aria CYBERSECURITY SOLUTIONS

DATASHEET

ARIA microHSM Secure Key Distributed Crypto Offload

The ARIA™ micro Hardware Security Module (HSM) provides a secure, simple to deploy way for organizations to adopt and off-load KMIP-based encryption for their critical applications.

microHSM benefits

- **Better approach:** PCIe based SmartNIC adapter that acts as a local HSM for the server in which it is hosted, communicating over the PCIe bus or over the 10/25G network ports.
- **Secure platform:** FIPS 140-2 Level 1 compliant code generates keys & certs out of TrustZone, securely encrypting content with on board chipset. Avoids X86 host vulnerabilities exploitable by hackers.
- **Add strong encryption to new, or existing servers, with negligible use of CPU cores:** Off-loads encryption from hosts. Allowing it to be applied on a per-app, per-tenant basis by supporting independent key trees and secrets.
- **Distributed:** Puts the HSM in the servers where you need it, 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.
- **Zero footprint:** ARIA microHSM can be deployed directly within an application server, storage server or HCI solutions, eliminating the need for network connectivity to an appliance.

An innovative solution

The market has been requesting a secure, easy-to-deploy, easy-to-manage HSM solution combined with KMIP enabled crypto offload capabilities. ARIA Cybersecurity has addressed this need with its ARIA microHSM comprised of an onboard HSM application deployed upon the Myricom Secure Intelligent Adapter (SIA) PCIe adapter card.

The advantage is that the microHSM fits in any server PCIe slot, hence encryption functions can be handled physically within a given server, but logically separate, off-loaded from the X86 host.

The ARIA microHSM creates a strong security domain, taking advantage of TrustZone on our SIA, providing a trusted execution environment for key-handling operations. This protects functions, such as key creation and storage, from hackers. The keys in use are locally cached on the card performing the encryption functions, safely off the local host's x86 CPU environment.

This is important because running encryption on the X86 host has been shown to be easily accessible to hackers wishing to access critical protected data. The keys are run in the clear, and easily captured by a hacker that penetrates the server, Once the keys are captured, data can be accessed anywhere by applications using those same keys. The ARIA microHSM prevents such harm – securely running all encryption functions on the PCIe based Card.

This powerful combination delivers:

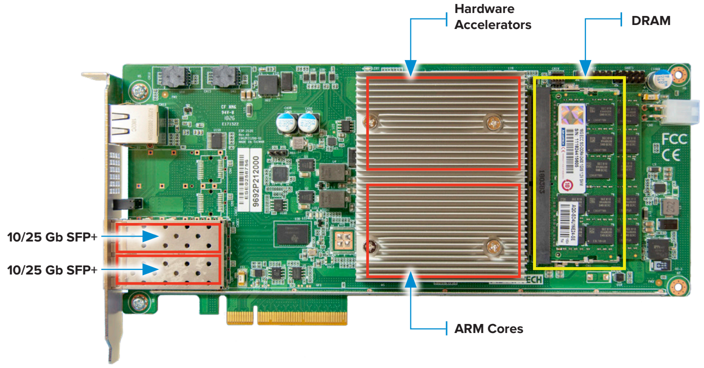
- Up to ten times the performance in server at half the cost when compared to a network connected HSM appliance
- The industry's most flexible but secure key management handling capabilities
- Open standard KMIP encryption with a large ecosystem of KMIP-capable applications
- FIPS 140-2 Level 1 compliance
- The ability to be deployed in minutes in any standard server
- Plug and play HA capabilities, unlike the painful configurations from legacy industry leading platforms

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

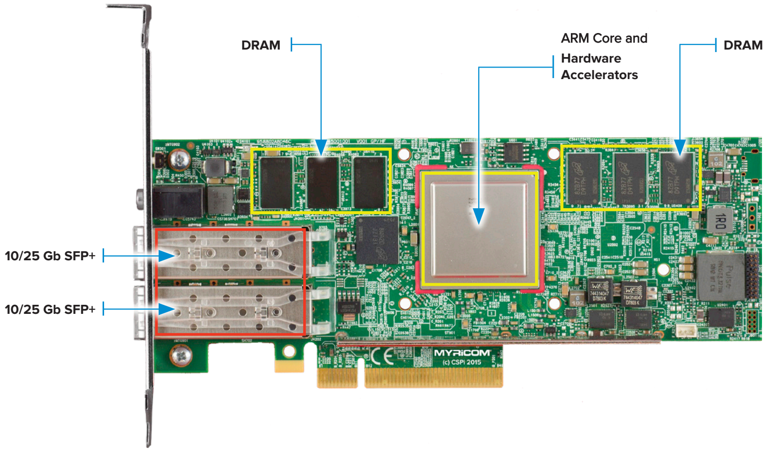
1. The first, via KMIP, provides out-of-the-box integration with any application that already supports KMIP.
2. The second is through the provided REST API. Either method allows customers to build their own integrations to the key server.

