ARQIT

Product Sheet

Arqit SKA-Platform™ Central Controller (CC)

Arqit SKA-Platform deployed as a Central Controller (SKA-CC) provides a crypto-agile, multi-tenant key management solution to enable telcos and service providers to deploy and deliver Network-as-a-Service (NaaS) software-defined networking and security services that are built on a foundation of high-grade encryption security. SKA-CC is installed in virtualised data centre environments to facilitate the delivery of automated and scalable quantum-safe communication services across thousands of endpoints. High Availability and Disaster Recovery features enable resilient network architectures to support telco-grade service SLAs.

Challenges

1

Threats to National Security
Sophisticated cyber-attacks by nation state and organized cyber-criminal groups pose significant threats to Critical National Infrastructure and Telco networks

2

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

3

Cryptographic Modernization
A changing threat landscape exposes traditional security methods which are unable to adapt and the migration to quantum-safe cryptography requires significant time and effort

4

Compliance with industry standards and regulations
Nations and organizations must meet the demands set out in US NSM-10[1] US and CSfC Symmetric Key Management Requirements Annex 2.1

SKA-Central Controller (SKA-CC) can be provisioned in virtualised data centre or cloud infrastructure to enable quantum-safe network communications across thousands of endpoints including mobile devices, uCPE and Private 5G base stations.

SKA-CC provides an easy installation and setup process on a single server with minimal supporting infrastructure. The platform supports High Availability and Disaster Recovery options to provide resilient architectures for Telco-grade SLAs for uptime and service recovery.

SKA-CC facilitates the dynamic generation of symmetric keys at scale on endpoints that can be used for authentication and/or encryption of communications across untrusted networks protecting sensitive data against classical cyber and quantum threats. SKA-CC provides a cost effective, crypto-agile software solution that enables zero trust architectures ensuring endpoints are actively authenticated using short-lived symmetric credentials, minimising PKI, and session keys are created securely and rotated frequently to achieve high grade, quantum safe data security.

Benefits

Operations:

- Real-time management of endpoints with granular device policies, ad-hoc creation and reforming of security groups, device quarantine, allows flexible network access control.
- Platform Rest APIs enable integration with remote monitoring and management NOC and SOC systems e.g. SIEM.
- Resiliency options – HA and DR for telco-grade SLAs

Economics:

- Tiered Annual License subscriptions allow flexibility to start with small number of endpoints and grow over time.
- Requires minimal infrastructure to operationalise and maintain.
- Compatibility with current encryption algorithms and industry standards, reducing integration costs.

Compliance

- Conforms to NIST SP 800-71 and CSNA 2.0 standards for cryptography e.g. AES-256, Hashing algorithms
- Compliance with National Security Memorandum NSM-10 and NSA CSfC Symmetric Key Management Requirements Annex 2.1, FIPS 140-3 Inside
- ISO 27001, Cyber Essentials certified

[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)

Security

- Dynamic creation and rotation of symmetric session and authentication keys, providing forward secrecy and eliminating provisioning of manual pre-shared Keys (PSKs).
- Supports zero-trust architectures to provide continuous device authentication and granular access control.
- Multiple Root of Trust (RoT) options for storing the SKA-CC master key to address different risk, cost and operational requirements.
- Cryptographic agility, adapting to any future key size without impacting speed and performance and is independent of any hardware requirements.

Widely deployable and scalable

SKA-CC is a small-footprint platform that can be deployed on a single physical or virtual server.

Other Resources:

- SKA-Platform Product Sheet
- NetworkSecure Product Sheets (Fortinet FortiGate, Juniper SRX, strongSwan, Cisco)

SKA-Platform requirements	Recommendation
Host (physical or virtual)	Minimum Specification: ◦ CPU - 8 vCPU ◦ RAM - 32GB ◦ Storage - 50 GB SSD ◦ OS - Linux ◦ CPU Architecture - x86_84 ◦ Docker Engine (v28), Docker Compose (v2)
External database - (physical or VM)	PostgreSQL (v14) configured with: ◦ max connections = 625 ◦ shared buffers= 512MB ◦ Note: Arqit is not responsible for the design and implementation of a Postgres database configured with HA and DR
SMTP provider	Sends transactional emails (account creation, password reset etc.)
(optional) - TPM Root of Trust	TPM v2.0 ◦ Software installed: tpm2_tools (v5.7)
(optional) – HSM Root of Trust	◦ Entrust nShield 5c (appliance) or Entrust nShield 5s (PCIe card) ◦ 1x Virtual Machine (minimum): ◦ CPU: 1 vCPU (x86_64), RAM: 4GB ◦ OS: *Linux, Storage: 20GB SSD Note: Arqit is not responsible for the design and implementation of an Entrust HSM configured with HA and DR
2x TLS certificates	Enables access to SKA-Platform APIs and UI (console)
DNS	DNS provider supports wildcards: ◦ 2x DNS entries: Platform APIs and tenant consoles (resolve to the exterior IP addresses allocated to the edge) ◦ 1x DNS entry (internal access only to Keycloak admin console) DNS provider does not support wildcards: ◦ Multiple DNS entries are required for each SKA-Platform sub-domain, tenant and Keycloak1x
(optional) Public static IP allocations (internet facing deployments)	1 IPv4 address required
(optional) - Private CA X.509 certificates/DNS	Required only for SKA-Platform deployment in a private/internal network. Note: Private CA root certs need to be imported into client devices.
NTP server	Network clock synconisation required between all components
Load Balancer	Required to manage automatic failover across active/passive SKA nodes e.g. Keepalived

**SKA Platform is expected to run on all Linux OS versions supported by Docker. Arqit has validated the platform on Ubuntu 24.04 LTS.*

Case study - Network-as-a-Service (NaaS)

SKA-CC serves as the foundational security pillar in the NaaS architecture, enabling automation and orchestration platforms to securely provision quantum-safe software-defined network services across uCPE.