

Arqit SKA-Platform™

SKA-Platform, Arqit's symmetric key agreement platform creates quantum-safe, computationally secure symmetric encryption keys between endpoints, allowing them to exchange data with perfect quantum-safe security.

SKA-Platform integrates with proprietary or commercially available off-the-shelf solutions, applications, network infrastructure, and common network protocols like IPsec and TLS. It can either be consumed on a cloud-fulfilled Platform as a Service basis or deployed on-premise.

Challenges



Threats to National Security

Sophisticated cyber-attacks by nationstate and organized cyber-criminal groups pose significant threats to Defence, Government, and Critical National Infrastructure



Operational Adaptability

Existing systems face challenges in maintaining pace and frequency aligned with modern operational needs.



Cryptographic Modernization

Changing threat landscape with traditional security methods unable to adapt to modern requirements and the time, skills and effort to migrate to most quantum-safe cryptography



Compliance with industry standards and regulations

Meeting the demands set out in US NSM-10² and CSfC Symmetric Key Management Requirements Annex 2.1

Benefits

- Zero-Trust architecture providing scalable, cloudbased dynamic symmetric keys with continuous re-authentication, verification, automation and orchestration, and defence-in-depth approach
- Conforms to NIST standards for cryptography e.g. AES-256, as well as NSA's recommended use of preshared keys to protect against the quantum threat
- Forward security protection against emerging quantum threats, ensuring data remains secure even as cryptographic technologies evolve
- Simple, small-footprint overlay to existing infrastructure, avoiding rip-and-replace by integrating seamlessly with PKI and IPsec
- Enables compliance with National Security Memorandum NSM-10 and NSA CSfC Symmetric Key Management Requirements Annex 2.1
- Seamlessly integrates with existing systems, minimising disruption and streamlining implementation.
- Ensuring optimal security for resource-constrained IoT devices with Size, Weight, and Power (SWaP) limitations. Facilitates the utilisation of symmetric keys in asset classes previously inaccessible.
- Facilitates real-time endpoint management and continuous device authentication.
- Facilitates dynamic network Rx reassignment, allowing flexible alteration of data recipients. Ideal for unplanned operations or international/inter-agency collaboration.
- Cryptographic agility, adapting to any future key size and is independent of any hardware requirements.

¹SNDL 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.

²White 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)

Features and functions

Quantum-safe communication between endpoint devices

Most forms of key exchange methods used in today's networks use mechanisms that are broken by quantum computers which risks SNDL attacks. Arqit's key exchange protocol keeps your data-in-transit safe from such attacks.

SKA-Platform allows for real-time management of endpoints, agreeing quantum-safe encryption keys as often as required. These keys can be used on top of existing network security like Public Key Infrastructure (PKI) and interoperate with protocols like TLS and IPsec by combining the new symmetric key with existing encryption keys.

Strong, lightweight authentication and policy enforcement

We use a strong form of authentication that's not vulnerable to attack by quantum computers and doesn't rely on public and private certificates that are difficult to manage and deploy at scale.

On top of authentication, SKA-Platform enforces policies onto groups of devices, ensuring that only specified devices can talk to one another. When a device reaches the end of its lifecycle it can be easily decommissioned from within SKA-Platform through its web console. Customers gain full control over their network, deciding which devices have access and, more importantly, which devices don't.

Widely deployable and scalable

SKA-Platform technology can be deployed onto a wide variety of endpoints using SDKs written in several different languages. Here are some examples how SKA-Platform can be deployed in your network.

- Between two data-centre firewalls (physical or virtual)
- Between a user device (e.g. a laptop) and a cloud service
- Among a group of IoT devices communicating with a base station

Endpoints require no specialist hardware – in fact, our protocol is so lightweight it uses fewer resources than both existing public-key cryptography and upcoming post-quantum algorithms, making it suitable for deployment on resource-constrained devices like IoT.

Capabilities in depth

SKA-Platform broadly provides four capabilities:

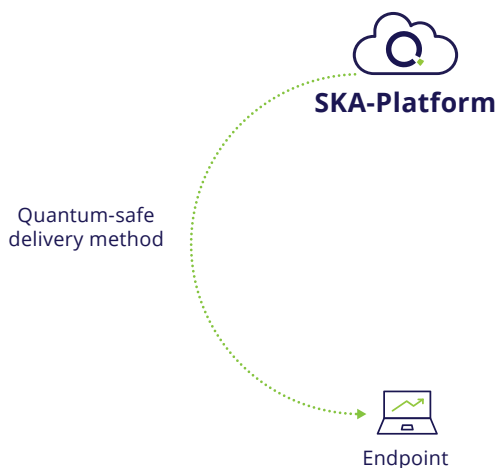
1. Secure registration and provisioning
2. Strong, forward-secret mutual authentication
3. Peer-to-peer session key agreement between endpoints
4. Device management and policy enforcement

These capabilities are delivered completely digitally and require only a lightweight software integration at the endpoint.

