

## KEY MANAGEMENT SDKs

### Complete Vendor-Independent Key Management Solutions

Cryptsoft's Key Management SDKs enable rapid addition of interoperable key management functionality to your existing products.

Providing both Client and Server SDKs, Cryptsoft KMIP SDKs have been integrated into the majority of all KMIP products on the market today, eliminating the need for rework to interact with another vendor's endpoint.

Cryptsoft's PKCS#11 Consumer and Provider SDKs provide access to a wide range of hardware security devices allowing application portability, migration and management control in complex secure environments.

As the security market's preferred key management vendor, Cryptsoft has the technology and the relationships to ensure your product delivers its maximum potential.

Using the Cryptsoft SDKs in C, C++, C#, Java and Python, you can support key management protocols with a single, consistent interface and provide your customers with a complete vendor independent key management solution to manage all of the points of encryption within your enterprise.

## KEY FEATURES

- Full OASIS KMIP compliance versions: 1.0, 1.1, 1.2, 1.3, 1.4, 2.0\*
- KMIP SDKs interoperable with all released KMIP server/client products
- PKCS#11 SDKs compliant with OASIS PKCS#11 versions: 2.40, 3.0\*
- 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

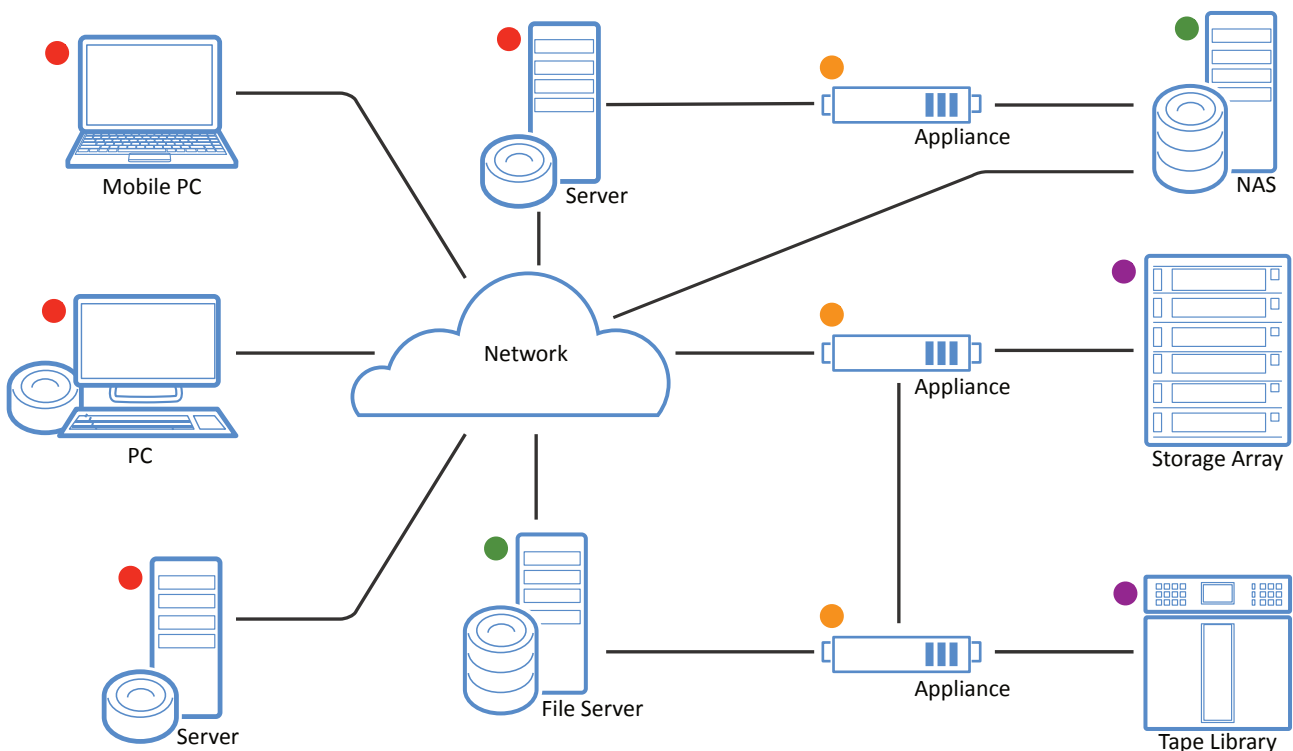
## Where Key Management is required

Key management is necessary for every point of encryption in the business environment. At every point where data is encrypted whether it be in use, in transit or at rest there will be a key to encrypt and decrypt that data. If data has been encrypted to protect it then managing the encryption key is as important as the data itself.

