aria CYBERSECURITY SOLUTIONS

DATASHEET

ARIA SDS microHSM Secure Key Management and Crypto Offload

The ARIA™ SDS micro Hardware Security Module (HSM) provides a secure, easy, and low-cost way for organizations to adopt and manage KMIP-based software encryption applications and still maintain a fully secured key management system server.

microHSM Benefits

- **Secure platform:** FIPS 140-2 Level 3-compliant hardware – serves content over PCIe bus or 10/25Gb interfaces.
- **Add strong encryption to new, or existing servers, with negligible use of CPU cores:** Run sustained aggregate 40Gb wire rate encryption applied on a per-app, per-tenant basis by supporting independent key trees and secrets.
- **Performance:** Serve tens of thousands of keys per minute, ideal for per-application or per-transaction crypto operations for compliance purposes.
- **Impenetrable encryption key storage and execution:** Secure key cache and TrustZone in hardware means keys in use can't be captured, stolen, or lost.
- **Rapid automated deployment:** Zero touch provisioning is provided via the ARIA SDS Orchestrator.
- **Zero footprint:** ARIA microHSM can be deployed directly within an application server, built into a vSAN configuration or other HCI solutions, eliminating the need for network connectivity to an appliance.

An innovative joint crypto with KMS solution

The market has been requesting a secure, easy-to-deploy, easy-to-manage key management service (KMS) combined with crypto offload capabilities. ARIA microHSM now addresses this need with a virtualized HSM application and the Myricom Secure Intelligent Adapter (SIA).

This powerful combination delivers:

- Up to ten times the performance at half the cost when compared to an HSM appliance
- The industry's most flexible key management service
- Open KMIP with a large ecosystem of KMIP-capable applications
- Full FIPS 140-2 Level 3 compliance
- 40Gb hardware-accelerated encryption at line rate
- The ability to be deployed in minutes in any standard server

Access to the key server functionality can be achieved in two ways:

1. The first, via KMIP, provides out-of-the-box integration with any application that already supports KMIP.
2. The second is through the provided REST API. Either method allows customers to build their own integrations to the key server.

Crypto acceleration functions are accessible using the standard connectors such as OpenSSL, JCE, and libcrypt.

The ARIA microHSM creates a strong security domain, taking advantage of TrustZone on the Myricom SIA adapter card. This separates security functions, such as key storage, from the host x86 CPU, which has been shown to be vulnerable to attack.

ARIA SDS MICROHSM SPECIFICATIONS

Bus Interface	PCIe Gen 3, 8 lanes wide
Form Factor	PCIe Full Height, ¾ Length
Electrical Power	<70W with transceivers installed
Network Connectivity	Dual SFP+/SFP28 ports; 10/25Gb use
Processor	16 Cores @ 2GHz
Compliance	FIPS 140-2 level 3 compliance
Management	Deployed and managed by ARIA SDS Orchestrator
Security	TrustZone based secure key storage Key storage – Greater than 40M keys. Supported key types - Generation of ECDSA (many named curves), RSA2048, 3072, 4096, AES128,192,256, and import of any of those types as well as CUSTOM data including SSL keys, SSH, application formatted keys, etc. Support X.509 PEM based certificates as well. Support for Symmetric and Asymmetric Encryption algorithms
Throughput	Sustained 4Gb wire rate encryption 900,000 key wrap or unwraps per second served from stored keys
Software Support	Drivers available for Linux (CentOS, RHEL, and Ubuntu) Supports DPDK for Linux (high-performance packet processing) Host-side driver support for Linux and Windows Network overlay offloads for NVGRE, VxLAN, and MPLS encapsulated traffic High performance network storage with full protocol offloads for SCSI, iSCSI Extensions for RDMA (iSER) to support NVMe, and FCoE
Warranty and add-on support	One year for hardware, and 90 days for software. Ninety (90) days of “get- started” telephone and email support, as well as any software upgrades shipped within that timeframe. Refer to the support datasheet for options to extend the 90-day window.

Contact Us Today: sales@ariacybersecurity.com or (978) 954-5038

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 O1854

Connect with Us: ariacybersecurity.com / Linkedin / Twitter / Blog

aria CYBERSECURITY SOLUTIONS ariaSDS nVoy SECURITY APPLIANCES Myricom NETWORK ADAPTERS