The Arqit Symmetric Key Agreement™ Platform (SKA)

Stronger, Simpler Encryption

Version 1.3

Public-key exchange methods used to secure data in networks today use mechanisms that are compromised.

The risk posed is grave: as stated in the White House published National Security Memorandum 10 (NSM-10)[1]

> *"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."*

Even before quantum computers become available, it's possible for attackers to store data today and decrypt it later. Information that needs to be kept secret for a long time (state secrets, personal health and genomics data, intellectual property, trade secrets, financial data, etc.) is already at risk since it can be easily siphoned from public networks and stored encrypted in a data silo until it can be decrypted.

This problem is exacerbated by the proliferation of endpoints across multiple domains, in many cases beyond the enterprise's direct control, and the increasing volume of data being created and shared. This greatly expands the cyber threat attack surface, and with bad actors heavily investing in emerging technologies such as machine learning, artificial intelligence and quantum technology, their first mover advantage will be devasting if our networks and data are not appropriately secured immediately.

The solution is symmetric keys: long, identical random numbers shared by both parties to encrypt and decrypt data. Whereas asymmetric keys rely on computationally hard mathematics which will be susceptible to future quantum attack, symmetric keys rely on both parties sharing a random secret which is not. But agreeing symmetric keys dynamically and at scale has always been challenging without the use of asymmetric techniques: organisations that don't wish to use asymmetric key-exchange algorithms and protocols typically rely on laborious and costly manual key distribution.

What if we could agree symmetric keys without public-key methods or human couriers at scale and on-demand?

Arqit Symmetric Key Agreement™ Platform (SKA) is a cloud-hosted or on-prem service that can replace traditional manually-couriered symmetric keys with a dynamic and scalable alternative, securing networks with keys that are unbreakable by a quantum computer. This allows endpoints to upgrade the security of communication channels they create, for example adding quantum protection to an IPsec tunnel.

This white paper is for those who want to understand more about how SKA works and how it achieves highly secure quantum-safe authentication and symmetric key agreement between endpoints in line with existing standards and recommendations, including NSM-10. We'll also explore how it can be used in practice to secure data in transit against current and future threats.

[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)

Arqit's solution: Symmetric Key Agreement

Arqit has developed the Arqit SKA™ platform as a full as a full security solution that can be used in endpoint and network protection. Robust methods for endpoint authentication, provisioning, key agreement and management that are provably secure form the bedrock of Arqit SKA™. While the focus of the platform is on symmetric methods, it also draws, where appropriate, on technologies such as post-quantum algorithms (PQAs) and other traditional methods in accordance with current government recommendations and standards. The resulting hybrid solution provides defence in depth and crypto-agility for future flexibility. The core protocols and their implementation have been the subject of peer and government reviews, details of which are available to select partners.

Overview

As mentioned earlier, symmetric keys are known to be extremely secure but very difficult to manage and agree at scale. At one extreme, organisations manually courier symmetric keys wherever they are needed, leading to large numbers of keys and long key lifetimes. At the other end of the spectrum, organisations use public-key methods to perform authentication and key agreement in a more scalable and dynamic way, but these methods are now known to be susceptible to future attack by quantum algorithms, and even future implementations of public key methods might have similar weaknesses.

Arqit's approach is to mitigate the disadvantages of both these approaches while enhancing their benefits.

Authentication

How can Alice and Bob be sure of each other's identity?

Authentication, or the ability to ensure the identity of an individual, has central importance in security. Authentication is not at as great a risk from quantum computing as data-in-transit encryption due to the relatively short-lived nature of authentication credentials. However, this isn't to say that authentication is not at risk from many other forms of attack, including the theft of credentials. Therefore Arqit takes an approach to authentication which ensures the highest level of security available today without compromising the convenience of the SKA approach.

This process begins with the establishment of a root of trust. In traditional network security this would be established either through manual key delivery or by using public and private certificates. The certificate approach is the most widely used but has several drawbacks.

1. Certificates have been subject to many well-known attacks and are a point of vulnerability in the system. It is also becoming impossible to manage certificates for very large estates of endpoint devices.
2. Private keys typically have relatively long lifetimes, e.g. more than six months, meaning theft of the private key can have wide-reaching repercussions.
3. Revocation of private keys can be difficult due to the inherent nature of public-private key cryptography.

