Solution Brief

Enterprises, Government Agencies

Achieve Zero-Trust with Arqit SKA-Platform* Powered by Intel

Intel and Arqit collaborate to develop a high-performance platform that delivers a future proof, quantum safe, standards-compliant ZTA system that aligns with an organization's zero trust journey

The Problem

The traditional defense-in-depth security model has been the standard for enterprise network security for many decades, but it has become broken with the adoption of cloud-based network services. An enterprise's network perimeter is no longer a discrete border to guard; the combination of both privately and publicly owned cloud-based services into hybridized organizational networks makes layering security around such infrastructure functionally impossible.

In the face of this security dilemma, the concept of zero trust (ZT) network security has seen broad adoption across industries at an accelerated rate over the past years.

What is Zero Trust (ZT)?

ZT is a set of network security concepts that shift network defense from a perimeter-based model – where users within the "castle walls" are inherently trusted – to one where no trusted entities or network space exists. Identification and authentication of users and their endpoint devices is required regardless of physical or digital network location.

ZT security is provided by always asking questions such as:

- Who is accessing the resources?
- From what endpoint or device?
- To what resources or systems?
- From what geographic location?
- At what time of day?
- Based on what historic activity?

A limitless number of datapoints can be aggregated, distilled, and analyzed by a ZT policy engine to determine whether access by assumed-untrusted subjects should be granted to secure resources.

Shifting to ZT

The significant rate of ZT adoption and investment in the private sector follows a demand signal in the public sector. U.S. Presidential Executive Order (EO) 14028 of May 12, 2021, "Improving the Nation's Cybersecurity," directs the U.S. Federal Government to "advance toward Zero Trust Architecture." The memorandum for the heads of executive departments and agencies, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles" (M-22-09), "... sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific

