Quantum Cyber Defense

Interoperability: Making the Best of KMIP

John Leiseboer, CTO, QuintessenceLabs

KMIP: Overview

OASIS
Advancing open standards for the information society

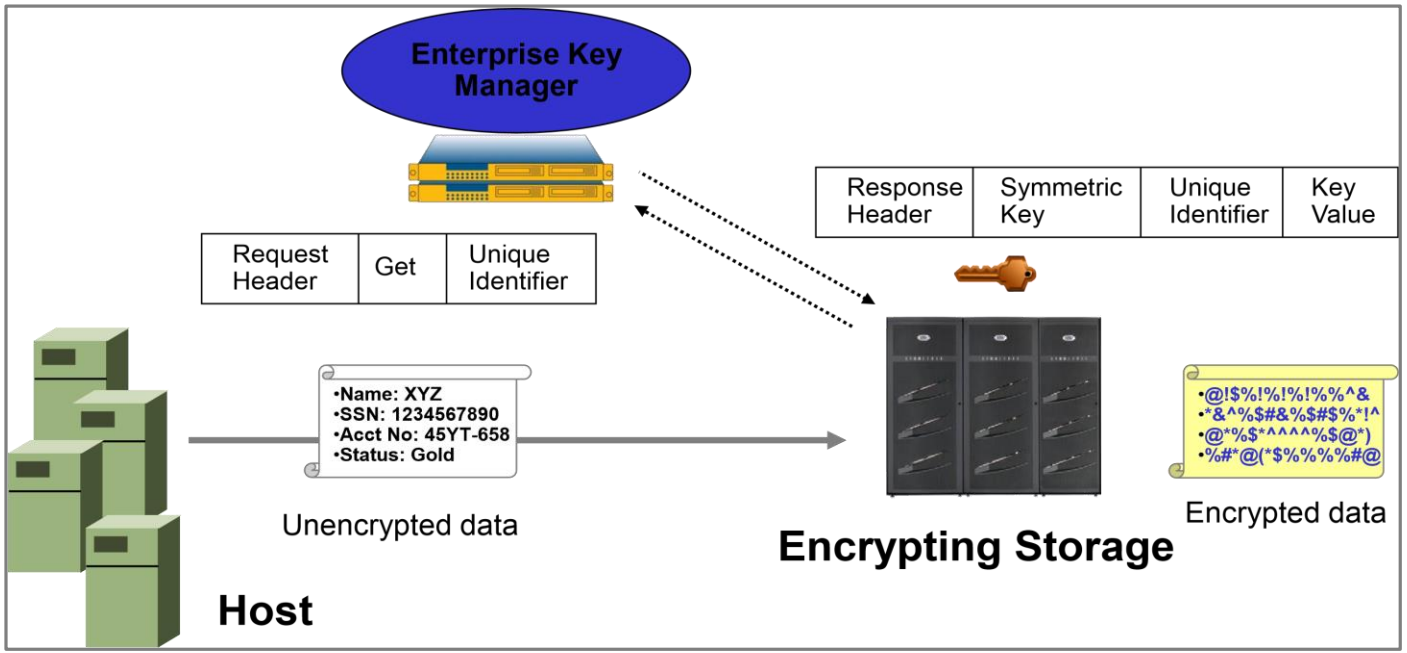
- **What is it?**
  - KMIP = Key Management Interoperability Protocol
  - Standard protocol for managing the creation, distribution and lifecycle of Cryptographic Objects
  - Part of OASIS: Organization for the Advancement of Structured Information Standards

- **What does it do?**
  - A single, comprehensive protocol for communication between encryption systems, including email, databases, and storage devices
  - Keys, certificates, secret data, split keys, wrapped keys, opaque objects, templates…

Will provide better data security and reduce costs by removing redundant, incompatible key management processes, enabling more pervasive encryption!