4. The mathematical relationship between public and private keys can be reverse engineered by quantum computers, meaning that in the future a CRQC could easily spoof a valid private certificate from a public key.

In contrast, Arqit has designed a hybrid approach which negates all these issues. A symmetric root-of-trust key is generated in SKA and is then encapsulated with keys generated through three post-quantum KEM algorithms. The encapsulated key is delivered to the endpoint at point of registration.

These algorithms are drawn from the candidates in NIST's Post-Quantum Cryptography Standardisation Process[2] and are intended as quantum-safe replacements for public-key protocols. Arqit shares the view of most cyber agencies (see FAQs) that PQAs, including KEMs, are not suitable for data-in-transit encryption due to the immaturity of their security analysis, as well as other issues such as latency and complexity. But in Arqit's patented bootstrap method multiple PQAs are only used in creating a one-time authentication key which is then ratcheted many times by the SKA platform.

These methods are not yet standardised so Arqit uses three KEMs of different types to increase assurance should any single KEM be weakened, and since this is a one-time registration process which is not time-sensitive KEMs with larger key sizes and compute requirements can be used (e.g. Classic McEliece), achieving quantum-safe protection at the level of AES 256.

All PQA KEM key exchanges are made over a TLS channel, ensuring at least classical protection[3], in line with recommendations from NIST and others that require hybrid cryptography. This process is described in outline below.

1. Alice (a compute device) makes a user-authenticated call to the platform.
2. For each type of KEM, a public-private key pair is created by the platform and the public keys are sent to Alice.
3. For each KEM, Alice creates a random secret and encapsulates it with the public key.
4. Alice sends her encapsulated secrets to the platform which decapsulates them using the private keys that it has retained.
5. Both Alice and the platform combine the secrets using a hash function[4] to create a combined key.
6. The platform creates a root-of-trust key, symmetrically encrypts it with the combined key from the previous step and sends it to Alice.
7. Alice uses her copy of the combined key to decrypt the root-of-trust key.

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

[3] Arqit can also operate with manually couriered root-of-trust keys if desired. This is not feasible in all contexts but could be done during manufacture or initial provisioning of endpoints, in which case a pre-provisioned enterprise device can be installed at the facility to generate root-of-trust keys on demand.

[4] A hash function is a one-way function that takes a variable length input and produces a fixed-length output (e.g. 256-bit). Hash functions have many desirable properties for cryptography and there are several implementations of hash functions that have been standardised for use by organisations such as NIST. They are known to be extremely robust against computational attacks, including by quantum computers.

Once the initial root-of-trust key has been delivered it is used by Alice to form the initial authentication key which will strongly authenticate with the SKA platform. In addition, the authentication key is ratcheted with each successive authentication, meaning a new authentication key is derived from the previous one in a way that cannot be reversed. This ensures that each authentication key has a relatively short lifetime (e.g., minutes or hours), configurable by the user, that mitigates spoofing attacks and simplifies key revocation. The authentication method used employs irreversible hash functions that are not breakable by any known classical or quantum algorithm.

This authentication key forms the basis of the security association between Alice and the platform and is used to generate a session encryption key related to the authentication session. This session encryption key is used to protect data between Alice and the platform, meaning that any information the platform sends to Alice can be considered quantum-safe. We'll use this fact when agreeing symmetric keys between two parties.

Provisioning

SKA endpoints must be *provisioned* for certain services in addition to being authenticated. The provisioning workflow is a series of stages which an endpoint can move through on request, assuming certain conditions are met (e.g. user authentication). Advancing through the provisioning states can grant endpoints greater permissions with SKA, such as the permission to agree symmetric keys with other endpoints.

The simplest provisioning workflow has two steps: 'unprovisioned', and 'provisioned'. Transitioning between two provisioning states not only updates the state in SKA, it also affects the key used for authentication: SKA creates a new ratchet value independently which it passes back (encrypted by the session key) to the endpoint.

The effect of this new ratchet is that it binds the new permissions of the endpoint together with the authentication key – if the key is lost or revoked, so are the endpoint's permissions. Creation of this new ratchet could be gated behind conditions, such as a given user authentication being used (e.g. an admin user), or the approval of multiple users through the SKA console, providing greater control over endpoint access to SKA services.

