Quintessence Labs

WHITE PAPER

An Introduction to KMIP

The OASIS Key Management Interoperability Protocol is a widely deployed and accepted standard for key management interoperability. Its adoption across the cybersecurity industry has significantly eased integration ensuring compatibility between security devices from different vendors.

Overview

The challenge of storing and managing encryption keys across an enterprise is exacerbated by encryption and key management systems (KMS) that use proprietary protocols. This fragmentation leads to redundant and incompatible key management processes, increasing the barrier to adoption of enterprise-wide encryption. The need to integrate different protocols results in higher costs for implementation and maintenance, ultimately increasing the total cost of ownership of the encryption solution.

To lower the barrier to adopting encryption, a common standard for key management in the cryptographic ecosystem is necessary. For enterprises, data centers, and other large businesses, integrating new solutions isn't trivial – it can be costly, and significant effort is required to ensure smooth setup and maintenance. A solution that allows integration into existing infrastructure is often preferred over a full-replacement approach.

History: Meeting Needs for a Standard

In 2010, the OASIS standards consortium released version 1.0 of the Key Management Interoperability Protocol (KMIP). The goal of KMIP is to enable communication between key management systems and cryptographically enabled applications via a common protocol.

At its heart, KMIP allows the manipulation of keys on a key management server. A KMIP conformant client-server pair facilitates the deployment of secure encryption across an organization by allowing cryptographic key and random number management to be quickly and easily integrated into any application. KMIP's common set of instructions for working with cryptographic objects lends cross-platform benefits that rarely existed beforehand. KMIP now enables cryptographic systems to interoperate, thereby letting end users benefit from each vendor's offerings.

Nearly a decade later, KMIP has matured. The 2.0 version of the protocol was released in 2019 and will continue to integrate lessons learned from industry. KMIP is being adopted more widely than ever and is now a common feature in key management systems in many organizations.

With Great Power...

KMIP has been designed for use by both legacy and new cryptographic applications. It supports many kinds of cryptographic objects, including symmetric keys, asymmetric keys, digital certificates, and authentication tokens. As described by OASIS:

> "KMIP simplifies the way companies manage cryptographic keys, eliminating the need for redundant, incompatible key management processes."

Key lifecycle management - including the generation, submission, retrieval and deletion of cryptographic keys - is enabled by the standard.

This table shows the full list of the operations, objects and attributes:

Supported Managed Object Types	- Certificate - Opaque Object - Private Key	- Public Key - Random Object - Secret Data	- Symmetric Key - Template
Supported Managed Object Attributes	- Activation Date - Always Sensitive - Application Specific Information - Archive Date - Certificate Identifier - Certificate Issuer - Certificate Length - Certificate Subject - Certificate Type - Compromise Occurrence Date - Compromise Date - Contact Information - Cryptographic Algorithm - Cryptographic Length	- Cryptographic Domain Parameters - Cryptographic Parameters - Cryptographic Usage Mask - Custom Attribute - Deactivation Date - Destroy Date - Digest - Digital Signature Algorithm - Extractable - Fresh - Initial Date - Last Change Date - Lease Time - Link - Name	- Never Extractable - Object Group - Object Type - Operation Policy Name - Process Start Date - Process Stop Date - Random Number Generator - Revocation Reason - Sensitive - State - Unique Identifier - Usage Limits - X.509 Certificate Identifier - X.509 Certificate Issuer - X.509 Certificate Subject
Supported KMIP Operations	- Activate - Add Attribute - Archive - Cancel - Certify - Check - Create - Create Key Pair - Delete Attribute - Derive Key	- Destroy - Discover Versions - Get - Get Attributes - Get Attributes List - Get Usage Allocation - Locate - Modify Attribute - Obtain Lease - Poll	- Query - Re-Certify - Recover - Register - Re-Key - Re-Key Key Pair - Revoke - RNG Retrieve - Validate

KMIP is an open specification, so any individual with technical expertise can implement their own KMIP client or KMIP server. However, in-depth technical expertise is required to correctly implement KMIP from scratch and accomplish the desired interoperability in a system and avoid unexpected (or even expected) complications that come with any hardware or software deployment.

