(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0052016
(43) 공개일자 2022년04월27일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 9/083 (2013.01)
H04L 9/0825 (2013.01)
(21) 출원번호 10-2020-0135849
(22) 출원일자 2020년10월20일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
추연성
경기도 용인시 수지구 고기로 89
(74) 대리인
박영우

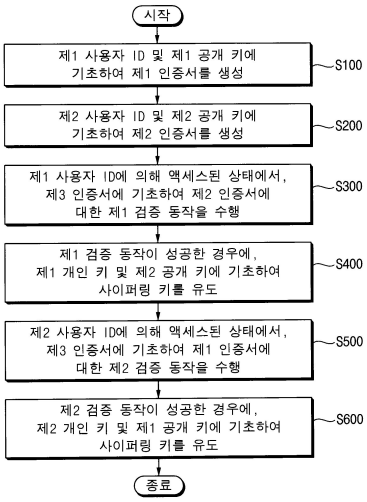
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **스토리지 장치에서의 보안 동작을 위한 키 교환 방법 및 이를 이용한 접근 권한 이관 방법**

(57) 요 약

스토리지 장치에서의 보안 동작을 위한 키 교환 방법에서, TTP에 의해, 제1 사용자 ID 및 제1 공개 키에 기초하여 제1 인증서를 생성한다. TTP에 의해, 제2 사용자 ID 및 제2 공개 키에 기초하여 제2 인증서를 생성한다. 제1 사용자 ID에 의해 액세스된 상태에서, TTP에 포함되는 제3 인증서에 기초하여 제2 인증서에 대한 제1 검증 동작을 수행한다. 제1 검증 동작이 성공한 경우에, 제1 개인 키 및 제1 검증 동작에 의해 획득된 제2 공개 키에 기초하여 사이퍼링 키를 유도한다. 제2 사용자 ID에 의해 액세스된 상태에서, 제3 인증서에 기초하여 제1 인증서에 대한 제2 검증 동작을 수행한다. 제2 검증 동작이 성공한 경우에, 제2 개인 키 및 제2 검증 동작에 의해 획득된 제1 공개 키에 기초하여 사이퍼링 키를 유도한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0838 (2013.01)
H04L 9/3263 (2013.01)

명 세 서

청구범위

청구항 1

복수의 사용자 ID(Identification)들에 의해 액세스되는 스토리지 장치에서의 보안 동작을 위한 키 교환 방법으로서,

상기 스토리지 장치에 포함되는 TTP(Trusted Third Party)에 의해, 제1 사용자 ID 및 제1 공개 키(public key)에 기초하여 상기 제1 사용자 ID에 대한 제1 인증서를 생성하는 단계;

상기 TTP에 의해, 제2 사용자 ID 및 제2 공개 키에 기초하여 상기 제2 사용자 ID에 대한 제2 인증서를 생성하는 단계;

상기 제1 사용자 ID에 의해 액세스된 상태에서, 상기 TTP에 포함되는 제3 인증서에 기초하여 상기 제2 인증서에 대한 제1 검증 동작을 수행하는 단계;

상기 제1 검증 동작이 성공한 경우에, 제1 개인 키(private key) 및 상기 제1 검증 동작에 의해 획득된 상기 제2 공개 키에 기초하여 사이퍼링 키(ciphering key)를 유도하는 단계;

상기 제2 사용자 ID에 의해 액세스된 상태에서, 상기 제3 인증서에 기초하여 상기 제1 인증서에 대한 제2 검증 동작을 수행하는 단계; 및

상기 제2 검증 동작이 성공한 경우에, 제2 개인 키 및 상기 제2 검증 동작에 의해 획득된 상기 제1 공개 키에 기초하여 상기 사이퍼링 키를 유도하는 단계를 포함하는 키 교환 방법.

청구항 2

제 1 항에 있어서, 상기 제1 인증서를 생성하는 단계는,

상기 TTP에 포함되는 제3 개인 키를 기초로 상기 제1 사용자 ID 및 상기 제1 사용자 ID에 대한 상기 제1 공개 키를 서명하여 상기 제1 인증서를 획득하는 단계; 및

상기 제1 인증서를 키 슬롯(key slot)에 포함되고 상기 제1 사용자 ID에 할당된 제1 키 슬롯 영역에 저장하는 단계를 포함하는 것을 특징으로 하는 키 교환 방법.

청구항 3

제 2 항에 있어서,

상기 제1 키 슬롯 영역에는 상기 제1 개인 키, 상기 제1 공개 키 및 상기 제3 인증서가 상기 제1 인증서와 함께 저장되는 것을 특징으로 하는 키 교환 방법.

청구항 4

제 2 항에 있어서, 상기 제2 인증서를 생성하는 단계는,

상기 제3 개인 키를 기초로 상기 제2 사용자 ID 및 상기 제2 사용자 ID에 대한 상기 제2 공개 키를 서명하여 상기 제2 인증서를 획득하는 단계; 및

상기 제2 인증서를 상기 키 슬롯에 포함되고 상기 제2 사용자 ID에 할당된 제2 키 슬롯 영역에 저장하는 단계를 포함하는 것을 특징으로 하는 키 교환 방법.

청구항 5

제 2 항에 있어서, 상기 제1 검증 동작을 수행하는 단계는,

상기 제3 인증서에 기초하여 상기 TTP에 포함되는 제3 공개 키를 추출하는 단계;

상기 제3 공개 키에 기초하여 상기 제2 인증서에 대한 서명을 검증하는 단계; 및

상기 제2 인증서에 대한 서명 검증이 성공한 경우에, 상기 제2 인증서에 포함되는 상기 제2 사용자 ID 및 상기 제2 공개 키를 추출하는 단계를 포함하는 것을 특징으로 하는 키 교환 방법.

청구항 6

제 5 항에 있어서, 상기 제1 개인 키 및 상기 제2 공개 키에 기초하여 상기 사이퍼링 키를 유도하는 단계는,

상기 제1 사용자 ID에 대응하는 제1 패스워드 및 랜덤 값에 기초하여 제1 KPK(Key-Protection-Key)를 획득하는 단계;

상기 제1 KPK에 기초하여 상기 제1 개인 키를 획득하는 단계; 및

상기 제1 개인 키 및 상기 제2 공개 키를 기초로 키 합의(key agreement)를 수행하여 상기 사이퍼링 키를 획득하는 단계를 포함하는 것을 특징으로 하는 키 교환 방법.

청구항 7

제 2 항에 있어서, 상기 제2 검증 동작을 수행하는 단계는,

상기 제3 인증서에 기초하여 상기 TTP에 포함되는 제3 공개 키를 추출하는 단계;

상기 제3 공개 키에 기초하여 상기 제1 인증서에 대한 서명을 검증하는 단계; 및

상기 제1 인증서에 대한 서명 검증이 성공한 경우에, 상기 제1 인증서에 포함되는 상기 제1 사용자 ID 및 상기 제1 공개 키를 추출하는 단계를 포함하는 것을 특징으로 하는 키 교환 방법.

청구항 8

제 7 항에 있어서, 상기 제2 개인 키 및 상기 제1 공개 키에 기초하여 상기 사이퍼링 키를 유도하는 단계는,

상기 제2 사용자 ID에 대응하는 제2 패스워드 및 랜덤 값에 기초하여 제2 KPK를 획득하는 단계;

상기 제2 KPK에 기초하여 상기 제2 개인 키를 획득하는 단계; 및

상기 제2 개인 키 및 상기 제1 공개 키를 기초로 키 합의를 수행하여 상기 사이퍼링 키를 획득하는 단계를 포함하는 것을 특징으로 하는 키 교환 방법.

청구항 9

제 1 항에 있어서,

상기 스토리지 장치는 상기 스토리지 장치의 동작을 제어하는 스토리지 컨트롤러를 포함하고,

상기 스토리지 컨트롤러는 상기 스토리지 장치의 일반 동작을 제어하는 제1 프로세서, 및 상기 보안 동작을 제어하는 제2 프로세서를 포함하며,

상기 TTP는 상기 제2 프로세서에 포함되는 것을 특징으로 하는 키 교환 방법.

청구항 10

복수의 사용자 ID(Identification)들에 의해 액세스되는 스토리지 장치에 포함되는 제1 저장 영역에 대한 접근 권한 이관 방법으로서,

상기 제1 저장 영역에 대한 제1 접근 권한을 가지고 있는 제1 사용자 ID와 상기 제1 접근 권한을 획득하고자 하는 제2 사용자 ID 사이에 키 교환 동작을 수행하는 단계;

상기 제1 사용자 ID에 의해 액세스된 상태에서, 상기 키 교환 동작에 의해 획득된 사이퍼링 키(ciphering key)에 기초하여 상기 제1 접근 권한에 대응하는 제1 KEK(Key-Encryption-Key)를 암호화하여 저장하는 단계; 및

상기 제2 사용자 ID에 의해 액세스된 상태에서, 상기 사이퍼링 키에 기초하여 암호화된 상기 제1 KEK를 복호화하여 저장하는 단계를 포함하고,

상기 키 교환 동작을 수행하는 단계는,

상기 스토리지 장치에 포함되는 TTP(Trusted Third Party)에 의해, 상기 제1 사용자 ID 및 제1 공개 키(public

key)에 기초하여 상기 제1 사용자 ID에 대한 제1 인증서를 생성하는 단계;

상기 TTP에 의해, 상기 제2 사용자 ID 및 제2 공개 키에 기초하여 상기 제2 사용자 ID에 대한 제2 인증서를 생성하는 단계;

상기 제1 사용자 ID에 의해 액세스된 상태에서, 상기 TTP에 포함되는 제3 인증서에 기초하여 상기 제2 인증서에 대한 제1 검증 동작을 수행하는 단계;

상기 제1 검증 동작이 성공한 경우에, 제1 개인 키(private key) 및 상기 제1 검증 동작에 의해 획득된 상기 제2 공개 키에 기초하여 상기 사이퍼링 키를 유도하는 단계;

상기 제2 사용자 ID에 의해 액세스된 상태에서, 상기 제3 인증서에 기초하여 상기 제1 인증서에 대한 제2 검증 동작을 수행하는 단계; 및

상기 제2 검증 동작이 성공한 경우에, 제2 개인 키 및 상기 제2 검증 동작에 의해 획득된 상기 제1 공개 키에 기초하여 상기 사이퍼링 키를 유도하는 단계를 포함하는 접근 권한 이관 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 반도체 집적 회로에 관한 것으로서, 더욱 상세하게는 스토리지 장치에서의 보안 동작을 위한 키 교환 방법 및 상기 키 교환 방법을 이용한 접근 권한 이관 방법에 관한 것이다.

배 경 기 술

[0002] 최근에는 메모리 장치를 이용하는 SSD(solid state drive)와 같은 스토리지 장치가 널리 사용되고 있다. 상기와 같은 스토리지 장치는 기계적인 구동부가 없어 안정성 및 내구성이 뛰어나며 정보의 액세스 속도가 매우 빠르고 전력 소모가 적다는 장점이 있다. 최근 들어 노트북과 같은 전자 시스템뿐만 아니라, 자동차, 항공기, 드론(drone) 등과 같은 다양한 종류의 시스템에 전자 회로가 적용됨에 따라, 스토리지 장치 역시 다양한 종류의 시스템에서 사용되고 있다.

[0003] 또한, 최근에는 스토리지 장치의 보안 성능 향상을 위해 하드웨어 기반의 FDE(full-disk encryption)가 사용되고 있다. 특히 FDE가 내장된 스토리지 장치를 SED(self-encrypting drive)라고 부를 수 있다. OPAL 스토리지 사양(storage specification) 또는 간단히 OPAL은 보안 강화를 위한 스토리지 장치의 기능에 대한 일련의 사양이며, TCG(Trusted Computing Group)에서 개발한 SED에 대한 일련의 사양을 나타낸다.

발명의 내용

해결하려는 과제

[0004] 본 발명의 일 목적은 SED와 같은 스토리지 장치에서의 보안 동작을 위한 키 교환 방법을 제공하는 것이다.

[0005] 본 발명의 다른 목적은 SED와 같은 스토리지 장치에서의 상기 키 교환 방법을 이용한 접근 권한 이관 방법을 제공하는 것이다.

과제의 해결 수단

[0006] 상기 일 목적을 달성하기 위해, 본 발명의 실시예들에 따른 복수의 사용자 ID(Identification)들에 의해 액세스되는 스토리지 장치에서의 보안 동작을 위한 키 교환 방법에서, 상기 스토리지 장치에 포함되는 TTP(Trusted Third Party)에 의해, 제1 사용자 ID 및 제1 공개 키(public key)에 기초하여 상기 제1 사용자 ID에 대한 제1 인증서를 생성한다. 상기 TTP에 의해, 제2 사용자 ID 및 제2 공개 키에 기초하여 상기 제2 사용자 ID에 대한 제2 인증서를 생성한다. 상기 제1 사용자 ID에 의해 액세스된 상태에서, 상기 TTP에 포함되는 제3 인증서에 기초하여 상기 제2 인증서에 대한 제1 검증 동작을 수행한다. 상기 제1 검증 동작이 성공한 경우에, 제1 개인 키(private key) 및 상기 제1 검증 동작에 의해 획득된 상기 제2 공개 키에 기초하여 사이퍼링 키(ciphering key)를 유도한다. 상기 제2 사용자 ID에 의해 액세스된 상태에서, 상기 제3 인증서에 기초하여 상기 제1 인증서에 대한 제2 검증 동작을 수행한다. 상기 제2 검증 동작이 성공한 경우에, 제2 개인 키 및 상기 제2 검증 동작에

의해 획득된 상기 제1 공개 키에 기초하여 상기 사이퍼링 키를 유도한다.

[0007] 상기 다른 목적을 달성하기 위해, 본 발명의 실시예들에 따른 복수의 사용자 ID(Identification)들에 의해 액세스되는 스토리지 장치에 포함되는 제1 저장 영역에 대한 접근 권한 이관 방법에서, 상기 제1 저장 영역에 대한 제1 접근 권한을 가지고 있는 제1 사용자 ID와 상기 제1 접근 권한을 획득하고자 하는 제2 사용자 ID 사이에 키 교환 동작을 수행한다. 상기 제1 사용자 ID에 의해 액세스된 상태에서, 상기 키 교환 동작에 의해 획득된 사이퍼링 키(ciphering key)에 기초하여 상기 제1 접근 권한에 대응하는 제1 KEK(Key-Encryption-Key)를 암호화하여 저장한다. 상기 제2 사용자 ID에 의해 액세스된 상태에서, 상기 사이퍼링 키에 기초하여 암호화된 상기 제1 KEK를 복호화하여 저장한다. 상기 키 교환 동작을 수행하는데 있어서, 상기 스토리지 장치에 포함되는 TTP(Trusted Third Party)에 의해, 상기 제1 사용자 ID 및 제1 공개 키(public key)에 기초하여 상기 제1 사용자 ID에 대한 제1 인증서를 생성한다. 상기 TTP에 의해, 상기 제2 사용자 ID 및 제2 공개 키에 기초하여 상기 제2 사용자 ID에 대한 제2 인증서를 생성한다. 상기 제1 사용자 ID에 의해 액세스된 상태에서, 상기 TTP에 포함되는 제3 인증서에 기초하여 상기 제2 인증서에 대한 제1 검증 동작을 수행한다. 상기 제1 검증 동작이 성공한 경우에, 제1 개인 키(private key) 및 상기 제1 검증 동작에 의해 획득된 상기 제2 공개 키에 기초하여 상기 사이퍼링 키를 유도한다. 상기 제2 사용자 ID에 의해 액세스된 상태에서, 상기 제3 인증서에 기초하여 상기 제1 인증서에 대한 제2 검증 동작을 수행한다. 상기 제2 검증 동작이 성공한 경우에, 제2 개인 키 및 상기 제2 검증 동작에 의해 획득된 상기 제1 공개 키에 기초하여 상기 사이퍼링 키를 유도한다.

발명의 효과

[0008] 상기와 같은 본 발명의 실시예들에 따른 스토리지 장치에서의 보안 동작을 위한 키 교환 방법에서는, 키 교환 동작을 안전하게 수행하기 위해 TTP가 이용될 수 있다. TTP에 의해 사용자 인증을 진행하기 위한 제1 인증서 및 제2 인증서를 생성할 수 있다. 제1 사용자는 제2 사용자의 공개 키를 기반으로 사이퍼링 키를 유도하는 것이 아니라, TTP가 서명하여 생성한 제2 사용자의 인증서를 기반으로 공개 키에 대한 인증을 수행하고 인증된 공개 키를 기반으로 사이퍼링 키를 유도할 수 있다. 따라서, 정당하지 않은 사용자와의 키 교환을 차단하고 정당한 사용자에 대해서만 키 교환을 수행함으로써, 보안 성능이 향상될 수 있다.