What is Symmetric Key Agreement?

Almost all secure communication today is based on two parties sharing a symmetric key. The party sending data uses the key to encrypt data, and the recipient uses the same key to decrypt it. The encryption and decryption ciphers (e.g., AES256) are extremely efficient and are often optimised at the hardware layer. If the key has sufficient length (i.e., greater than 128 bits), these methods are known to be extremely secure and robust against even quantum-based attacks.

The problem with these methods is how Alice and Bob agree a shared symmetric key in the first place. This is known as the key distribution problem – if Alice must transmit the key to Bob in advance it creates the opportunity for a bad actor to steal the key and eavesdrop on their communication.

There are two widely used methods to solve this problem[5]:

1. *Manual key delivery/pre-shared keys*. A trusted courier manually delivers the key to Alice and Bob without using a network. This can be highly secure but is also extremely impractical and expensive for large, disparate networks. These keys are also infrequently replaced, meaning large volumes of information can be decrypted if one is lost or stolen. This can be an O[n^2] solution in the worst case.
2. *Public-key protocols*. These rely on a mathematical problem which is difficult for a classical computer to invert, e.g. factorising large integers. The most used protocol is Diffie-Hellman key exchange. While these methods are much more convenient than manual delivery, the functions they rely on will be efficiently inverted by quantum computers in the future making them much less secure than initially believed.

Arqit's alternative solution is *Symmetric Key Agreement* which combines the high security of manual key delivery with the convenience and scalability of public-key protocols.

We achieve this through the introduction of a third party, the Arqit SKA™ Platform, which assists Alice and Bob in creating symmetric keys on demand. Entities register once with the platform and dynamically agree keys between themselves, leading to a much simpler O[n] solution.

This method of key agreement is secure because it relies on symmetric cryptography, which is a type of post-quantum cryptography (PQC) that's extremely secure against attacks including by quantum computers. It's also efficient and scalable due to the hub-and-spoke topology of a single platform coordinating key agreement among all endpoints.

Symmetric Key Agreement in practice

Alice now wants to create a shared key with another endpoint, Bob, which they can use to secure communication between them. We assume that both Alice and Bob are fully authenticated and provisioned with the platform. Arqit has created its own protocol which allows Alice and Bob to create a shared symmetric key using the platform as a broker. We describe this protocol in outline below.

1. Alice and Bob use a confidential channel to create a shared secret using a traditional (not necessarily quantum-safe) method, e.g. over TLS[6].
2. Alice sends a request to the SKA™ platform over the quantum-safe channel (using the session key created when she authenticated using her authentication key) to create an *intermediate key* based on knowledge of Alice's ID (from her authentication token) and Bob's ID (sent by Alice). Arqit's SKA™ platform takes a key from its HSM[7] and hashes it with this information to create the intermediate key, which is then returned to Alice.

[5] Another known method is quantum-key distribution (QKD). However, this method is relatively difficult to implement, particularly at scale, and has several shortcomings which are well publicised. Our solution can either complement QKD or provide a classical alternative.

[6] Note that Alice and Bob could secure their channel with a PQA if desired, but we don't require this as the channel between endpoint and platform is already quantum safe.

[7] A Hardware Security Module, or HSM, is a highly-secure appliance for the creation and storage of keys and for performing cryptographic operations. Arqit's SKA™ platform uses an HSM for storage of its most important key material.

3. Bob sends a request to the Server, also over a quantum-safe connection using his session key, and receives the same intermediate key based on his ID (from his authentication token) and Alice's ID (sent by Bob).
4. Both Alice and Bob now hash the intermediate key with their shared secret and recover the same shared symmetric key.

Importantly, the platform does not have all the information it needs to create the same key as it does not know the shared secret that Alice and Bob shared in Step 1. This is a split-trust mechanism, meaning that information is split between multiple channels. Any attack on SKA would not result in the loss of encryption keys, keeping your data secure.

