FORNETIX™

KEY ORCHESTRATION™

CENTRALIZING ENCRYPTION KEY MANAGEMENT WITH INTEROPERABILITY

Key Management Interoperability Protocol (KMIP) was introduced by OASIS in 2010. OASIS is a non-profit consortium that focuses on bringing standards to information technology industries. This includes standards for information security and the Internet of Things (IoT). KMIP is a protocol that defines message formats for the management of cryptographic key material.

As the need for encrypting data at rest, in transit, and in motion grows, so does the need for a standard and central way to manage data encryption keys. Historically, encryption keys have been managed on the devices or within the technology that perform the encryption, however managing keys on each device is labor-intensive, limiting, and costly. The lack of an efficient way to manage keys on devices creates a huge security liability. Because of this, encryption keys are not managed at all or they are managed poorly, lending themselves to risk and compromise. KMIP was created to help bring all those devices together by providing a standard protocol that allows devices (clients) to talk to centralized key management servers.

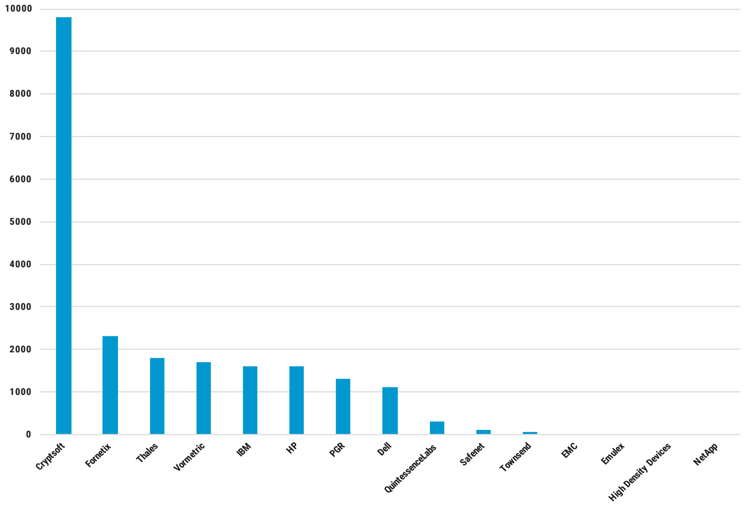
EXTENSIBILITY VS. INTEROPERABILITY

Most key management solutions today focus on extensibility without interoperability. Meaning, they build proprietary integrations with specific encryption solution providers and network device manufacturers, creating management overhead as those integrations need to be maintained and new integrations need to be built. This also means that those integrations are useless if one of the technologies is swapped out with another.
With interoperability; however, any of the technologies, even the key management solution itself, can be lifted and swapped seamlessly for another KMIP-interoperable technology without any additional integration necessary.

BRINGING KMIP AND INTEROPERABILITY TO NON-KMIP DEVICES

As with any standard, adoption can be slow, especially in industries that were long established before such standards were created. This is especially true with encryption management, since there are so many different types of technology and devices that use encryption. The data storage industry has been the first to embrace KMIP, other industries, especially those focusing on encrypting data in transit, have been slower adopters. For customers that have invested in KMIP and KMIP-enabled technologies, Key Orchestration has out-of-the-box integration.

In cases where a client can be installed, the Key Orchestration Client provides KMIP interoperability. In cases where a client cannot be installed, the Key Orchestration Agent provides KMIP interoperability by being a KMIP-driven proxy to any device that does not talk KMIP. For enterprise services that are not directly involved in encryption and encryption management, Key Orchestration's RESTful Services can be used to align Key Orchestration with existing business systems and technologies. As KMIP adoption grows and compliance becomes more prevalent, devices that are KMIP-compliant can be quickly and easily swapped and integrated into Key Orchestration—minimizing change management costs.



INTEROPERABILITY EVANGELISTS

At Fornetix, we are interoperability evangelists. Interoperability is crucial in providing effective and affordable key management. Our Key Orchestration Appliance, Clients, and Agents are KMIP-compliant allowing the Key Orchestration Appliance to manage keys on any device that talks KMIP, right out of the box. Similarly, the Key Orchestration Client can be installed on a device (e.g., on a database, web, or application server) and talk to any KMIP-compliant server.

As demonstrated by our KMIP Interoperability test results, the Fornetix Key Orchestration Appliance and Client are leaders in interoperability support.

Summary of KMIP Interoperability Testing 2010-2015
Source: Cryptsoft Pty Ltd

| www.fornetix.com

FORNETIX™