FOUNDATION SECURITY TECHNOLOGIES
TRUSTED² | EMBEDDED | INTEROPERABLE

CRYPTSOFT®

KMIP CLIENT SDK

C, C++, C#, JAVA, PYTHON

A complete range of vendor-independent key management solutions.

Cryptsoft's Key Management Interoperability Protocol (KMIP) SDKs let you rapidly add interoperable, standards-based, enterprise key management capability to your existing applications. This allows applications to use encryption functionality available from a wide range of key managers making it easier to deploy and preventing vendor lock-in to proprietary solutions.

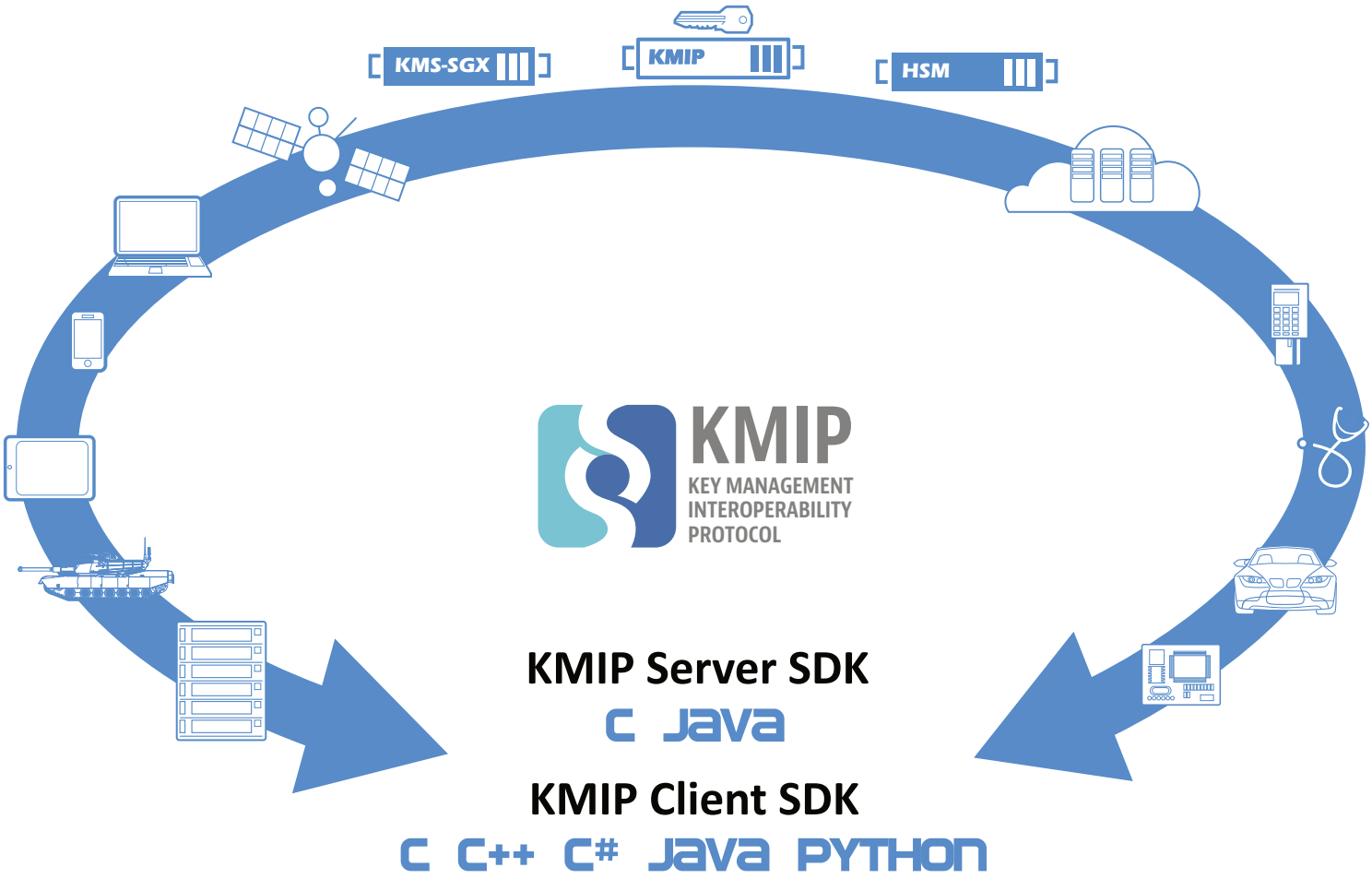
Cryptsoft's C, C++ and Java SDKs are all pure native code not wrapped versions, ensuring the most portable code for your application.