This shared symmetric key can now be used in many ways to secure the data passing between endpoints, e.g. in an IPsec tunnel, or at the application level to encrypt data with AES. A new key can be requested as often as required for the use case. Since the key is a standard 256-bit symmetric key it can also be easily mixed with other keys generated through other methods for a robust defence-in-depth approach.

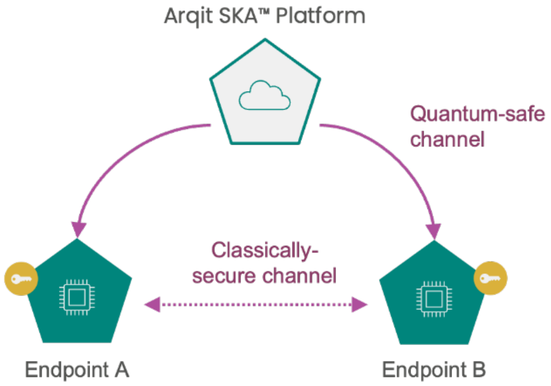

Figure 1: Schematic showing how two endpoints interact with the SKA to create a symmetric key.

Endpoint management

SKA offers system administrators tools to manage their network and control device access and permissions. Since every endpoint is securely authenticated with SKA it's easy for administrators to quarantine devices or even fully revoke permissions. This active approach to authentication contrasts with traditional private certificates which are more passive and are notoriously difficult to revoke. This approach works particularly well for closed, private enterprise networks where devices need to be both known and trusted to share data with each other.

Administrators can enforce these rules at either the endpoint level, or at a group level, making it easy to control large numbers of devices. Policies can influence all aspects of an endpoint's registration, provisioning, authentication, and key agreement with other endpoints.

This allows more fine-grained control over endpoint permissions. For example, policy can be set so that only endpoints within the same security group are able to agree keys, limiting which endpoints may communicate. In many cases this removes the need for attribute-based encryption typically used with PKI which has many drawbacks, including challenges associated with key coordination and revocation.

SKA adheres to relevant standards

Arqit's SKA™ platform and its protocols have been subjected to a high degree of scrutiny from independent third parties to assure its security properties. In particular, the protocols have been formally evaluated using the Tamarin Prover, both by Arqit's internal cryptography team, and the UK's University of Surrey.

> *"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 SKA™ were independently assured in 2022."*
>
> —Statement from the Surrey Centre for Cyber Security, at the University of Surrey in the UK.

A copy of the report which summarises this work is available on request.

Furthermore, Arqit has confirmed its conformance to a wide range of standards and guidance published by internationally recognised bodies. These include NIST Special Publications on algorithms and protocols, as well as guidance documents such as NIST SP 800-71 on how these protocols should be implemented. We also conform to the latest version of CNSA Suite 2.0 published by the NSA. Our platform can run in FIPS mode and uses FIPS 140-2 validated cryptographic modules and HSMs.

Because of our emphasis on symmetric key cryptography and our method for creating pre-shared keys on demand, Arqit's SKA™ platform conforms to both NSM-10 and the Commercial Solutions for Classified (CSfC) Symmetric Key Management Requirements Annex[8,9] 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 latest version of this Annex, v2.1, improved and clarified pre-shared key (PSK) usage and added requirements for the implementation of RFC8784[10] for IKE v2. This RFC is a mandatory requirement for commercial VPN solutions to be added to the CSfC Approved Components List.

More information on Arqit's conformance to standards and recommendations and relationship with US regulators is available on request.

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

[9] Arqit, Arqit Symmetric Key Agreement for Quantum-Safe Security of Classified Solutions (London: Arqit, 2023)

[10] Fluhrer, S, "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security", RFC 8784, 10.17487/RFC8784, June 2020, <https://www.rfc-editor.org/info/rfc8784>.

Summary of Arqit SKA properties

- **Quantum-safe root-of-trust key delivery** using an over-the-air hybrid PQA method that's robust against current and future cyberattacks.
- **Strong, mutual authentication with forward secrecy** of authentication keys to minimise impact in the unlikely event of loss or compromise.
- **Security groups and policy management** enforced in real time to simplify endpoint management.
- **Split-trust key agreement protocol** which ensures the final encryption key is only known to participating endpoints, not the platform.
- **Fully symmetric and hash-based Symmetric Key Agreement** based on well-characterised and standardised cryptographic primitives known to be computationally secure.
- **Crypto-agile** as our underlying cryptographic primitives can be upgraded or replaced.
- **Scalable and lightweight at the endpoint.**
- **The SKA Platform can run on any cloud infrastructure** and can be installed within the secure perimeter of a customer, meaning that this can be a sovereign platform within any export control approved territory. As per recent changes to export control laws, the Arqit SDK is not subject to export control.