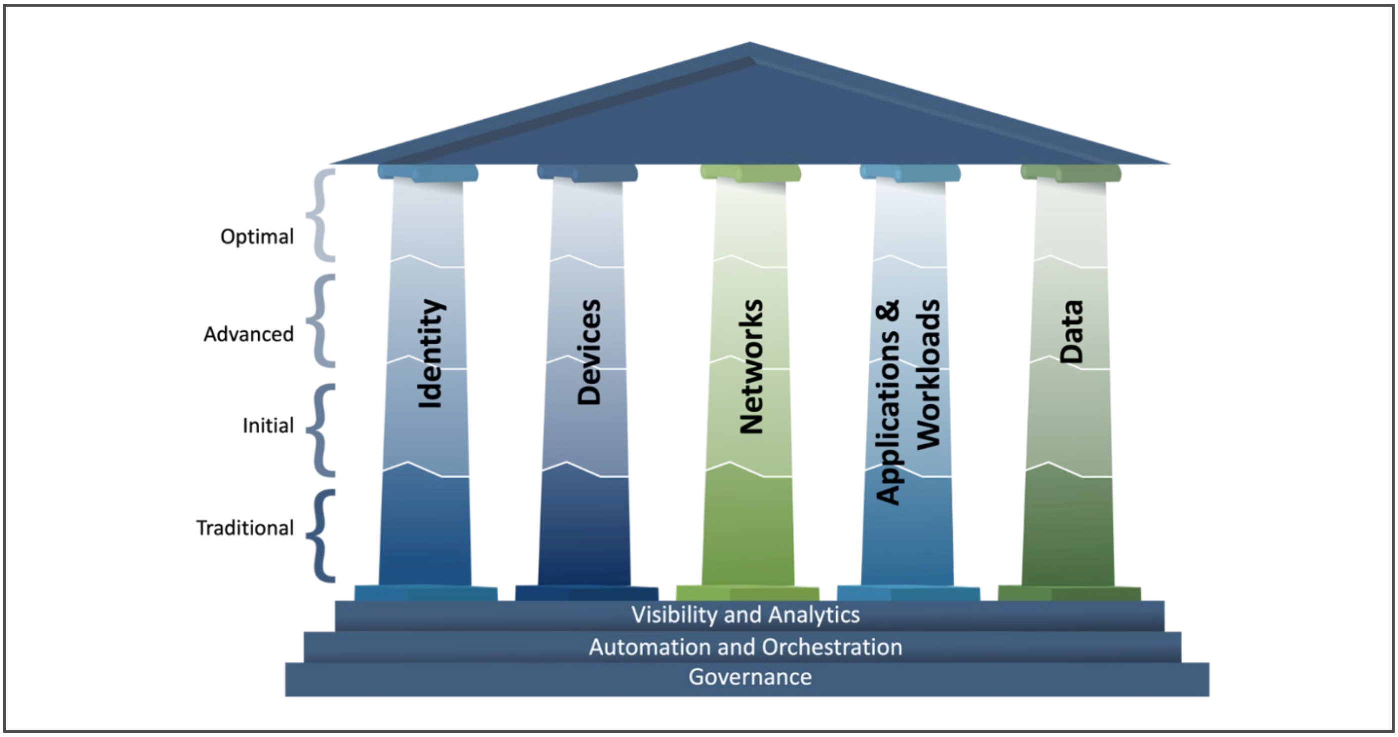


Figure 1. The five pillars of ZTA as defined by CISA (© US Cybersecurity and Infrastructure Security Agency).

cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns."

Recognizing the magnitude of this shift, Arqit, an Intel® Industry Solution Builder member, and Intel are collaborating on a joint ZTA solution.

The Zero Trust Maturity Model

To help both government agencies and enterprises achieve ZT in practice, the US Cybersecurity and Infrastructure Security Agency (CISA) published its Zero Trust Maturity Model v2.0 in January 2022. In outline, the model divides zero trust into five pillars: identity, devices, networks, applications and workloads, and data. For each of these, there is a scale of maturity, from "traditional" (the lowest) to "optimal" (the highest). Implicit in this model is the recognition that ZT adoption is a journey of maturity across many aspects of cybersecurity and network architecture design.

Many treatments of ZTA focus primarily on identity, devices, and applications, ensuring that only trusted users on known platforms can access the relevant information. Less attention is paid to the equally important network and data pillars that emphasize how networks themselves should be segmented and made resilient and how the data in those networks should be protected.

Networks

Networks consist of communication channels connected by network nodes. These might be public networks, like the internet, routed over external nodes, or internal networks routed through internal nodes. It also includes different channel wired and wireless media. In ZTA environments, networks play the critical role of providing encryption of data-in-transit.

Data

In the data pillar, ZTA looks at data-at-rest (encrypted in storage) and data-in-transit (encrypted in the network) and emphasizes the importance of robust protection throughout the data journey. Data classification and inventory management is also extremely important so that security controls can be applied properly and adjusted when needed.

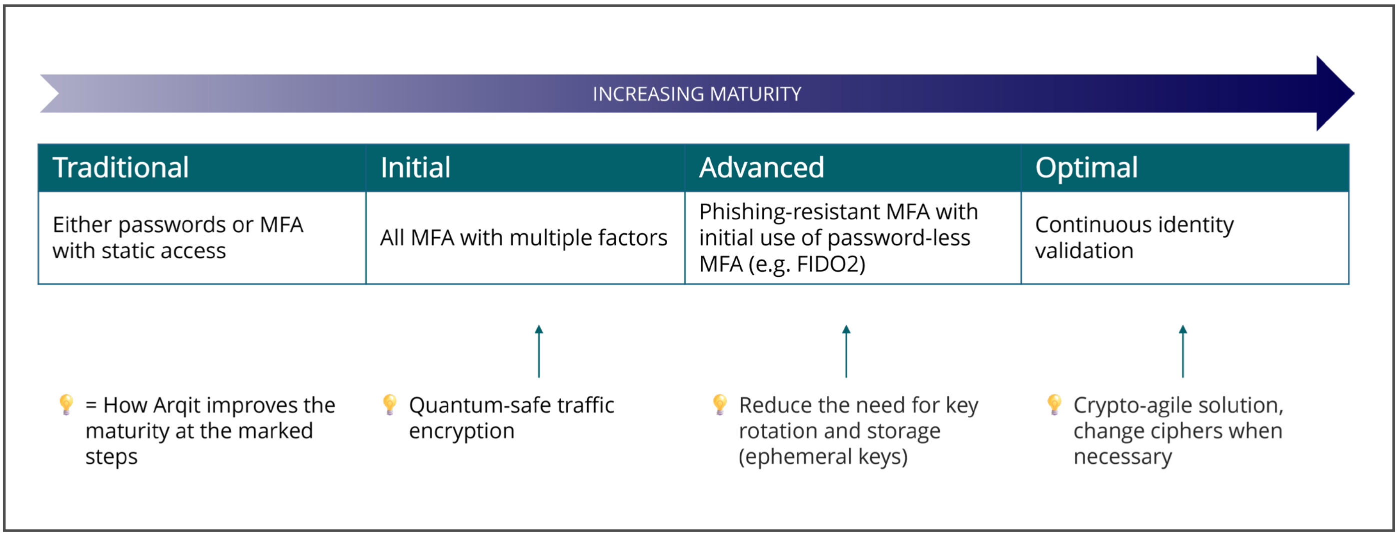
Robust encryption plays a critical role in keeping valuable data safe no matter where it resides and who is accessing it. Often, encryption controls are static, difficult to expose, and even more difficult to update. The emphasis in ZTA is on crypto-agility (having the means to upgrade encryption easily as needed) and least-privilege through frequent rekeying of encryption channels, rather than using keys for long periods.

