THALES

Vormetric Data Security
암호화 키 관리 및 전송

2018년 10월
Thales Korea

www.vormetric.com

암호화 키 관리 개요

데이터 암호화 키 보안

- 키 생성 시 키 값은 자동 생성
- 자동 생성한 키 값은 키 관리자 또는 보메트릭 솔루션의 어떤 관리자도 알 수 없음
- 키는 솔루션 전체 라이프 사이클에 걸쳐 항상 암호화 유지
- 키 백업 시 별도 Wrapper Key를 통해 암호화

데이터 암호화 키 생성 (간단한 키 관리)

- 키 이름 및 길이 (Algorithm)
- 다른 암호화 솔루션에서 암호화 한 데이터 관리를 위해 수동 입력 모드 지원

데이터 암호화 키 저장 및 배포

- 암호화 키 저장소: 키 관리 서버 (DSM: Data Security Manager) 중앙 관리 방식
- DSM은 Network HSM으로, 내부에 키의 안전한 저장을 위한 Key Store가 있음
- 배포 시기: 호스트 (암호화 데이터를 저장하는 서버들) 재부팅 또는 에이전트 재시작 시

데이터 암호화 키 폐기

- 키 설정에 유효 기간 설정: 유효 기간 만료 시 관리자에게 통보
- 사용 중인 암호화 키 보호를 위해 실제 폐기 작업은 관리자에 의한 수동 폐기

암호화 키 백업 보호 – Wrapper Key

키관리 서버 백업/복원, 개별 키 백업 복원 시 백업본 암호화에 사용

M of N 키 지원

- 복원 시 단일 관리자에 의한 키 복원 방지

키 분리를 위해 Shamir Shared Secret 사용

- Wrapper Key Share를 할당된 관리자에게만 제공 (관리콘솔 대시보드에 표시)
- 실제 키 값은 확인 불가

Server security mode	Compatible mode
RSA CA fingerprint	30:01:E0:89:77:56:BF:E1:CA:D1:5D:66:DF:27:1F:40:75:24:B7:D5
EC CA fingerprint	7C:76:1B:B7:EF:83:04:3F:7F:73:FB:5C:D7:C2:00:50:9E:E0:A5:63
Wrapper Key Share	2331cb9fd508d827d1bc450b68493cbd8fed3ab1a033ef2935ac8be949ba3163

Wrapper Key 관리

- 관리 콘솔 Wrapper Key 메뉴에서 생성 및 관리
- 신규 Wrapper Key 생성 시 기존 Wrapper Key로 암호화된 백업은 복원되지 않음
- Wrapper Key 가져오기 기능을 통해 기존 Wrapper Key로 암호화된 백업 복원

암호화 키의 안전한 전송을 위하여...

에이전트 구성 요소 및 보안 통신

- 사용자 영역에 통신을 담당하는 vmd, 커널 영역에 암호화를 담당하는 SecFS로 구성
- vmd 및 SecFS 모두 자신의 인증서 보유
- DSM에게 Public Key를 제공하고 인증된 DSM에게만 접속 허용

암호화 키 전송 절차 개요

1. 데이터 암호화 키 (DEK)를 암호화 하기 위해 일회용 AES256 “Random Key” (RK)를 생성
2. 호스트로 전송할 패키지 구성
   - 호스트 암호 (SecFS의 Public Key로 암호화)
   - 호스트 암호로 RK 암호화 (SecFS의 Public Key로 암호화)
   - 호스트 호스트에 적용할 정책 및 구성 정보
   - 적용할 정책에서 사용하는 암호화 키 (“Random Key”로 암호화)
3. 에이전트의 vmd 및 DSM 모두 SSL 서버이므로 양방향 SSL 채널 설정
4. 안전한 전송을 위해 현재 OpenSSL에서 지원되는 가장 강력한 Cipher Suite인 "AES256-SHA (RSA_WITH_AES_256_CBC_SHA)“로 암호화하여 호스트에 전송
5. vmd 가 수신된 패키지를 secfs에 전달
6. secfs가 자신의 Private Key로 호스트 암호 등을 복호화 하여 RK를 획득하고 이를 통해 DEK 복호화

키 전송 전 DSM 준비 사항

호스트 암호 (PWD)