Arqit's products

Arqit NetworkSecure™

Arqit NetworkSecure™ Adaptor is a lightweight software application that hardens VPN communications against both traditional man-in-the-middle attacks and store now, decrypt later[11] quantum attacks. Through a simple integration with existing network infrastructure, NetworkSecure allows organisations to easily and cost-effectively adopt a defence-in-depth approach, complying with the latest cybersecurity recommendations from standards bodies like NIST, and protecting themselves from devastating future breaches.

Arqit TradeSecure™

Arqit TradeSecure™ generates and distributes digital trade finance instruments, protecting finance supply chains against disruption and fraud and improving their cash flow at the same time. Our first-of-its-kind technology can be deployed into any trade financing platform, giving our customers quantum-safe security against all current and future cyber threats. Using distributed ledger technology, we provide customers with a unique referenceable and transferable digital finance instrument - which is easier to manage than paper-based alternatives. The technology is now being applied to notarize other forms of digital asset.

[11] Store now, decrypt later (SNDL) attacks – encrypted data is harvested today and stored by adversaries with the intent to decrypt it in the future when quantum computers reach sufficient maturity.

Frequently asked questions

What if the SKA service is unreachable?

Endpoints do need access to the SKA when first registering with the platform and when communicating with another endpoint for the first time. However, once a key has been agreed between two endpoints they may continue to derive new keys from this key without communication with SKA. We also offer SKA as a standalone private instance for use in network constrained environments which may not have regular access to external networks like the internet.

How do I use Arqit's keys?

The keys agreed by endpoints together with SKA are 256-bit symmetric keys. They can be used directly by a wide range of block and stream ciphers including common options like AES256 and ChaCha20. Arqit recommends that its keys are mixed with keys agreed through other methods, like Diffie-Hellman, to provide better defence in depth. Some standards exist for protocols like IPsec (see RFC8784) and TLS 1.3 which explain how to do this in a safe and standards-based manner.

To simplify the interaction with SKA for specific platforms and applications Arqit offer a range of SDKs written in different languages which assist in endpoint registration, provisioning, authentication, and key agreement. We also provide solutions for specific use cases: see Section "Arqit's products".

Why is symmetric cryptography and related methods like hash functions thought to be robust against quantum computers, but asymmetric methods like RSA are not?

The most straightforward way to break any form of encryption is to try to guess the key. In most cases cryptography is designed to make this search extremely time consuming, typically millions of years. More sophisticated attacks attempt to exploit mathematical structure present in the underlying cryptography to find shortcuts that help narrow down this search much more quickly. Asymmetric methods like RSA have much more of this structure than methods like AES and hash functions, and while these structures have previously been difficult to exploit, we now know that quantum-computing based algorithms exist that can exploit these structures. The unstructured search methods, such as Grover's algorithm, used to attack symmetric cryptography using a quantum computer are known to be the best possible such algorithms[12].

What's the difference between Arqit's approach to post-quantum algorithms (PQAs) from other companies?

While Arqit employs post-quantum algorithms it's important to point out the differences between our approach and the many ongoing efforts to replace classically-secure cryptography with their post-quantum counterparts.

Firstly, we only rely on PQAs in the one-time root-of-trust delivery process. This significantly reduces our reliance on PQAs which is an advantage both for security, given that we still do not know how secure PQAs will be in the long term, and efficiency, since many PQAs are resource intensive. In other words, while PQAs are already thought to be highly secure, Arqit consider them the *weakest*

[12] Zalka, C, "Grover's Quantum Search Algorithm is Optimal", Phys. Rev. A **60** 2746 (1999).

part of its solution and has therefore minimised their use overall. We shall see when discussing the rest of Arqit's protocols that PQAs are not required.

