Key Management Interoperability Protocol

Participants in the OASIS 2017 interop at the 2017 RSA conference.

The **Key Management Interoperability Protocol** (**KMIP**) is an extensible communication protocol that defines message formats for the manipulation of cryptographic keys on a key management server. This facilitates data encryption by simplifying encryption key management. Keys may be created on a server and then retrieved, possibly wrapped by other keys. Both symmetric and asymmetric keys are supported, including the ability to sign certificates. KMIP also allows for clients to ask a server to encrypt or decrypt data, without needing direct access to the key.

The KMIP standard was first released in 2010. Clients and servers are commercially available from multiple vendors. The KMIP standard effort is governed by the OASIS standards body. Technical details can also be found on the official KMIP page and wiki.

Contents

Description

A KMIP server stores and controls *Managed Objects* such as symmetric and asymmetric keys, certificates, and user defined objects. Clients then use the protocol to access these objects subject to a security model that is implemented by the servers. Operations are provided to create, locate, retrieve and update managed objects.

Each managed object has an immutable *Value* such as a key block that contains a cryptographic key. They also contain mutable *Attributes* which can be used to store meta data about the keys. Some attributes are derived directly from the Value, such as the cryptographic algorithm and length of a key. Other attributes are defined in the specification for the management of objects such as the Application Specific Identifier which is usually derived from tape identification data. Additional identifiers can be defined by the server or client as need by the application.

Each object is identified by a unique and immutable object identifier that is generated by the server and is used to Get object values. Managed objects may also be given a number of mutable but globally unique *Name* attribute which can be used to Locate objects.

The types of managed objects that are managed by KMIP include

- Symmetric Keys.
- Public and Private Keys.
- Certificates and PGP Keys.
- Split Keys.
- Secret Data (passwords).
- Opaque Data for client and server defined extensions.

The operations provided by KMIP include

- Create—to create a new managed object such as a symmetric key, and return the identifier.
- Get—to retrieve an object's value given its unique identifier.
- Register—to store an externally generated key value.
- Add Attributes, Get Attributes, and Modify Attributes—to manipulate the attributes of a managed object.
- Locate—to retrieve a list of objects based on a conjunction of predicates.
- Re-Key—to create a new key that can replace an existing key.

- Create Key Pair—create asymmetric keys.
- (Re-)Certify—to certify a certificate.
- Split and Join n of m keys.
- Encrypt, Decrypt, MAC etc. -- cryptographic operations performed on the key management server.
- Export and Import keys to other KMIP servers.
- Operations to implement the NIST key life cycle.

Each key has a cryptographic state such as initial, Active, Deactive, Compromised. Operations are provided that manipulate the state in conformance with the NIST life cycle guidelines. The dates of each transformation are recorded, such as the date that a key was activated. Dates can be specified into the future so that keys automatically become unavailable for specified operations as they expire.

Message encoding

The KMIP protocol specifies a modified form of type-length-value for binary encoding of messages, called **TTLV** (tag, type, length, value). Nested TTLV structures allow for encoding of complex, multi-operation messages in a single binary message. TTLV encoding has several deliberate design choices:

- Padding: TTLV aligns data to the nearest 4 or 8 bytes to allow for optimal processor alignment.
- Extensibility: deliberately leaving room within

enumerations to allow for easy addition of new tags, data types and attribute values.
- Mapping to other encodings: the protocol allows for encoding of KMIP messages in the form of XML and JSON, as described in the KMIP Additional Message Encodings document.

There are also well defined XML and JSON encodings of the protocol for environments where binary is not appropriate.

TTLV alone is a raw binary format and does not provide for the encryption of transmitted messages. TLS is mandated for link level security in communication between clients and servers.

KMIP profiles

KMIP also defines a set of **profiles**, which are subsets of the KMIP specification showing common usage for a particular context. A particular KMIP implementation is said to be *conformant* to a profile when it fulfills all the requirements set forth in a profile specification document. OASIS has put forth various profiles describing the requirements for compliance towards storage arrays[1] and tape libraries,[2] but any organization can create a profile.

Relationship to PKCS#11

PKCS#11 is an API used to control a hardware security module. PKCS#11 provides cryptographic operations to encrypt and decrypt, as well as operations for simple key management. There is considerable amount of overlap between the PKCS#11 API and the KMIP protocol.

The two standards were originally developed independently. PKCS#11 was created by RSA Security, but the standard is now also governed by an OASIS technical committee. It is the stated objective of both the PKCS#11 and KMIP committees to align the standards where practical. For example, the PKCS#11 Sensitive and Extractable attributes are being added to KMIP version 1.4. Many of the same people are on the technical committees of both KMIP and PKCS#11.