[0009] 본 발명의 실시예들에 따른 스토리지 장치에서의 접근 권한 이관 방법에서는, 상술한 키 교환 방법에 의해 제1 사용자 및 제2 사용자는 동일한 사이퍼링 키를 획득할 수 있으며, 사이퍼링 키를 이용하여 제1 저장 영역에 대한 제1 접근 권한에 대응하는 제1 KEK를 제2 사용자에게 안전하게 전달할 수 있다. 따라서, 보안 성능이 향상될 수 있다.

도면의 간단한 설명

[0010] 도 1은 본 발명의 실시예들에 따른 스토리지 장치에서의 보안 동작을 위한 키 교환 방법을 나타내는 순서도이다.

도 2는 본 발명의 실시예들에 따른 스토리지 장치에서의 보안 동작을 위한 키 교환 방법을 설명하기 위한 도면이다.

도 3은 본 발명의 실시예들에 따른 스토리지 장치 및 이를 포함하는 스토리지 시스템을 나타내는 블록도이다.

도 4는 본 발명의 실시예들에 따른 스토리지 장치에 포함되는 스토리지 컨트롤러의 일 예를 나타내는 블록도이다.

도 5는 본 발명의 실시예들에 따른 스토리지 장치에 포함되는 저장 영역의 구성을 나타내는 도면이다.

도 6은 도 1의 제1 인증서를 생성하는 단계의 일 예를 나타내는 순서도이다.

도 7은 도 1의 제2 인증서를 생성하는 단계의 일 예를 나타내는 순서도이다.

도 8a 및 8b는 도 6 및 7의 동작을 설명하기 위한 도면들이다.

도 9는 도 1의 제1 검증 동작을 수행하는 단계의 일 예를 나타내는 순서도이다.

도 10은 도 1의 제1 개인 키 및 제2 공개 키에 기초하여 사이퍼링 키를 유도하는 단계의 일 예를 나타내는 순서도이다.

도 11은 도 9 및 10의 동작을 설명하기 위한 도면이다.

도 12는 도 1의 제2 검증 동작을 수행하는 단계의 일 예를 나타내는 순서도이다.

도 13은 도 1의 제2 개인 키 및 제1 공개 키에 기초하여 사이퍼링 키를 유도하는 단계의 일 예를 나타내는 순서도이다.

도 14는 도 12 및 13의 동작을 설명하기 위한 도면이다.

도 15는 본 발명의 실시예들에 따른 스토리지 장치에서의 접근 권한 이관 방법을 나타내는 순서도이다.

도 16은 도 15의 제1 KEK를 암호화하여 저장하는 단계의 일 예를 나타내는 순서도이다.

도 17은 도 16의 동작을 설명하기 위한 도면이다.

도 18은 도 15의 암호화된 제1 KEK를 복호화하여 저장하는 단계의 일 예를 나타내는 순서도이다.

도 19는 도 18의 복호화된 제1 KEK를 저장하는 단계의 일 예를 나타내는 순서도이다.

도 20은 도 18 및 19의 동작을 설명하기 위한 도면이다.

도 21은 본 발명의 실시예들에 따른 스토리지 장치에서의 접근 권한 이관 방법을 나타내는 순서도이다.

도 22 및 23은 본 발명의 실시예들에 따른 스토리지 장치 및 이를 포함하는 스토리지 시스템을 나타내는 블록도들이다.

도 24는 본 발명의 실시예들에 따른 스토리지 시스템이 적용된 데이터 센터를 나타내는 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0011] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0012] 도 1은 본 발명의 실시예들에 따른 스토리지 장치에서의 보안 동작을 위한 키 교환 방법을 나타내는 순서도이다. 도 2는 본 발명의 실시예들에 따른 스토리지 장치에서의 보안 동작을 위한 키 교환 방법을 설명하기 위한 도면이다.

[0013] 도 1 및 2를 참조하면, 본 발명의 실시예들에 따른 보안 동작을 위한 키 교환 방법은, 복수의 사용자 ID(Identification)들에 의해 액세스되는 스토리지 장치에서 수행된다. 예를 들어, 상기 복수의 사용자 ID들은 제1 사용자 ID 및 제2 사용자 ID를 포함할 수 있다. 또한, 상기 스토리지 장치는 데이터를 저장하는 복수의 비휘발성 메모리들 및 상기 복수의 비휘발성 메모리들의 동작을 제어하는 스토리지 컨트롤러를 포함하며, 상기 키 교환 동작을 수행하는데 이용되는 TTP(Trusted Third Party)를 더 포함한다. 상기 스토리지 장치 및 이를 포함하는 스토리지 시스템의 구체적인 구조에 대해서는 도 3 등을 참조하여 후술하도록 한다.

[0014] 본 발명의 실시예들에 따른 스토리지 장치에서의 보안 동작을 위한 키 교환 방법에서, 제1 사용자에 대응하는 제1 사용자 ID(ID_{U1}) 및 제1 사용자 ID(ID_{U1})에 대한 제1 공개 키(public key)(PK_{U1})에 기초하여 제1 사용자 ID(ID_{U1})에 대한 제1 인증서($Cert_{U1}$)를 생성한다(단계 S100). 또한, 제2 사용자에 대응하는 제2 사용자 ID(ID_{U2}) 및 제2 사용자 ID(ID_{U2})에 대한 제2 공개 키(PK_{U2})에 기초하여 제2 사용자 ID(ID_{U2})에 대한 제2 인증서($Cert_{U2}$)를 생성한다(단계 S200). 단계 S100 및 S200에 대해서는 도 6 내지 8을 참조하여 후술하도록 한다.

[0015] 단계 S100 및 S200은 상기 스토리지 장치에 포함되는 상기 TTP에 의해 수행된다. 상기 TTP는 상기 키 교환 동작을 안전하게 수행하기 위해 이용되며, 특히 사용자 인증을 진행하기 위한 제1 인증서($Cert_{U1}$) 및 제2 인증서($Cert_{U2}$)를 생성함으로써 정당하지 않은 사용자와의 키 교환을 차단하는데 이용될 수 있다.

[0016] 일 실시예에서, 도 3에 도시된 것처럼 상기 TTP는 상기 스토리지 장치에 포함되는 상기 스토리지 컨트롤러에 포함될 수 있다. 다른 실시예에서, 도 22에 도시된 것처럼 상기 TTP는 상기 스토리지 컨트롤러의 외부에 배치되거나 도 23에 도시된 것처럼 상기 스토리지 장치의 외부에 배치될 수도 있다.

[0017] 제1 사용자 ID(ID_{U1})에 의해 상기 스토리지 장치가 액세스된 상태에서, 상기 TTP에 포함되는 제3 인증서에 기초하여 제2 인증서($Cert_{U2}$)에 대한 제1 검증 동작을 수행한다(단계 S300). 상기 제1 검증 동작이 성공한 경우에, 제1 사용자 ID(ID_{U1})에 대한 제1 개인 키(private key)(SK_{U1}) 및 상기 제1 검증 동작에 의해 획득된 제2 사용자

ID(ID_{U2})에 대한 제2 공개 키(PK_{U2})에 기초하여 사이퍼링 키(ciphering key)(CK)를 유도한다(단계 S400). 단계 S300 및 S400에 대해서는 도 9 내지 11을 참조하여 후술하도록 한다.

[0018] 상기 제3 인증서는 제1 인증서($Cert_{U1}$) 및 제2 인증서($Cert_{U2}$)와 다르며, 단계 S300에서와 같이 제2 인증서($Cert_{U2}$)가 상기 TTP에 의해 서명된 인증서인지 확인하는데 이용될 수 있다. 상기 제1 검증 동작에 의해 제2 사용자 ID(ID_{U2}) 및 이에 대응하는 상기 제2 사용자가 정당한 사용자인지 확인할 수 있다.

[0019] 제2 사용자 ID(ID_{U2})에 의해 상기 스토리지 장치가 액세스된 상태에서, 상기 제3 인증서에 기초하여 제1 인증서($Cert_{U1}$)에 대한 제2 검증 동작을 수행한다(단계 S500). 상기 제2 검증 동작이 성공한 경우에, 제2 사용자 ID(ID_{U2})에 대한 제2 개인 키(SK_{U2}) 및 상기 제2 검증 동작에 의해 획득된 제1 사용자 ID(ID_{U1})에 대한 제1 공개 키(PK_{U1})에 기초하여 사이퍼링 키(CK)를 유도한다(단계 S600). 단계 S500 및 S600에 대해서는 도 12 내지 14를 참조하여 후술하도록 한다.

[0020] 상기 제3 인증서는 단계 S500에서와 같이 제1 인증서($Cert_{U1}$)가 상기 TTP에 의해 서명된 인증서인지 확인하는데 이용될 수 있다. 상기 제2 검증 동작에 의해 제1 사용자 ID(ID_{U1}) 및 이에 대응하는 상기 제1 사용자가 정당한 사용자인지 확인할 수 있다.

[0021] 도 2에 도시된 것처럼, 동작 초기에 상기 제1 사용자(즉, 제1 사용자 ID(ID_{U1}))는 제1 개인 키(SK_{U1}) 및 제1 공개 키(PK_{U1})를 가지고 있으며, 상기 제2 사용자(즉, 제2 사용자 ID(ID_{U2}))는 제2 개인 키(SK_{U2}) 및 제2 공개 키(PK_{U2})를 가지고 있을 수 있다. 단계 S100 및 S200이 수행됨에 따라 제1 인증서($Cert_{U1}$) 및 제2 인증서($Cert_{U2}$)가 획득되고, 단계 S300 및 S400이 수행됨에 따라 상기 제1 사용자는 사이퍼링 키(CK)를 획득하며, 단계 S500 및 S600이 수행됨에 따라 상기 제2 사용자는 사이퍼링 키(CK)를 획득할 수 있다. 예를 들어, 제1 개인 키(SK_{U1}), 제1 공개 키(PK_{U1}), 제2 개인 키(SK_{U2}), 제2 공개 키(PK_{U2}), 제1 인증서($Cert_{U1}$) 및 제2 인증서($Cert_{U2}$)는 키 슬롯(key slot)에 저장될 수 있다.

[0022] 일 실시예에서, 상기 키 교환 동작에 의해 획득된 사이퍼링 키(CK)를 이용하여 상기 보안 동작이 수행될 수 있다. 예를 들어, 상기 보안 동작은 도 15 등을 참조하여 후술하는 특정 저장 영역에 대한 접근 권한을 이관하는 동작을 포함할 수 있다. 다만 본 발명은 이에 한정되지 않으며, 상기 보안 동작은 그 밖에 다양한 동작들 중 적어도 하나를 포함할 수 있다.

[0023] 일 실시예에서, 단계 S400에서 제1 개인 키(SK_{U1}) 및 제2 공개 키(PK_{U2})에 기초하여 유도된 사이퍼링 키(CK)와 단계 S600에서 제2 개인 키(SK_{U2}) 및 제1 공개 키(PK_{U1})에 기초하여 유도된 사이퍼링 키(CK)는 실질적으로 동일할 수 있다.

[0024] 일 실시예에서, 상기 키 교환 동작은 Diffie-Hellman(DH) 방식 및/또는 Elliptic Curve Diffie-Hellman(ECDH) 방식에 기초하여 수행될 수 있다. 예를 들어, 제1 개인 키(SK_{U1})는 "a"이고, 제1 공개 키(PK_{U1})는 "g^a mod p"이고, 제2 개인 키(SK_{U2})는 "b"이며, 제2 공개 키(PK_{U2})는 "g^b mod p"일 수 있다(p는 소수, g는 1 이상 (p-1) 이하의 정수, a 및 b는 각각 1 이상 (p-2) 이하의 정수이며, mod는 모듈러(modular 연산임). 이 경우, 제1 인증서($Cert_{U1}$)는 "ID_{U1} | PK_{U1} | Sign {SK_{TTP}, ID_{U1} | PK_{U1}}"이고, 제2 인증서($Cert_{U2}$)는 "ID_{U2} | PK_{U2} | Sign {SK_{TTP}, ID_{U2} | PK_{U2}}"이고, 단계 S400에서 유도된 사이퍼링 키(CK)는 "$(g^b)^a$ mod p"이고, 단계 S600에서 유도된 사이퍼링 키(CK)는 "$(g^a)^b$ mod p"이며, 단계 S400 및 S600에서 동일한 사이퍼링 키가 획득될 수 있다. 다만 본 발명은 이에 한정되지 않으며, 상기 키 교환 동작은 그 밖에 다양한 알고리즘들 중 적어도 하나에 기초하여 수행될 수 있다.

[0025] 한편, 도 2에서는 상기 제1 사용자(즉, 제1 사용자 ID(ID_{U1}))와 상기 제2 사용자(즉, 제2 사용자 ID(ID_{U2})) 사이에서 제1 인증서($Cert_{U1}$) 및 제2 인증서($Cert_{U2}$)가 서로 전송되는 것으로 도시하였으나, 이는 설명의 편의를 위한 것일 수 있다. 실제로 상기 스토리지 장치는 2 이상의 사용자들에 의해 동시에 액세스될 수는 없으며, 하나의 사용자(즉, 사용자 ID)에 의해서만 액세스될 수 있다. 상기 키 슬롯에 저장된 제1 개인 키(SK_{U1}), 제1 공개

키(PK_{U1}), 제2 개인 키(SK_{U2}) 및 제2 공개 키(PK_{U2})를 이용하여, 상기 제1 사용자에 의해 액세스된 상태에서(즉, 제1 사용자 ID(ID_{U1})를 이용하여 로그인된 상태에서) 단계 S100, S300 및 S400이 순차적으로 및/또는 한번에 수행될 수 있고, 상기 제2 사용자에 의해 액세스된 상태에서(즉, 제2 사용자 ID(ID_{U2})를 이용하여 로그인된 상태에서) 단계 S200, S500 및 S600이 순차적으로 및/또는 한번에 수행될 수 있다.

[0026] 한편, 어떤 실시예가 달리 구현 가능한 경우에 특정 블록 내에 명기된 기능 또는 동작이 순서도에 명기된 순서와 다르게 일어날 수도 있다. 예를 들어, 연속하는 두 블록이 실제로는 실질적으로 동시에 수행될 수도 있고, 관련된 기능 또는 동작에 따라서는 상기 블록들이 거꾸로 수행될 수도 있다.

[0027] 본 발명의 실시예들에 따른 스토리지 장치에서의 보안 동작을 위한 키 교환 방법에서, 상기 키 교환 동작을 안전하게 수행하기 위해 상기 TTP가 이용될 수 있다. 상기 TTP에 의해 사용자 인증을 진행하기 위한 제1 인증서($Cert_{U1}$) 및 제2 인증서($Cert_{U2}$)를 생성할 수 있다. 상기 제1 사용자(즉, 제1 사용자 ID(ID_{U1}))는 상기 제2 사용자(즉, 제2 사용자 ID(ID_{U2}))의 제2 공개 키(PK_{U2})를 기반으로 사이퍼링 키(CK)를 유도하는 것이 아니라, 상기 TTP가 서명하여 생성한 상기 제2 사용자의 제2 인증서($Cert_{U2}$)를 기반으로 제2 공개 키(PK_{U2})에 대한 인증을 수행하고 인증된 제2 공개 키(PK_{U2})를 기반으로 사이퍼링 키(CK)를 유도할 수 있다. 따라서, 정당하지 않은 사용자와의 키 교환을 차단하고 정당한 사용자에 대해서만 키 교환을 수행함으로써, 보안 성능이 향상될 수 있다.

[0028] 도 3은 본 발명의 실시예들에 따른 스토리지 장치 및 이를 포함하는 스토리지 시스템을 나타내는 블록도이다.

[0029] 도 3을 참조하면, 스토리지 시스템(100)은 호스트 장치(200) 및 스토리지 장치(300)를 포함한다.

[0030] 호스트 장치(200)는 스토리지 시스템(100)의 전반적인 동작을 제어한다. 예를 들어, 상세하게 도시하지는 않았으나, 호스트 장치(200)는 호스트 프로세서 및 호스트 메모리를 포함할 수 있다. 상기 호스트 프로세서는 호스트 장치(200)의 동작을 제어하고, 예를 들어 운영 체제(Operating System; OS)를 실행할 수 있다. 상기 호스트 메모리는 상기 호스트 프로세서에 의해 실행 및 처리되는 명령어(instruction) 및 데이터를 저장할 수 있다. 예를 들어, 상기 호스트 프로세서에 의해 실행되는 상기 운영 체제는 파일 관리를 위한 파일 시스템(file system), 및 스토리지 장치(300)를 포함하는 주변 기기를 상기 운영 체제 레벨에서 제어하기 위한 장치 드라이버(device driver)를 포함할 수 있다.