For a quicker adoption, it is usually safer and most cost effective to leverage a vendor KMIP client that can tap into the KMIP ecosystem more easily than by developing one's own.

KMIP for Key Management Client Applications

There are many KMIP-enabled applications usable with a supported key management system (KMS) out of the box; all that is required is to simply configure the application to use the KMS. For client applications that already support encryption and key management, the adoption of KMIP can enhance the interoperability of the application and lower the barrier to adoption.

For clients enabled with encryption and key management, KMIP speeds up development, as the basic cryptographic management functions do not have to be redeveloped on the client. The client application may benefit from offloading the generation, management, and secure storage requirements of the cryptographic objects to a secure key management system.

The fastest way to enable KMIP in an application is to use a KMIP client SDK, several of which are available in multiple programming languages. Important factors when selecting a KMIP client are correctness, level of interoperability, and ease of use for integration. Specifically, for the integration point, it is important that APIs are well documented and easy to use.

QuintessenceLabs offers qClient, a full KMIP-supported client that can be easily used to enable KMIP in your applications. The QuintessenceLabs qClient SDK is available alongside qCrypt products or as a stand-alone SDK, again conformant with KMIP, that can work with any KMIP server.

Use case is from VMware, which integrated qClient into all VMware vSphere instances 6.5 and above. This provides a solid basis to support vSphere's encryption and key management requirements, since it enables easy interfacing to any KMIP conformant key management server. For enterprises that often use thousands of virtualized servers -- responsible for data at rest, in use or in transit -- encryption is the utmost priority. This integration of QuintessenceLabs' KMIP client into vSphere 6.5 and above enables enterprises to more easily integrate key management solutions and effectively implement encryption.

For Key Management Systems

The staggering volume of encryption keys and other cryptographic objects stored in an enterprise infrastructure demands a KMS that can keep up, but proprietary systems can create silos and, in return, reduce protection. KMIP's interoperability can alleviate this in a KMS by keeping track of keys, and storing, retrieving, or otherwise managing them as needed.

A KMIP key management system allows for the consolidation and centralization of key management, reducing the number of key managers that need to be deployed and maintained. The benefits of centralizing key management across different encryption solution include lowering system administration and compliance cost. The reduction in the number of locations a key is stored also reduces the attack surface, allowing the organization to concentrate the security fortification and monitoring.

QuintessenceLabs offers full-featured, KMIP-conformant KMS capabilities in its qCrypt product line. Considering the inherent advantages of KMIP, plus the number of organizations with a range of new or legacy systems, QuintessenceLabs built qCrypt to be vendor-neutral -- it meets the guidelines set forth by KMIP for all released interoperability protocols, including support for PKCS#11 standards.

QuintessenceLabs qCrypt 350TSF is an all-in-one appliance that gives an organization enhanced security with minimal complexity. It includes the full-featured KMIP functionality of the qCrypt key manager software, as well as hardware-based true random number generation from the quantum-based qStream module, and a dedicated FIPS 140-2 L3 HSM. This integrated system simplifies deployment as there is no need to separately load KMS software onto an appliance; no need to manage internal or external third-party HSMs or RNG devices, and no need to install and manage a keystore database and replication.

Learn More

QuintessenceLabs has numerous additional resources related to KMIP and key management in general. Our paper on Key Management Best Practices details several steps administrators can take to keep their key management systems protected and maintained.

For a specific guide to the qCrypt 350TSF, check out our dedicated Solution Guide, which highlights the all-in-one capabilities of the qCrypt 350TSF to enable enterprises to get a running start on advanced, KMIP conformant key management.

For organizations with large virtualization deployments, our guide on Purpose-Built Key Management for VMware vSphere further illustrates how QuintessenceLabs technology makes it easy to encrypt virtual servers.

Finally, for the full complement of information on KMIP direct from the source, visit the OASIS KMIP website.

Get in Touch

If you have any questions or would like to learn more about QuintessenceLabs' advances in key management and further developments in quantum-safe cybersecurity, send us a message at **info@quintessencelabs.com** or request a product demo.