What's often overlooked is the importance of protecting the encryption keys – ZTA not only looks at the encryption itself but on how the keys used for encryption are managed safely for as long as necessary, i.e. for the lifetime of the data.

This even applies to data-in-transit keys – while these are often ephemeral session keys, the data they protect could have long-term value. Organizations must ensure the keys are of sufficient strength, agreed using appropriate key-agreement protocols, and are handled safely when in use to prevent theft or future exposure.

Identity

In ZTA, ensuring that only the right people have access to the right data has central importance. This means both determining who is accessing the data, and what they have



INCREASING MATURITY

Traditional	Initial	Advanced	Optimal
Either passwords or MFA with static access	All MFA with multiple factors	Phishing-resistant MFA with initial use of password-less MFA (e.g. FIDO2)	Continuous identity validation

💡 = How Arqit improves the maturity at the marked steps

💡 Quantum-safe traffic encryption

💡 Reduce the need for key rotation and storage (ephemeral keys)

💡 Crypto-agile solution, change ciphers when necessary

Figure 2. Pillar 1, Identity. Arqit's authentication key is an additional identity factor and is ratcheted with every new authentication.

access to. The latter can change frequently, so access management needs to be dynamic and fully integrated.

Multi-factor authentication considers not just what a user knows (e.g., a password that could be easily stolen through a phishing attack) but also what they are (e.g., a biometric proof, like a fingerprint) and what they have (e.g., the device they are using). Traditional device-based authentication factors use public-key protocols, like a private certificate, to assert identity, but we know these methods have many well-publicized flaws. A more robust option is to use pre-shared keys – strong, symmetric key-pairs that are installed on the device at manufacture or initial provisioning that live with the device throughout its lifetime. While the cryptography is more secure, this method is let down by the long-lived nature of the key. Manual rekey processes are logistically impractical in networks that are either large scale or made up of components that are geographically dispersed.

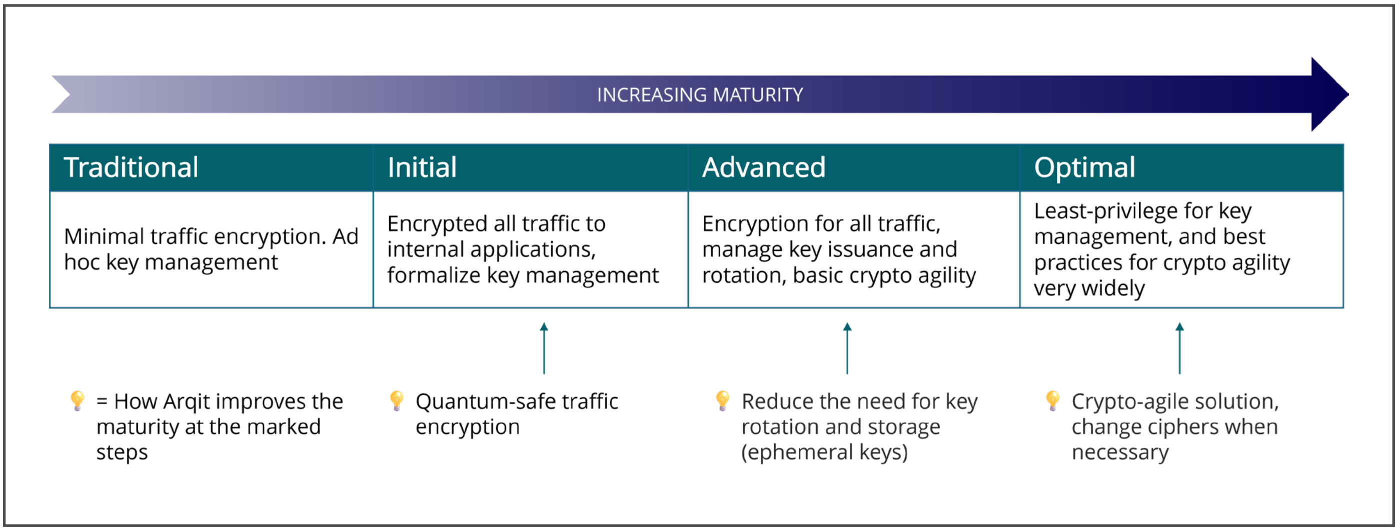
Networks and Devices - Traffic and Data Encryption