1. Registration and provisioning

All endpoints that use SKA-Platform must be registered and provisioned, meaning they are known to SKA-Platform and have been given the correct permissions to use its services.

Figure 1: Provisioning. A bootstrap key is securely delivered from SKA-Platform to the endpoint.



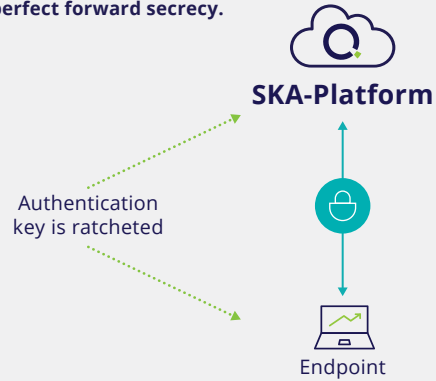
Registration relies on the quantum-safe delivery of a root key, called the bootstrap key, to every device. There are several possible methods for safe bootstrap key delivery depending on the device and the environment. Delivery methods include both manual delivery of keys and over-the-air. Once the bootstrap key is installed a device registers with SKA-Platform via a simple API call.

2. Authentication

Once an endpoint has its bootstrap key it can authenticate with SKA-Platform. We use a zero-trust approach that requires an endpoint to re-authenticate every time and whose permissions are validated in real-time. We use a strong, symmetric form of authentication that's quantum safe and provides forward secrecy with our novel ratcheting process that transforms the key every time an endpoint authenticates.

Figure 2: Authentication. The shared, symmetric key between SKA-Platform and the endpoint is used for active, strong, mutual authentication. The authentication key is ratcheted each time the endpoint authenticates ensuring perfect forward secrecy.

- Zero-trust model – no endpoint is assumed authentic and permissions are validated in real-time
- Authentication keys are ratcheted to ensure perfect forward secrecy
- Strong, mutual authentication based on a symmetric key using hash-based cryptography (HMAC)
- The authentication token is returned as a signed JWT which includes the endpoints claims



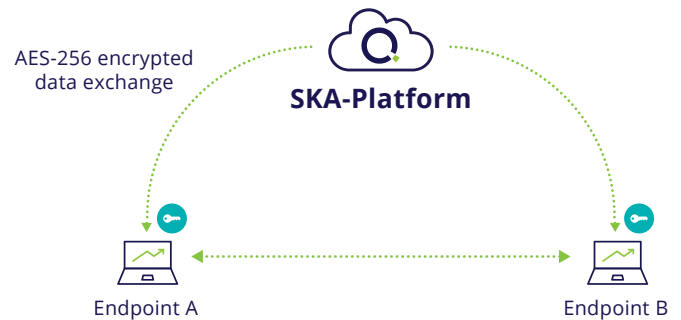
3. Symmetric key agreement

When two or more devices want to create a symmetric key they first authenticate and establish a quantum-safe tunnel with the SKA-Platform cloud service. Each endpoint then takes part in Arqit's protocol to receive high-quality key material (or entropy) from SKA-Platform over the quantum-safe link. This key material is shared with other endpoints and is used to synthesise the final key in a way that isn't known to SKA-Platform, meaning the cloud service never knows or stores the final key.

Figure 3: Key agreement. Endpoints receive identical high-quality entropy from SKA-Platform and create a shared symmetric key using Arqit's proprietary key agreement protocol.

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.

- Quantum-safe key agreement using a novel protocol
- Removes the need for public-key cryptography, although can also easily be done in parallel
- Split-trust model ensures only the endpoints know the final shared key
- Key can be refreshed as often as required for the specific use case



4. Device management and policy enforcement

SKA-Platform offers system administrators tools to manage their network and control device access and permissions. Since every endpoint is authenticated with SKA-Platform, 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. Our 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.

- Control endpoint access and permissions using policies enforced by SKA-Platform
- Group devices together to make management easier and apply policies consistently across devices

Implement commissioning processes so that endpoints are only onboarded after approval from designated personnel.