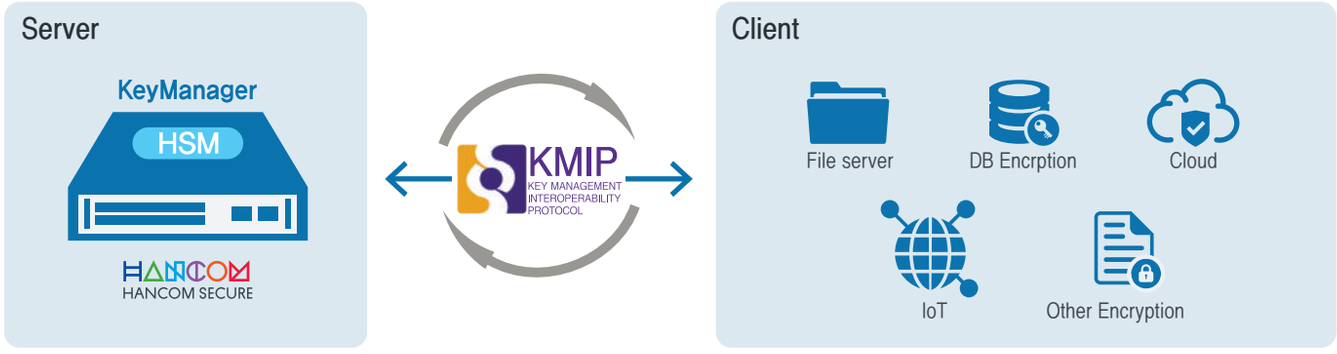
HancomSecure **KeyManager**

Integrated Key Management Solution complying with Key Management Interoperability Protocol (KMIP)



Key Features

KMIP Compliance
- Full compatibility between various encryption solutions by complying with OASIS KMIP

Various Key Formats Support
- Centralized policy management on symmetric keys, asymmetric keys, secret data and X.509 certificates

Centralized Key Management for Various Encryption Solutions
- Centralized management of encryption keys from Hancom Secure solutions (DB encryption, file encryption, etc.) and KMIP-compliant solutions (Oracle TDE, IBM, HP, NetApp, Trend Micro, etc.)

Proven KMIP Client SDK tested with multiple KMIP servers
- Enable easy and quick integration with a variety of third party solutions
- Support most platforms (Linux, Windows, MacOS, etc.)

HSM-based Key Management Server
- A high level of safety as a confidential military information level with a FIPS 140-2 Level 3, CC EAL 4+ certified hardware security module (HSM)

Verified Encryption Algorithm
- Reliable encryption with a Korea Cryptographic Module Validation Program(KCMVP)-certified encryption module

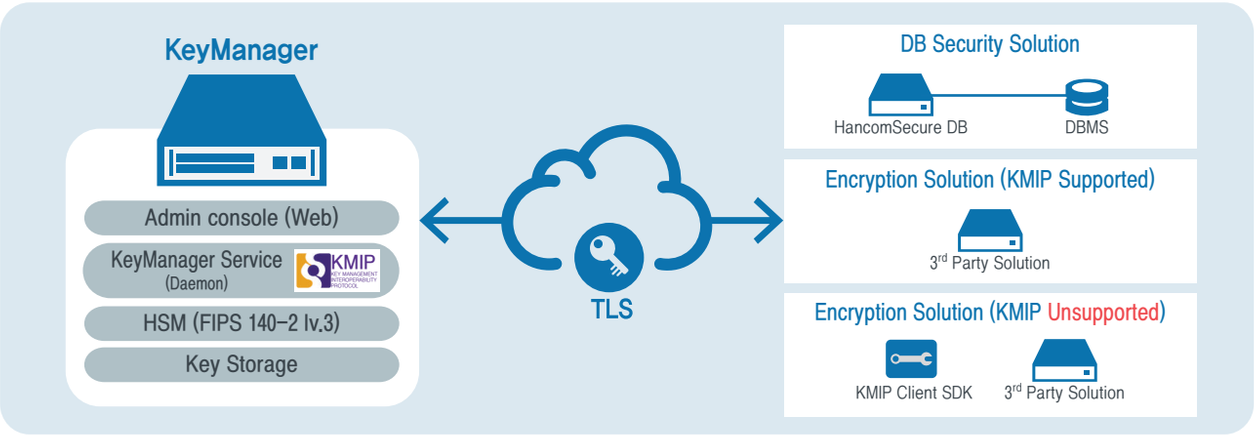
Comply with Key Management Guide
- Comply with the key management standard guide of NIST
- Automated management of complex encryption key lifecycle by policy

High Availability Support
- Easy system addition/removal to the KeyManager Cluster in service
- Automated failure recovery

Minimize Management Costs
- Minimization of operational cost by centralized key management
- No extra cost for additional deployment of KMIP-compliant encryption solutions

Cloud Environment Support
- Secured service with On-premise KeyManager for data stored in virtualized public cloud environment

Architecture



Components	Details
Admin Console (Web)	▪ KeyManager configuration, key management policy setting, access-permitted client list, client group management, HA function handling, key list check, key backup and restoration, operation and statistics per key, audit
KeyManager Service (Daemon)	▪ KMIP operation support, implementation of TLS communication channel with registered clients, lightening key management message exchange using TTLV(Tag Type Length Value)
HSM	▪ Encryption of generated key and decryption of requested key without leakage of a master key
Key Storage	▪ Securely store keys encrypted by HSM

Specifications – Server

Solution	Model Name	Descriptions
HancomSecure KeyManager (Appliance Type)	HancomSecure KeyManager 1000	▪ 1U ▪ Support max. 10K keys ▪ Available to integrate with 2 systems
	HancomSecure KeyManager 2000	▪ 2U ▪ Support max. 100K keys ▪ Available to integrate with 10 systems
	HancomSecure KeyManager 3000	▪ 2U ▪ Support max. 1,000K keys ▪ Available to integrate with 20 systems

Specifications – KMIP Client SDK

Languages	▪ Implemented in C++, other language bindings provided (Java, Python, etc.)
Supported Objects	▪ Certificate, Symmetric Key, Public Key, Private Key, Split Key, Template, Secret Data, Opaque Object, PGP Key
Supported KMIP Operations	▪ Create, Create Key Pair, Register, Re-key, Re-key Key Pair, Derive Key, Certify, Re-certify, Locate, Check, Get, Get Attributes, Get Attribute List, Add Attribute, Modify Attribute, Delete Attribute, Obtain Lease, Get Usage Allocation, Activate, Revoke, Destroy, Archive, Recover, Validate, Query, Discover Versions, Cancel, Poll, Encrypt, Decrypt, Sign, Signature Verify, MAC, MAC Verify, RNG Retrieve, RNG Seed, Hash, Create Split Key, Join Split Key

HANCOM SECURE
A: 9FL Hancom Tower, 49, Daewangpangyo-ro 644beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
E: overseas@hsecure.co.kr T:+82-31-622-6321 F: +82-31-622-6277
en.hsecure.co.kr