Encryption can be difficult to manage, particularly in legacy systems where it's not always obvious if encryption is being performed at all. It's tempting to think that we can segment data carefully enough to mean some data may not need to be encrypted, but the ZTA philosophy says that all traffic should be encrypted, keys should be rotated often, and a crypto-agile approach is needed to stay ahead of emerging threats. Arqit provides support in all three of these areas.

Arqit SKA-Platform Accelerates ZTA Maturity

In the critical areas of identity, network, and data, Arqit offers powerful security products that help organizations advance in their journey toward ZTA.

Arqit's solution uses authentication keys that are fully symmetric, but that are ratcheted (or rotated) every time the



INCREASING MATURITY

Traditional	Initial	Advanced	Optimal
Minimal traffic encryption. Ad hoc key management	Encrypted all traffic to internal applications, formalize key management	Encryption for all traffic, manage key issuance and rotation, basic crypto agility	Least-privilege for key management, and best practices for crypto agility very widely

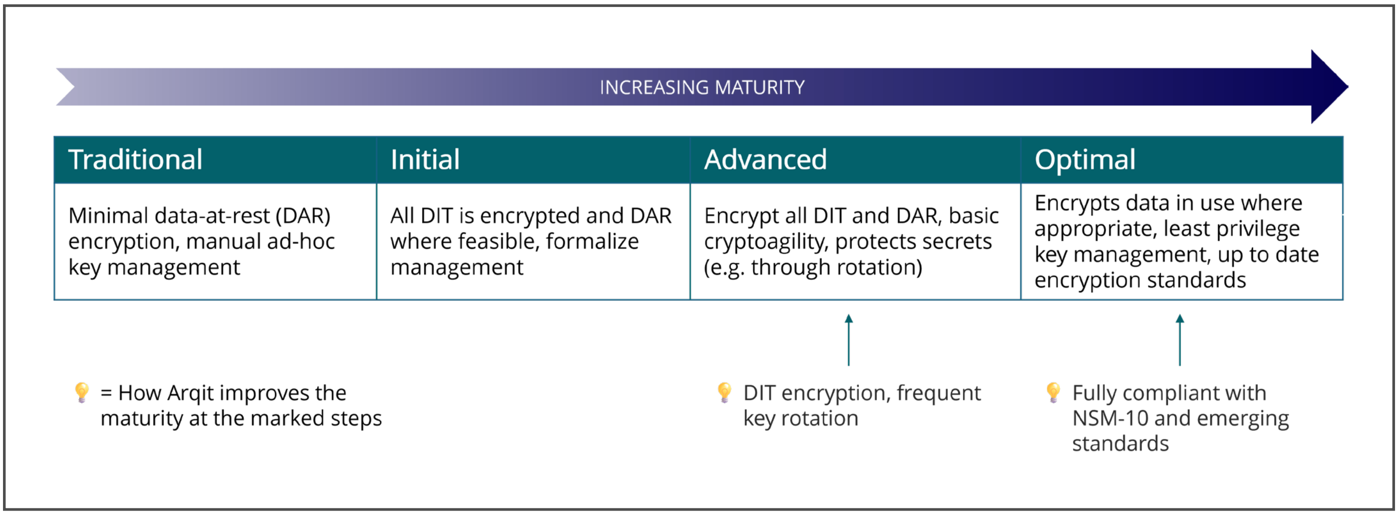
💡 = How Arqit improves the maturity at the marked steps

💡 Quantum-safe traffic encryption

💡 Reduce the need for key rotation and storage (ephemeral keys)

💡 Crypto-agile solution, change ciphers when necessary

Figure 3. Pillar 3, Network Segmentation. Arqit SKA-Platform ensures all traffic is quantum-safe encrypted and that keys are rotated as often as required.



