ARIA SDS KMS Application

CSPi's ARIA™ Key Management Server (KMS) is an easy-to-deploy application that takes advantage of the widely accepted key management interoperability protocol (KMIP) for integration with other existing applications. When ARIA KMS is deployed on the Myricom Secure Intelligent Adapter (SIA), organizations gain additional security and performance since it provides a trusted execution environment for key handling operations.

The market has been requesting a simple-to-deploy and easy-to-manage key management solution. VMware allows users to encrypt the output of each VM with its standard ESXi KMIP-based client. While hyper-converged interface solutions, including VMware vSAN™, have embraced the use of KMIP clients to perform encryption, both solutions still need a compliant key server to complete the solution. CSPi has addressed these needs with its ARIA KMS application. The ARIA KMS application allows you to:

- Leverage native encryption and bring your own key (BYOK) in storage and applications
- Use optional end-to-end KMIP server and client
- Provide high-availability, secure key storage in a virtual server, on premise or in the cloud
- Centrally control keys in a one-to-many deployment
- Manage policies across platforms through a single user interface
- Establish consistent configuration and enforcement, including revocation

The ARIA KMS solution provides two ways to access the key server. The first, via KMIP, provides out-of-box integration with the large number of applications that already support clients based on KMIP standard. The second, is via the provided REST API. Either method allows customers to build their own integrations to the key server.

FEATURES

ARIA KMS Benefits:

- KMIP Key Server
    - Includes integrated features and capabilities like intelligent key management, advanced policy control, and enhanced access control for users and keys.
- Rapid automated deployment
    - VM-based, on-premises KMS deployment in under one hour.
- High availability
    - Multi-node high availability with master-master server configurations to help you meet resiliency planning and latency-reduction goals.
- Secure platform availability
    - FIPS 140-2 level 1-compliant software standard with optional FIPS 140-2 Level 3-compliant PCIe adapter for enhanced security and performance.
- Performance
    - Serves thousands of keys per minute – ideal for per-application or per-transaction crypto operations for compliance purposes.
- Impenetrable encryption key storage and execution
    - When deployed on CSPi's Myricom® SIA, the solution provides the advantages of a Secure Key Cache – TrustZone in hardware, where keys in use cannot be captured/ stolen/lost.
- Zero footprint
    - ARIA KMS can be deployed directly, or built in to a vSAN configuration or other HCI solutions, eliminating the need for connectivity outside of the HCI solution.

When deployed as part of the ARIA SDS platform, license keys are securely deployed, configured, and managed, which is beneficial for "zero-touch provisioning," remote management, and health monitoring. The ARIA KMS deployments include both FIPS 140-2 level 1 for virtual instances, for cloud or on-premise use, as well as FIPS 140-2 level 3 for hosted instances using the Myricom SIA.

CSPi's Myricom SIA is a secure deployment platform combining a next-generation high-speed network adapter with the programmability of multi-core ARM processing in order to provide application-specific feature support.

This 10 or 25 GB dual-port network interface card (NIC) provides a local secure zone-of-trust required to generate and store keys and even execute crypto operations based on those stored keys. When running the ARIA KMS application, it delivers a trusted execution environment for key handling operations utilizing TrustZone based TPM. This shields the keys from exposure, even if the host server is breached, unlike Intel's® vulnerable Xeon™ SGX-based TPM environments.

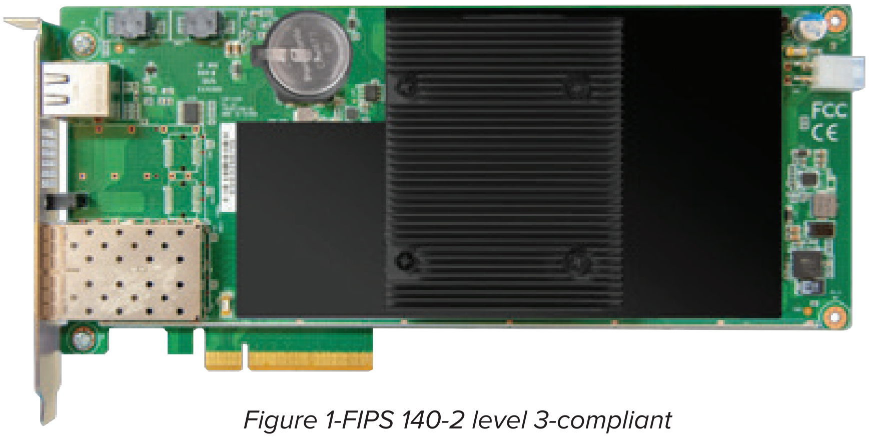

Figure 1-FIPS 140-2 level 3-compliant

The Myricom SIA allows organizations to dramatically reduce server costs while protecting the use of the keys during encryption. The SIA can also can also be deployed into the devices they are protecting, such as storage arrays, for a zero footprint implementation for a key server solution. High-availability functionality, as well as scaled up performance, can be achieved by grouping together multiple SIA cards.

For organizations that need to encrypt the output of their ESXi VMs - the I/O including VM files, virtual disk files and core dumps can utilize VMware vSphere virtual machine encryption capabilities provided within the hypervisor. This requires a third-party KMS, such as the ARIA KMS, installed in a high-availability cluster to serve the keys, and vCenter handles the configuration of the clients' access to the ARIA KMS. The ARIA KMS automatically provisions the cluster, thus making a formerly complicated process executable by a single command. Utilizing the ARIA KMS solution reduces the entire process to a few minutes of time, including the configuration within vCenter.