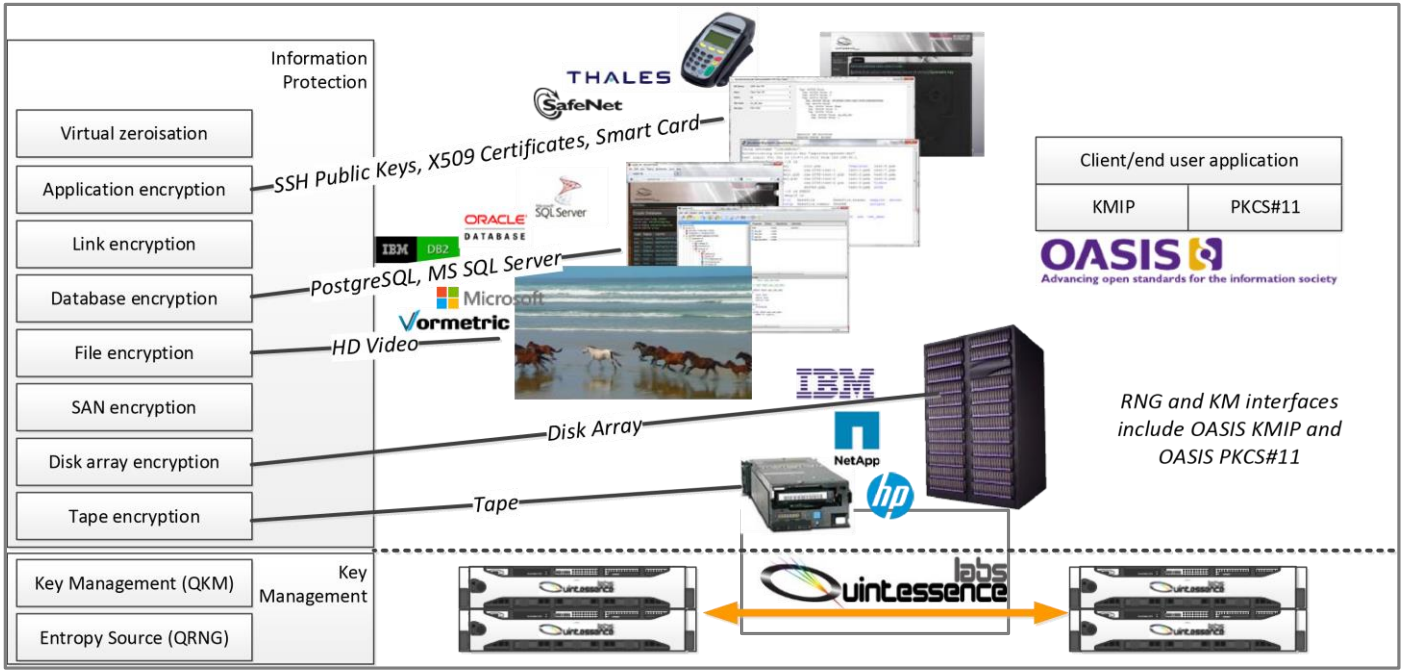
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip

KMIP: How it Works



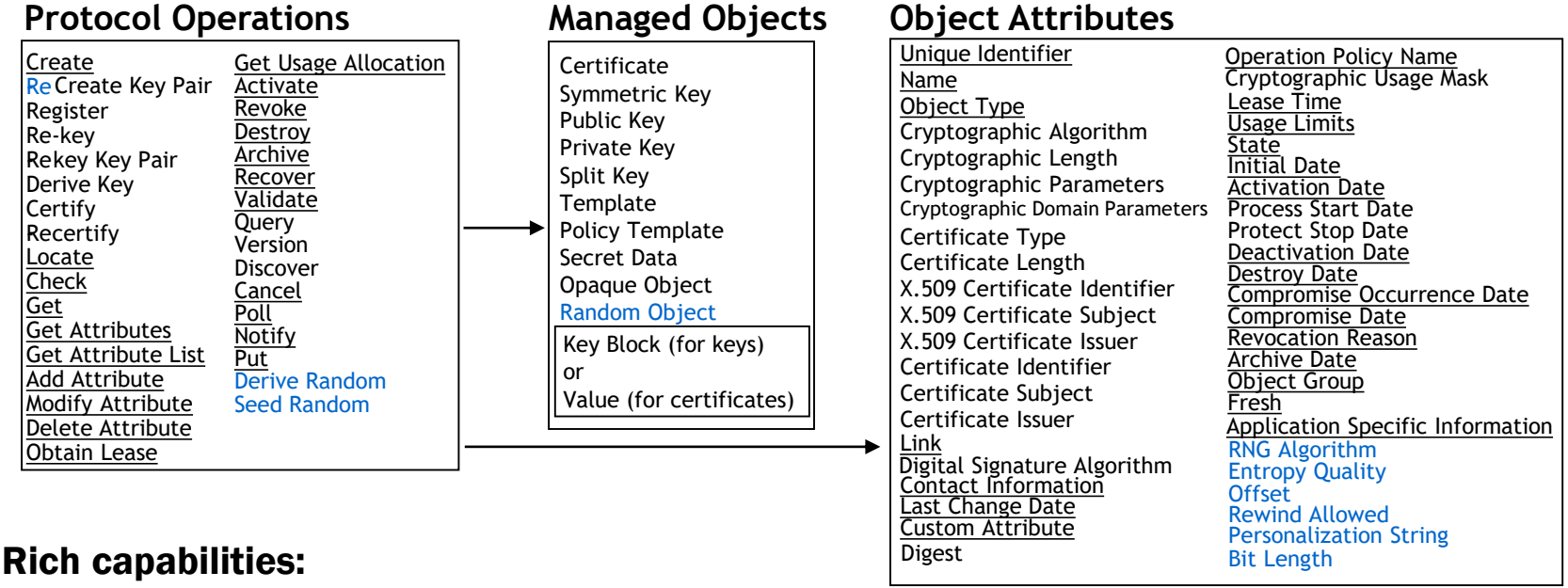
- The IETF (Internet Engineering Task Force) allocated Port 5696 for KMIP
- Messages are encoded in a compact, binary format: TTLV (Tag, Type, Length and Value)

