



Easily Encrypt VMware vSphere Environments with ARIA KMS



While encryption of virtual machines has been happening for many years, it hasn't gained much in popularity because of the impact on performance and operational challenges. In release 6.5, VMware added the ability to encrypt a VM's I/O.

Encryption occurs for all user-level files (such as core dumps) prior to being sent to the hypervisor layer beneath the virtual machine. With this approach VMware has addressed many security and policy issues, including implementing encryption as a policy, resulting in simplified administration and operational overhead.

However, in order to take advantage of these new VMware encryption features, organizations using vSphere must use an external Key Management System (KMS). This can be done easily through a KMIP standard solution.

How vSphere Encryption Works

The VMware vCenter manages the encryption process, acting at the behest of individual hypervisor instances to request the keys from an external KMS. It is the KMS that generates the actual keys, as well as stores and passes them to vCenter for distribution to each VM. Each VM receives a unique encryption key. In addition, the vCenter can also request keys from the KMS to encrypt a vSAN data store. In this case only one key is requested and it encrypts the entire data store.

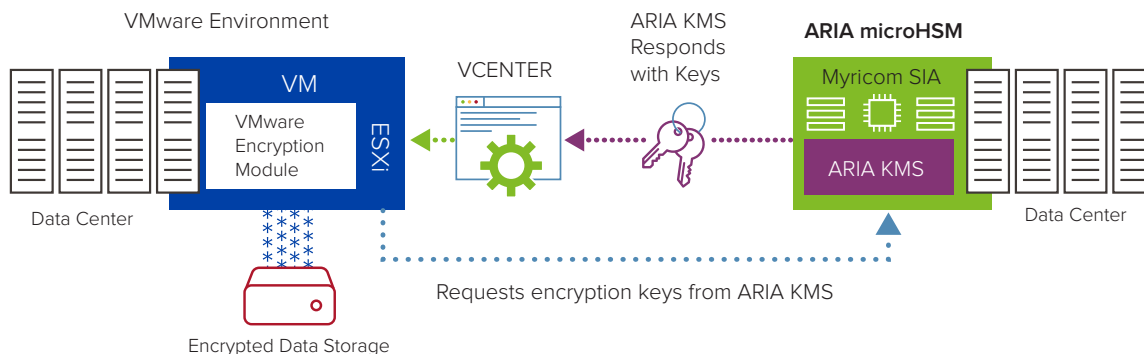
The generation, issue and storing of the keys is critical because they are what controls encryption. Key management is just what it sounds like - the ability to serve and update keys as desired. In the case that the KMS becomes non-responsive, data cannot be ensured to be properly encrypted or decrypted - making the KMS the linchpin of data encryption.

ARIA microHSM solves this single point of failure possibility by providing a high performance secured hardware approach which can be clustered for transparent high reliability. This assures the KMS is both secure and completely backed up by up to five other individual KMS instances in its cluster. High availability functionality is built in and available out of the box.

Simple vSphere Key Management Using ARIA microHSM

The 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 - like VMware vSphere.

The KMS solution is deployed on the Myricom Secure Intelligent Adapter (SIA), for not only a trusted execution environment for key handling, but also for added security and performance, as well as plug-and-play, one-step configuration. For organizations that must comply with government encryption requirements, the ARIA KMS deployments can provide a FIPS 140-2 Level 1 solution.



Myricom SIA Provides a Zero Footprint Key Management Server

The Myricom SIA is a 10 or 25GB dual-port network interface card (NIC) and provides a local secure zone-of-trust required to generate and store keys and even execute crypto operations based on those stored keys. Running the ARIA KMS application, shields the keys from exposure, even if the host server is breached, unlike Intel’s® vulnerable Xeon™ SGX-based TPM environments.

Utilizing the SIA allows organizations to improve server network connectivity while protecting the use of the keys during encryption. The SIA can also be deployed into the devices they are protecting, such as storage arrays, for a zero footprint implementation for a key server solution.

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 01854

Connect with Us: ariacybersecurity.com / [Linkedin](#) / [Twitter](#) / [Blog](#)

