ARQIT

Product Sheet

Arqit SKA Edge Controller (EC)

Arqit SKA-Platform™ deployed as an Edge Controller (SKA-EC) provides a key management solution on small form-factor hardware appliances to support dynamic operational environments. SKA-EC facilitates the rapid establishment of deployable headquarters to provide secure, scalable and agile command and control (C2) communications infrastructure to ensure mission success in modern military operations and operational superiority over adversaries. SKA-EC delivers improved flexibility, high assurance security, enhanced maneuverability, reduction in size, weight and power (SWaP), hardware costs and overheads to address the evolving requirements of deployed and disaggregated military operations.

Challenges

1

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

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] and CSfC Symmetric Key Management Requirements Annex 2.1

SKA-EC can be provisioned at the edge on hardware appliances to enable rapidly deployable headquarters with distributed C2 nodes that can operate independently or collectively to facilitate secure and agile military operations. The installation and setup process on ruggedized hardware appliances allows for distributed C2 node deployments in hostile terrains e.g. Forward C2 nodes closer to operations or mobile C2 nodes that can rapidly relocate as the battlefield evolves.

Additionally, SKA-EC can be deployed in private or public clouds on a single virtual machine to support ephemeral cloud missions where C2 nodes can be spun up rapidly to support covert communications in dynamic environments e.g. VPN communications between Unmanned Submarine Vehicles (USVs) and operational headquarters.

SKA-EC eliminates current restrictions on deployed C2 infrastructure. By overcoming the complexities, cost implications and limitation of pre-shared keys (PSKs) and avoiding the risks associated with use of PKI, SKA-EC provides a cost effective, crypto-agile and secure-by-design solution that can seamlessly integrate into existing hardware and software solutions. SKA-EC enables split trust and zero trust architectures whilst providing dynamic generation of symmetric keys across trusted endpoints.

Features / Benefits

Operations:

- Extends security to the edge, providing flexibility and agility
- Bearer agnostic – removes operational limitations associated with reliance on physical network connections, enabling utilization of wireless technologies and commercial networks
- Enables dispersed and distributed operations to support current future deployment models
- Real-time management of endpoints with granular device policies, ad-hoc creation and reforming of security groups, device quarantine, allows flexible network access control

Economics:

- Provide security at the edge without expensive hardware-based encryption, support costs and associated SWaP restrictions
- Reduce manual key distribution, storage and management costs
- Compatibility with current encryption algorithms and industry standards, reducing integration costs

[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 generation and forward rotation of symmetric session and authentication keys, providing forward secrecy, eliminating manual key management errors and risks of long-lived static PSKs
- Anti-spoofing capability is supported by forward rotating individual device authentication keys
- Supports split trust/zero trust architectures to provide continuous device authentication and granular access control
- Cryptographic agility - easily adaptable to future key size or algorithm changes as standards evolve, with minimal impact to latency and performance

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

Other Resources:

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

Widely deployable and scalable

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

SKA-Platform requirements	Recommendation
Single 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)
(optional) - External database - (physical or VM)	PostgreSQL (v14) configured with: ◦ max connections = 625 ◦ shared buffers= 512MB
SMTP provider	notification and validation of console user accounts/password setting
(optional) - Hardware Root of Trust (storage of Platform Master Key)	TPM v2.0 Entrust HSM - nShield 5c (appliance) Entrust HSM - nShield 5s (PCIe card)
2x wildcard X.509 certificates	SKA-Platform certificate - client APIs and UI (console) Keycloak admin console certificate
2 x DNS entries (resolve to the exterior IP addresses allocated to the edge)	Enables access to SKA-Platform APIs and UI (console)
Public static IP allocations (for internet facing deployments)	1 IPv4 address required
(optional) - Private CA X.509 certificates/DNS	SKA-Platform deployments in a private/internal network (the private CA root cert needs to be imported into client devices)
NTP server	Network clock syncronization required between all components

**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 - Dispersed and Distributed Headquarters

SKA-EC serves as a central pillar in architecting a scalable HQ, delivering cost and operational efficiencies and a dynamic PACE concept.

- Assurable solution
- Bearer agnostic
- Dynamic generation and forward rotation of symmetric keys
- Eliminate hardware costs, security implications and support requirements
- Manage user groups and information sharing at the encryption layer

Figure 1a: Isolated Node with Multiple Bearers

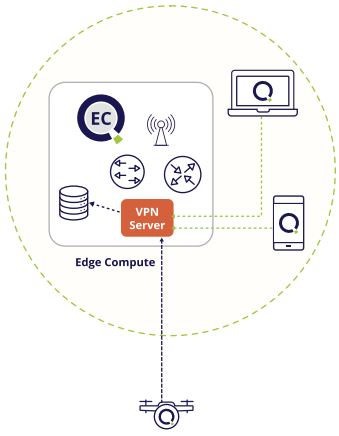

Figure 1b: Interconnected Multi-Node Network