[0031] 스토리지 장치(300)는 호스트 장치(200)에 의해 액세스된다. 스토리지 장치(300)는 스토리지 컨트롤러(310), 복수의 비휘발성 메모리들(320a, 320b, 320c) 및 버퍼 메모리(330)를 포함한다.

[0032] 스토리지 컨트롤러(310)는 스토리지 장치(300)의 동작을 제어할 수 있다. 예를 들어, 스토리지 컨트롤러(310)는 호스트 장치(200)로부터 수신된 커맨드 및 데이터에 기초하여 복수의 비휘발성 메모리들(320a, 320b, 320c)의 동작을 제어할 수 있다. 스토리지 컨트롤러(310)는 TTP(312)를 포함한다. 도 1을 참조하여 상술한 것처럼, TTP(312)는 키 교환 동작을 안전하게 수행하기 위해 이용된다.

[0033] 복수의 비휘발성 메모리들(320a, 320b, 320c)은 복수의 데이터들을 저장할 수 있다. 예를 들어, 복수의 비휘발성 메모리들(320a, 320b, 320c)은 메타 데이터들 및 그 밖의 사용자 데이터들을 저장할 수 있다. 도 5를 참조하여 후술하는 것처럼, 복수의 비휘발성 메모리들(320a, 320b, 320c)은 복수의 저장 영역들로 구분될 수 있다.

[0034] 일 실시예에서, 복수의 비휘발성 메모리들(320a, 320b, 320c) 각각은 NAND 플래시 메모리(Flash Memory)를 포함할 수 있다. 다른 실시예에서, 복수의 비휘발성 메모리들(320a, 320b, 320c) 각각은 EEPROM(Electrically Erasable Programmable Read-Only Memory), PRAM(Phase Change Random Access Memory), RRAM(Resistance Random Access Memory), NFGM(Nano Floating Gate Memory), PoRAM(Polymer Random Access Memory), MRAM(Magnetic Random Access Memory), FRAM(Ferroelectric Random Access Memory) 또는 이와 유사한 메모리를 포함할 수 있다.

[0035] 버퍼 메모리(330)는 스토리지 컨트롤러(310)에 의해 실행 및 처리되는 명령어 및 데이터를 저장할 수 있고, 복수의 비휘발성 메모리들(320a, 320b, 320c)에 저장되어 있거나 저장하고자 하는 데이터를 임시로 저장할 수 있다. 예를 들어, 버퍼 메모리(330)는 DRAM(Dynamic Random Access Memory) 등과 같은 휘발성 메모리를 포함할 수 있다.

[0036] 도 1 및 2를 참조하여 상술한 것처럼, 스토리지 장치(300)는 호스트 장치(200)를 통해 복수의 사용자 ID들 중 하나에 의해 액세스될 수 있다. 예를 들어, 호스트 장치(200)를 통해 제1 사용자 ID(ID_{U1}) 및 이에 대응하는 제1

패스워드가 입력되는 경우에, 스토리지 장치(300)는 제1 사용자 ID(ID_{U1}) 및 이에 대응하는 상기 제1 사용자에 의해 액세스될 수 있다. 호스트 장치(200)를 통해 제2 사용자 ID(ID_{U2}) 및 이에 대응하는 제2 패스워드가 입력되는 경우에, 스토리지 장치(300)는 제2 사용자 ID(ID_{U2}) 및 이에 대응하는 상기 제2 사용자에 의해 액세스될 수 있다.

[0037] 스토리지 컨트롤러(310) 및 TTP(312)는 도 1 및 2를 참조하여 상술한 본 발명의 실시예들에 따른 키 교환 방법을 수행한다. 예를 들어, 스토리지 컨트롤러(310)는 보안 동작을 수행하기 위한 적어도 하나의 프로세서를 포함하며, 상기 프로세서 및 TTP(312)는 제1 인증서($Cert_{U1}$) 및 제2 인증서($Cert_{U2}$)를 생성한다. 제1 사용자 ID(ID_{U1})에 의해 액세스된 상태에서, 상기 프로세서는 TTP(312)의 인증서에 기초하여 제2 인증서($Cert_{U2}$)에 대한 제1 검증 동작을 수행하고, 상기 제1 검증 동작이 성공한 경우에 사이퍼링 키(CK)를 유도한다. 제2 사용자 ID(ID_{U2})에 의해 액세스된 상태에서, 상기 프로세서는 TTP(312)의 인증서에 기초하여 제1 인증서($Cert_{U1}$)에 대한 제2 검증 동작을 수행하고, 상기 제2 검증 동작이 성공한 경우에 사이퍼링 키(CK)를 유도한다. 또한, 스토리지 컨트롤러(310) 및 TTP(312)는 도 15 및 21을 참조하여 후술하는 본 발명의 실시예들에 따른 접근 권한 이관 방법을 수행할 수도 있다.

[0038] 일 실시예에서, 스토리지 장치(300)는 SSD(Solid State Drive)일 수 있다. 예를 들어, 스토리지 장치(300)는 SED(self-encrypting drive)의 형태로 구현될 수 있다. 다른 실시예에서, 스토리지 장치(300)는 UFS(Universal Flash Storage), MMC(Multi Media Card) 또는 eMMC(embedded MMC)일 수 있다. 또 다른 실시예에서, SD(Secure Digital) 카드, 마이크로 SD 카드, 메모리 스틱(memory stick), 칩 카드(chip card), USB(Universal Serial Bus) 카드, 스마트 카드(smart card), CF(Compact Flash) 카드 또는 이와 유사한 형태로 구현될 수 있다.

[0039] 일 실시예에서, 스토리지 장치(300)는 SATA(Serial Advanced Technology Attachment) 버스, SCSI(Small Computer Small Interface) 버스, NVMe(Non-Volatile Memory Express) 버스, SAS(Serial Attached SCSI) 버스, UFS, eMMC 등의 버스를 포함하는 블록 액세서블 인터페이스(block accessible interface)를 통해 호스트 장치(200)와 연결되고, 호스트 장치(200)에 의해 상기 블록 액세서블 인터페이스를 통하여 블록 단위로 액세스될 수 있다.

[0040] 일 실시예에서, 스토리지 시스템(100)은 PC(Personal Computer), 서버 컴퓨터(server computer), 데이터 센터(data center), 워크스테이션(workstation), 디지털 TV(digital television), 셋-탑 박스(set-top box) 등의 임의의 컴퓨팅 시스템일 수 있다. 다른 실시예에서, 스토리지 시스템(100)은 휴대폰(mobile phone), 스마트 폰(smart phone), 태블릿(tablet) PC(Personal Computer), 노트북(laptop computer), PDA(Personal Digital Assistant), PMP(Portable Multimedia Player), 디지털 카메라(digital camera), 캠코더(camcorder), 휴대용 게임 콘솔(portable game console), 음악 재생기(music player), 동영상 재생기(video player), 네비게이션(navigation) 기기, 웨어러블(wearable) 기기, IoT(Internet of Things) 기기, e-북(e-book), VR(Virtual Reality) 기기, AR(Augmented Reality) 기기, 드론(drone) 등의 임의의 모바일 시스템일 수 있다.

[0041] 도 4는 본 발명의 실시예들에 따른 스토리지 장치에 포함되는 스토리지 컨트롤러의 일 예를 나타내는 블록도이다.

[0042] 도 4를 참조하면, 스토리지 컨트롤러(400)는 제1 프로세서(410), 메모리(420), 제2 프로세서(430), 호스트 인터페이스(440), ECC(Error Correction Code) 블록(450) 및 메모리 인터페이스(460)를 포함할 수 있다.

[0043] 제1 프로세서(410) 및 제2 프로세서(430)는 호스트 장치(도 3의 200)로부터 호스트 인터페이스(440)를 통하여 수신된 커맨드에 응답하여 스토리지 컨트롤러(400)의 동작을 제어할 수 있다. 예를 들어, 제1 프로세서(410)는 스토리지 장치(도 3의 300)의 노멀 동작을 제어하며, 스토리지 장치(300)를 구동하기 위한 펌웨어(Firmware)를 채용하여 각각의 구성들을 제어할 수 있다. 예를 들어, 제2 프로세서(430)는 스토리지 장치(300)의 보안 동작을 제어하며, TTP(432)를 포함할 수 있다. 제2 프로세서(430) 및 TTP(432)는 도 3을 참조하여 상술한 스토리지 컨트롤러(310)에 포함되는 상기 프로세서 및 TTP(312)에 대응하는 구성일 수 있다.

[0044] 제2 프로세서(430)는 암호키(cryptographic key), 주요 데이터(sensitive data), 주요 코드 등의 보안 데이터를 처리 및/또는 저장할 수 있다.

[0045] 메모리(420)는 제1 프로세서(410) 및 제2 프로세서(430)에 의해 실행 및 처리되는 명령어 및 데이터를 저장할 수 있다. 예를 들어, 메모리(420)는 SRAM(Static Random Access Memory), 캐시(cache) 메모리 등과 같은 상대

적으로 작은 용량 및 빠른 속도를 가지는 휘발성 메모리로 구현될 수 있다.

[0046] 에러 정정을 위한 ECC 블록(450)은 BCH(Bose-Chaudhuri-Hocquenghem) 코드, LDPC(Low Density Parity Check) 코드, 터보 코드(Turbo Code), 리드-솔로몬 코드(Reed-Solomon Code), 콘볼루션 코드(Convolution Code), RSC(Recursive Systematic Code), TCM(Trellis-Coded Modulation), BCM(Block Coded Modulation) 등의 부호화된 변조(Coded Modulation), 또는 다른 에러 정정 코드를 이용하여 ECC 인코딩 및 ECC 디코딩을 수행할 수 있다.

[0047] 호스트 인터페이스(440)는 호스트 장치(200)와 스토리지 장치(300) 사이의 물리적 연결을 제공할 수 있다. 즉, 호스트 인터페이스(440)는 호스트 장치(200)의 버스 포맷(bus format)에 대응하여 스토리지 장치(300)와의 인터페이싱을 제공할 수 있다. 일 실시예에서, 호스트 장치(200)의 버스 포맷은 SCSI 또는 SAS일 수 있다. 다른 실시예에서, 호스트 장치(200)의 버스 포맷은 USB, PCIe(peripheral component interconnect express), ATA, PATA, SATA, NVMe 등일 수 있다.

[0048] 메모리 인터페이스(460)는 비휘발성 메모리들(도 3의 320a, 320b, 320c)과 데이터를 교환할 수 있다. 메모리 인터페이스(460)는 데이터를 비휘발성 메모리들(320a, 320b, 320c)에 전송할 수 있고, 비휘발성 메모리들(320a, 320b, 320c)로부터 독출된 데이터를 수신할 수 있다. 일 실시예에서, 메모리 인터페이스(460)는 비휘발성 메모리들(320a, 320b, 320c)과 하나의 채널을 통하여 연결될 수 있다. 다른 실시예에서, 메모리 인터페이스(460)는 비휘발성 메모리들(320a, 320b, 320c)과 2 이상의 채널들을 통하여 연결될 수 있다.

[0049] 도 5는 본 발명의 실시예들에 따른 스토리지 장치에 포함되는 저장 영역의 구성을 나타내는 도면이다.

[0050] 도 5를 참조하면, 저장 영역(500)은 키 슬롯(510), 사용자 전용 저장 영역(520) 및 복수의 저장 영역들(RANGE1, RANGE2, ..., RANGEM)(530a, 530b, 530c)을 포함할 수 있다.

[0051] 일 실시예에서, 저장 영역(500)은 스토리지 장치(도 3의 300)에 포함되는 비휘발성 메모리들(도 3의 320a, 320b, 320c)을 논리적으로 구분한 저장 공간을 나타낼 수 있다. 다만 본 발명은 이에 한정되지 않으며, 저장 영역(500)은 비휘발성 메모리들(320a, 320b, 320c)에 액세스하기 위해 이용되는 버퍼 메모리(도 3의 330)의 저장 공간 및/또는 스토리지 컨트롤러(도 4의 400)에 포함되는 프로세서(도 4의 410, 430)의 처리 공간을 포함하는 것으로 이해할 수 있을 것이다.

[0052] 키 슬롯(510)은 각각의 사용자 및 사용자 ID가 가지는 키들, 인증서들을 할당/저장하는 영역일 수 있다. 예를 들어, 스토리지 장치에 액세스할 수 있는 복수의 사용자 ID들은 제1 내지 제N(N은 2 이상의 자연수) 사용자 ID들을 포함하며, 키 슬롯(510)은 상기 제1 내지 제N 사용자 ID들에 대응하고 할당된 제1 내지 제N 키 슬롯 영역(key slot region, KSR)들(KSR1, KSR2, ..., KSRN)을 포함할 수 있다. 예를 들어, 제1 키 슬롯 영역(KSR1)은 상기 제1 사용자 ID에 대응하며, 상기 제1 사용자 ID에 할당될 수 있다.

[0053] 키 슬롯(510) 및 키 슬롯 영역들(KSR1, KSR2, ..., KSRN)은 모든 사용자들 및 사용자 ID들이 액세스할 수 있다. 이 때, 도 8 등을 참조하여 후술하는 것처럼 특정 키는 암호화 또는 랩핑된(wrapped) 상태로 저장되기 때문에, 암호화 또는 랩핑된 특정 키는 권한이 있는 특정 사용자만이 이용할 수 있다.

[0054] 사용자 전용 저장 영역(520)은 각각의 사용자 및 사용자 ID가 보안 동작 및/또는 연산을 수행하는데 이용되는 영역일 수 있다. 예를 들어, 사용자 전용 저장 영역(520)은 상기 제1 내지 제N 사용자 ID들에 대응하고 할당된 제1 내지 제N 사용자 저장 영역(user storage region, USR)들(USR1, USR2, ..., USRN)을 포함할 수 있다. 예를 들어, 제1 사용자 저장 영역(USR1)은 상기 제1 사용자 ID에 대응하며, 상기 제1 사용자 ID에 할당될 수 있다.

[0055] 사용자 저장 영역들(USR1, USR2, ..., USRN)은 특정 사용자 및 사용자 ID만이 액세스할 수 있다. 예를 들어, 제1 사용자 저장 영역(USR1)은 상기 제1 사용자 ID에 의해서만 액세스될 수 있다. 도시하지는 않았으나, 사용자 전용 저장 영역(520)은 모든 사용자들 및 사용자 ID들이 공통으로 액세스할 수 있는 영역을 더 포함할 수 있다.

[0056] 복수의 저장 영역들(530a, 530b, 530c)은 데이터(예를 들어, 일반 데이터, 보안 데이터 등)를 저장하는 영역일 수 있다. 복수의 저장 영역들(530a, 530b, 530c)은 레인지(range), 파티션(partition) 등으로 부를 수 있다.

[0057] 복수의 저장 영역들(530a, 530b, 530c)은 접근 권한이 있는 사용자 및 사용자 ID만이 액세스할 수 있다. 예를 들어, 상기 제1 사용자 ID는 제1 저장 영역(530a)에 대한 제1 접근 권한을 가지고 있고 상기 제2 사용자 ID는 상기 제1 접근 권한을 가지고 있지 않은 경우에, 제1 저장 영역(530a)은 상기 제1 사용자 ID에 의해서는 액세스되고 상기 제2 사용자 ID에 의해서는 액세스되지 않을 수 있다. 도 15 등을 참조하여 후술하는 것처럼, 상기 제

1 접근 권한은 상기 제2 사용자 ID로 이관될 수도 있다.

[0058] 이하에서는 Diffie-Hellman 방식에 기초하여 본 발명의 실시예들을 상세하게 설명하도록 한다. 다만 본 발명은 이에 한정되지 않으며, 그 밖에 다양한 알고리즘들 중 적어도 하나를 이용할 수도 있다.

[0059] 도 6은 도 1의 제1 인증서를 생성하는 단계의 일 예를 나타내는 순서도이다. 도 7은 도 1의 제2 인증서를 생성하는 단계의 일 예를 나타내는 순서도이다. 도 8a 및 8b는 도 6 및 7의 동작을 설명하기 위한 도면들이다.