Reduce time to market, KMIP-enable your client solutions 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 and government 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, 1.4, 2.0*
- Guaranteed interoperability with all released KMIP server products
- Available as a binary SDK
  - Source license option
- Comprehensive example code
  - Custom examples available for rapid integration
- Supported on 200+ different platforms including Linux, Windows, Legacy and a range of embedded platforms
  - Custom platform ports on request
  - Intel SGX support available



FOUNDATION SECURITY TECHNOLOGIES
TRUSTED[2] | EMBEDDED | INTEROPERABLE

CRYPTSOFT®

KMIP CLIENT SDK - SPECIFICATIONS

C, C++, C#, JAVA, PYTHON

KMIP Client Examples

- Simple Protocol Format Parsing
  TTLV, HEX, BIN, JSON, XML
- Simple Servers
  Query, Notify, Put
- Simple Clients
  Locate Objects, Create and Return Objects
- Locating Managed Objects
  Simple, Extended, IBM TKLM/SKLM, XML
- KMIP Standard Operations
  Create, Register, Destroy, Get, Get Attribute List, GetAttributes, Create Key Pair, Re-Key, Re-KeyKeyPair, Archive, Recover, Activate, Derive Key
- Creating Keys
  Simple, Advanced, Extensions
- Managing Attributes
  Add, Modify, Delete Attribute
- LinearTape Open (LTO)
  LTO-4 Key Management, LTO-5/6 Key Management, KAD, AKAD, UKAD naming, Generic LTO-4
- Random Number Generator (RNG)
  Retrieve Server RNG, Seed Server RNG
- Server Cryptographic Operations
  Encrypt, Decrypt, Sign, Signature Verify MAC, MAC Verify, Hash
- Determine Capabilities
  Server SDKVersion, Discover Protocol Versions, Query Server Basic, Query Server Extensions, Query Advanced Capabilities
- Split Key (Multi-Party Controls)
  Create Split Key, Join Split Key
- Cryptsoft Vendor Extensions
  SQL Insert, SQL Update, SQL Delete
- Generic Multi-Protocol Key Handling
  GetKey, PutKey, DelKey
- Request/Response Handling
  Recording, Replaying, Batching, Bulk Data Loading
- Client Credential Handling
  Password-protected TLS Credentials, Device Credentials, IBM TKLM/SKLM

Supported KMIP Client Profiles

- Advanced Cryptographic Client[1.2]
- Advanced Symmetric Key Foundry Client
- AES XTS Client
- Asymmetric Key Lifecycle Client
- Baseline Client Basic
- Baseline Client TLS v1.2
- Basic Cryptographic Client[1.2]
- Basic Symmetric Key Foundry Client
- HTTPS Client
- Intermediate Symmetric Key Foundry Client
- JSON Client
- Opaque Managed Object Store Client
- PKCS#11 Client[2.0]
- Quantum Safe Client[2.0]
- RNG Cryptographic Client[1.2]
- Storage Array With SED Client
- Suite-B Min LOS_128 Client[1.x]
- Suite-B Min LOS_192 Client[1.x]
- Symmetric Key Lifecycle Client
- Tape Library Client
- XML Client

Supported KMIP Operations

- Activate
- Add Attribute
- Adjust Attribute[2.0]
- Allocation
- Archive
- Cancel
- Certify
- Check
- Create
- Create Key Pair
- Create Split Key[1.2]
- Decrypt[1.2]
- Delegated Login[2.0]
- Delete Attribute
- Derive Key
- Destroy
- Discover Versions[1.1]
- Encrypt[1.2]
- Export[1.4]
- Get
- Get Attribute List
- Get Attributes
- Get Usage Allocation
- Hash[1.2]
- Import[1.4]
- Interop[2.0]
- Join Split Key[1.2]
- Locate
- Log[2.0]
- Login[2.0]
- Logout[2.0]
- MAC[1.2]
- MAC Verify[1.2]
- Modify Attribute
- Notify
- Obtain Lease
- PKCS11[2.0]
- Poll
- Put
- Query
- Re-Certify
- Recover
- Register
- Re-Key
- Re-Key Key Pair
- Re-Provision[2.0]
- Revoke
- RNG Retrieve[1.2]
- RNG Seed[1.2]
- Set Attribute[2.0]
- Set Endpoint Role[2.0]
- Sign[1.2]
- Signature Verify[1.2]
- Validate

Supported KMIP Object Types

- Certificate
- Certificate Request[2.0]
- Opaque Object
- PGP Key
- Private Key
- Public Key
- Secret Key
- Split Key
- Symmetric Key
- Template

Supported Cryptographic Providers

- OpenSSL 1.0.x
- OpenSSL 1.1.x
- OpenSSL 3.0.x (dev)
- OpenSSL 0.9.8 (option)
- OpenSSL FIPS 2.0 (option)
- Oracle JCE Java
- IBM JCE Java
- RSA BSAFE MES 3.x, 4.x (option)
- RSA BSAFE Share-C (option)
- RSA BSAFE Crypto-J Java
- Bouncy Castle JCE Java
- wolfSSL (option)

Supported KMIP Encodings

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

Supported KMIP Server Vendors

- Cryptsoft
- DellEMC
- Fornetix
- Gemalto
- HyTrust
- IBM
- KeyNexus
- Kryptus
- MarkLogic
- Oracle
- SafeNet
- Thales
- Townsend Security
- Trend Micro
- Unbound
- Utimaco
- Vormetric

SALES@CRYPTSOFT.COM +61 7 3103 0321 | US +1 650 918 4362 WWW.CRYPTSOFT.COM

Copyright © 2019 Cryptsoft Pty Ltd. All rights reserved. All trademarks, service marks, trade names, product names and logos are property of their respective owners.

@CRYPTSOFT CRYPTSOFT-SECURITY-SPECIALISTS @CRYPTSOFT

2019-03