

## KMIP Java Client SDK

Complete vendor-independent key management solution



KEY MANAGEMENT

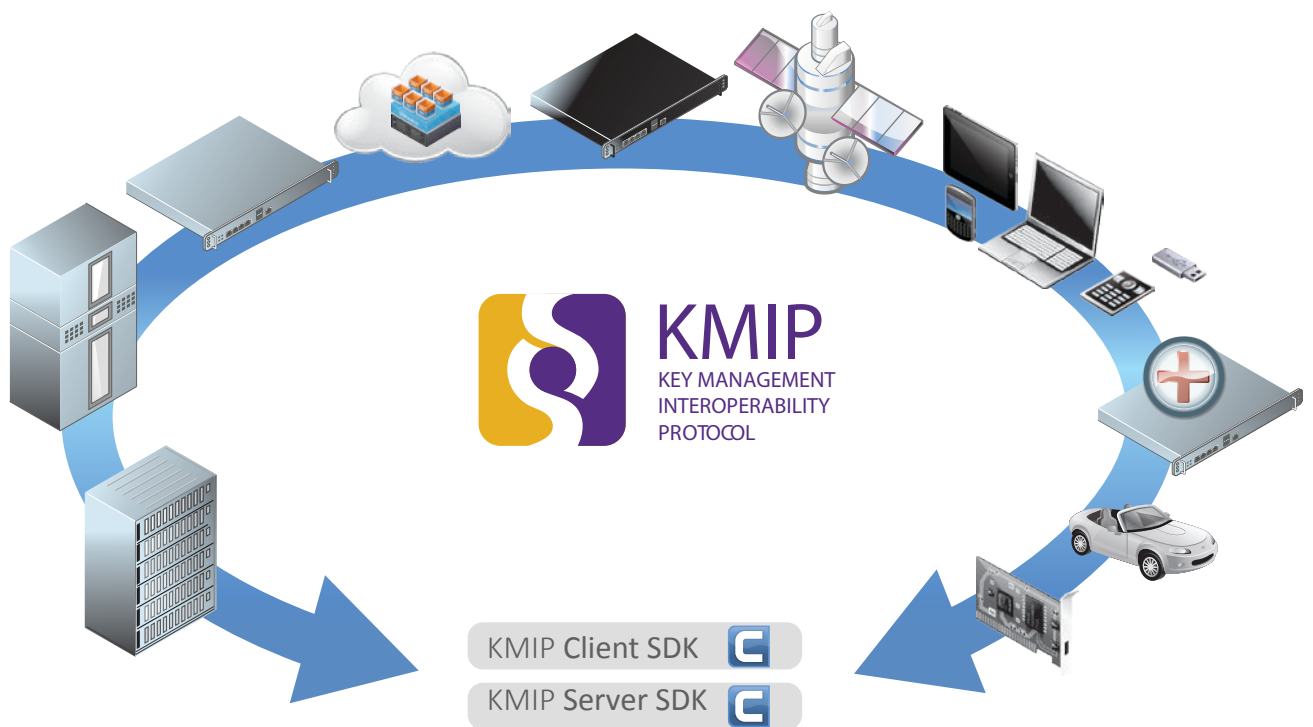
Cryptsoft's Key Management Interoperability Protocol (KMIP) SDKs let you rapidly add interoperable, standards-based, enterprise key management capability to your existing applications.

Reduce time to market, KMIP-enable your solution within days, not months, using our comprehensive collection of example code provided by the market leader in key management SDKs.

From specialised embedded systems through to scalable, whole of enterprise solutions, your KMIP SDK license is backed by a global support network, offering a total key management solution.