[0060] 도 8a 및 8b에 도시된 것처럼, 상기 제1 사용자 및 제1 사용자 ID(ID_{U1})는 제1 개인 키($WDHSK_{U1}$) 및 제1 공개 키($DHPK_{U1}$)를 가지고 있고, 상기 제2 사용자 및 제2 사용자 ID(ID_{U2})는 제2 개인 키($WDHSK_{U2}$) 및 제2 공개 키($DHPK_{U2}$)를 가지고 있으며, TTP(610)는 제3 개인 키(SK_{TTP}), 제3 공개 키(PK_{TTP}) 및 제3 인증서($Cert_{TTP}$)를 가지고 있을 수 있다. 동작 초기에, 제1 개인 키($WDHSK_{U1}$) 및 제1 공개 키($DHPK_{U1}$)는 제1 사용자 ID(ID_{U1})에 할당된 제1 키 슬롯 영역(KSR1)에 저장되어 있고, 제2 개인 키($WDHSK_{U2}$) 및 제2 공개 키($DHPK_{U2}$)는 제2 사용자 ID(ID_{U2})에 할당된 제2 키 슬롯 영역(KSR2)에 저장되어 있으며, 제3 개인 키(SK_{TTP}), 제3 공개 키(PK_{TTP}) 및 제3 인증서($Cert_{TTP}$)는 TTP(610) 내에 저장되어 있을 수 있다. 상세하게 도시하지는 않았으나, 제3 공개 키(PK_{TTP})를 포함하는 제3 인증서($Cert_{TTP}$)를 생성하는 동작이 미리 수행될 수 있다.

[0061] 도 1, 6 및 8a를 참조하면, 제1 인증서($DHCert_{U1}$)를 생성하는데 있어서(단계 S100), TTP(610)에 포함되는 제3 개인 키(SK_{TTP})를 기초로 제1 사용자 ID(ID_{U1}) 및 제1 사용자 ID(ID_{U1})에 대한 제1 공개 키($DHPK_{U1}$)를 서명하여 제1 인증서($DHCert_{U1}$)를 획득할 수 있다(단계 S110). 예를 들어, 제1 사용자 ID(ID_{U1}) 및 제1 공개 키($DHPK_{U1}$)에 대한 전자 서명을 생성하여 제1 인증서($DHCert_{U1}$)를 생성할 수 있다. 예를 들어, 제1 인증서($DHCert_{U1}$)는 "ID_{U1} | $DHPK_{U1}$ | Sign {SK_{TTP}, ID_{U1} | $DHPK_{U1}$}"일 수 있다. 도 8a의 인증서 생성 동작(CERT_GEN)(620)이 도 6의 단계 S110에 대응할 수 있다.

[0062] 제1 인증서($DHCert_{U1}$)를 제1 키 슬롯 영역(KSR1)에 저장할 수 있다(단계 S120). 이 때, 제3 인증서($Cert_{TTP}$) 또한 제1 키 슬롯 영역(KSR1)에 저장될 수 있다. 이에 따라, 단계 S100이 완료되면 제1 키 슬롯 영역(KSR1)에는 제1 개인 키($WDHSK_{U1}$), 제1 공개 키($DHPK_{U1}$) 및 제3 인증서($Cert_{TTP}$)가 제1 인증서($DHCert_{U1}$)와 함께 저장될 수 있다.

[0063] 도 1, 7 및 8b를 참조하면, 제2 인증서($DHCert_{U2}$)를 생성하는데 있어서(단계 S200), TTP(610)에 포함되는 제3 개인 키(SK_{TTP})를 기초로 제2 사용자 ID(ID_{U2}) 및 제2 사용자 ID(ID_{U2})에 대한 제2 공개 키($DHPK_{U2}$)를 서명하여 제2 인증서($DHCert_{U2}$)를 획득할 수 있다(단계 S210). 단계 S210은 도 6의 단계 S110과 유사할 수 있다. 도 8b의 인증서 생성 동작(CERT_GEN)(630)이 도 7의 단계 S120에 대응할 수 있다.

[0064] 제2 인증서($DHCert_{U2}$)를 제2 키 슬롯 영역(KSR2)에 저장할 수 있다(단계 S220). 단계 S220은 도 6의 단계 S120과 유사할 수 있다. 단계 S200이 완료되면 제2 키 슬롯 영역(KSR2)에는 제2 개인 키($WDHSK_{U2}$), 제1 공개 키($DHPK_{U2}$) 및 제3 인증서($Cert_{TTP}$)가 제2 인증서($DHCert_{U2}$)와 함께 저장될 수 있다.

[0065] 일 실시예에서, 제1 개인 키($WDHSK_{U1}$) 및 제2 개인 키($WDHSK_{U2}$)는 랩핑된 키일 수 있다. 이에 따라, 제1 사용자 ID(ID_{U1}) 및 제2 사용자 ID(ID_{U2})를 포함하는 복수의 사용자 ID들이 모두 제1 개인 키($WDHSK_{U1}$) 및 제2 개인 키($WDHSK_{U2}$)에 액세스할 수 있다고 하더라도, 제1 개인 키($WDHSK_{U1}$)에 랩핑 해제 권한이 있는 제1 사용자 ID(ID_{U1})만이 제1 개인 키($WDHSK_{U1}$)를 이용할 수 있고, 제2 개인 키($WDHSK_{U2}$)에 랩핑 해제 권한이 있는 제2 사용자 ID(ID_{U2})만이 제2 개인 키($WDHSK_{U2}$)를 이용할 수 있다.

[0066] 일 실시예에서, 상술한 인증서 생성 동작 및 생성된 인증서를 키 슬롯에 저장하는 동작은 모든 사용자 계정에 동일하게 진행될 수 있다.

[0067] 도 9는 도 1의 제1 검증 동작을 수행하는 단계의 일 예를 나타내는 순서도이다. 도 10은 도 1의 제1 개인 키 및 제2 공개 키에 기초하여 사이퍼링 키를 유도하는 단계의 일 예를 나타내는 순서도이다. 도 11은 도 9 및 10의

동작을 설명하기 위한 도면이다.

[0068] 도 1, 9 및 11을 참조하면, 제1 사용자 ID(ID_{U1})에 의해 액세스된 상태에서 상기 제1 검증 동작을 수행하는데 있어서(단계 S300), 먼저 제1 사용자 ID(ID_{U1}) 및 이에 대응하는 제1 패스워드(PWD_{U1})를 이용하여 로그인할 수 있고, 제2 키 슬롯 영역(KSR2)에 저장된 제2 인증서($DHCert_{U2}$)를 불러올 수 있다.

[0069] 이후에 제3 인증서($Cert_{TTP}$)에 기초하여 TTP(610)에 포함되는 제3 공개 키(PK_{TTP})를 추출할 수 있고(단계 S310), 제3 공개 키(PK_{TTP})에 기초하여 제2 인증서($DHCert_{U2}$)에 대한 서명을 검증할 수 있다(단계 S320). 도 11의 인증서 검증 동작(VERT_VFY)(710)이 도 9의 단계 S310 및 S320에 대응할 수 있다.

[0070] 제2 인증서($DHCert_{U2}$)에 대한 서명 검증이 성공한 경우에(단계 S330: 예), 제2 인증서($DHCert_{U2}$)에 포함되는 제2 사용자 ID(ID_{U2}) 및 제2 공개 키($DHPK_{U2}$)를 추출할 수 있고(단계 S340), 이에 기초하여 제2 사용자 ID(ID_{U2})에 대응하는 상기 제2 사용자가 정당한 사용자임을 확인할 수 있다.

[0071] 제2 인증서($DHCert_{U2}$)에 대한 서명 검증이 실패한 경우에(단계 S330: 아니오), 제2 사용자 ID(ID_{U2})에 대응하는 상기 제2 사용자가 정당하지 않은 사용자인 것으로 판단하여 프로세스가 종료될 수 있다.

[0072] 도 1, 10 및 11을 참조하면, 상기 제1 검증 동작이 성공한 경우에 제1 개인 키($WDHSK_{U1}$) 및 제2 공개 키($DHPK_{U2}$)에 기초하여 사이퍼링 키(CK_{U1U2})를 유도하는데 있어서(단계 S400), 제1 사용자 ID(ID_{U1})에 대응하는 제1 패스워드(PWD_{U1}) 및 랜덤 값(Salt1)에 기초하여 제1 KPK(Key-Protection-Key)(KPK_{U1})를 획득할 수 있다(단계 S410). 예를 들어, 도 11에 도시된 것처럼 KDF(Key Derivation Function)(720)를 이용하여 제1 KPK(KPK_{U1})를 도출할 수 있다. 단계 S410은 제1 사용자 ID(ID_{U1}) 및 제1 패스워드(PWD_{U1})를 이용한 로그인 시에 수행될 수 있다.

[0073] 제1 KPK(KPK_{U1})에 기초하여 랩핑 해제된 제1 개인 키($DHSK_{U1}$)를 획득할 수 있다(단계 S420). 예를 들어, 도 11에 도시된 것처럼 제1 KPK(KPK_{U1})를 기초로 랩핑된 제1 개인 키($WDHSK_{U1}$)에 대한 복호화 동작(DEC)(730)을 수행하여 랩핑 해제된 제1 개인 키($DHSK_{U1}$)를 생성할 수 있다. 예를 들어, 복호화 동작(730)은 AES(Advanced Encryption Standard) 알고리즘에 기초하여 수행될 수 있다.

[0074] 제1 사용자 ID(ID_{U1})에 대한 제1 개인 키($DHSK_{U1}$) 및 상기 제1 검증 동작에 의해 획득된 제2 사용자 ID(ID_{U2})에 대한 제2 공개 키($DHPK_{U2}$)를 기초로 키 합의(key agreement)를 수행하여 사이퍼링 키(CK_{U1U2})를 획득할 수 있다(단계 S430). 도 11의 키 합의 동작(KEY_AGR)(740)이 도 10의 단계 S430에 대응할 수 있다.

[0075] 일 실시예에서, 상기 제1 검증 동작, 및 제1 개인 키($DHSK_{U1}$) 및 제2 공개 키($DHPK_{U2}$)에 기초하여 사이퍼링 키(CK_{U1U2})를 유도하는 동작은 제1 사용자 ID(ID_{U1})에 의해서만 액세스되는 제1 사용자 저장 영역(USR1)을 이용하여 수행될 수 있다.

[0076] 도 12는 도 1의 제2 검증 동작을 수행하는 단계의 일 예를 나타내는 순서도이다. 도 13은 도 1의 제2 개인 키 및 제1 공개 키에 기초하여 사이퍼링 키를 유도하는 단계의 일 예를 나타내는 순서도이다. 도 14는 도 12 및 13의 동작을 설명하기 위한 도면이다. 이하 도 9, 10 및 11과 중복되는 설명은 생략한다.

[0077] 도 1, 12 및 14를 참조하면, 제2 사용자 ID(ID_{U2})에 의해 액세스된 상태에서 상기 제2 검증 동작을 수행하는데 있어서(단계 S300), 먼저 제2 사용자 ID(ID_{U2}) 및 이에 대응하는 제2 패스워드(PWD_{U2})를 이용하여 로그인할 수 있고, 제1 키 슬롯 영역(KSR1)에 저장된 제1 인증서($DHCert_{U1}$)를 불러올 수 있다.

[0078] 이후에 제3 인증서($Cert_{TTP}$)에 기초하여 TTP(610)에 포함되는 제3 공개 키(PK_{TTP})를 추출할 수 있고(단계 S510), 제3 공개 키(PK_{TTP})에 기초하여 제1 인증서($DHCert_{U1}$)에 대한 서명을 검증할 수 있다(단계 S520). 단계 S510 및 S520은 도 9의 단계 S310 및 S320과 유사할 수 있고, 도 14의 인증서 검증 동작(VERT_VFY)(810)이 도 12의 단계 S510 및 S520에 대응할 수 있다.

[0079] 제1 인증서($DHCert_{U1}$)에 대한 서명 검증이 성공한 경우에(단계 S530: 예), 제1 인증서($DHCert_{U1}$)에 포함되는 제1

사용자 ID(ID_{U1}) 및 제1 공개 키($DHPK_{U1}$)를 추출할 수 있다(단계 S540). 제1 인증서($DHCert_{U1}$)에 대한 서명 검증이 실패한 경우에(단계 S530: 아니오), 프로세스가 종료될 수 있다. 단계 S530 및 S540은 도 9의 단계 S330 및 S340과 유사할 수 있다.

[0080] 도 1, 13 및 14를 참조하면, 상기 제2 검증 동작이 성공한 경우에 제2 개인 키($WDHSK_{U2}$) 및 제1 공개 키($DHPK_{U1}$)에 기초하여 사이퍼링 키(CK_{U1U2})를 유도하는데 있어서(단계 S600), 제2 사용자 ID(ID_{U2})에 대응하는 제2 패스워드(PWD_{U2}) 및 랜덤 값(Salt1)에 기초하여 제2 KPK(KPK_{U2})를 획득할 수 있다(단계 S610). 단계 S610은 도 10의 단계 S410과 유사할 수 있다. 도 14의 KDF(820)를 이용하는 동작이 도 13의 단계 S610에 대응할 수 있다.

[0081] 제2 KPK(KPK_{U2})에 기초하여 랩핑 해제된 제2 개인 키($DHSK_{U2}$)를 획득할 수 있다(단계 S620). 단계 S620은 도 10의 단계 S420과 유사할 수 있다. 도 14의 복호화 동작(DEC)(830)이 도 13의 단계 S620에 대응할 수 있다.

[0082] 제2 사용자 ID(ID_{U2})에 대한 제2 개인 키($DHSK_{U2}$) 및 상기 제2 검증 동작에 의해 획득된 제1 사용자 ID(ID_{U1})에 대한 제1 공개 키($DHPK_{U1}$)를 기초로 키 합의를 수행하여 사이퍼링 키(CK_{U1U2})를 획득할 수 있다(단계 S630). 단계 S630은 도 10의 단계 S430과 유사할 수 있다. 도 14의 키 합의 동작(KEY_AGR)(840)이 도 13의 단계 S630에 대응할 수 있다.

[0083] 일 실시예에서, 상기 제2 검증 동작, 및 제2 개인 키($DHSK_{U2}$) 및 제1 공개 키($DHPK_{U1}$)에 기초하여 사이퍼링 키(CK_{U1U2})를 유도하는 동작은 제2 사용자 ID(ID_{U2})에 의해서만 액세스되는 제2 사용자 저장 영역(USR2)을 이용하여 수행될 수 있다.

[0084] 상술한 과정에 의해 제1 사용자 ID(ID_{U1}) 및 제2 사용자 ID(ID_{U2})는 동일한 사이퍼링 키(CK_{U1U2})를 획득할 수 있다. 제1 사용자 ID(ID_{U1})는 제2 사용자 ID(ID_{U2})의 인증된 제2 공개 키($DHPK_{U2}$) 기반으로 사이퍼링 키(CK_{U1U2})를 유도하며, 제2 개인 키($DHSK_{U2}$)를 소유한 제2 사용자 ID(ID_{U2})만이 동일한 사이퍼링 키(CK_{U1U2})를 유도할 수 있다.

[0085] 도 15는 본 발명의 실시예들에 따른 스토리지 장치에서의 접근 권한 이관 방법을 나타내는 순서도이다. 이하 도 1과 중복되는 설명은 생략한다.

[0086] 도 15를 참조하면, 본 발명의 실시예들에 따른 스토리지 장치에서의 접근 권한 이관 방법에서, 제1 사용자 ID와 제2 사용자 ID 사이에 키 교환 동작을 수행한다(단계 S1100). 상기 제1 사용자 ID는 상기 스토리지 장치에 포함되는 제1 저장 영역에 대한 제1 접근 권한을 가지고 있는 사용자에 대응하며, 상기 제2 사용자 ID는 상기 제1 접근 권한을 획득하고자 하는 사용자에 대응한다.

[0087] 단계 S1100은 도 1 내지 14를 참조하여 상술한 본 발명의 실시예들에 따른 키 교환 방법에 기초하여 수행될 수 있다. 상기 키 교환 동작을 안전하게 수행하기 위해 상기 TTP가 이용되며, 각 사용자 ID는 상기 TTP가 서명하여 생성한 인증서를 기반으로 공개 키에 대한 인증을 수행하고 인증된 공개 키를 기반으로 사이퍼링 키를 유도함으로써, 정당하지 않은 사용자와의 키 교환을 차단하고 정당한 사용자에 대해서만 키 교환을 수행할 수 있다. 상기 키 교환 동작이 성공적으로 완료되는 경우에 상기 제1 사용자 ID 및 상기 제2 사용자 ID는 동일한 사이퍼링 키를 획득할 수 있다.

