



ARIA Key Management as a Service

Easy to deploy, enterprise-wide key management for any encryption workload.

The ARIA Key Management as a Services (KMaaS) application is a cloud-based encryption key management service that delivers painless security for any encryption workload. It allows organizations of all sizes to centrally store, manage, and consolidate key management functions across on-premise, private cloud, public cloud, hybrid cloud, SaaS, and a range of edge applications and endpoints.

Key Features

- Offered as a fully managed, multi-tenanted cloud service.
- Secured and powered by redundant, FIPS 140- 2 compliant, hardened virtual appliance.
- Delivered through a highly available, geo-dispersed architecture.

Flexible Cloud-based Key Life-cycle management

The ARIA KMaaS provides the ability to integrate with any virtual machine encryption workflow, such as VSphere, and connect to any location, anywhere. It supports data-at-rest encryption for database, storage, application, and custom use cases, as well as data-in-transit for authentication, transactions, and data transfer.

Powerful performance, continual access

With ARIA KMaaS, customer encryption keys are always secure, and always accessible. Through a virtual appliance's hardened design, it delivers powerful high availability, and load balances clusters that protect against distributed denial-of-service (DDoS) attacks. Superior data protection is achieved through the solution's multi-level key security and strong authorization methods. The multi-tenanted architecture secures data through tenancy isolation, segmented databases, and workload boundary enforcement.

Simple installation and management

The ARIA KMaaS solution is easy to deploy, enabling customers to implement enterprise-wide key management in less than five minutes. It offers an exceptionally intuitive user interface, to easily manage users, groups and integrations, quickly create keys, and oversee the full key lifecycle. Administration is effortless, thanks to the step-by-step “wizard” setup, painless backup and restore capabilities, and the ability to implement role-based access control. Advanced reporting and behavioral insight enable detailed auditing and logging, dashboard alerts, and syslog exportable to popular SIEMs.

Specifications

Robust Crypto Operators	<p>Supports many different key algorithms, including symmetric and asymmetric key types.</p> <p>Formats include the following: AES 128, 192, 256, - RSA 2048, 3072, 4096 Elliptic curve (ECDSA) - support of 85 curve algorithms</p> <p>Enables users to choose the algorithm that fits their needs</p>
Programmatic Key Rotation	<p>Retires outdated encryption keys and generates new cryptographic keys to replace them</p>
Painless Backup and Restore	<p>Saves and stores the current ARIA KMaaS state for future restoration</p> <p>Set on-demand and scheduled backups to an external location, restoring them when required</p>
KMIP Server	<p>Only one key management service is necessary to facilitate all key encryption requirements</p> <p>Deploy as a KMIP server in a virtual environment in minutes, for a fraction of the cost and effort of an HSM Reduce overheads/administration related to managing encrypted data, such as tape drives, databases, storage array and software, through centralized management</p>
REST API	<p>Applications can connect, interact and integrate directly with ARIA KMaaS</p> <p>A common interface for key management operations (get, fetch, rotate, etc)</p> <p>Build automation workflows and integrate with use cases limited by previous standards like PKCS#11</p>
Any Workflow	<p>BYOK allows companies to encrypt data and retain control and management of encryption keys, even in the cloud</p> <p>Leading edge KMIP adoption, to enable communication with all systems and environments</p> <p>Extend the reach of HSM's to a multitude of new workflows</p>
Full Key Lifecycle Management	<p>Ensure compliance and enact robust key policies</p>
Advanced Authentication	<p>Secure single-sign-on (SSO)</p> <p>Cryptographically layered key wrapping</p> <p>Tokenization and Certificate authentication</p>
Detailed Auditing and Logging	<p>Analyze and report on key management activities to uncover potential threats</p> <p>Collects data through the use of the syslog format, which can then be exported to external SIEM tools</p>

Supported Virtual Environments Integrations

Third-party integrations are generally achieved through the use of KMIP, below are the supported environments:

VMware, vSphere and vSAN	Enables vSphere VM encryption, via KMIP integration
Nutanix	Enables the use of self-encrypting drives (SEDs), via KMIP integration
IBM DB2	ARIA KMaaS can create a centralized key store when using DB2 native encryption
MongoDB	Enables data-at-rest encryption through storage-based symmetric key encryption, via KMIP
NetApp ONTAP	ARIA KMaaS can act as a key management server for volume encryption, via KMIP
Veritas	ARIA KMaaS can act as the key management server for Veritas Netbackup encryption, via KMIP
Commvault	Using KMIP, ARIA KMaaS protects Commvault software encryption keys stored in a CommServe database.

Order Details

subscription service purchasable for 1, 2 or 3 year terms. Encryption keys must be purchased separately, on an annual basis, and are available in key packs, starting at 50 keys.

SDS-KMaaS-BASE 1YR	KMaaS Base Charge, 1 year – Zero keys included
SDS-KMaaS-KEYPAK-250	Annual KMaaS pack of 250 encryption keys
SDS-KMaaS-KEYPAK-100	Annual KMaaS pack of 100 encryption keys
SDS-KMaaS-KEYPAK-50	Annual KMaaS pack of 50 encryption keys
SDS-KMaaS-BASE-3YR	KMaaS Base Charge, 3 year – Zero keys included
SDS-KMaaS-BASE-2YR	KMaaS Base Charge, 2 year – Zero keys included
SDS-KMaaS-KEYPAK-500	Annual KMaaS pack of 500 encryption keys

Other ARIA KMS offerings

ARIA Cybersecurity offers additional key management solutions to fit a variety of user environments

- ARIA KMS – a hosted, on-premise application.
- ARIA microHSM – pre-installed on a secure intelligent adapter (SIA) for advanced security using TrustZone and offload capabilities.
- ARIA HSM Appliance – turn-key solution deployed in 1U rack mounted server, consult with ARIA Cybersecurity sales.

Contact Us to Schedule a Technical Demonstration or Arrange an Evaluation ✉ ARIAsales@ariacybersecurity.com

ABOUT ARIA CYBERSECURITY SOLUTIONS

ARIA Cybersecurity Solutions recognizes that better, stronger, more effective cybersecurity starts with a smarter approach. Our solutions provide new ways to monitor all internal network traffic, while capturing and feeding the right data to existing security tools to improve threat detection and surgically disrupt intrusions. Customers in a range of industries rely on our solutions each and every day to accelerate incident response, automate breach detection, and protect their most critical assets and applications. With a proven track record supporting the Department of Defense and many intelligence agencies in their war on terror, and an award-winning portfolio of security solutions, ARIA Cybersecurity Solutions is committed to leading the way in cybersecurity success.

ARIA Cybersecurity Solutions • 175 Cabot St, Suite 210 • Lowell, MA 01854

Connect with Us: ariacybersecurity.com • ARIAsales@ariacybersecurity.com • 800.325.3110

Follow Us: [Linkedin](#) • [Facebook](#) • [Twitter](#) • [Blog](#)

