thalestct.com

THALES

The Importance of KMIP Standard for Centralized Key Management

How Thales Trusted Cyber Technologies Can Help

White Paper

Executive Summary

Today, protecting sensitive data is a fundamental requirement in virtually every business. What's also nearly universal is this: operations and security teams continue to struggle with managing the proliferation of encryption keys that enable in protection of sensitive data.. The Key Management Interoperability Protocol (KMIP) was developed to enable more unified, efficient management of keys from multiple encryption technologies and vendors. This white paper offers a look at the KMIP standard, and it shows how Thales solutions help you maximize the advantages of this standard.

The promise of KMIP

Organizations deploy specific encryption solutions based on their unique use cases, technologies, businesses, security threats and more. To address all their requirements, organizations employ many different solutions from different vendors. Historically these different technologies lacked common standards for key management.

KMIP changed that. KMIP advances interoperability standards for enterprise encryption key management in order to help organizations centrally manage keys from a number of vendors. KMIP represents a comprehensive protocol for communication between a client and a server. In most scenarios, customers will need to integrate a KMIP Client with a KMIP Server. The KMIP Server within the Key Management System (KMS) provides life-cycle management of keys sent by the KMIP Client, as well as perform cryptographic operations whose results can be returned to the client.

The KMIP standard is governed by the Organization for the Advancement of Structured Information Standards, or OASIS, a nonprofit organization that promotes the development, convergence and adoption of open standards. The KMIP standard has been developed with the support of top security experts and leading vendors, including Thales In fact, Thales was one of the four pioneering vendors responsible for original development of the protocol, and the company's representatives have served in leadership capacities on the OASIS KMIP technical committee since the standard's inception in 2007.

How Thales enables customers to capitalize on the KMIP Standard

With its advanced solutions, deep expertise and extensive partnerships, Thales is uniquely equipped to help organizations quickly, effectively and broadly harness the advantages of the KMIP standard. Through its support of KMIP and other standards, Thales solutions enable more efficient, centralized management of the entire data protection ecosystem.

Thales has a track record of successful KMIP integrations and deployments, and continues to work with technology partners and customers to expand its ecosystem. Our solutions have been proven in organizations with the most stringent security requirements, including financial services institutions, health care organizations, retailers and government agencies.

Solution: CipherTrust Manager

With the CipherTrust Manager from Thales, organizations can maximize the advantages of the KMIP standard. In addition, CipherTrust Manager delivers centralized controls that enable consistent and repeatable management of encryption keys, access policies and improved security intelligence.

CipherTrust Manager makes it easy and efficient to manage data-at-rest security across the entire organization by offering a diverse portfolio of encryption solutions to protect data wherever it resides in the organization.. As a result, security teams can address data security policies, compliance mandates and best practices, while reducing administration effort and total cost of ownership. CipherTrust Manager can be deployed with a physical HSM Root of Trust. Optionally, the virtual appliance can use an external HSM. Both solutions provide improved key security and entropy.

The CipherTrust Manager is uniquely equipped to enable organizations to centralize and streamline key management across an organization. Here's why:

- CipherTrust Manager enables security teams to manage keys and policies for a broad range of data protection solutions from Thales, which feature broad capabilities for protecting and controlling access to databases, files and containers—and securing assets residing in cloud, virtual, big data and physical environments.
- CipherTrust Manager can manage keys and policies for a number of third-party platforms, including Transparent Data Encryption (TDE) products from Microsoft, Oracle and IBM.
- CipherTrust Manager offers comprehensive support for the KMIP standard. Effectively, any device or client software that is KMIP-enabled can communicate with CipherTrust Manager to facilitate management of encryption keys. Examples of KMIP clients include management systems in hyperconverged environments (Nutanix), self-encrypting drives in storage systems (Netapp, Dell, IBM, HPE) and native encryption in next-generation databases and virtualized environments.