[0088] 상기 제1 사용자 ID에 의해 액세스된 상태에서, 상기 키 교환 동작에 의해 획득된 상기 사이퍼링 키에 기초하여 상기 제1 접근 권한에 대응하는 제1 KEK(Key-Encryption-Key)를 암호화하여 저장한다(단계 S1200). 상기 제1 KEK는 상기 제1 저장 영역에 액세스하기 위해 필요한 키일 수 있다. 상기 제1 사용자 ID는 상기 제1 접근 권한 및 이에 대응하는 상기 제1 KEK를 이미 가지고 있는 상태이며, 단계 S1200은 상기 제1 KEK를 상기 제2 사용자 ID에 전달하기 위한 동작일 수 있다. 단계 S1200에 대해서는 도 16 및 17을 참조하여 후술하도록 한다.

[0089] 상기 제2 사용자 ID에 의해 액세스된 상태에서, 상기 사이퍼링 키에 기초하여 암호화된 상기 제1 KEK를 복호화하여 저장한다(단계 S1300). 예를 들어, 상기 제1 KEK는 상기 제2 사용자 ID에 할당된 제2 키 슬롯 영역에 저장될 수 있다. 단계 S1300이 수행됨에 따라 상기 제2 사용자 ID는 상기 제1 KEK를 가지게 될 수 있다. 단계 S1300에 대해서는 도 18 내지 20을 참조하여 후술하도록 한다.

[0090] 상술한 것처럼, 상기 제1 사용자 ID 및 상기 제2 사용자 ID가 모두 상기 제1 KEK를 소유함에 따라, 상기 제1 사용자 ID 및 상기 제2 사용자 ID 모두는 상기 제1 저장 영역에 대한 상기 제1 접근 권한을 가지게 될 수 있다.

[0091] 본 발명의 실시예들에 따른 스토리지 장치에서의 접근 권한 이관 방법에서, 상기 TTP를 이용하여 정당한 사용자에 대해서만 키 교환을 수행할 수 있고, 키 교환이 수행됨에 따라 상기 제1 사용자 ID 및 상기 제2 사용자 ID는 동일한 사이퍼링 키를 획득할 수 있으며, 상기 사이퍼링 키를 이용하여 상기 제1 저장 영역에 대한 상기 제1 접근 권한에 대응하는 상기 제1 KEK를 상기 제2 사용자 ID에게 안전하게 전달할 수 있다. 따라서, 보안 성능이 향상될 수 있다.

[0092] 도 16은 도 15의 제1 KEK를 암호화하여 저장하는 단계의 일 예를 나타내는 순서도이다. 도 17은 도 16의 동작을 설명하기 위한 도면이다.

[0093] 도 15, 16 및 17을 참조하면, 제1 사용자 ID(ID_{U1})에 의해 액세스된 상태에서 제1 KEK(KEK_{R1})를 암호화하여 저장하는데 있어서(단계 S1200), 제1 사용자 ID(ID_{U1})에 대응하는 제1 패스워드(PWD_{U1}) 및 랜덤 값(Salt1)에 기초하여 제1 KPK(KPK_{U1})를 획득할 수 있다(단계 S1210). 단계 S1210은 도 10의 단계 S410과 실질적으로 동일하며, 도 17의 KDF(910)를 이용하는 동작이 도 16의 단계 S1210에 대응할 수 있다. 단계 S410이 이미 수행된 경우에 단계 S1210은 생략될 수 있다.

[0094] 제1 KPK(KPK_{U1})에 기초하여 제1 KEK(KEK_{R1})를 획득할 수 있다(단계 S1220). 예를 들어, 상세하게 도시하지는 않았으나, 제1 사용자 ID(ID_{U1})는 제1 KPK(KPK_{U1})를 기초로 제1 KEK(KEK_{R1})를 암호화(또는 랩핑)하여 암호화된 제1 KEK($WKEK_{R1}$)를 제1 키 슬롯 영역(KSR1)에 저장하는 방식으로 제1 KEK(KEK_{R1})를 소유하고 있을 수 있다. 예를 들어, 암호화된 제1 KEK($WKEK_{R1}$)를 불러온 이후에, 도 17에 도시된 것처럼 복호화 동작(DEC)(920)을 수행하여 제1 KEK(KEK_{R1})를 생성할 수 있다. 예를 들어, 복호화 동작(920)은 AES 알고리즘에 기초하여 수행될 수 있다.

[0095] 사이퍼링 키(CK_{U1U2})에 기초하여 제1 KEK(KEK_{R1})를 암호화할 수 있고(단계 S1230), 암호화된 제1 KEK($WKEK_{R1}'$)를 저장할 수 있다(단계 S1240). 예를 들어, 도 17에 도시된 것처럼 암호화 동작(ENC)(930)을 수행하여 암호화된 제1 KEK($WKEK_{R1}'$)를 생성할 수 있다. 예를 들어, 암호화 동작(930)은 AES 알고리즘에 기초하여 수행될 수 있다. 예를 들어, 암호화된 제1 KEK($WKEK_{R1}'$)는 제2 사용자 ID(ID_{U2})에 의해 액세스 가능한 영역에 저장될 수 있다. 예를 들어, 암호화된 제1 KEK($WKEK_{R1}'$)는 암호화된 제1 KEK($WKEK_{R1}$)와 다를 수 있다.

[0096] 한편, 도 17에 도시된 것처럼, 제1 사용자 ID(ID_{U1})는 상기 제1 저장 영역에 액세스할 수 있다. 구체적으로, 제1 사용자 ID(ID_{U1})가 상기 제1 저장 영역에 액세스하고자 하는 경우에, 제1 KPK(KPK_{U1})를 기초로 복호화 동작(920)을 수행하여 제1 KEK(KEK_{R1})를 획득한 이후에, 상기 제1 저장 영역에 저장된 암호화된 제1 MEK(Media-Encryption-Key)($WMEK_{R1}$) 및 암호화된 제1 데이터(E_DATA_{R1})를 불러오고, 제1 KEK(KEK_{R1})를 기초로 복호화 동작(DEC)(1010)을 수행하여 제1 MEK(MEK_{R1})를 획득하며, 제1 MEK(MEK_{R1})를 기초로 복호화 동작(DEC)(1020)을 수행하여 제1 데이터($DATA_{R1}$)를 획득할 수 있다. 예를 들어, 복호화 동작들(1010, 1020)은 AES 알고리즘에 기초하여 수행될 수 있다.

[0097] 일 실시예에서, 단계 S1210, S1220, S1230 및 S1240의 동작들은 제1 사용자 ID(ID_{U1})에 의해서만 액세스되는 제1 사용자 저장 영역(USR1)을 이용하여 수행될 수 있다.

[0098] 도 18은 도 15의 암호화된 제1 KEK를 복호화하여 저장하는 단계의 일 예를 나타내는 순서도이다. 도 19는 도 18의 복호화된 제1 KEK를 저장하는 단계의 일 예를 나타내는 순서도이다. 도 20은 도 18 및 19의 동작을 설명하기 위한 도면이다.

[0099] 도 15, 18, 19 및 20을 참조하면, 제2 사용자 ID(ID_{U2})에 의해 액세스된 상태에서 암호화된 제1 KEK($WKEK_{R1}'$)를 복호화하여 저장하는데 있어서(단계 S1300), 사이퍼링 키(CK_{U1U2})에 기초하여 암호화된 제1 KEK($WKEK_{R1}'$)를 복호화할 수 있다(단계 S1310). 예를 들어, 도 20에 도시된 것처럼 복호화 동작(DEC)(1110)을 수행하여 제1 KEK(KEK_{R1})를 생성할 수 있다. 제1 사용자 ID(ID_{U1}) 및 제2 사용자 ID(ID_{U2})는 동일한 사이퍼링 키(CK_{U1U2})를 가지므로, 제2 사용자 ID(ID_{U2})에 의해 획득된 제1 KEK(KEK_{R1})는 제1 사용자 ID(ID_{U1})가 전달한 제1 KEK(KEK_{R1})와 동일할 수 있다.

[0100] 복호화된 제1 KEK(KEK_{R1})를 저장할 수 있다(단계 S1320). 구체적으로, 먼저 제2 사용자 ID(ID_{U2})에 대응하는 제2 패스워드(PWD_{U2}) 및 랜덤 값(Salt1)에 기초하여 제2 KPK(KPK_{U2})를 획득할 수 있다(단계 S1322). 단계 S1322는 도 13의 단계 S610과 실질적으로 동일하며, 도 20의 KDF(1120)를 이용하는 동작이 도 19의 단계 S1322에 대응할 수 있다. 단계 S610이 이미 수행된 경우에 단계 S1322는 생략될 수 있다.

[0101] 제2 KPK(KPK_{U2})에 기초하여 복호화된 제1 KEK(KEK_{R1})를 다시 암호화할 수 있다(단계 S1324). 예를 들어, 도 20에 도시된 것처럼 암호화 동작(ENC)(1130)을 수행하여 암호화된 제1 KEK($WKEK_{R1}$")를 생성할 수 있다. 예를 들어, 암호화 동작(1130)은 AES 알고리즘에 기초하여 수행될 수 있다. 예를 들어, 암호화된 제1 KEK($WKEK_{R1}$")는 암호화된 제1 KEK($WKEK_{R1}$') 및 암호화된 제1 KEK($WKEK_{R1}$)와 다를 수 있다.

[0102] 암호화된 제1 KEK($WKEK_{R1}$")를 저장할 수 있다(단계 S1326). 예를 들어, 상세하게 도시하지는 않았으나, 제2 사용자 ID(ID_{U2})는 암호화된 제1 KEK($WKEK_{R1}$")를 제2 키 슬롯 영역(KSR2)에 저장하는 방식으로 제1 KEK(KEK_{R1})를 소유할 수 있다.

[0103] 한편, 도 20에 도시된 것처럼, 제2 사용자 ID(ID_{U2})는 제1 KEK(KEK_{R1})를 소유하게 된 이후에 상기 제1 저장 영역에 액세스할 수 있다. 구체적으로, 제2 사용자 ID(ID_{U2})가 상기 제1 저장 영역에 액세스하고자 하는 경우에, 제2 KPK(KPK_{U2})를 기초로 복호화 동작(DEC)(1210)을 수행하여 제1 KEK(KEK_{R1})를 획득하고, 상기 제1 저장 영역에 저장된 암호화된 제1 MEK($WMEK_{R1}$) 및 암호화된 제1 데이터(E_DATA_{R1})를 불러오고, 제1 KEK(KEK_{R1})를 기초로 복호화 동작(DEC)(1220)을 수행하여 제1 MEK(MEK_{R1})를 획득하며, 제1 MEK(MEK_{R1})를 기초로 복호화 동작(DEC)(1230)을 수행하여 제1 데이터($DATA_{R1}$)를 획득할 수 있다. 예를 들어, 복호화 동작들(1210, 1220, 1230)은 AES 알고리즘에 기초하여 수행될 수 있다.

[0104] 도 21은 본 발명의 실시예들에 따른 스토리지 장치에서의 접근 권한 이관 방법을 나타내는 순서도이다. 이하 도 15와 중복되는 설명은 생략한다.

[0105] 도 21을 참조하면, 본 발명의 실시예들에 따른 스토리지 장치에서의 접근 권한 이관 방법에서, 단계 S1100, S1200 및 S1300은 도 15의 단계 S1100, S1200 및 S1300과 실질적으로 동일할 수 있다.

[0106] 상기 제1 사용자 ID 및 상기 제2 사용자 ID 모두가 상기 제1 접근 권한을 가지게 된 이후에, 상기 제1 사용자 ID 및 상기 제2 사용자 ID 중 적어도 하나는 상기 제1 저장 영역에 액세스할 수 있다.

[0107] 예를 들어, 상기 제1 사용자 ID에 의해 액세스된 상태에서, 상기 제1 KEK를 획득하고(단계 S2100), 상기 제1 KEK에 기초하여 제1 MEK를 획득하며(단계 S2200), 상기 제1 MEK에 기초하여 상기 제1 저장 영역에 저장된 제1 데이터를 획득할 수 있다(단계 S2300). 이 경우, 단계 S2100, S2200 및 S2300은 도 17의 복호화 동작들(920, 1010, 1020)에 대응할 수 있다.

[0108] 다른 예에서, 상기 제2 사용자 ID에 의해 액세스된 상태에서, 단계 S2100, S2200 및 S2300이 수행될 수 있다. 이 경우, 단계 S2100, S2200 및 S2300은 도 20의 복호화 동작들(1210, 1220, 1230)에 대응할 수 있다.

[0109] 한편, 도 21의 스토리지 장치에서의 접근 권한 이관 방법은 스토리지 장치의 구동 방법으로 설명될 수도 있다.

[0110] 한편, 본 발명의 실시예들은 컴퓨터로 판독 가능한 매체에 저장된 컴퓨터로 판독 가능한 프로그램 코드를 포함하는 제품 등의 형태로 구현될 수도 있다. 상기 컴퓨터로 판독 가능한 프로그램 코드는 다양한 컴퓨터 또는 다른 데이터 처리 장치의 프로세서로 제공될 수 있다. 상기 컴퓨터로 판독 가능한 매체는 컴퓨터로 판독 가능한 신호 매체 또는 컴퓨터로 판독 가능한 기록 매체일 수 있다. 상기 컴퓨터로 판독 가능한 기록 매체는 명령어 실행 시스템, 장비 또는 장치 내에 또는 이들과 접속되어 프로그램을 저장하거나 포함할 수 있는 임의의 유형적인 매체일 수 있다. 예를 들어, 상기 컴퓨터로 판독 가능한 매체는 비일시적(non-transitory) 저장 매체의 형태로 제공될 수 있다. 여기서, 비일시적은 저장 매체가 신호(signal)를 포함하지 않으며 실재(tangible)한다는 것을 의미할 뿐 데이터가 저장 매체에 반영구적 또는 임시적으로 저장됨을 구분하지 않는다.

[0111] 도 22 및 23은 본 발명의 실시예들에 따른 스토리지 장치 및 이를 포함하는 스토리지 시스템을 나타내는 블록도들이다. 이하 도 3과 중복되는 설명은 생략한다.

[0112] 도 22를 참조하면, 스토리지 시스템(100a)은 호스트 장치(200) 및 스토리지 장치(300a)를 포함한다. 스토리지

장치(300a)는 스토리지 컨트롤러(310a), 복수의 비휘발성 메모리들(320a, 320b, 320c) 및 버퍼 메모리(330)를 포함하며, 보안 소자(Secure Element; SE)(340)를 더 포함할 수 있다.

[0113] TTP(342)가 스토리지 컨트롤러(310a)에 포함되지 않고 보안 소자(340)에 포함되는 것을 제외하면, 스토리지 시스템(100a)은 도 3의 스토리지 시스템(100)과 실질적으로 동일할 수 있다.

[0114] 보안 소자(340)는 암호키(cryptographic key), 주요 데이터(sensitive data), 주요 코드 등의 보안 데이터를 처리 및/또는 저장할 수 있다. 예를 들어, 보안 소자(340)는 마이크로프로빙(microprobing), 소프트웨어 공격(software attack), 도청(eavesdropping), 오류 주입(fault injection) 등과 같은 부정 조작(tampering) 공격으로부터 보호되도록 부정 조작 방지(tamper-resistant) 기능을 가질 수 있다. TTP(342)가 보안 소자(340)에 포함됨으로써, 보안 성능이 보다 향상될 수 있다.

[0115] 도 23을 참조하면, 스토리지 시스템(100b)은 호스트 장치(200) 및 스토리지 장치(300b)를 포함하며, 인증 기관(Certificate Authority; CA)(2000)을 더 포함할 수 있다.

[0116] TTP(2100)가 스토리지 컨트롤러(310b)에 포함되지 않고 스토리지 장치(300b)의 외부에 위치하는 인증 기관(2000)에 포함되는 것을 제외하면, 스토리지 시스템(100b)은 도 3의 스토리지 시스템(100)과 실질적으로 동일할 수 있다.

[0117] 도 1 내지 22를 참조하여 인증서 생성이 스토리지 장치의 내부에서 수행하는 것으로 설명하였으나, 제조 공정이나 제조 이후의 인프라 스트럭처(Infrastructure)를 마련할 경우, 도 23에 도시된 것처럼 외부의 인증 기관(2000) 기반의 PKI (Public Key Infrastructure)를 통해 인증서를 생성하고 이에 기초하여 본 발명의 실시예들이 수행될 수 있다. X.509 표준 인증서 사용으로 본 발명의 기술이 확대 적용 가능하다.

[0118] 도 24는 본 발명의 실시예들에 따른 스토리지 시스템이 적용된 데이터 센터를 나타내는 블록도이다.