KMIP: Use Cases and Vendor Interoperability



KMIP can be applied to a wide range of use cases and has been tested with many vendors.

KMIP: Capabilities



Black: Standard KMIP
Black: Extended KMIP
Blue: New operations within KMIP capability

- **Rich capabilities:**
  - Operations
  - Objects
  - Attributes
- **But… drives complexity: important to understand protocol very well**

KMIP Challenges

- **Like many protocols, KMIP has challenges and limitations.**
  - Does not prevent implementation of Key Management solutions across multiple vendors
  - But… does require more in-depth knowledge to implement

- **Next sections: highlight main pitfalls to be aware of:**
  - Useability
  - Interoperability
  - Security
  - Standards compliance
  - Performance

KMIP Challenges: Useability and Interoperability

- **Useability**
  - Locate can return nothing: Not an issue - just need to be aware of it.
  - Templates: Deprecated in 1.2. ; solution: keep using 1.0 and 1.1 templates.
  - Redundant fields in Key Derivation operations

- **Interoperability**
  - No/incomplete limits specified for message sizes, attribute lengths, or number of attributes
  - Trial and error or a-priori knowledge required

  => KMIP does enable interoperability, however implementation can be tricky due to above issues

KMIP Challenges: Security

- **Random Number Generation**
  - Any client is permitted to seed the server RNG
  - Potential for a client to control another client's random numbers and key values

- **Cryptographic Operations**
  - Client can force server to perform cryptographic operations that violate permitted operating parameters for managed keys
    Example: a key may require crypto to be performed in CBC mode only, but the client can instruct the server to perform crypto in ECB mode
  - Note: This is explicitly disallowed for key wrapping performed on the server

In both cases, appropriate controls need to be implemented requiring in-depth knowledge of protocol capabilities

KMIP Challenges: Standards compliance

- **NIST SP 800-57 Part 1 is a normative reference to KMIP**

  But… some KMIP test cases specify responses that violate NIST SP 800-57 Part 1 requirements (Asymmetric key lifecycle operations, Derived key lifecycle operations).

- **TTLV is a required message encoding**
  - Test cases used to be specified with TTLV example messages but are now specified using XML (XML is an optional binding)
  - No DTD or schema specified for the XML bindings

User needs judicious implementation to fully comply with standards

KMIP Challenges: Performance

- **KMIP is mostly a stateless protocol: the server is not required to retain session information for the duration of multiple requests**
- **This is partly changing with release 1.3: Cryptographic streaming operations require the server to maintain state**
  - No state management provisions are currently in the standard
    - What happens if a stream is interrupted? How is it recovered?
    - What happens if a stream is prematurely terminated?
    - How does a server know if a stream has failed, or is just waiting?
  - The streaming protocol is extremely inefficient
    - Full round-trip time latency between each stream part
    - No possibility to pipeline messages

If performance is an issue, do not use KMIP cryptographic operations. Perform crypto in the client, or use a different network protocol.

KMIP: What next?

- ✓ Follow OASIS KMIP
- ✓ Comment on proposed standards
- ✓ Join OASIS KMIP
- ✓ Lobby your vendors to fully implement KMIP and participate in process
- ✓ At the very least read the standards documents - “caveat emptor”

The phrase *caveat emptor* arises from the fact that buyers often have less information about the good or service they are purchasing, while the seller has more information. Defects in the good or service may be hidden from the buyer, and only known to the seller. Thus, the buyer should beware.*

* http://en.wikipedia.org/wiki/Caveat_emptor

Quantum Cyber Defense

jl@quintessencelabs.com