

KMIP SERVER SDK

C, JAVA

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 server solutions.

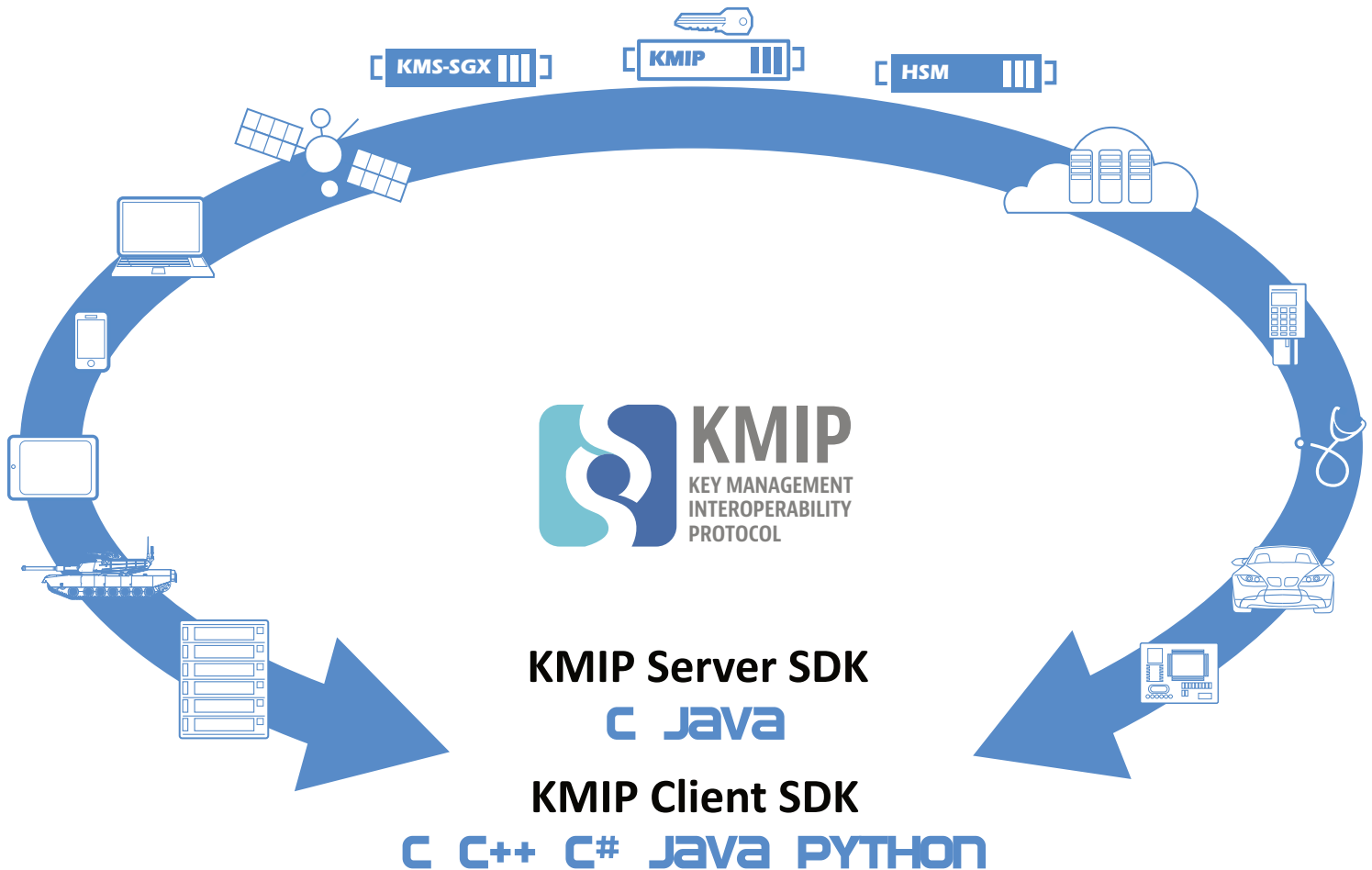
Cryptsoft's C and Java SDKs are all pure native code not wrapped versions, ensuring the most optimised, portable code for your application.

Reduce time to market, KMIP-enable your server 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



KMIP SERVER SDK - SPECIFICATIONS

C, JAVA

KMIP Server Examples

- Simple Protocol Format Parsing
TTLV, HEX, BIN, JSON, XML
- Simple Clients Operations
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, Get Attributes, Create Key Pair, Re-Key, Re-Key Key Pair^{1,1}, Archive, Recover, Activate, Derive Key
- Server Cryptographic Operations^{1,2}
Encrypt, Decrypt, Sign, Signature Verify, MAC, MAC Verify, Hash
- Managing Attributes
Add, Modify, Delete Attribute
- Random Number Generator (RNG)^{1,2}
Retrieve Server RNG, Seed Server RNG
- Split Key (Multi-Party Controls)^{1,2}
Create Split Key, Join Split Key
- Creating Keys
Simple, Advanced, Extensions
- Determine Capabilities
Server SDK Version, Discover Protocol Versions^{1,1}, Query Server Basic, Query Server Extensions^{1,1}, Query Advanced Capabilities^{1,3}
- Cryptsoft Vendor Extensions
SQL Insert, SQL Update, SQL Delete
- Request/Response Handling
Recording, Replaying, Batching, Bulk Data Loading
- Administration
Create, Modify, Delete Users, Partitions, Groups, Manage Group Privileges, Serialize, Deserialize, Managed Objects
- Database
Schema Management and Migration, Fixture Loading, SQL Replay
- Simple Servers
Query, Notify, Put
- JCE Examples
Key Store Provider

Supported KMIP Server Profiles

- Advanced Cryptographic Server^{1,2}
- AES XTS Server
- Asymmetric Key Lifecycle Server
- Baseline Server Basic
- Baseline Server TLS v1.2
- Basic Cryptographic Server^{1,2}
- Complete Server Basic
- Complete Server TLS v1.2
- HTTPS Server
- JSON Server
- Opaque Managed Object Store Server
- PKCS#11 Server^{2,0}
- Quantum Safe Server^{2,0}
- RNG Cryptographic Server^{1,2}
- Storage Array With SED Server
- Suite-B Min LOS_128 Server^{1,x}
- Suite-B Min LOS_192 Server^{1,x}
- Symmetric Key Foundry Server
- Symmetric Key Lifecycle Server
- Tape Library Server
- XML Server

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 Databases

- HSQLDB [Java](#)
- SQLite3
- MySQL 5,6,7,8
- Oracle 11.x, 12.x
- SQL Server 2003+
- IBM DB2 9 & 10
- PostgreSQL 8 & 9

Supported KMIP Encodings

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

Supported KMIP Client Vendors

- ADDGrup
- BDT
- Bracket
- Brocade
- Cohesity
- Cisco
- Cryptsoft
- CSC
- DataStax
- Dell
- DellEMC
- ETI-NET
- Fernetix
- Fujitsu
- Gemalto
- Hewlett Packard Enterprise
- Hitachi Data Systems
- Huawei
- HyTrust
- IBM
- Integrated Research
- Intersystems
- Iskraemeco
- MarkLogic
- NetApp
- Netskope
- Panzura
- Pluribus Networks
- Quantum
- Reduxio
- RSD SA
- SafeNet
- Sepaton
- Skyhigh Networks
- SpectraLogic
- Trend Micro
- TrustedConcepts
- VMWare
- Zettaset

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 Crypto-J [Java](#)
- Bouncy Castle JCE [Java](#)