[0119] 도 24를 참조하면, 데이터 센터(3000)는 각종 데이터를 모아두고 서비스를 제공하는 시설로서, 데이터 스토리지 센터라고 지칭될 수도 있다. 데이터 센터(3000)는 검색 엔진 및 데이터 베이스 운용을 위한 시스템일 수 있으며, 은행 등의 기업 또는 정부기관에서 사용되는 컴퓨팅 시스템일 수 있다. 데이터 센터(3000)는 어플리케이션 서버들(3100~3100n) 및 스토리지 서버들(3200~3200m)을 포함할 수 있다. 어플리케이션 서버들(3100~3100n)의 개수 및 스토리지 서버들(3200~3200m)의 개수는 실시예에 따라 다양하게 선택될 수 있고, 어플리케이션 서버들(3100~3100n)의 개수 및 스토리지 서버들(3200~3200m)의 개수는 서로 다를 수 있다.

[0120] 어플리케이션 서버(3100) 또는 스토리지 서버(3200)는 프로세서(3110, 3210) 및 메모리(3120, 3220) 중 적어도 하나를 포함할 수 있다. 스토리지 서버(3200)를 예시로 설명하면, 프로세서(3210)는 스토리지 서버(3200)의 전반적인 동작을 제어할 수 있고, 메모리(3220)에 액세스하여 메모리(3220)에 로딩된 명령어 및/또는 데이터를 실행할 수 있다. 메모리(3220)는 DDR SDRAM(Double Data Rate Synchronous DRAM), HBM(High Bandwidth Memory), HMC(Hybrid Memory Cube), DIMM(Dual In-line Memory Module), Optane DIMM 또는 NVMDIMM(Non-Volatile DIMM)일 수 있다. 실시예에 따라, 스토리지 서버(3200)에 포함되는 프로세서(3210)의 개수 및 메모리(3220)의 개수는 다양하게 선택될 수 있다. 일 실시예에서, 프로세서(3210)와 메모리(3220)는 프로세서-메모리 페어를 제공할 수 있다. 일 실시예에서, 프로세서(3210)와 메모리(3220)의 개수는 서로 다를 수도 있다. 프로세서(3210)는 단일 코어 프로세서 또는 다중 코어 프로세서를 포함할 수 있다. 스토리지 서버(3200)에 대한 상기 설명은, 어플리케이션 서버(3100)에도 유사하게 적용될 수 있다. 실시예에 따라, 어플리케이션 서버(3100)는 스토리지 장치(3150)를 포함하지 않을 수도 있다. 스토리지 서버(3200)는 적어도 하나 이상의 스토리지 장치(3250)를 포함할 수 있다. 스토리지 서버(3200)에 포함되는 스토리지 장치(3250)의 개수는 실시예에 따라 다양하게 선택될 수 있다.

[0121] 어플리케이션 서버들(3100~3100n) 및 스토리지 서버들(3200~3200m)은 네트워크(3300)를 통해 서로 통신할 수 있다. 네트워크(3300)는 FC(Fiber Channel) 또는 이더넷(Ethernet) 등을 이용하여 구현될 수 있다. 이 때, FC는 상대적으로 고속의 데이터 전송에 사용되는 매체이며, 고성능/고가용성을 제공하는 광 스위치를 사용할 수 있다. 네트워크(3300)의 액세스 방식에 따라 스토리지 서버들(3200~3200m)은 파일 스토리지, 블록 스토리지, 또는 오브젝트 스토리지로서 제공될 수 있다.

[0122] 일 실시예에서, 네트워크(3300)는 SAN(Storage Area Network)과 같은 스토리지 전용 네트워크일 수 있다. 예를 들어, SAN은 FC 네트워크를 이용하고 FCP(FC Protocol)에 따라 구현된 FC-SAN일 수 있다. 다른 예에서, SAN은 TCP/IP 네트워크를 이용하고 iSCSI(SCSI over TCP/IP 또는 Internet SCSI) 프로토콜에 따라 구현된 IP-SAN일 수 있다. 다른 실시예에서, 네트워크(3300)는 TCP/IP 네트워크와 같은 일반 네트워크일 수 있다. 예를 들어, 네

트워크(3300)는 FCoE(FC over Ethernet), NAS(Network Attached Storage), NVMe-oF(NVMe over Fabrics) 등의 프로토콜에 따라 구현될 수 있다.

[0123] 이하에서는, 어플리케이션 서버(3100) 및 스토리지 서버(3200)를 중심으로 설명하기로 한다. 어플리케이션 서버(3100)에 대한 설명은 다른 어플리케이션 서버(3100n)에도 적용될 수 있고, 스토리지 서버(3200)에 대한 설명은 다른 스토리지 서버(3200m)에도 적용될 수 있다.

[0124] 어플리케이션 서버(3100)는 사용자 또는 클라이언트가 저장 요청한 데이터를 네트워크(3300)를 통해 스토리지 서버들(3200~3200m) 중 하나에 저장할 수 있다. 또한, 어플리케이션 서버(3100)는 사용자 또는 클라이언트가 독출 요청한 데이터를 스토리지 서버들(3200~3200m) 중 하나로부터 네트워크(3300)를 통해 획득할 수 있다. 예를 들어, 어플리케이션 서버(3100)는 웹 서버 또는 DBMS(Database Management System) 등으로 구현될 수 있다.

[0125] 어플리케이션 서버(3100)는 네트워크(3300)를 통해 다른 어플리케이션 서버(3100n)에 포함된 메모리(3120n) 또는 스토리지 장치(3150n)에 액세스할 수 있고, 또는 네트워크(3300)를 통해 스토리지 서버(3200~3200m)에 포함된 메모리(3220~3220m) 또는 스토리지 장치(3250~3250m)에 액세스할 수 있다. 이로써, 어플리케이션 서버(3100)는 어플리케이션 서버들(3100~3100n) 및/또는 스토리지 서버들(3200~3200m)에 저장된 데이터에 대해 다양한 동작들을 수행할 수 있다. 예를 들어, 어플리케이션 서버(3100)는 어플리케이션 서버들(3100~3100n) 및/또는 스토리지 서버들(3200~3200m) 사이에서 데이터를 이동 또는 카피(copy)하기 위한 명령어를 실행할 수 있다. 이 때 데이터는 스토리지 서버들(3200~3200m)의 스토리지 장치로(3250~3250m)부터 스토리지 서버들(3200~3200m)의 메모리들(3220~3220m)을 거쳐서, 또는 바로 어플리케이션 서버들(3100~3100n)의 메모리(3120~3120n)로 이동될 수 있다. 네트워크(3300)를 통해 이동하는 데이터는 보안 또는 프라이버시를 위해 암호화된 데이터일 수 있다.

[0126] 스토리지 서버(3200)를 예시로 설명하면, 인터페이스(3254)는 프로세서(3210)와 컨트롤러(3251)의 물리적 연결 및 NIC(3240)와 컨트롤러(3251)의 물리적 연결을 제공할 수 있다. 예를 들어, 인터페이스(3254)는 스토리지 장치(3250)를 전용 케이블로 직접 접속하는 DAS(Direct Attached Storage) 방식으로 구현될 수 있다. 또한, 예를 들어, 인터페이스(3254)는 ATA(Advanced Technology Attachment), SATA(Serial ATA), e-SATA(external SATA), SCSI(Small Computer Small Interface), SAS(Serial Attached SCSI), PCI(Peripheral Component Interconnection), PCIe(PCI express), NVMe(NVM express), IEEE 1394, USB(universal serial bus), SD(secure digital) 카드, MMC(multi-media card), eMMC(embedded multi-media card), UFS(Universal Flash Storage), eUFS(embedded Universal Flash Storage), CF(compact flash) 카드 인터페이스 등과 같은 다양한 인터페이스 방식으로 구현될 수 있다.

[0127] 스토리지 서버(3200)는 스위치(3230) 및 NIC(3240)을 더 포함할 수 있다. 스위치(3230)는 프로세서(3210)의 제어에 따라 프로세서(3210)와 스토리지 장치(3250)를 선택적으로 연결시키거나, NIC(3240)과 스토리지 장치(3250)를 선택적으로 연결시킬 수 있다. 이와 유사하게, 어플리케이션 서버(3100)는 스위치(3130) 및 NIC(3140)을 더 포함할 수 있다.

[0128] 일 실시예에서 NIC(3240)는 네트워크 인터페이스 카드, 네트워크 어댑터 등을 포함할 수 있다. NIC(3240)는 유선 인터페이스, 무선 인터페이스, 블루투스 인터페이스, 광학 인터페이스 등에 의해 네트워크(3300)에 연결될 수 있다. NIC(3240)는 내부 메모리, DSP, 호스트 버스 인터페이스 등을 포함할 수 있으며, 호스트 버스 인터페이스를 통해 프로세서(3210) 및/또는 스위치(3230) 등과 연결될 수 있다. 호스트 버스 인터페이스는, 앞서 설명한 인터페이스(3254)의 예시들 중 하나로 구현될 수도 있다. 일 실시예에서, NIC(3240)는 프로세서(3210), 스위치(3230), 스토리지 장치(3250) 중 적어도 하나와 통합될 수도 있다.

[0129] 스토리지 서버(3200~3200m) 또는 어플리케이션 서버(3100~3100n)에서 프로세서는 스토리지 장치(3150~3150n, 3250~3250m) 또는 메모리(3120~3120n, 3220~3220m)로 커맨드를 전송하여 데이터를 프로그램하거나 리드할 수 있다. 이 때 데이터는 ECC(Error Correction Code) 엔진을 통해 에러 정정된 데이터일 수 있다. 데이터는 데이터 버스 변환(Data Bus Inversion: DBI) 또는 데이터 마스킹(Data Masking: DM) 처리된 데이터로서, CRC(Cyclic Redundancy Code) 정보를 포함할 수 있다. 데이터는 보안 또는 프라이버시를 위해 암호화된 데이터일 수 있다.

[0130] 스토리지 장치(3150~3150m, 3250~3250m)는 프로세서로부터 수신된 리드 커맨드에 응답하여, 제어 신호 및 커맨드/어드레스 신호를 NAND 플래시 메모리 장치(3252~3252m)로 전송할 수 있다. 이에 따라 NAND 플래시 메모리 장치(3252~3252m)로부터 데이터를 독출하는 경우, RE(Read Enable) 신호는 데이터 출력 제어 신호로 입력되어, 데이터를 DQ 버스로 출력하는 역할을 할 수 있다. RE 신호를 이용하여 DQS(Data Strobe)를 생성할 수 있다. 커맨드와 어드레스 신호는 WE(Write Enable) 신호의 상승 엣지 또는 하강 엣지에 따라 페이지 버퍼에 래치될 수 있

다.

[0131] 컨트롤러(3251)는 스토리지 장치(3250)의 동작을 전반적으로 제어할 수 있다. 일 실시예에서, 컨트롤러(3251)는 SRAM(Static Random Access Memory)을 포함할 수 있다. 컨트롤러(3251)는 기입 커맨드에 응답하여 낸드 플래시(3252)에 데이터를 기입할 수 있고, 또는 독출 커맨드에 응답하여 낸드 플래시(3252)로부터 데이터를 독출할 수 있다. 예를 들어, 기입 커맨드 및/또는 독출 커맨드는 스토리지 서버(3200) 내의 프로세서(3210), 다른 스토리지 서버(3200m) 내의 프로세서(3210m) 또는 어플리케이션 서버(3100, 3100n) 내의 프로세서(3110, 3110n)로부터 제공될 수 있다. DRAM(3253)은 낸드 플래시(3252)에 기입될 데이터 또는 낸드 플래시(3252)로부터 독출된 데이터를 임시 저장(버퍼링)할 수 있다. 또한, DRAM(3253)은 메타 데이터를 저장할 수 있다. 여기서, 메타 데이터는 사용자 데이터 또는 낸드 플래시(3252)를 관리하기 위해 컨트롤러(3251)에서 생성된 데이터이다.

[0132] 스토리지 장치(3150~3150m, 3250~3250m)는 도 1 내지 23을 참조하여 상술한 본 발명의 실시예들에 따른 스토리지 장치에 기초하여 구현되며, 본 발명의 실시예들에 따른 키 교환 방법 및 접근 권한 이관 방법을 수행하도록 구현될 수 있다.

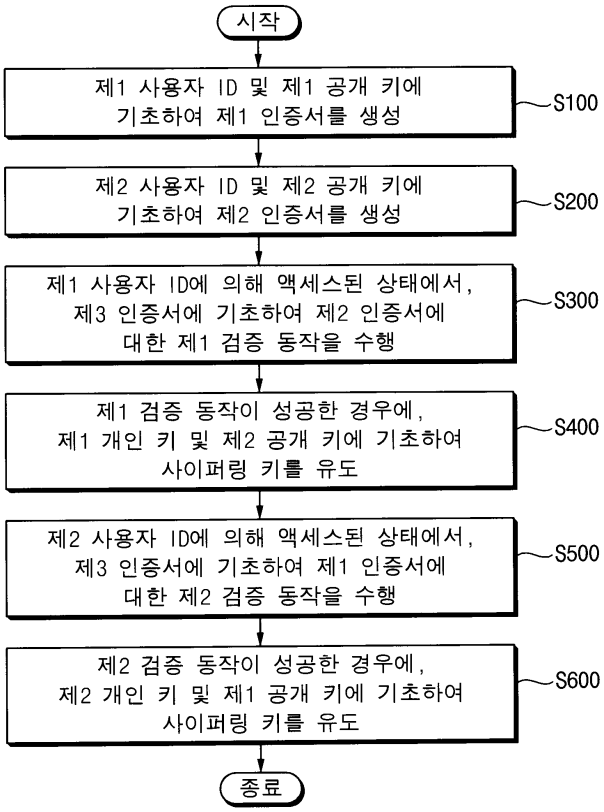
산업상 이용가능성

[0133] 본 발명의 실시예들은 스토리지 장치 및 이를 포함하는 임의의 전자 장치 및 시스템에 유용하게 이용될 수 있다. 예를 들어, 본 발명의 실시예들은 PC(Personal Computer), 서버 컴퓨터(server computer), 데이터 센터(data center), 워크스테이션(workstation), 노트북(laptop), 핸드폰(cellular), 스마트 폰(smart phone), MP3 플레이어, PDA(Personal Digital Assistant), PMP(Portable Multimedia Player), 디지털 TV, 디지털 카메라, 포터블 게임 콘솔(portable game console), 네비게이션(navigation) 기기, 웨어러블(wearable) 기기, IoT(Internet of Things) 기기, IoE(Internet of Everything) 기기, e-북(e-book), VR(Virtual Reality) 기기, AR(Augmented Reality) 기기, 드론(drone) 등과 같은 전자 시스템에 더욱 유용하게 적용될 수 있다.

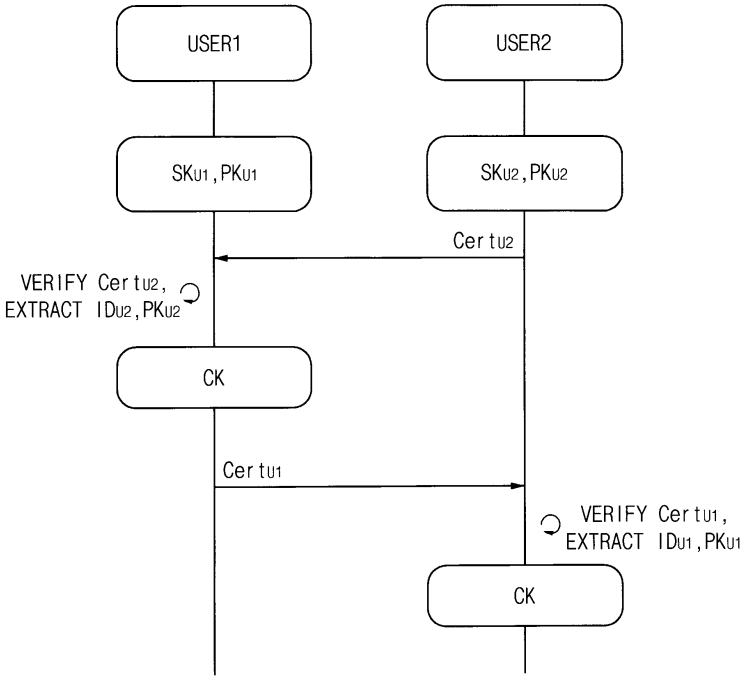
[0134] 상기에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술분야의 숙련된 당업자는 하기의 특허청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 것이다.

