Arqit Platform Standards Conformity

Version 3.0. Issued 29th January 2025.

Executive Summary

In its design of a novel secure key agreement platform, Arqit has used only approved NIST cryptographic modules, can be deployed as “FIPS 140-3 Inside 4743”, and has developed protocols which strongly conform to NIST guidance and requirements. This applies both to the platform itself, and to Arqit’s NetworkSecure™ product designed for VPN integration.

Arqit’s platform can be deployed in any environment where NIST standards or FIPS 140-3 validation must be upheld.

Detailed discussion

Standardised and approved primitives and algorithms

Arqit's platform implements cryptographic primitives and algorithms standardised by NIST and, in some cases, included in CNSA Suite 2.0.

Primitive name	Use	Approved	CNSA 2.0	Relevant NIST documents
AES256-GCM	Block cipher	✓	✓	SP800-175B, SP800-38D, SP800-38F, FIPS 197
SHA-256	Hash function	✓		SP800-175B, FIPS 180
ML-KEM*	Key encapsulation mechanism	✓	✓	FIPS 203

*Note that PQAs are optional for the delivery of initial root-of-trust key material. Arqit's platform can operate using entirely symmetric cryptography if desired.

The platform is agnostic to the choice of cipher and hashing algorithm so that they could be replaced at any time with other standards, such as SHA-3 specified in FIPS 202, or the alternative AES modes specified in SP800-38F.

Conformance of our key agreement protocol to SP 800-71 guidelines

NIST does not approve protocols, though they do make recommendations on how protocols may be implemented. SP 800-71 outlines NIST's recommendations for key establishment using symmetric block ciphers, one of the fundamental functions of the platform[1].

Arqit closely follows the recommendations outlined in SP 800-71. In particular:

- §3.4 – Key distribution using symmetric-key techniques. Arqit supports both manual and automated distribution of keys in accordance with the given guidance.
- §4.1 – Center-based key establishment architectures. Arqit's platform can be considered a key centre as described, but with the advantage that it never has total knowledge of the final shared symmetric key used for encryption.
- §5.1 – General communication requirements.
    - (a) An authenticated AES-GCM is used, which provides confidentiality, integrity and authentication for messages used in key establishment.

[1] This document remains at initial public draft status.

- (b) The key-ratcheting mechanism can create new authentication keys for each key agreement process, where required.
- (d) The key establishment protocol includes checks on authentication and protections against replay attacks using nonces.
- (f) All keys are labelled by the entity that generates them.

Arqit's key establishment protocols were also reviewed and assured by a third party.

> *"The security proofs for the design aspects of the key-establishment protocols used to enable symmetric key agreement over classical IP network infrastructures within Arqit's platform were independently assured in 2022."* –Statement from the Surrey Centre for Cyber Security, at the University of Surrey in the United Kingdom

No restrictions on encryption method

The platform places no restriction on the encryption method with the keys that are provided by the platform and therefore can fully comply with the approved guidance in SP 800-175B.

Interfaces with standard protocols

Beyond key agreement, Arqit's platform can also use its keying methods in existing communication standards such as IPsec and TLS. The use of a post-quantum pre-shared key (PPK) in IPsec as defined in RFC 8784 is covered by NIST in SP 800-77, with specific mention of PPKs in §3.7. Similarly, use of a pre-shared key (PSK) in TLS 1.3 is discussed in SP 800-52 Rev. 2 with a PSK specifically mentioned in §3.4.2.9–10. Again, NIST do not strictly approve these (or any other) protocols, but Arqit can demonstrate conformance with their recommendations for best practice implementation.

We expect that other protocols, such as MACsec and DNSSEC, can also make use of key material from Arqit's platform.

Conformance to Commercial Solutions for Classified (CSfC) requirements on symmetric key management

In May 2022, the Commercial Solutions for Classified (CSfC) group, part of the NSA, published an update to their Symmetric Key Management Requirements Annex (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. Arqit, together with a vendor partner, tested a joint implementation of Arqit's solution with VPN hardware to secure IPsec tunnels, using an architecture defined in the Enterprise Gray Implementation Requirements Annex published by CSfC. Our results show that Arqit's solution meets the operational and security demands of Government agencies and strongly conforms to NSA requirements.

Alignment with ISO/IEC 11770-2:2018

The International Standards Organisation (ISO) maintain standards for symmetric key management in ISO/IEC 11770-2:2018. Arqit's key agreement mechanism follows the guidelines set out in this standard in its implementation of key establishment using symmetric cryptographic techniques.

FIPS 140-3 Inside

Arqit's platform is "FIPS 140-3 Inside #4743" meaning it safely employs a FIPS-validated cryptographic module to provide cryptographic services. The platform can be operated in FIPS 140-3 mode in compliance with BouncyCastle #4743 security policy.

NIST promotes near-term use of symmetric key agreement

For completeness, we note that NIST have written that "the protection of symmetric keys using symmetric key-wrapping schemes and replacing asymmetric digital signature schemes with symmetric-key message authentication schemes is one approach to replacing public key cryptographic key management in the relatively near term" (SP 800-71, lines 468–478). We fully support this view.

Conclusion

Arqit's platform is a classical key agreement architecture that is fully conformant with NIST best practice and approved cryptographic algorithms. We believe Arqit's solution is an ideal solution for environments where NIST standards must be upheld.