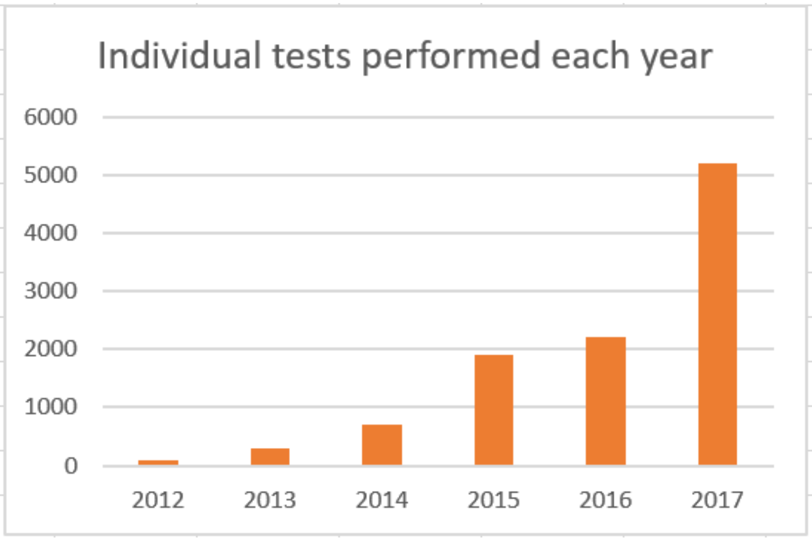
KMIP implementations

The OASIS KMIP Technical Committee maintains a list of known KMIP implementations, which can be found on the OASIS website. As of March 2017, there are 28 implementations and 61 KMIP products in this list.

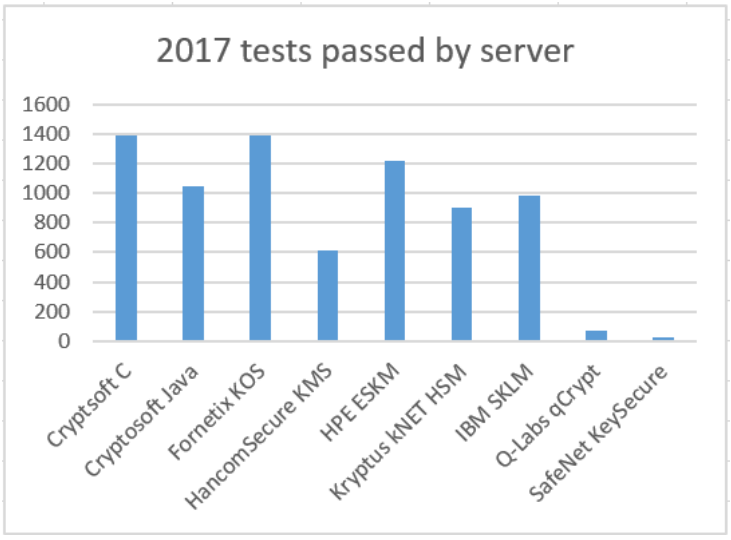
Interoperability between implementations

The KMIP standard is defined using a formal specification document, testcases, and profiles put forth by the OASIS KMIP technical committee. These documents are publicly available on the OASIS website.

Vendors demonstrate interoperability during a process organized by the OASIS KMIP technical committee in the months before each RSA security conference. These demonstrations are informally known as **interop**. KMIP interop has been held every year since 2010. The following chart shows the number of individual tests performed by each client and server vendor combination since 2012.



- Individual interoperability tests performed by each server/client vendor combination since 2012



- Results of 2017 OASIS KMIP interoperability testing

Full details of the result of the 2017 interop can be found on the OASIS website.

In 2014 the Storage Networking Industry Association (SNIA) announced a similar, but distinct KMIP testing platform.[3] It is known as the SSIF KMIP Conformance Test Program. However, The SSIF KMIP Conformance Test Program was retired effective September 1, 2017, and according to the SNIA website, no new testing can be scheduled at this time.

Version history

Summary of KMIP versions and features.

Version	Committee Draft	Main Features
1.0	Oct 2010	Initial version
1.1	Jan 2013	
1.2	Jun 2014	Cryptographic Operations. Introduction of Profiles, including Application Identifiers for tape libraries.
1.3	2015	Streaming Cryptographic Operations; Client Registration; Locate offset/Limit; Deprecate Templates; RNG queries;
1.4	2017	Better asynchronous operations; Import/export of keys to other servers; Support of PKCS #12; Better error handling; Standardized key wrapping; Certify Attributes; Client & Server Correlation Values; Descriptive Attributes; AEAD

		support; AES-XTS support; Create Secret Data; RSA PSS Support; Many extensions to Query.
2.0	Current development version, accepted proposals February 2017	Removal of deprecated items; Replacement of "x-" convention for custom attributes; Client Log operation; Date Time resolution 1 microsecond; Locate Destroyed & Patterns; Better Error Handling; new CSR object; Removal of Attribute Index; Support for tokenization; NIST Key Type; Fixed length Unique Identifiers; Several new attributes and query extensions.

See also

- Key management
- Key (cryptography)
- Encryption
- IEEE P1619 Security in Storage Working Group

References

External links

- *"OASIS KMIP Technical Committee"*.
- *"KMIP Implementations known to the KMIP TC"*.
- *"KMIP Storage Array with Self-Encrypting Drives Profile Version 1.0"*.

- "KMIP Tape Library Profile Version 1.0".
- "SNIA KMIP Test Program Announced". *Official web site*. SNIA. 2014-02-24. Retrieved 2014-03-20.