Secondly, we mix different types of PQA together to avoid loss of the root-of-trust should any one of the PQAs be weakened.

Thirdly, we don't have a strong dependence or preference for any one PQA, meaning it can be easily replaced in a crypto-agile fashion.

What is defence-in-depth?

A defence-in-depth strategy ensures continuous protection of data and communications by employing multiple protections. This means potential attackers now face the increased complexity of breaching two or more distinct systems. Furthermore, by diversifying cryptographic methods, any systemic or inherent flaws in one approach might not be present in the other, reducing the risk of widespread breaches. In an era where trust in technology is paramount, layered cryptographic defence is essential. SKA provides defence-in-depth because an attacker must attack the protocol in many different ways in order to weaken its security.

What is store now, decrypt later (SNDL)?

'Store now, decrypt later' attacks occur when malicious actors collect encrypted data today, which they store until there are capabilities to perform decryption in the future. It is well-established that National Signal Intelligence organizations already do this – even during World War II, the British collected and stored encrypted communications even through immediate decryption wasn't possible. As cryptanalysis improved, messages were decrypted later. The risk of 'store now, decrypt later' attacks is a critical concern for national security and economic competitiveness. Beyond military secrets, there are other areas of long-time valued data that are targeted by SNDL attacks. This can potentially lead to devastating breaches resulting in significant competitive disadvantage. Examples of long-time valued data include:

- Pharmaceutical research
- Health-related data/ patience records
- Disease surveillance data; biological and chemical threat
- Financial information / long-term investment strategies
- Corporate Intellectual Property / trade secrets / proprietary technologies
- Research and development especially for cutting-edge advancements
- Sensitive legal information
- Genomic data, personal information, and retirement records

What is NIST and their PQA process?

The National Institute of Standards and Technology is part of the United States Department of Commerce. It publishes security guidelines and cryptographic guidelines that are commonly followed throughout much of the world. In 2016, NIST began a process to standard post-quantum algorithms (PQAs). In 2023, NIST has released one key exchange mechanism and three digital signatures for public comment with the hopes of being able to publish final standards in 2024/25.

Are we certain about the safety of PQAs?

No, far from it. At the start of the NIST process there were three main types of PQAs being proposed for key agreement standards: code-based, lattice-based, and supersingular isogeny (SIDH). In July 2022, SIDH was discovered to have a critical flaw exploitable by a classical computer, rendering it insecure, and thus all SIDH methods were dropped from the NIST process. Lattice-based methods are relatively new in cryptographic terms: the first was introduced in 1996, and the only key agreement algorithm currently selected for standardisation by NIST is a lattice-based method called CRYSTALS-Kyber, derived from a method first published in 2005. Lattice methods are favoured for their relative efficiency compared to code-based methods but they are also still being heavily investigated for possible attacks – a side-channel attack was published by Dubrova et al. in 2022[13], and a 2024 paper by Yilei Chen[14] put forward a method for an attack using a quantum computer which might, subject to further research, create compromises. While not definitive, this research calls into question the long-term security of lattice-based methods and highlights the relative immaturity of research in this area, especially given the proposal for these methods to become widely used. Code-based methods like Classic McEliece are more promising from a security standpoint but their extremely large key sizes make them impractical as a like-for-like replacement.

We further note that some signature schemes have also been broken over the course of the NIST process, most notably Rainbow which was selected as a finalist but broken over a weekend by Ward Beullens from IBM Research[15]. A paper published by Phong Nguyen in April 2024[16] describes a proposal which might be used as a basis for the compromise of Falcon, another NIST finalist.

In summary, there are good reasons to believe that the current batch of PQAs may not endure, and this may be the reason behind recent efforts promoting cryptoagile solutions that can be replaced more quickly as research continues.

What do international security agencies say about symmetric keys?

Cyber agencies are currently moving away from recommending for short term Classified use the post-quantum algorithms (PQAs) of the NIST competition and are recommending the adoption of symmetric key protections as part of a crypto-agile strategy. Arqit is unique in being able to orchestrate symmetric key creation from the cloud.

In the USA they have gone further: the NSA/NIAP in the USA specifically mandated recently that all Classified Network vendors of VPN solutions must incorporate symmetric encryption via RFC8784, which Arqit and its OEM partners Fortinet, Juniper and HPE employ.

