ARIA SDS KMS

CSPi's ARIA™ Key Management Server (KMS) is an easy to deploy application taking advantage of the widely accepted KMIP protocol for integration with existing applications. When deployed on CSPI's Myricom SIA you gain added security and performance.

The market has been requesting a simple to deploy and easy to manage key management solution. HCI solutions including vSAN™ have embraced the use of KMIP clients to perform encryption – they now 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
- End-to-end KMIP server and client options available
- High-availability secure key storage in a virtual server, on premise or in the cloud
- Control keys centrally – one to many deployment
- Manage policies across platforms through a single UI
- Consistent configuration and enforcement, including revocation

CSPi provides two ways to access the Key Server. The first, via KMIP, provides out-of-the-box integration with the large number of applications that already support clients based on the KMIP standard. The second, is via the provided REST API. Both methods allow customers to build their own integrations to the key server.

When securely deployed, configured and managed as part of the orchestrated ARIA SDS platform, benefits include "zero touch provisioning", remote management and health monitoring. These Key Server deployments include both FIPS 140-2 level 1 virtual instances, for cloud or on premise use, as well as FIPS 140-2 level 3 SIA hosted instances.

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 premise 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 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
  - When deployed on CSPi's Myricom® SIA you gain 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

CSPi's Myricom SIA as a secure deployment platform combines a next-generation high-speed network adapter with the programmability of multi-core ARM processing to provide application-specific feature support. This 10/25 GB dual port network interface card (NIC) provides a local secure zone-of-trust 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 keeps 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 SIA

Myricom SIA ensures organizations will be able to dramatically reduce server costs and protect 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, requiring zero footprint for a key server solution. Multiple SIA cards can be logically grouped together to provide High Availability functionality as well as scaled up performance.

For organizations that leverage the VMware NSX™ architecture, the SIA deploys within the NSX architecture by allowing NSX to access specific traffic flows between any VMs, intra-server or inter-server, to take advantage of the ARIA security features. NSX installations leveraging SIA functionality can experience a 10-fold improvement in application performance by offloading key functions such as encryption and key management to a Myricom ARC Series SIA network adapter.

Single key self encrypting drive 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 meets these challenges by providing a software scalable solution that provides the ability to serve 10's of 1000's of key per second providing secure access to critical data on a record by record or object by object basis without incurring additional latency.

Working with a growing list of storage array vendors, the combination of the ARIA KMS deployed on the Myricom SIA installed in the storage array (Shown in Figure 2 below) provides significant advantages. In addition to providing high speed NIC functionality the SIA 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. Alternative solutions would require an external device to provide this functionality.

For storage arrays where crypto applications contain a KMIP client, the integration with ARIA KMS is provided out of the box. 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

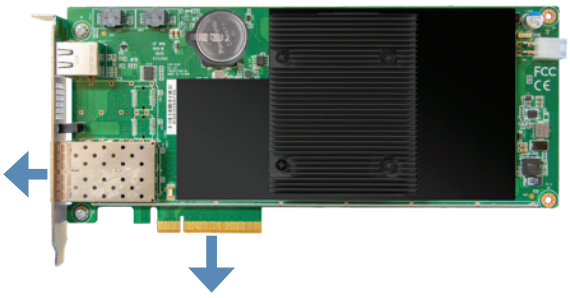

Figure 3 - ARIA KMS and SIA at a glance

ARIA KMS SPECIFICATIONS	
Compliance	KMS virtual instance - FIPS 140-2 Level 1 KMS deployed on CSPi's Myricom SIA - FIPS 140-2 Level 3
Key Storage	Trust Zone based secure key storage of greater than 40 million keys*
Throughput*	900,000 key wrap or unwraps per second 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

All companies and logos mentioned herein may be trademarks and/or registered trademarks of their respective companies.

MYRICOM Network Products