSM-10 mandates the adoption of "quantum-resistant cryptography", i.e., those techniques for securing data known to be resistant to quantum attack. Some of these techniques are still undergoing development and standardisation and may be for some time. However, one approach available today is the use of *symmetric cryptography* which is known to be extremely quantum resistant and has been in use for many decades in a variety of forms.

[1] White House, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems" (official memorandum, Washington, DC: White House, 2022)

This method is so effective that NSM-10 mandates its application to agencies maintaining [National Security Systems by December 31, 2023. This highlights the importance of symmetric keys in combatting the quantum threat and the US Government's preference for symmetric protection over other quantum-resistance cryptography that relies on *asymmetric cryptography* (which includes the algorithms being considered in NIST's Post-Quantum Cryptography Standardisation Process[2]). The NSA has also reiterated that symmetric protections must be used, at least as an interim solution, until other quantum-resistant protections can be developed.

3 CSfC's Symmetric Key Management Requirements

Government agencies therefore must respond quickly to this mandate and offer agencies new guidance on handling vulnerable data. Two weeks after publication of NSM-10 the Commercial Solutions for Classified (CSfC) group, part of the NSA, published an update to their Symmetric Key Management Requirements Annex[3] (SKM Annex) which dictates how Government agencies can incorporate quantum-safe symmetric key protections into solutions which use off-the-shelf commercial products to protect classified networks. This version improved and clarified pre-shared key (PSK) usage and added requirements for the implementation of RFC-8784 for IKE v2.

NSM-10, however, creates a problem for more complex, dynamic solutions where several classified solutions need to be interconnected as the standard mechanisms offered by asymmetric methods are no longer safe. This creates a need for a more dynamic, scalable method of symmetric key agreement between devices which still conforms to applicable standards and requirements.

4 Arqit's Symmetric Key Agreement Platform

Arqit's Symmetric Key Agreement Platform™ (SKA) allows endpoints to create pairs of PSKs on-demand for use as both authentication and data-in-transit encryption keys. These keys are ephemeral, minimising the opportunity for theft and reducing the impact if theft occurs. Once an initial symmetric "bootstrap key" is agreed between each endpoint and the SKA platform (e.g. through using a secure manual-distribution process or automated key-establishment scheme) the platform is used as a broker to create all subsequent keys, as well as strongly authenticating each endpoint with each request. The SKA platform can also enforce policies on which devices may communicate with each other, as well as quarantining devices believed to be compromised.

Unlike other quantum-safe protections that rely on asymmetric cryptography, Arqit's SKA platform relies on well-established cryptographic primitives which have been standardised by NIST and are known to be extremely robust against quantum attack. These include algorithms like AES and SHA, but other primitives can be adopted for specific use cases, e.g., the lightweight ASCON suite. The

[2] "Post-Quantum Cryptography", NIST, https://csrc.nist.gov/projects/post-quantum-cryptography

[3] CSfC, *Symmetric Key Management Requirements Annex V2.1* (Washington, DC: NSA, 2022)

SKA platform conforms to the standards outlined in ISO/IEC 11770-2:2018[4] for its key agreement mechanism, as well as the requirements stipulated in CSfC's SKM Annex v2.1. The security proofs for the design aspects of the key-establishment protocols used to enable symmetric key agreement over classical IP network infrastructures within QuantumCloud™ were independently assured in 2022 by the Surrey Centre for Cyber Security at the University of Surrey.

5 Arqit SKA™ and NetworkSecure™

To simplify the integration of Arqit's SKA platform into Government agency network solutions, Arqit offers NetworkSecure™ which provides an interface for network devices, like firewalls, to agree quantum-safe symmetric keys and upgrade the security of VPN connections over IPsec. Working with our Technology Alliance Partner Juniper Networks, we successfully tested a joint Arqit NetworkSecure and Juniper Networks® vSRX Virtual Firewall solution against a representative architecture outlined in the Multi-Site Connectivity Capability Package[5] and the Enterprise Gray Implementation Requirements Annex[6] published by CSfC. Our results show that Arqit and Juniper's joint solution meets the operational and security demands of Government agencies and strongly conforms to NSA requirements.

6 Conclusion

Arqit's SKA platform is uniquely positioned to help agencies meet their mandate to use strong symmetric key protections for NSS. We provide a modern, standards-compliant product that is highly scalable, dynamic, and quantum-secure.

For more information on Arqit SKA please visit our website at arqit.uk.

[4] International Standards Organisation. (2018). *IT Security techniques — Key management — Part 2: Mechanisms using symmetric techniques* (ISO/IEC 11770-2:2018)

[5] CSfC, *Multi-Site Connectivity (MSC) Capability Package v1.2.0* (Washington, DC: NSA, 2023)

[6] CSfC, *Enterprise Gray Implementation Requirements Annex v1.1.1* (Washington, DC: NSA, 2023)