- 내구 구현 로직에 의해 변형

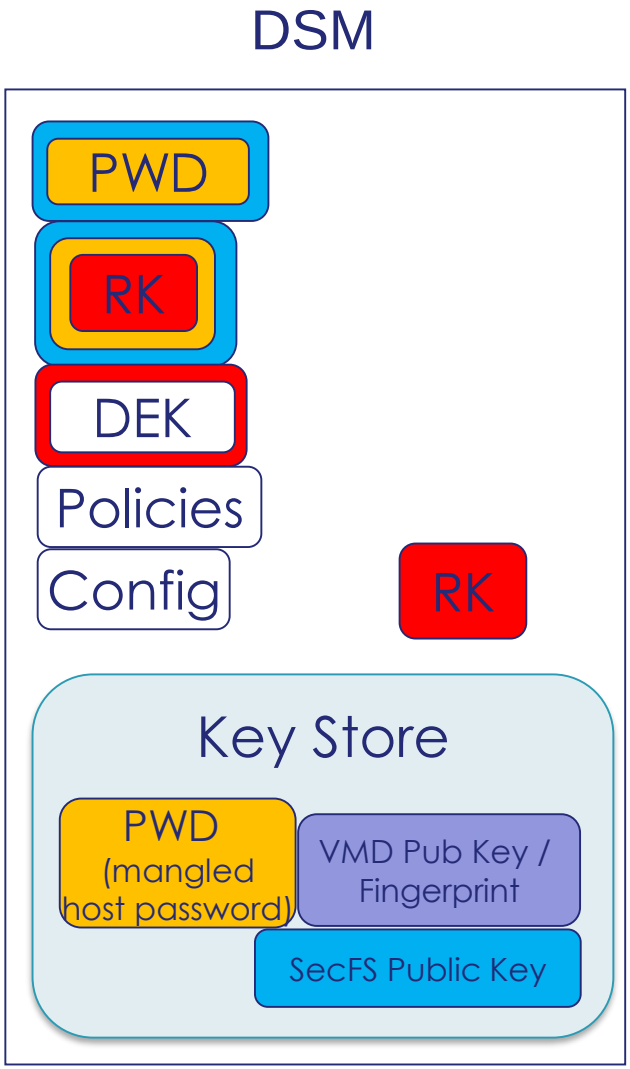
Random Key 생성 (RK)

- 데이터 암호화 키 (DEK) 암호화를 위한 키
- 전송 시마다 즉시 생성
- AES256

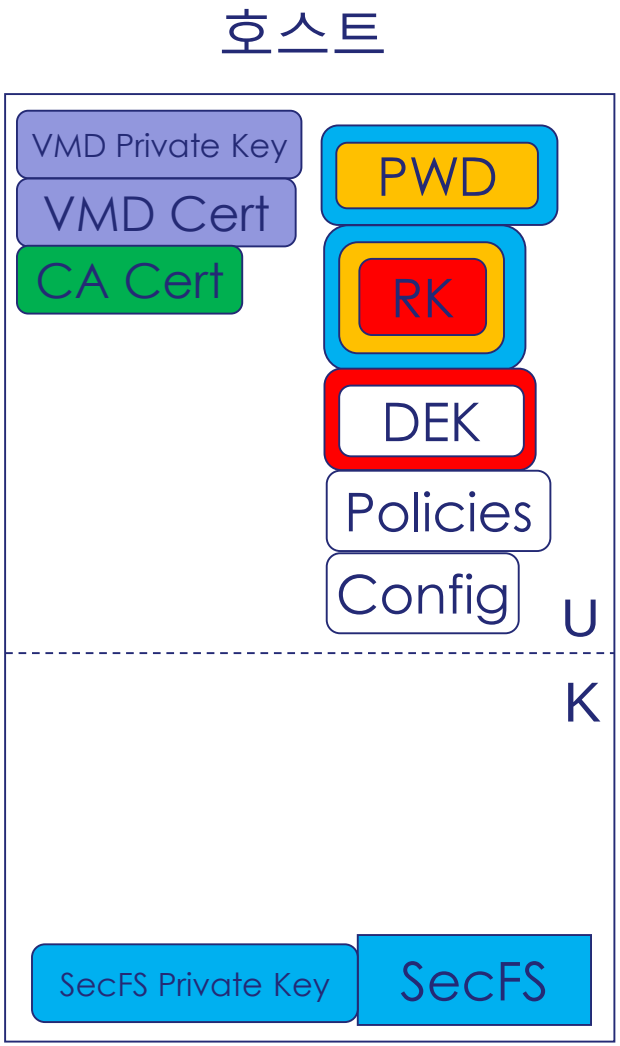
전송 패키지 구성

- 변형된 PWD (SecFS의 Public Key로 암호화)
- PWD로 RK 암호화 (SecFS의 Public Key로 암호화)
- 암호화 정책
- 구성 정보
- 정책에 포함된 DEK (RK로 암호화)