INCREASING MATURITY

Traditional	Initial	Advanced	Optimal
Minimal data-at-rest (DAR) encryption, manual ad-hoc key management	All DIT is encrypted and DAR where feasible, formalize management	Encrypt all DIT and DAR, basic cryptoagility, protects secrets (e.g. through rotation)	Encrypts data in use where appropriate, least privilege key management, up to date encryption standards

💡 = How Arqit improves the maturity at the marked steps

💡 DIT encryption, frequent key rotation

💡 Fully compliant with NSM-10 and emerging standards

Figure 4. Pillar 5, Data Encryption. Arqit SKA- Platform provides frequent data-in-transit (DIT) key rotation and is fully compliant with NSM-10 and emerging standards.

device authenticates. This drastically reduces the lifetime of the authentication key and mitigates the opportunity for a device to be "spoofed" or impersonated on the network. The keys are unique to the device and are simple to manage centrally through policy.

The ratcheting process is done using a newly generated, random value each time that cannot be guessed in advance. This gives each authentication key the property of forward secrecy: knowing a given authentication key doesn't tell you anything about previous keys.

1. Arqit SKA-Platform allows endpoints to create hardened symmetric encryption keys that protect data against both existing and future threats, including those posed by advancements in AI and quantum computers.
2. Encryption keys are treated as ephemeral meaning least-privilege can be re-established for each key agreement, and they can be rotated as often as required.
3. The underlying cryptographic primitives in use, e.g. hash functions, can be swapped out easily as standards evolve without any changes at the endpoint. These changes can be made at policy level in the management plane.

Encryption keys might need to be kept safe for decades, depending on the data they secure. If we are moving beyond ad-hoc processes then we need to not just consider encryption of the data but security of the keys themselves, particularly in a large estate where data can move around a lot. Arqit's keys are compatible with existing key management systems and provide long-term resistance to many forms of attacks, including those emerging from advances in quantum computing.

A Next-Gen ZTA Hardware Solution

To help customers adopt ZTA, Intel® processors have technologies that support Arqit's ZTA solution. The 5th Gen Intel Xeon Scalable processor offers enhanced performance and flexibility, featuring up to 64 cores per processor, and catering to diverse workload requirements. These processors support DDR5 memory, PCIe Gen5, Intel® Ultra Path Interconnect (Intel® UPI) 2.0, and Compute Express Link (CXL) to enhance overall data throughput. Additionally, the processors come with built-in accelerators for cryptography, AI and other workloads.

The processor comes with several critical Intel technologies for ZTA systems, including Intel® Trust Domain Extensions (Intel® TDX), Intel® Software Guard Extensions (Intel® SGX), Intel® Total Memory Encryption (Intel® TME), Intel® Quick Assist Technology (Intel® QAT), Intel® Deep Learning Boost (Intel DL Boost), and Intel® Platform Firmware Resilience (Intel® PFR) (see Addendum 1 for more details).

