Samsung Cloud Platform

Security

Key Management Service

암호화 키를 편리하게 생성하고 안전하게 보호하는 서비스

Key Management Service(KMS)는 애플리케이션의 중요한 데이터를 안전하게 보호하기 위해, 암호화 키를 간편하게 생성하고 안전하게 저장/관리하는 서비스입니다. 사용자는 암호화 키를 이용하여 데이터를 암/복호화하며, 암호화 키는 계층적으로 암호화 된 중앙 집중 암호화 키 방식으로 안정적으로 관리됩니다.

계층적 키 관리

KMS는 데이터 키, 마스터 키, 루트 키 등 계층적 암호화 방식을 통해 안전한 키 관리를 제공합니다. 마스터 키는 FIPS 140-2 Lv3 표준을 준수하는 HSM(Hardware Security Module)에 저장되어 있는 루트 키를 통해 생성하며, KMS에 안전하게 분산 저장하여 보호합니다. 사용자는 마스터 키를 활용하여 데이터를 암호화 하는 데이터 키를 직접 생성합니다.

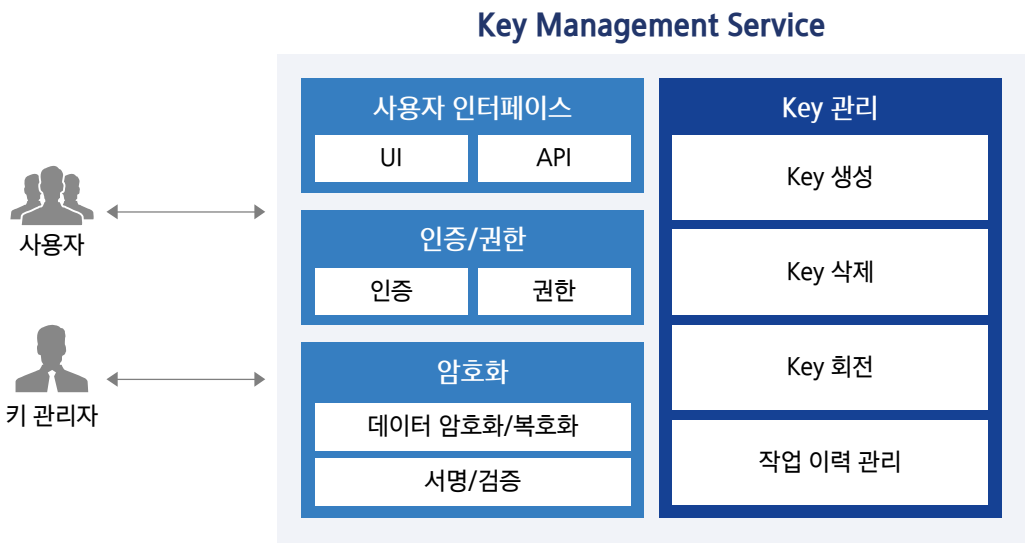
키 라이프 사이클 관리

키 회전을 통해 키를 새로 생성하지 않아도 해당 마스터 키에 대한 새로운 암호화 자료를 생성할 수 있으며, 키 회전 주기는 고객 정책에 따라 자유롭게 선택할 수 있습니다. 또한 KMS 모니터링을 통해 키 이력을 손쉽게 관리할 수 있으며, 암호화 키의 라이프 사이클 관리를 통해 더 이상 사용하지 않는 암호화 키는 비 활성화하거나 삭제하여 암호학적 위협으로부터 데이터를 안전하게 보호합니다.

고 가용성 인프라

KMS는 고 가용성 인프라를 통해 안정적인 서비스를 제공합니다. 마스터 키를 생성하는 KMS 엔진, KMS 엔진의 루트 키를 저장하는 HSM 등 다중화 구성을 바탕으로 높은 가용성을 제공합니다.

서비스 구성도



주요 기능

- **제공 키 종류**
  - 암호화/복호화(AES256) : 대칭 키 방식의 AES256 키를 생성해 최대 32KB 데이터 암호화에 사용
  - 암/복호화 및 서명/검증(RSA-2048) : 비대칭 키 방식의 RSA(2048비트) 키를 생성해 최대 190B 데이터 암호화 또는 8KB 서명에 사용
  - 생성/검증(HMAC) : 해시 기반 메시지 인증코드(HMAC) 생성 및 확인에 사용
  - 서명/검증(ECDSA) : 비대칭 키 방식의 ECDSA 키를 생성해 최대 8KB 데이터 서명에 사용
    ※ SCP Sovereign의 경우 국내 공공 인증 알고리즘인 ARIA 사용 가능
- **키 권한 관리**
  - 마스터 키 사용 권한을 부여할 계정 선택(동일 Account 내 계정)
  - 키 역할 선택 : Key Manager, Encryptor/Decryptor, Encryptor, Decryptor, Key Reviewer
- **키 라이프 사이클 관리**
  - 키 회전 : 새로운 키 버전 생성. 자동 회전 주기는 1~730일 선택
  - 키 삭제 : 삭제 요청 시 해당 키는 즉시 사용 중지되며, 72시간 후 영구 삭제
  - 키 작업 이력 보기 : 작업 일시, 작업 내역 및 결과, 작업 계정