Cryptsoft KMIP Server and Client SDKs provide a ready made set of tested toolkits able to provide standards compliant key management for your solution at any point where encryption is required.

### LEGEND:

- Application Level
- Network Level
- Filesystem Level
- Device Level



## KEY MANAGEMENT SDKs

### Complete Vendor-Independent Key Management Solutions

#### KMIP Client SDK Products

- KMIP C Client SDK
- KMIP C Client SGX Module SDK
- KMIP C++ Client SDK
- KMIP C++ Client SGX Module SDK
- KMIP C# Client SDK
- KMIP C# Client SGX Module SDK
- KMIP Java Client SDK
- KMIP Java Client SGX Module SDK
- KMIP Python Client SDK
- KMIP Python Client SGX Module SDK
- KMIP C Client PKCS#11 Adapter
- KMIP RKM/DPM C Client SDK
- KMIP C Client Layered Protocol SDK
- KMIP Interoperability Test Suite (C/Java)
- KMIP Client Online Test Service

#### KMIP Server SDK Products

- KMIP C Server SDK
- KMIP C Server SGX Module SDK
- KMIP Java Server SDK
- KMIP Java Server SGX Module SDK
- KMIP Alert Server SDK
- KMIP Alert Server SGX Module SDK
- KMIP Authentication Server SDK
- KMIP Authentication Server SGX Module SDK
- KMIP Server Administration Interface (C/Java)
- KMIP Server VM Annual Subscription (C/Java)
- KMIP C Proxy Servers for Proprietary Protocols
- KMIP C Server (PKCS#11/HSM/RNG) Module
- KMIP C Server (PKCS#11/HSM/RNG) SGX Module
- KMIP C Server (Audit/Analytics) Module
- KMIP C Server OTP Module
- KMIP Server Online Test Service

#### PKCS#11 Consumer SDK Products

- PKCS#11 C Consumer SDK
- PKCS#11 C Consumer SGX Module SDK
- PKCS#11 C++ Consumer SDK
- PKCS#11 C++ Consumer SGX Module SDK
- PKCS#11 C# Consumer SDK
- PKCS#11 C# Consumer SGX Module SDK
- PKCS#11 Java Consumer SDK
- PKCS#11 Java Consumer SGX Module SDK
- PKCS#11 Python Consumer SDK
- PKCS#11 Python Consumer SGX Module SDK
- PKCS#11 Consumer Online Test Service

#### PKCS#11 Provider SDK Products

- PKCS#11 C Provider SDK
- PKCS#11 C Provider SGX Module SDK
- PKCS#11 C++ Provider SDK
- PKCS#11 C++ Provider SGX Module SDK
- PKCS#11 C# Provider SDK
- PKCS#11 C# Provider SGX Module SDK
- PKCS#11 Java Provider SDK
- PKCS#11 Java Provider SGX Module SDK
- PKCS#11 Python Provider SDK
- PKCS#11 Python Provider SGX Module SDK
- PKCS#11 Provider Online Test Service

## Supported Hardware Devices/Solutions

#### Supported Hardware Security Modules and Random Number Generators

- AWS - CloudHSM V1/V2 (RNG/HSM) [PKCS#11]
- Cavium - LiquidSecurity (RNG/HSM) [PKCS#11]
- Cryptsoft<sup>®</sup> - CloudHSM<sup>™</sup> (RNG/HSM) [PKCS#11]
- Engage Black - BlackVault (HSM) [PKCS#11]
- ID Quantique - Quantis USB (RNG) [Vendor]
- ID Quantique - Quantis PCI (RNG) [Vendor]
- ID Quantique - Quantis PCIe (RNG) [Vendor]
- nCipher - nShield Connect (RNG/HSM) [PKCS#11]
- nCipher - nShield Edge (RNG/HSM) [PKCS#11]
- nCipher - nShield Solo (RNG/HSM) [PKCS#11]
- SafeNet - Luna SA4/SA5 (RNG/HSM) [PKCS#11]
- SafeNet - Luna PCI (RNG/HSM) [PKCS#11]
- SafeNet - Protect Server (RNG/HSM) [PKCS#11]
- Utimaco - CryptoServerCSe10/100 (RNG/HSM) [PKCS#11]

#### Supported One Time Password Devices

- Android Soft Token [OATH-TOTP]
- Cryptsoft<sup>®</sup> [OATH-TOTP/U2F]
- Feitian [OATH-HOTP/TOTP]
- Google Authenticator Soft Token [OATH-TOTP]
- FIDO Devices [U2F]
- RSA Security SecurID [SecurID]
- Yubico [OATH-HOTP/TOTP/YubiKey]