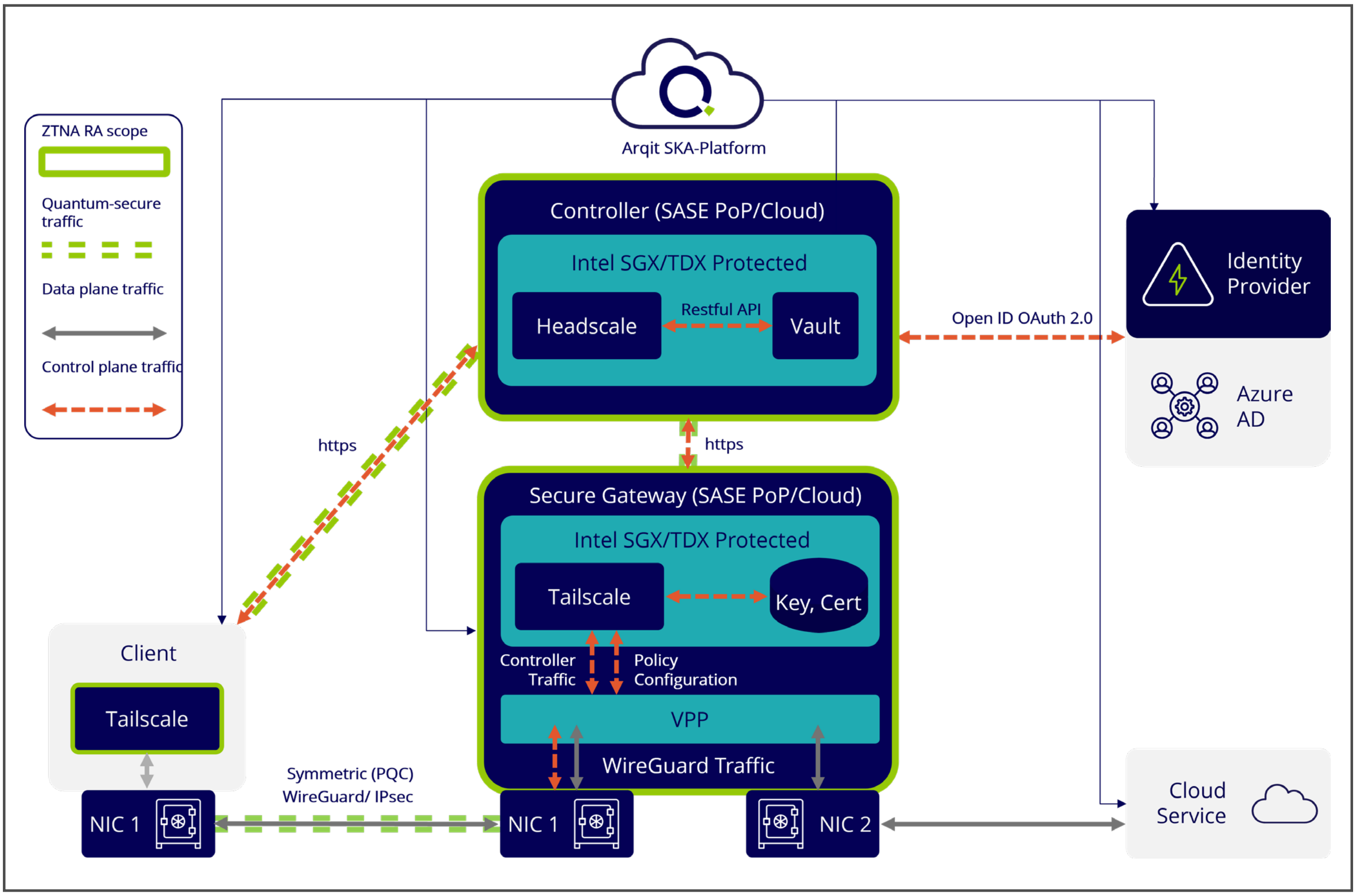


Figure 5. Block diagram of Arqit SKA-Platform enhanced by Intel security technologies.

Advanced Zero Trust Architecture and Benefits

Figure 5 shows how Arqit and Intel built a solution that takes the selected components of Intel technologies and data security technology based on Intel Zero Trust Network Access Reference Architecture and combines them with the Arqit SKA-Platform. Arqit and Intel's policy controls are combined to establish clear workflows and to define how devices should authenticate, the authentication key rotation rate, how session keys are secured, and more.

The client and secure gateway are registered with Arqit SKA-Platform, providing a quantum-safe link with rotating authentication keys. If an authentication event fails, it is simple to revoke access temporarily for investigation, or even permanently.

Existing VPN-protected data channels, such as those protected by both WireGuard and strongSwan IPsec, are upgraded with Arqit SKA-Platform. All data channels are secured with symmetric keys and are made quantum safe. Keys are updated frequently reducing the impact of any compromised keys.

Arqit and Intel can also utilize Vector Packet Processing (VPP) routing and other acceleration technologies to provide high throughput without compromising performance. There is no longer any reliance on long-lived keys, which are difficult to revoke.

