

Crown
Commercial
Service
Supplier



nine23

The High Assurance MSP

Symmetric Key Agreement (SKA) Platform

SERVICE DEFINITION

nine23.co.uk

Service Definition

The Symmetric Key Agreement Platform creates quantum-safe, computationally secure symmetric encryption keys between endpoints, allowing them to exchange data with perfect quantum-safe security. The platform integrates with proprietary or commercially available off-the-shelf solutions, applications, network infrastructure, and common network protocols like IPsec and TLS to enable PQC migrations using quantum-safe VPNs.

Service Features

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.

Service Benefits

- Zero-Trust architecture providing scalable, cloud based 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

Challenges

- Sophisticated cyber-attacks by nation state and organised cyber-criminal groups pose significant threats to Defence, Government, and Critical National Infrastructure (CNI)
- Existing systems face challenges in maintaining pace and frequency aligned with modern operational needs
- 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
- Meeting the demands set out in US NSM-10² and CSfC Symmetric Key Management Requirements Annex 2.1

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.

What Nine23 Do & Why

Nine23 is a veteran-owned **UK Sovereign, High-Assurance Managed Service Provider (MSP)** delivering cyber secure, resilient digital services for mission-critical operations.

Our service offerings include:

- InfoSec Advisory and Assurance
- Private/Hybrid Cloud
- Secure Collaboration
- Interoperability

Our solutions are built to meet the most stringent regulatory compliance requirements and are fully aligned with NCSC/DSIT guidance and Secure by Design principles. We enable individuals and organisations to operate with confidence, security and compliance.

Who Nine23 Work With

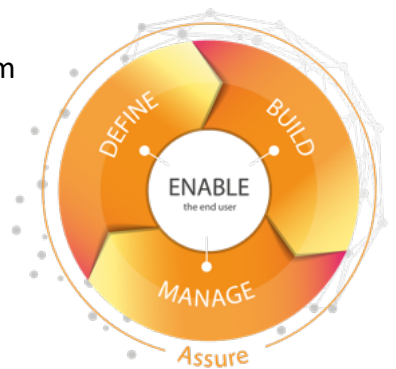
Nine23 delivers exceptional services to Discerning Clients in **UK Regulated Sectors who handle protectively marked data at above OFFICIAL**. We enable the HM Government, National Security and Public Safety, Defence Industry and their supply chains to collaborate and interoperate with simplicity, without ever compromising on security.

We have demonstrated significant achievements in difficult to break into sectors and have a stellar list of clients which demonstrates our credibility.

How Nine23 Work

Our Model

Our operating model builds security, usability, and compliance in from day one, so your technology, people, and processes work seamlessly together. As cyber threats evolve, so do we – keeping your users secure, empowered, and productive through continuous improvement, user-focused design, and UK sovereign solutions that meet national security standards.



Define - Your Problem

We understand information security and assurance as a business enabler, not a constraint. Our experts will conduct a comprehensive discovery phase to assess current capabilities and risks, define key security objectives, compliance standards, and end-user requirements, and develop a clear roadmap that enables digital transformation with high assurance at its core.

Build - Your Solution

We combine the best technology from the best vendors to create an environment that enables individuals to work together effectively and securely. Leveraging trust, innovation, and a depth of sector experience to provide collaboration and interoperability.

Manage - Your Service

We deliver high assurance and resilient managed services that enable seamless interoperability for teams to access the data and applications they need to work collaboratively. Our managed services include:

- 24/7 monitoring, proactive risk management, and compliance assurance
- Threat detection, response, and continuous security improvements
- A transparent Service Level Agreement (SLA) ensuring clear accountability

Why Choose Nine23?

Enabling the end user is the heart of everything we do, empowering them to work with the same simplicity and usability they expect at home, without ever compromising on security.

We are **trusted, proven experts with a strong track record** of delivering nationally accredited, user-focused solutions in complex and highly regulated environments.

We deliver high assurance solutions **accredited for use at OFFICIAL (including SENSITIVE and other caveats) through to SECRET**, meeting the most stringent cyber security

requirements. As a fully UK-owned and operated company, with all staff, infrastructure, and data located in the UK, we provide genuine **100% UK data sovereignty**.

Above all, we are **refreshingly honest**. Building long-term relationships through transparency and integrity, with no jargon or hidden risks, just secure solutions that deliver real operational value.