도면

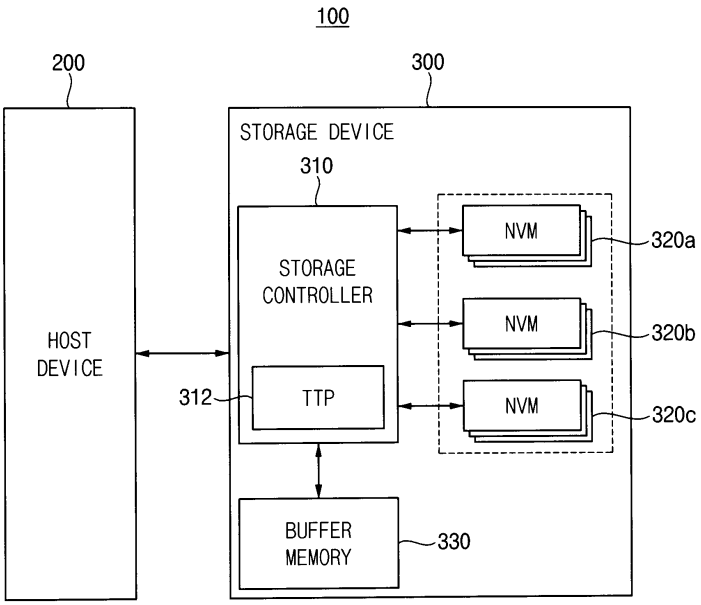
도면1


시작
제1 사용자 ID 및 제1 공개 키에 기초하여 제1 인증서를 생성
S100
제2 사용자 ID 및 제2 공개 키에 기초하여 제2 인증서를 생성
S200
제1 사용자 ID에 의해 액세스된 상태에서, 제3 인증서에 기초하여 제2 인증서에 대한 제1 검증 동작을 수행
S300
제1 검증 동작이 성공한 경우에, 제1 개인 키 및 제2 공개 키에 기초하여 사이퍼링 키를 유도
S400
제2 사용자 ID에 의해 액세스된 상태에서, 제3 인증서에 기초하여 제1 인증서에 대한 제2 검증 동작을 수행
S500
제2 검증 동작이 성공한 경우에, 제2 개인 키 및 제1 공개 키에 기초하여 사이퍼링 키를 유도
S600
종료

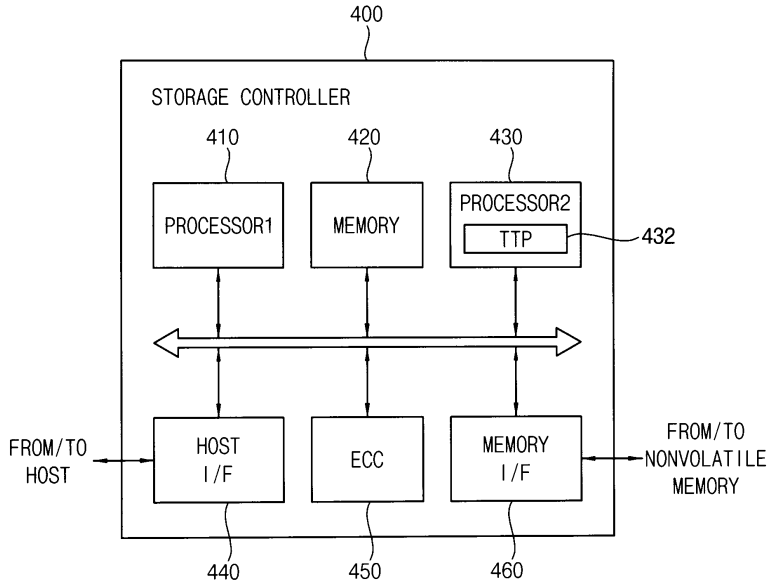
도면2


USER1
USER2
SKU1,PKU1
SKU2,PKU2
Cert U2
VERIFY Cert U2,
EXTRACT IDU2,PKU2
CK
Cert U1
VERIFY Cert U1,
EXTRACT IDU1,PKU1
CK

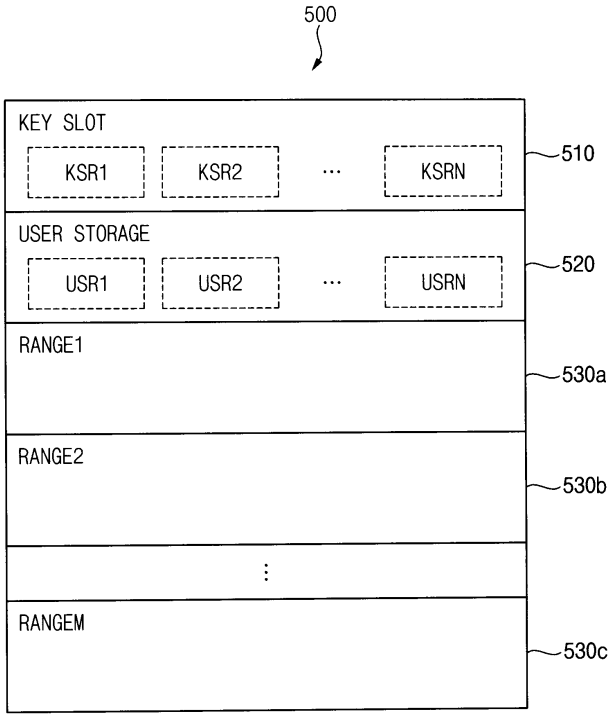
도면3


100
200
300
HOST DEVICE
STORAGE DEVICE
310
STORAGE CONTROLLER
312
TTP
NVM
NVM
NVM
320a
320b
320c
BUFFER MEMORY
330

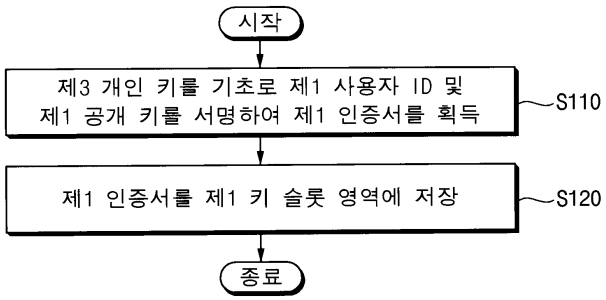
도면4


400
STORAGE CONTROLLER
410
420
430
PROCESSOR1
MEMORY
PROCESSOR2
TTP
432
FROM/TO HOST
HOST I/F
ECC
MEMORY I/F
FROM/TO NONVOLATILE MEMORY
440
450
460

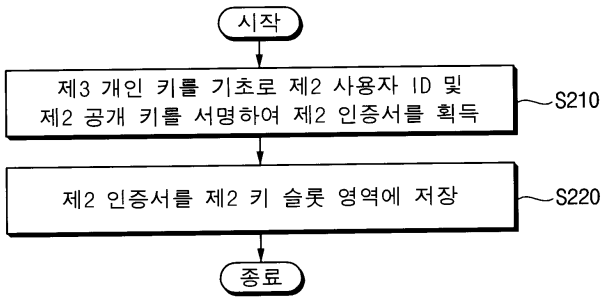
도면5


500
KEY SLOT
KSR1
KSR2
···
KSRN
510
USER STORAGE
USR1
USR2
···
USRN
520
RANGE1
530a
RANGE2
530b
⋮
RANGEM
530c

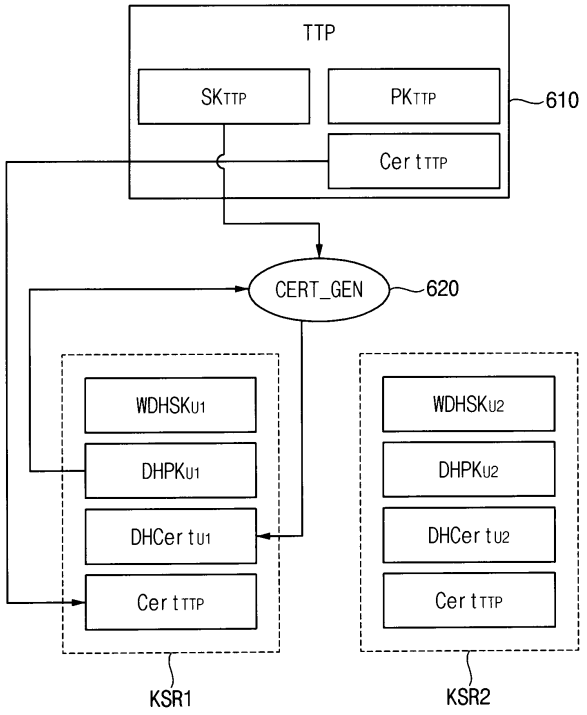
도면6


시작
제3 개인 키를 기초로 제1 사용자 ID 및
제1 공개 키를 서명하여 제1 인증서를 획득
S110
제1 인증서를 제1 키 슬롯 영역에 저장
S120
종료

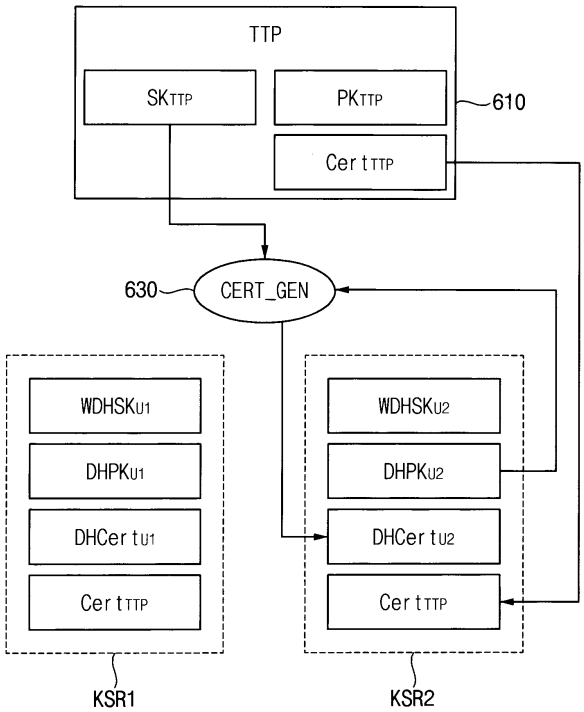
도면7


시작
제3 개인 키를 기초로 제2 사용자 ID 및
제2 공개 키를 서명하여 제2 인증서를 획득
S210
제2 인증서를 제2 키 슬롯 영역에 저장
S220
종료

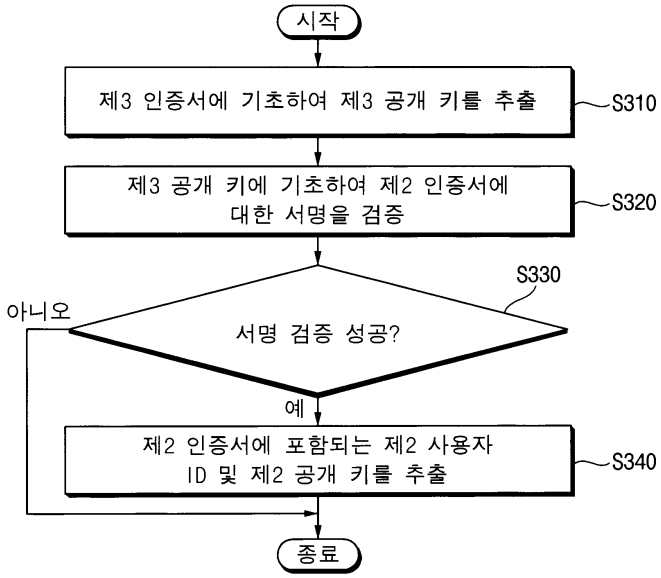
도면8a


TTP
SKTTP
PKTTP
610
Cert TTP
CERT_GEN
620
WDHSKU1
DHPKU1
DHCert U1
Cert TTP
KSR1
WDHSKU2
DHPKU2
DHCert U2
Cert TTP
KSR2

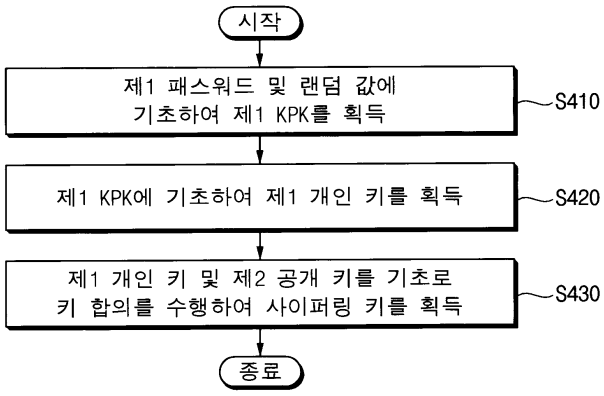
도면8b


TTP
SKTTP
PKTTP
610
Cert TTP
630
CERT_GEN
WDHSKU1
DHPKU1
DHCert U1
Cert TTP
KSR1
WDHSKU2
DHPKU2
DHCert U2
Cert TTP
KSR2

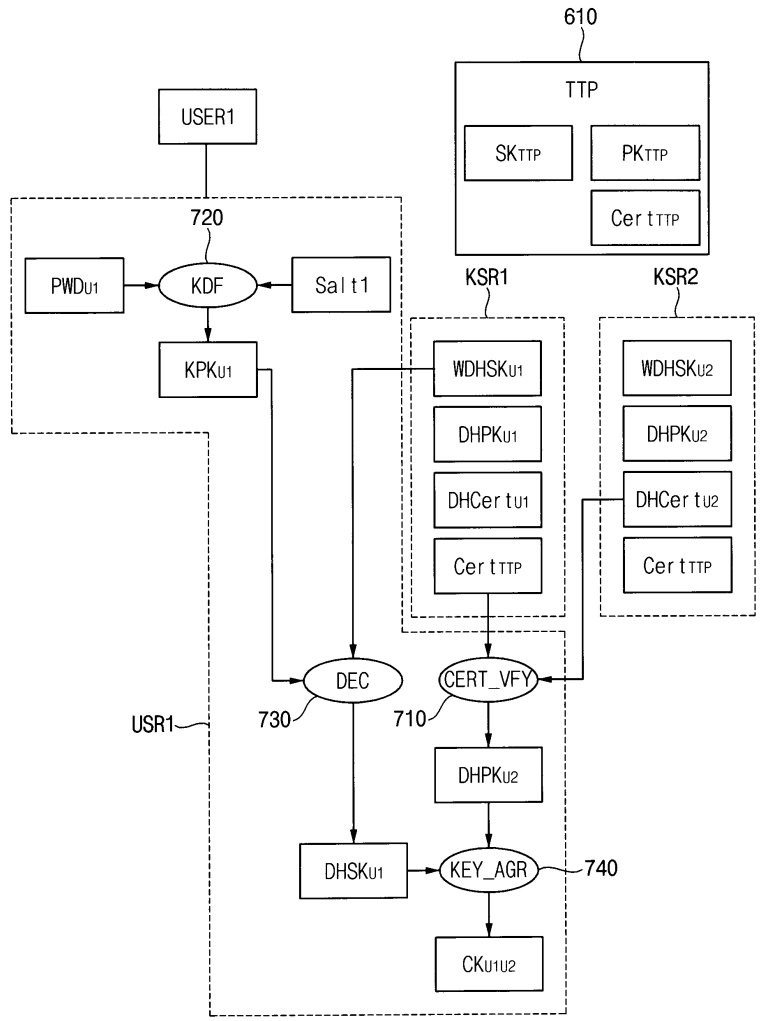
도면9


시작
제3 인증서에 기초하여 제3 공개 키를 추출
S310
제3 공개 키에 기초하여 제2 인증서에 대한 서명을 검증
S320
S330
서명 검증 성공?
아니오
예
제2 인증서에 포함되는 제2 사용자 ID 및 제2 공개 키를 추출
S340
종료

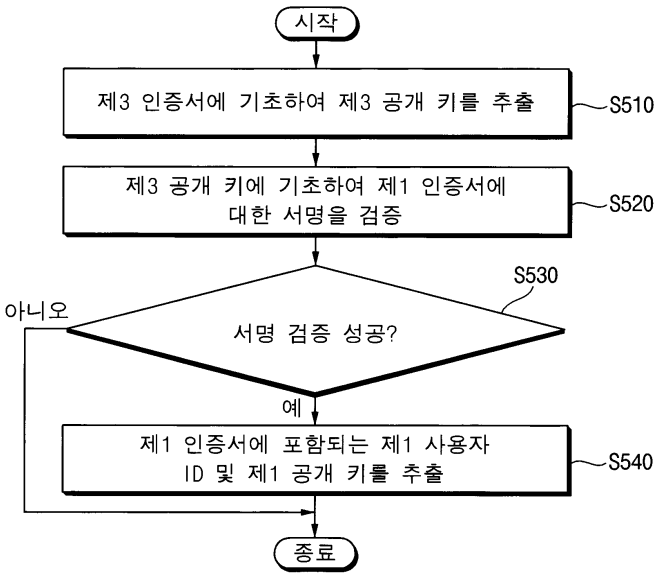
도면10


시작
제1 패스워드 및 랜덤 값에 기초하여 제1 KPK를 획득
S410
제1 KPK에 기초하여 제1 개인 키를 획득
S420
제1 개인 키 및 제2 공개 키를 기초로 키 합의를 수행하여 사이퍼링 키를 획득
S430
종료