Standards Compliance

Arqit 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 by the University of Surrey.

Furthermore, Arqit has confirmed its conformance to a wide range of standards and guidance published by internationally recognized standards bodies, some of which are listed in the Learn More section at the end of this paper. 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. Arqit also conforms to the latest version of CNSA Suite 2.0 published by the NSA. SKA-Platform can run in FIPS mode and uses FIPS 140-2-validated cryptographic modules and HSMs.

Because of an emphasis on symmetric key cryptography and Arqit's methods for rotating authentication keys and creating pre-shared encryption keys on demand, Arqit SKA-Platform conforms to both NSM-10 and the Commercial Solutions for Classified (CSfC) Symmetric Key Management Requirements Annex v2.1 which dictates how government agencies can incorporate quantum-safe symmetric key protections into solutions that use off-the-shelf commercial products to protect classified networks.

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

This version improved and clarified pre-shared key (PSK) usage and added requirements for the implementation of RFC 8784 for IKEv2. This RFC is a mandatory requirement for commercial VPN solutions to be added to the CSfC Approved Components List.

Conclusion: Comprehensive Solution for ZTA Deployments

Arqit's Symmetric Key Agreement Platform (SKA-Platform) is unique in providing a standards-based, quantum- safe authentication and key agreement solution.

- Strong, mutual authentication with forward secrecy of authentication keys to minimize impact in the unlikely event of loss or compromise.
- Crypto-agile, as the underlying cryptographic primitives can be upgraded or replaced.
- Standards-based cryptography conforming to relevant NIST and NSA standards for symmetric cryptography and key management.
- Security groups and policy management enforced in real time to simplify endpoint management.
- Fully symmetric and hash-based symmetric key agreement based on well-characterized and standardized cryptographic primitives known to be computationally secure.
- Split-trust key agreement protocol which ensures the final encryption key is only known to participating endpoints, not the platform.
- Scalable and lightweight at the endpoint.
- Supports and enhances ZTA adoption with focus on device identity and data encryption.
- Arqit 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.

Arqit SKA-Platform utilizes the security protection and performance enhancers available in 5th Gen Intel Xeon Scalable processors. Together the companies offer a complete tool set for an organization moving investing in future-proof ZTA security.

Learn More

Arqit Homepage

Arqit SKA-Platform*

5th Gen Intel Xeon Scalable Processor

Intel Zero Trust Network Access Reference Architecture

Intel® Industry Solution Builders

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

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

[3] 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>.

ADDENDUM 1: Intel Technologies that Secure the ZTA Solution

Intel® Software Guard Extensions (Intel® SGX) allow developers to create isolated execution environments called trusted execution environments (TEE) that ensure that sensitive data and code are protected from access or modification, even by privileged software such as the operating system or hypervisor.

Intel® Total Memory Encryption (Intel® TME) is designed to encrypt all the data on the memory and external memory buses of a CPU with the NIST Standard AES-XTS algorithm with 128-bit keys.

Intel® QuickAssist Technology (Intel® QAT) is an on-chip cryptography and data compression accelerator.

Intel® Deep Learning Boost (Intel® DL Boost) with Vector Neural Network Instructions (VNNI), enhances AI performance by accelerating deep learning inference tasks.

Intel® Platform Firmware Resilience (Intel® PFR) is designed to protect, detect, and recover the platform firmware from cyberattacks or corruption.

Intel® Trust Domain Extensions (Intel® TDX) is Intel's newest confidential computing technology. This hardware-based trusted execution environment (TEE) facilitates the deployment of trust domains (TD), which are hardware-isolated virtual machines (VM) designed to protect sensitive data and applications from unauthorized access.

Notices & Disclaimers

Performance varies by use, configuration and other factors.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See configuration disclosure for details. No product or component can be absolutely secure.

Intel optimizations, for Intel compilers or other products, may not optimize to the same degree for non-Intel products.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

See our complete legal Notices and Disclaimers.

Intel is committed to respecting human rights and avoiding causing or contributing to adverse impacts on human rights. See Intel's Global Human Rights Principles. Intel's products and software are intended only to be used in applications that do not cause or contribute to adverse impacts on human rights.

0125/AL/DJA/PDF Please Recycle 363950-001US