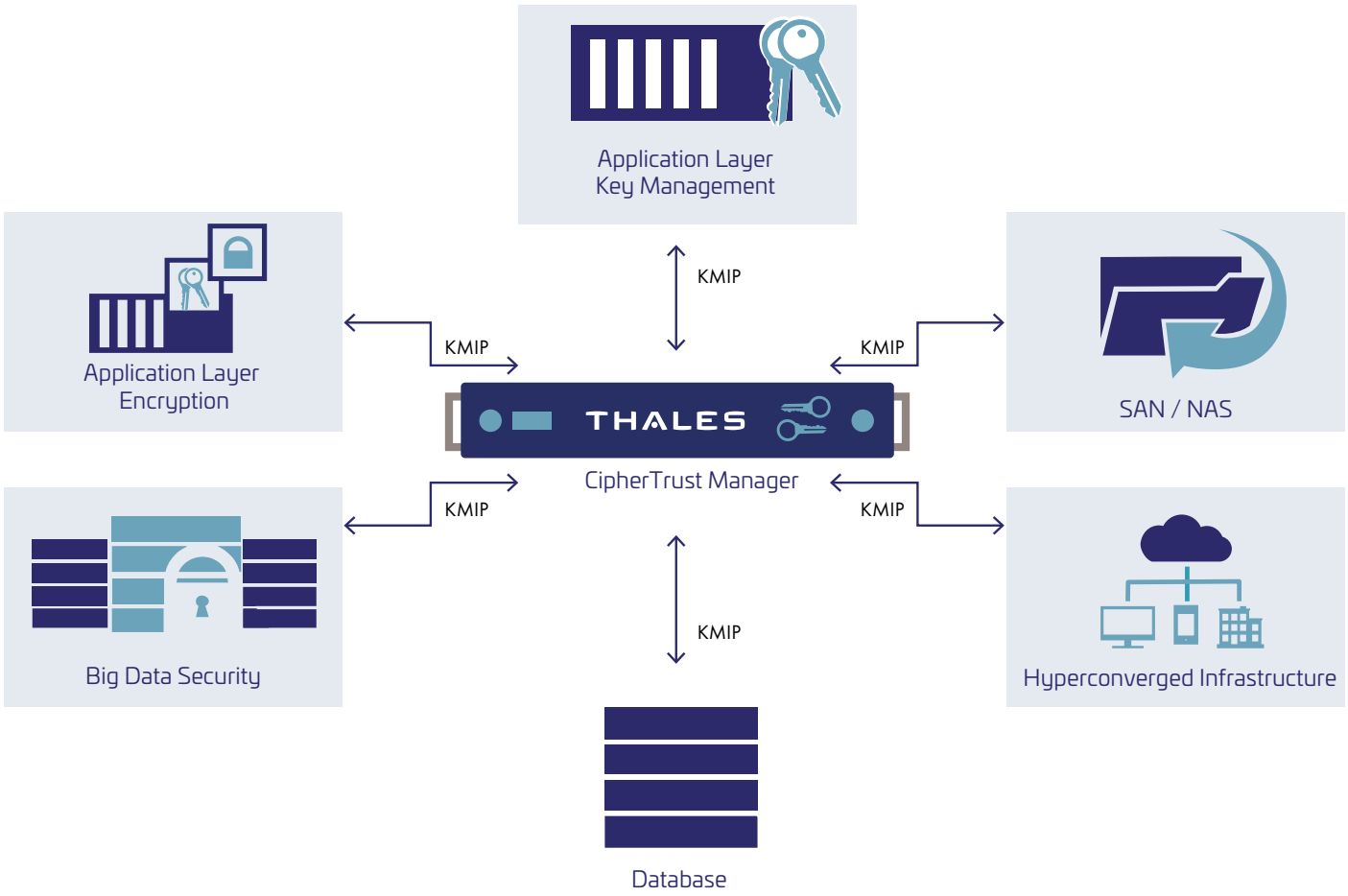

Figure 1: Thales CipherTrust Manager serves a variety of applications and client types using KMIP.

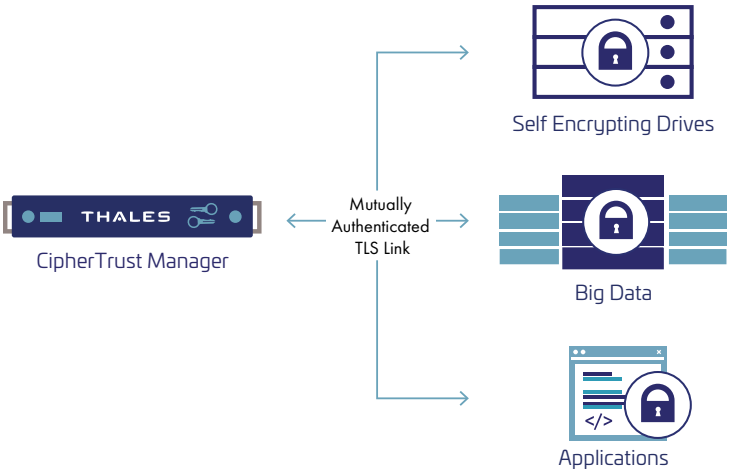

Figure 2. KMIP Client-Server Communications

1. Purchase and install KMIP Client licenses on CipherTrust Manager
2. Generate token to register each KMIP Client
3. Add token and restart KMIP service on CipherTrust Manager
4. Sign the KMIP Client Certificate Signing Request (CSR)
5. Upload CipherTrust Manager signedn CSR to the KMIP Client

KMIP-based communications: How it works

Following is a high-level overview of how the process works:

- CipherTrust Manager needs to be prepared for KMIP support, which entails adding a KMIP client to the KMIP client list.
- A KMIP client is registered with the CipherTrust Manager
- Trust between the CipherTrust Manager and the KMIP client needs to be established. The KMIP protocol requires a mutually authenticated TLS connection between clients and servers. Once the client is registered with the CipherTrust Manager for secure communications, a certificate for the KMIP client will be created. This certificate will be used by the KMIP client for TLS authentication.

