ARIA SDS microHSM

Secure Key Management and Crypto Offload

CSPi's 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.

The market has been requesting a secure, simple to deploy and manage key management service (KMS) combined with crypto offload capabilities. CSPi has addressed this need with its ARIA microHSM, which consists of a virtualized HSM application and the CSPi 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 KMS
- 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. The first, via KMIP, provides out-of-the-box integration with any application that already supports KMIP. 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.

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

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**
  Serves 10s of 1000s of keys per second – ideal for per application or per transaction crypto operations for compliance purposes.
- **Impenetrable encryption key storage and execution**
  Secure Key Cache – TrustZone in hardware
  Keys in use cannot be captured/stolen/lost
- **Rapid automated deployment**
  Zero touch provisioning provided via the ARIA SDS orchestrator platform
- **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

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 iSCSI, iSCSI Extensions for RDMA (iSER) to support NVMe, and FCoE
OTHER DETAILS	
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.

Secure your Enterprise today. Contact us: myricomsales@cspi.com

About CSPi

CSPi (NASDAQ: CSPi) is a global technology innovator driven by a long history of business ingenuity and technical expertise. A market leader since 1968, we are committed to helping our customers meet the demanding performance, availability, and security requirements of their complex network, applications and services that drive success.

CSPi Corporate Headquarters
175 Cabot Street - Suite 210
Lowell, MA 01854
800.325.3110 (US & Canada)

CSPi High Performance Products
800.325.3110 (US & Canada)
us-hpp-sales@cspi.com

CSPi Technology Solutions
800.940.1111
us-ts-sales@cspi.com

www.linkedin.com/company/csp-inc
@ThisIsCSPi
us-hpp-sales@cspi.com
www.cspi.com

MYRICOM Network Products