### Key Features

- Full OASIS KMIP compliance  
Versions: 1.0, 1.1, 1.2, 1.3\* (committee draft)
- Guaranteed interoperability  
With all released KMIP server products
- Available as a binary SDK  
Source license option
- Comprehensive example code  
Custom examples available - rapid integration



# KMIP Java Client SDK

Complete vendor-independent key management solution



## KMIP Java Client Examples

- KMIP Standard Operations
  - Create, Register, Destroy, Get, Get Attribute List, Get Attributes, Create Key Pair, Re-key, Re-key KeyPair<sup>1,1</sup>, Archive, Recover, Activate, Derive Key
- Determine Capabilities
  - Client SDK Version, Discover Protocol Versions<sup>1,1</sup>, Query Server Basic, Query Server Extensions<sup>1.1</sup>, Query Advanced Capabilities<sup>1,3</sup>
- Creating Keys
  - Simple, Advanced, Extensions
- Managing Attributes
  - Add, Modify, Delete Attribute
- Random Number Generator (RNG)<sup>1,2</sup>
  - Retrieve Server RNG, Seed Server RNG
- Server Cryptographic Operations<sup>1,2</sup>
  - Encrypt, Decrypt, MAC, MAC Verify, Hash
- Simple Protocol Format Parsing
  - TTLV, HEX, BIN, JSON, XML
- Simple Servers
  - Query, Notify, Put
- Locating Managed Objects
  - Simple, Extended, XML
- Simple Clients
  - Locate Objects, Create and Return
- Objects
  - Cryptosoft Vendor Extensions
  - SQL Insert, SQL Update, SQL Delete
- Request/Response Handling
  - Replay, Batching
- JCE Examples
  - Key Store Provider

## Supported KMIP Profiles

- Advanced Cryptographic Client<sup>1,2</sup>
- Advanced Symmetric Key Foundry Client
- Asymmetric Key Lifecycle Client
- Baseline Client Basic
- Baseline Client TLS v1.2
- Basic Cryptographic Client<sup>1,2</sup>
- Basic Symmetric Key Foundry Client
- HTTPS Client
- Intermediate Symmetric Key Foundry Client
- JSON Client
- Opaque Managed Object Store Client
- RNG Cryptographic Client<sup>1,2</sup>
- Storage Array With SED Client
- Suite-B MinLOS\_128 Client
- Suite-B MinLOS\_192 Client
- Symmetric Key Lifecycle Client
- Tape Library Client
- XML Client

## Supported KMIP Operations

- Activate
- Add Attribute
- Archive
- Cancel
- Certify
- Check
- Create
- Create Key Pair
- Create Split Key<sup>1,2</sup>
- Decrypt<sup>1,2</sup>
- Delete Attribute
- Derive Key
- Destroy
- Discover Versions<sup>1,1</sup>
- Encrypt<sup>1,2</sup>
- Get
- Get Attribute List
- Get Attributes
- Get Usage Allocation
- Hash<sup>1,2</sup>
- Join Split Key<sup>1,2</sup>
- Locate
- MAC<sup>1,2</sup>
- MAC Verify<sup>1,2</sup>
- Modify Attribute
- Notify
- Obtain Lease
- Poll
- Put
- Register
- Register Query
- Re-certify
- Recover
- Re-key
- Re-key Key Pair<sup>1,1</sup>
- Revoke
- RNG Retrieve<sup>1,2</sup>
- RNG Seed<sup>1,2</sup>
- Sign<sup>1,2</sup>
- Signature Verify<sup>1,2</sup>
- Validate

## KMIP Object Types

- Certificate
- Opaque Object
- PGP Key
- Private Key
- Public Key
- Secret Key
- Split Key
- Symmetric Key
- Template

## Cryptographic Providers

- Sun/Oracle JCE
- IBM JCE
- RSA BSAFE Crypto-J
- Bouncy Castle JCE

## Encodings

- TTLV
- HTTPS/TTLV
- HTTPS/JSON
- HTTPS/XML

## Supported KMIP Servers

CRYPTOSOFT



FORNETIX



THALES



SALES@CRYPTOSOFT.COM

+61 7 3103 0321 | US +1 650 918 4362

WWW.CRYPTOSOFT.COM



@CRYPTOSOFT



@CRYPTOSOFT



CRYPTOSOFT-SECURITY-SPECIALISTS