How Thales KMIP support benefits your organization

By leveraging Thales solutions, expertise and partnerships, organizations can realize a number of benefits:

- **Extend and maximize the value of your investments**. Thales support for KMIP allows organizations to more fully take advantage of their existing investments. CipherTrust Manager enables organizations to centrally manage the keys associated with their applications. As the encryption deployments grow, organizations can continue to employ CipherTrust Manager to manage keys for more technologies.
- **Streamline and enhance operations.** When organizations centralize key management on CipherTrust Manager, they can significantly simplify their operations. For example, administrators can centrally establish and enforce controls and policies for a number of systems. In addition, the solution enables centralized reporting for more effective and efficient compliance auditing, monitoring and reporting.
- **Enhance agility.** CipherTrust Manager helps organizations realize simplified operations and greater integration flexibility. As a result, the solution helps organizations adapt more quickly to evolving technologies and objectives. With the solution, organizations can more quickly and broadly leverage the advantages of innovative technologies like hyperconverged infrastructures and next-generation databases.

Technology support: featured KMIP partners and technologies

Today, many leading technology vendors offer encryption within their solutions, including hyperconverged infrastructures, databases, storage systems and more. This technology-centric encryption represents a vital line of defense. However, if keys are managed in a distributed, insecure fashion, it can erode or even eradicate any of the security benefits that can be gained through encryption.

That's why security experts and even the technology vendors themselves strongly recommend the use of purpose-built, centralized key management platforms, which is critically important for effectively safeguarding the keys generated by encryption. In fact, some vendors don't even allow the use of their encryption capabilities in production without the use of a third-party key management platform.

By leveraging CipherTrust Manager and the KMIP standard, customers can employ the encryption capabilities of their preferred technology vendors, while benefitting from a best-of-breed system for managing and securing keys. The CipherTrust Manager KMIP server enables seamless integration with a number of products across several categories. The sections below highlight some of the most important technologies that are currently supported.

Hyperconverged infrastructure

Hyperconverged infrastructures provide packaged, fully integrated technology stacks, including computing, storage, virtualization and networking. By leveraging these solutions, customers can significantly improve the efficiency of up-front deployment and ongoing administration, more quickly adapt to new business and technology requirements and more. The Thales KMIP server offers proven integration with a number of hyperconverged infrastructure technologies, including the following:

- **VMware vSAN and vSphere.** VMware vSAN powers leading hyperconverged infrastructure solutions. vSAN delivers secure, flash-optimized storage for workloads running on vSphere, VMware's virtualization platform. The vSAN solution delivers native encryption of flash devices. In addition vSphere offers encryption capabilities, securing the inputs and outputs from virtual machines before they get stored in disks. Customers can use CipherTrust Manager to manage keys generated by vSAN and vSphere encryption, enabling secure key management and strong role separation.

Storage

Enterprises rely on massive and rapidly growing storage infrastructures to manage data, and these repositories now invariably contain the organization's most sensitive, highly regulated assets. Encryption of these environments therefore represents a bedrock requirement. In response, many storage system vendors have added system-level encryption into their products. By leveraging CipherTrust Manager and the KMIP standard, customers can employ the encryption capabilities of their storage systems, while centralizing key management. Through its KMIP support, CipherTrust Manager enables seamless integration with a number of storage platforms, including the following:

- **NetApp ONTAP.** NetApp ONTAP enables administrators to assign, promote and retire storage resources without disrupting applications or business operations. ONTAP also unifies customers' control of their entire storage infrastructure, offering robust certificate-based authentication for access control and built-in encryption for data confidentiality. CipherTrust Manager and KMIP enables customers to consolidate key manager for ONTAP data encryption.

Next-generation data management

Database management systems very often house some of an organization's most sensitive data assets, and this is particularly true for next-generation database management platforms like MongoDB. Whether organizations are looking to comply with external regulations or internal policies, encryption of data at rest in these platforms is now an absolute mandate. Through its support for KMIP, CipherTrust Manager enables central, efficient and highly secure management of the keys generated by encryption in the following next-generation data management platforms:

- **MongoDB.** MongoDB is a NoSQL database that equips organizations with a number of significant advantages, including agility, scalability and high availability. In the MongoDB use case, the CipherTrust Manager provides high availability, standards-based enterprise encryption key management for MongoDB TDE using the KMIP standard, and offers vaulting and inventory of certificates. Consolidating enterprise encryption key management delivers consistent policy implementation between systems while reducing training and maintenance costs.

Conclusion

As enterprises expand the use of encryption to protect their sensitive data and assets, so grows the need to unify the management of encryption keys throughout their lifecycle. With the CipherTrust Manager from Thales, organizations can centrally manage keys and policies for Thales data protection solutions. Through its leading KMIP support, CipherTrust Manager can manage keys associated with encryption technologies in hyperconverged infrastructures, storage systems and next-generation data management platforms. As a result, organizations can address their most urgent security objectives, while significantly improving the efficiency of their operations.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com