

# XecureKeyManager

국제 키 관리 상호 운용 표준(KMIP)을 준수하는 HSM 기반의 통합 키 관리 서버



## 주요 특징

**국제 키 관리 상호 운용 표준 (KMIP) 준수**

- OASIS의 키 관리 상호 운용 프로토콜 (Key Management Interoperability Protocol, KMIP)을 준수하여 다양한 솔루션 사이의 완벽한 호환성 제공

**다양한 암호 솔루션의 통합 키 관리 가능**

- 한컴시큐어의 DB암호화 솔루션(XecureDB), 파일 암호화 솔루션(XecureFileCrypto)등 자사 솔루션의 암호 키 통합 관리
- KMIP를 지원하는 타사(IBM, HP, NetApp, Trend Micro, Oracle 등) 솔루션의 암호 키 통합 관리

**HSM 기반 키 관리 서버**

- 미 NIST의 FIPS 140-2 Level 3, CC EAL 4+ 인증을 받은 HSM이 내장되어 군사 기밀 처리 등급의 높은 안전성을 제공

**키 관리 가이드 준수**

- KISA 및 미 NIST의 키 관리 표준 가이드를 준수
- 복잡한 암호 키의 생명주기를 정책에 따라 자동화 관리

**관리 비용의 최소화**

- 중앙화된 키 관리를 통해 운용 비용의 최소화 가능
- KMIP를 지원하는 암호 솔루션의 추가 도입 시 키 관리 서버의 구축비용이 발생하지 않음

**다양한 종류의 키 지원**

- 다양한 종류의 대칭키, 비대칭키, 비밀데이터, X.509 인증서 등을 중앙화된 정책으로 관리

**검증된 클라이언트 SDK**

- KMIP를 지원하는 다양한 서버와 쉽고 빠르게 통합 운용 가능
- 다양한 플랫폼 지원 (Linux, Windows, MacOS 등)

**검증된 암호화 알고리즘**

- 국정원 암호모듈인증(KCMVP)을 획득한 암호 모듈 탑재로 신뢰성 있는 암호화 기능 지원

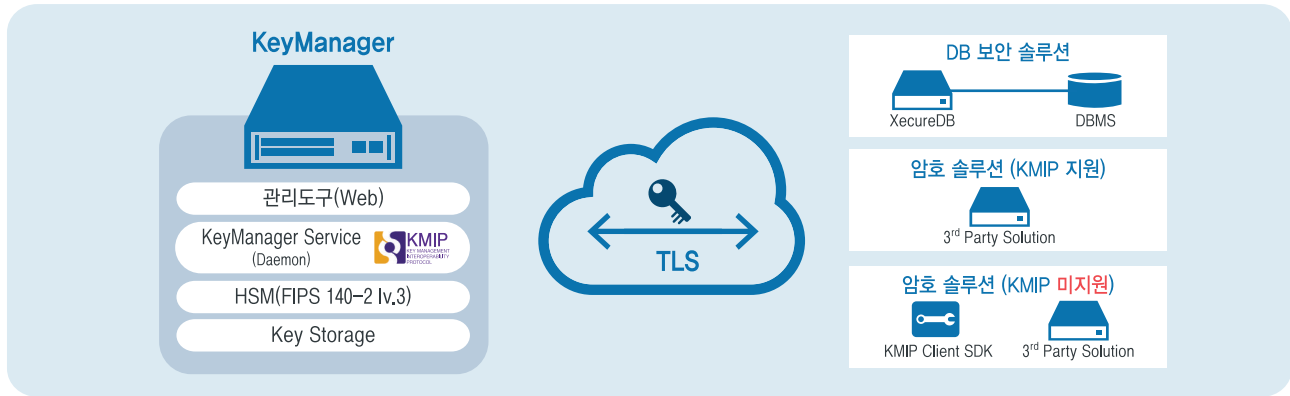
**고 가용성**

- 이중화 및 다중화를 지원
- 서비스 중 KeyManager Cluster에 자유로운 장비의 추가/삭제 가능
- 자동화된 장애 복구

**클라우드 환경 대응**

- 가상화된 퍼블릭 클라우드 환경에 저장된 데이터도 On-premise된 KeyManager 도입으로 안심하고 서비스 이용 가능

## 구성도



구성 요소	기능
관리도구 (Web)	<ul style="list-style-type: none"> <li>XecureKeyManager 환경설정, 키 관리 정책 설정 및 관리, 접속 허용 클라이언트 목록 관리, 클라이언트 그룹 관리, HA 기능 관리, 키 목록 조회, 키 백업 및 복구, 연산 및 키 별 통계, 감사</li> </ul>
Xecure KeyManager Service (daemon)	<ul style="list-style-type: none"> <li>KMIP 연산 대응, 등록된 클라이언트와 TLS 통신 채널 구축, TTLV(Tag Type Length Value)를 이용한 경량화 키 관리 메시지 송수신</li> </ul>
HSM	<ul style="list-style-type: none"> <li>생성된 키의 암호화 및 요청된 키의 복호화를 내부에서 마스터키 유출 없이 수행</li> </ul>
Key Storage	<ul style="list-style-type: none"> <li>키를 HSM으로 암호화하여 안전하게 저장</li> </ul>

## 사양 - Server

Solution	Model Name	규격
Xecure KeyManager (Appliance Type)	Xecure KeyManager 1000	<ul style="list-style-type: none"> <li>1U</li> <li>최대 관리 키 개수 : 10,000</li> <li>연동 시스템 : 2개(기본제공)</li> </ul>
	Xecure KeyManager 2000	<ul style="list-style-type: none"> <li>2U</li> <li>최대 관리 키 개수 : 100,000</li> <li>연동 시스템 : 10개(기본제공)</li> </ul>
	Xecure KeyManager 3000	<ul style="list-style-type: none"> <li>2U</li> <li>최대 관리 키 개수 : 1,000,000</li> <li>연동 시스템 : 20개(기본제공)</li> </ul>

## 사양 - KMIP Client SDK

Languages	<ul style="list-style-type: none"> <li>C, C++, Java, Python 등</li> </ul>
Supported Objects	<ul style="list-style-type: none"> <li>Certificate, Symmetric Key, Public Key, Private Key, Split Key, Template, Secret Data, Opaque Object, PGP Key</li> </ul>
Supported KMIP Operations	<ul style="list-style-type: none"> <li>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</li> </ul>