패키지를 전송 시 VMD Public 키로 한 번 더 암호화



전송 후 에이전트 상태 – 사용자 영역



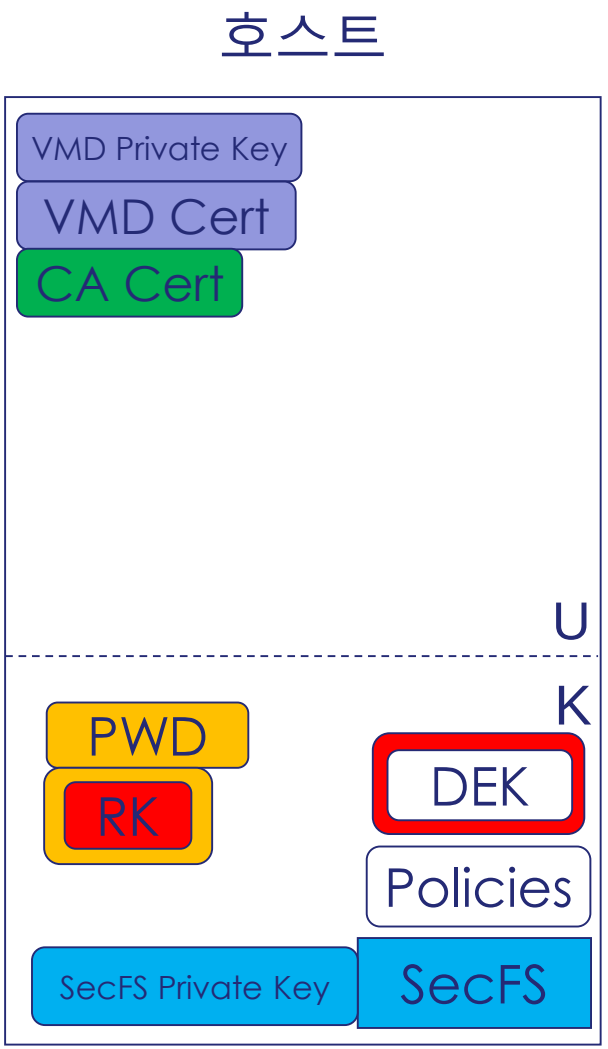
전송

- vmd Private Key/Public Key는 vmd 서비스 시작 시 DSM에 설치된 인증기관에서 생성
- 디스크에 저장하지 않음 ➔ **해킹 방지**

vmd가 메모리에서 작업

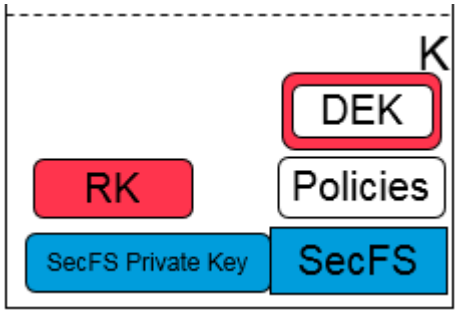
- 패키지 수신 후 vmd Private Key로 복호화
- 구성 정보 적용
- 암호화 정책을 SecFS에 전달
- PWD, PWD로 암호화 된 RK는 SecFS Public Key로 암호화 되어 읽을 수 없음 ➔ **해킹 방지**
- DEK는 RK로 암호화 되어 읽을 수 없음 ➔ **해킹 방지**
- PWD, PWD로 암호화 된 RK, RK로 암호화 된 DEK 패키지를 SecFS에 전달

전송 후 에이전트 상태 – 커널 영역

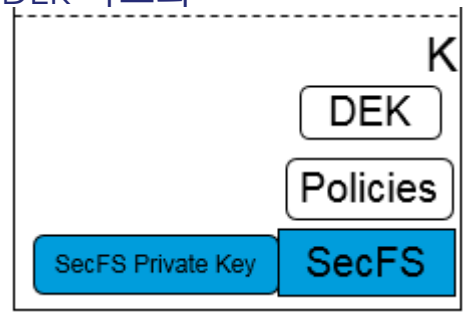


SecFS 작업 절차

- SecFS Private Key는 별도 AES256키로 암호화. 에이전트 프로그램 없이 복호화 불가능 ➔ **해킹 방지**
- SecFS Private Key로 PWD, PWD로 암호화 된 RK 복호화
- PWD로 RK 값 복호화



- RK로DEK 복호화



- 데이터 암호화/복호화 서비스

암호화 키 전송 다이어그램