Storage drives that utilize single key self-encrypting technologies have been called in to question as the industry guidance calls for a more "security-in-depth" approach to the protection of PII and PHI data. The ARIA KMS solves this concern by providing a scalable software solution that provides the ability to serve tens of thousands of keys per second providing secure access to critical data on a record-by-record or object-by-object basis without incurring additional latency.

The combination of the ARIA KMS deployed on the Myricom SIA and installed in storage array (Shown in Figure 2 below) provides significant advantages. The first is the high-speed functionality in the Myricom SIA. The second benefit is that it can provide keys to the storage array locally via the PCIe bus or anywhere else that they are needed via the high-speed network ports, all with additional performance and security. Any alternative solution would require an external device to provide this functionality – taking up space and potentially impacting network performance.

Integration with the ARIA KMS is available out of the box for storage arrays where crypto applications contain a KMIP client. Conversely, arrays that do not utilize a KMIP-compatible key management solution, the combination of REST API access to the key storage as well as the availability of well tested KMIP client software provides an easy path to high performance key management.

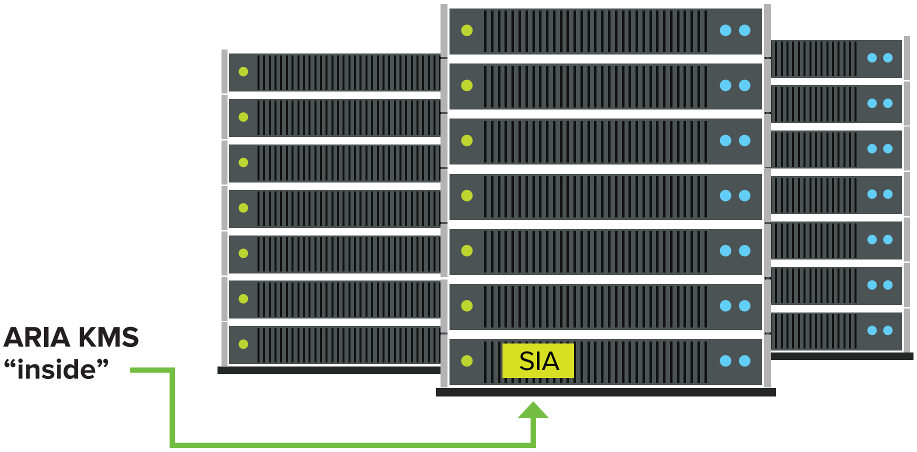

Figure 2 - SIA installed in a storage array

In summary, CSPi's ARIA KMS application is a scalable key management solution that is easy to deploy in the cloud or on premises. When paired with CSPi's Myricom SIA (as shown in Figure 3 below) it provides additional functionality unique in the industry.

Flexible Use

- Connects over PCIe to the host server
  Serves keys to local applications
- Supports any VM or bare-metal environment
- Communicates over network IO ports
- Serves keys to any client-supported application
- Supports other security applications along with KMS
- Operates as a NIC card

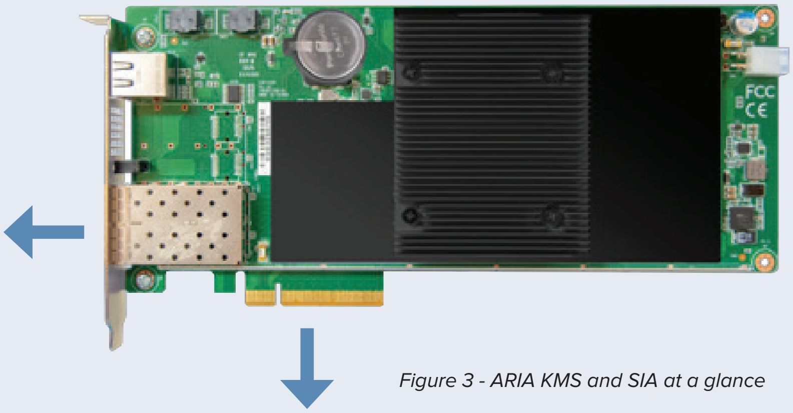

Figure 3 - ARIA KMS and SIA at a glance

ARIA KMS SPECIFICATIONS

Compliance	KMS virtual instance – FIPS 140-2 Level 1
Key Storage	KMS deployed on CSPi's Myricom SIA – FIPS 140-2 Level 3 Trust Zone-based secure key storage of greater than 40 million keys*
Throughput*	900,000 key wrap or unwraps per minute served from stored keys
Management	Deployed and managed by ARIA SDS Orchestrator
High-availability	Zero touch provisioning of redundant nodes deployed and managed by SDS Orchestrator
KMIP	KMIP Supported profiles: • Baseline Server TLS v1.2 KMIP 1.0,1.1,1.2 Profile Conformance • Baseline Server KMIP 1.3 (1.4 Profile Pending) • Secret Data KMIP Profile • Basic Symmetric Key Store and Server KMIP Profile • Basic Symmetric Key Foundry and Server KMIP Profile
Software Support	Drivers available for Linux (CentOS, RHEL, and Ubuntu) Supports DPDK for Linux 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

* When running on CSPi's Myricom SIA

Secure your Enterprise today. Contact us: sales@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