We'll briefly review the position of major national security organisations.

[13] Dubrova, E, et al., "Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste", Cryptology ePrint Archive, Paper 2022/1713 (2022).

[14] Chen, Y, "Quantum Algorithms for Lattice Problems", Cryptology ePrint Archive, Paper 2024/555 (2024).

[15] Beullens, W, "Breaking Rainbow Takes a Weekend on a Laptop", Cryptology ePrint Archive, Paper 2022/214 (2022).

[16] Bambury, H, "Improved Provable Reduction of NTRU and Hypercubic Lattices", Cryptology ePrint Archive, Paper 2024/601 (2024).

US – The NSA: The White House mandated use of symmetric encryption in 2022[17] which directs National Security Systems (NSS) to use symmetric keys. Arqit made a public response[18] which we released with the knowledge of the NSA CSfC.

The NSA published a statement via NIAP in August 2023 which mandates the use of RFC8784 by all VPN vendors selling under NSA CSfC authority . RFC8784 is the IETF standard which describes how symmetric keys must be injected into networking appliances like VPNs. NSA CSfC/NIAP is therefore demanding that all classified user VPNs use symmetric keys using this standard. We are certain that at present Arqit is the only cloud-software-fulfilled method of delivering symmetric keys which allow true RFC8784 compliance. The only other secure way to inject symmetric keys into appliances using this standard is to use a hardware crypto device, which is cumbersome and expensive and does not allow dynamic creation of multi-cloud connections wherever you want them.

France/Germany/Sweden/Netherlands: A joint paper[19] was issued on 26 January 2024. It is a relatively high level paper on the perceived constraints and issues on use of QKD. The paper also contains statements about symmetric encryption with which we agree:

- "*In light of the urgent need to stop relying only on quantum-vulnerable public-key cryptography for key establishment, the clear priorities should therefore be the migration to post-quantum cryptography* ***and/or the adoption of symmetric keying*** *".*
- *"and post-quantum cryptography and* ***symmetric keying (with pre-shared symmetric keys) must be the primary solutions for quantum-safe cryptography****."*
- "*In light of the urgent need to stop relying only on quantum-vulnerable public-key cryptography for key establishment, the clear priority should therefore be the migration to post-quantum cryptography in hybrid solutions with traditional* ***symmetric keying or classically secure public-key cryptography*****."**

France – ANSSI: The December 2023 paper by ANSSI recommends hybrid methods for authentication and encryption should be used[20]

- *"ANSSI encourages all industries to define a progressive transition strategy towards quantum-resistant cryptography for relevant cryptographic products. The use of hybrid post-quantum mitigation is recommended especially for security products aimed at offering a long-lasting protection of information (until after 2030) or that will potentially be used after 2030 without updates. "*
- *"While there is no concrete evidence that symmetric cryptographic mechanisms would be significantly threatened by quantum computers, a speedup can be expected in certain cases*

[17] See : White House National Security Memorandum 10 (May 4, 2022)

[18] https://7543877.fs1.hubspotusercontent-na1.net/hubfs/7543877/li041023arqit-symmetric-key-agreement-for-quantum-safe-security-of-classified-solutions.pdf

[19] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf

[20] See §1.2 and §1.3 of https://cyber.gouv.fr/en/publications/follow-position-paper-post-quantum-cryptography

with Grover algorithm and other advanced Grover-based algorithms. Thus, as a conservative measure, ANSSI also encourages to dimension the parameters of symmetric primitives as to ensure a conjectured post-quantum security – in practice at least the same security level as AES-256 for block ciphers and at least the same security level as SHA2-384 for hash functions. This encouragement is slightly more conservative than NIST's and BSI's current recommendation."

Germany – BSI:

The BSI recently published a report[21] stating PQCs are not going to help to mitigate the quantum threat in time.

- *"On average, this means the participating organisations expect to complete the migration to quantum-safe cryptography 6.5 years too late. If confidential information can be read for many years, possibly while going unnoticed, this could have serious consequences."*

[21] BSI, "Market Survey on Cryptography and Quantum Computing", August 2023. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Marktumfrage_EN_Kryptografie_Quantencomputing.pdf