The ARIA microHSM is offered in two options:

Myricom SIA



Myricom SIA Express



SPECIFICATIONS	SIA	SIA Express
Dimensions	4.2” x 9.6”	2.7” x 6.6”
Bus interface	PCI Express Gen 3, 8 lanes wide	PCI Express Gen 3, 8 lanes wide
Form factor	PCI Express full height, three quarter length	PCI Express half-height, half-length (HHHL)
Electrical power	< 65W	<45W
Cooling Requirements	It is required that adapters be installed into servers that provide air flow over the PCIe slots.	It is required that adapters be installed into servers that provide air flow over the PCIe slots.
Cooling Options	Passive cooling	Active cooling
Operating Temperature	0-50 deg C (250 LFM min at max ambient temperature)	0-50 deg C (290 LFM min at max ambient temperature)
Storage Temperature	-40 to 70 deg C	-40 to 70 deg C
Storage Humidity	5% to 90% non-condensing	5% to 90% non-condensing
Processor	Network SoC – 16x, 2.0 GHz Arm cores	Network SoC – 8x, 3.0 GHz Arm cores
Hardware Acceleration	Support for, and the acceleration of, various security functions, such as symmetrical and asymmetrical encryption Line rate packet classification Deep packet inspection (DPI) Flow generation	Traffic flow accelerator engine. Public Key Acceleration (PKA) engine 100 Gb/s cryptography engine with single-pass hashing and encryption/decryption
Memory	8-32GB DDR4 64GB Flash	16GB Flash
Network Connectivity	Dual SFP+/SFP28 ports; 10 or 25G 1 x 1000Base-T - RJ-45	Dual SFP+/SFP28 ports; 10 or 25G
Software Support	Drivers available for Linux (CentOS, RHEL, and Ubuntu) Supports DPDK for Linux (high-performance packet processing)	Drivers available for Linux (CentOS, RHEL, and Ubuntu) Supports DPDK for Linux (high-performance packet processing)
SW Version supported	ARIA SDS	ARIA SDS

SPECIFICATIONS	SIA	SIA Express
Security	ARIA Packet Intelligence ARIA KMS ARM TrustZone Secure Boot Secure Key Storage	ARIA Packet Intelligence ARIA KMS ARM TrustZone Secure Boot Secure Key Storage
Throughput	2x 10/25Gb per Second	2x 10/25Gb per Second
Timestamp (if applicable)	N/A	N/A
Regulatory approvals, compliance	RoHS (Reduction of Hazardous Substances). EMI and EMC, Class A USA, Canada, and Europe.	RoHS (Reduction of Hazardous Substances). EMI and EMC, Class B USA, Canada, and Europe.
Country of Origin	Taiwan	Taiwan
Warranty	One year for hardware defects and 90 days for software defects. 90 days of "getting started" telephone and email support, as well as any software upgrades shipped within that window. Refer to the support datasheet for options extending the 90-day window. Extended warranty available	One year for hardware defects and 90 days for software defects. 90 days of "getting started" telephone and email support, as well as any software upgrades shipped within that window. Refer to the support datasheet for options extending the 90-day window. Extended warranty available
Ordering Details **(license can be purchased separately on already sold adapter).**	25G-PCIE3-8B-2S-HSM SIA – Dual 10/25G Security Intelligent Adapter for Key Management. This version is configured as a Hardware Security Module (HSM) supporting encryption key management.	25G-PCIE3-8C-2S-HSM SIA - Dual 10/25G Security Intelligent Adapter (low profile) for Key Management. This version is configured as a Hardware Security Module (HSM) supporting encryption key management.
Cables and transceivers	Contact your Account/Sales representative for more information on cables and transceivers that are compatible with this adapter.	

Contact Us Today: ARIAsales@ariacybersecurity.com or 800.325.3110

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 • ARIAsales@ariacybersecurity.com • 800.325.3110

Follow Us: Linkedin • Facebook • Twitter • Blog

aria CYBERSECURITY SOLUTIONS ariaSDS nVoy SECURITY APPLIANCES Myricom NETWORK ADAPTERS