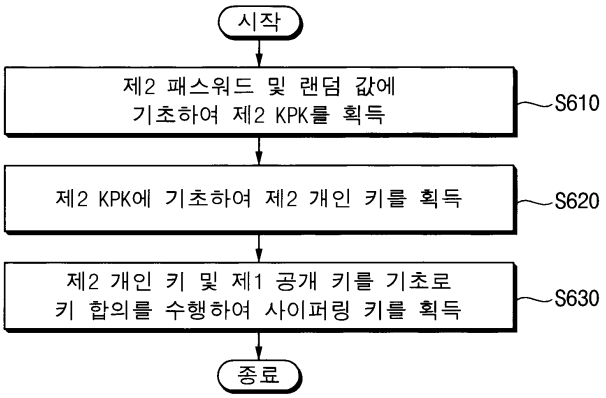
도면11


610
TTP
SKTTP
PKTTP
CertTTP
USER1
720
PWDU1
KDF
Salt1
KPKU1
KSR1
KSR2
WDHSKU1
DHPKU1
DHCertU1
CertTTP
WDHSKU2
DHPKU2
DHCertU2
CertTTP
DEC
CERT_VFY
730
710
USR1
DHPKU2
DHSKU1
KEY_AGR
740
CKU1U2

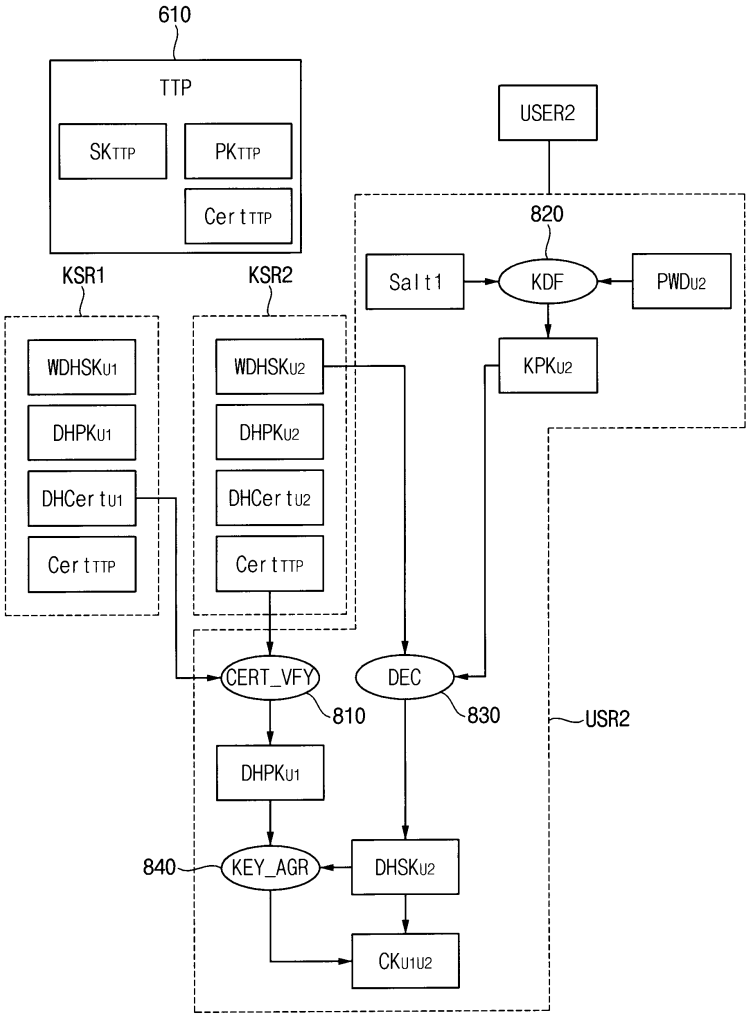
도면12


시작
제3 인증서에 기초하여 제3 공개 키를 추출
S510
제3 공개 키에 기초하여 제1 인증서에 대한 서명을 검증
S520
S530
서명 검증 성공?
아니오
예
제1 인증서에 포함되는 제1 사용자 ID 및 제1 공개 키를 추출
S540
종료

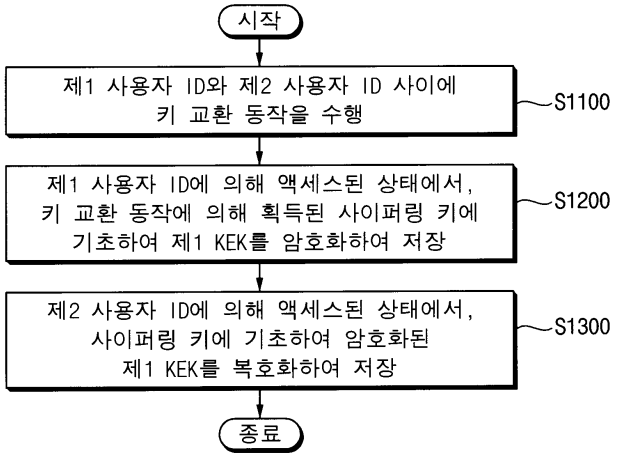
도면13


시작
제2 패스워드 및 랜덤 값에
기초하여 제2 KPK를 획득
S610
제2 KPK에 기초하여 제2 개인 키를 획득
S620
제2 개인 키 및 제1 공개 키를 기초로
키 합의를 수행하여 사이퍼링 키를 획득
S630
종료

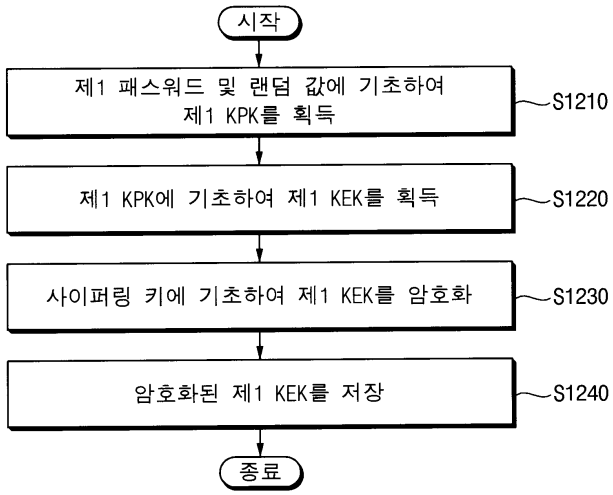
도면14


610
TTP
SKTTP
PKTTP
CertTTP
USER2
820
Salt1
KDF
PWDU2
KPKU2
KSR1
KSR2
WDHSKU1
DHPKU1
DHCertU1
CertTTP
WDHSKU2
DHPKU2
DHCertU2
CertTTP
CERT_VFY
DEC
810
830
USR2
DHPKU1
840
KEY_AGR
DHSKU2
CKU1U2

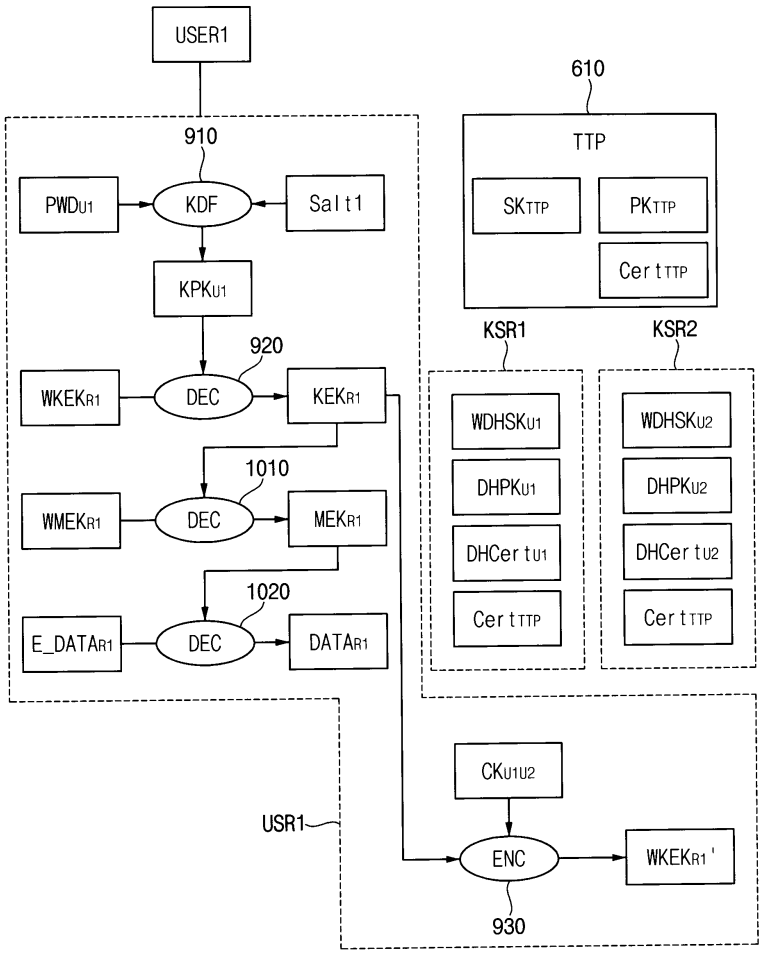
도면15


시작
제1 사용자 ID와 제2 사용자 ID 사이에 키 교환 동작을 수행
S1100
제1 사용자 ID에 의해 액세스된 상태에서, 키 교환 동작에 의해 획득된 사이퍼링 키에 기초하여 제1 KEK를 암호화하여 저장
S1200
제2 사용자 ID에 의해 액세스된 상태에서, 사이퍼링 키에 기초하여 암호화된 제1 KEK를 복호화하여 저장
S1300
종료

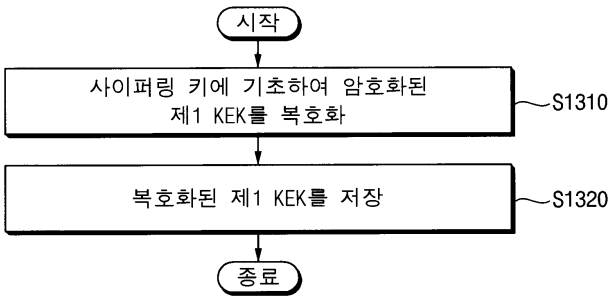
도면16


시작
제1 패스워드 및 랜덤 값에 기초하여 제1 KPK를 획득
S1210
제1 KPK에 기초하여 제1 KEK를 획득
S1220
사이퍼링 키에 기초하여 제1 KEK를 암호화
S1230
암호화된 제1 KEK를 저장
S1240
종료

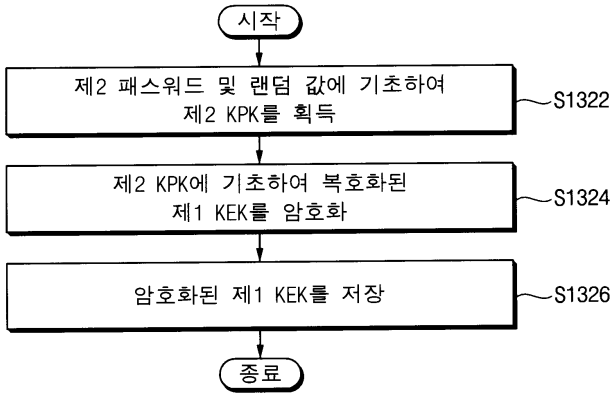
도면17


USER1
610
910
TTP
PWDU1
KDF
Salt1
SKTTP
PKTTP
CertTTP
KPKU1
KSR1
KSR2
920
WKEKR1
DEC
KEKR1
WDHSKU1
WDHSKU2
DHPKU1
DHPKU2
DHCertU1
DHCertU2
CertTTP
CertTTP
1010
WMEKR1
DEC
MEKR1
1020
E_DATAR1
DEC
DATAR1
CKU1U2
USR1
ENC
WKEKR1'
930

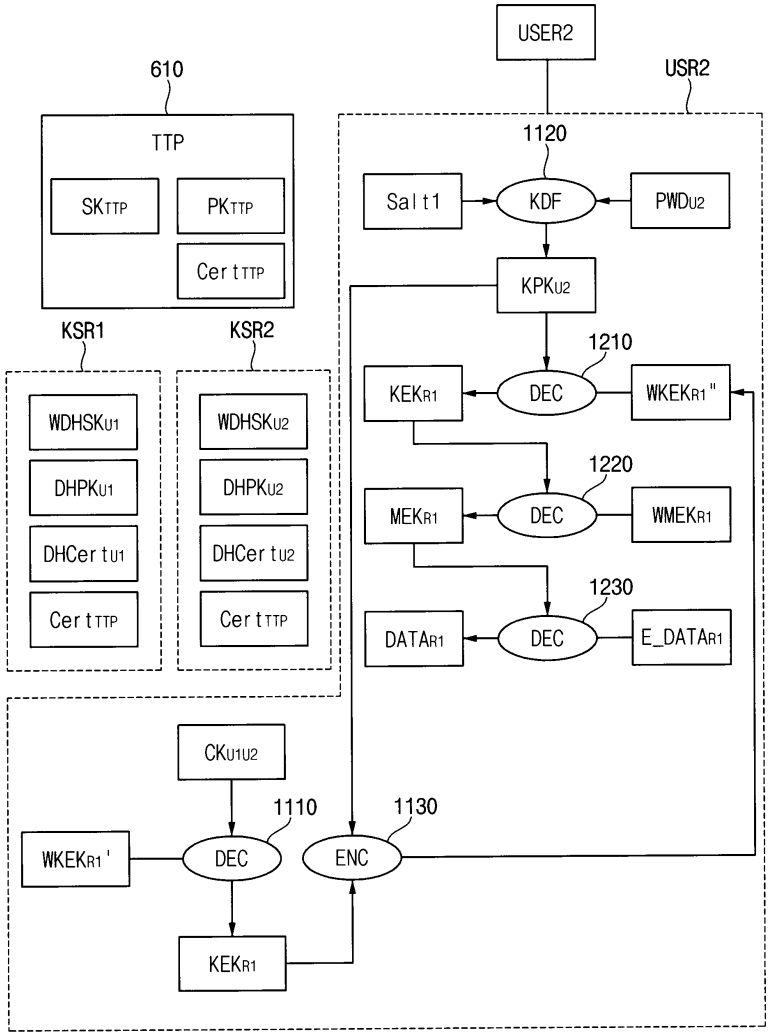
도면18


시작
사이퍼링 키에 기초하여 암호화된
제1 KEK를 복호화
S1310
복호화된 제1 KEK를 저장
S1320
종료

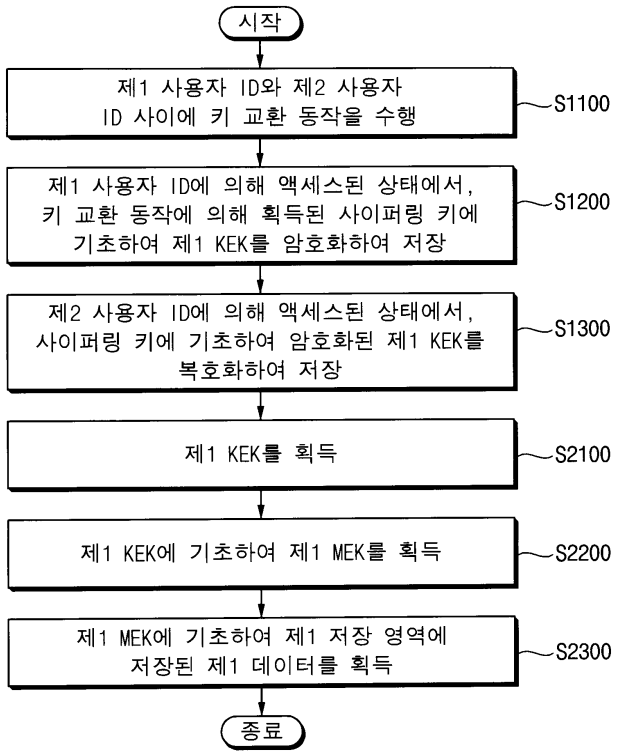
도면19


시작
제2 패스워드 및 랜덤 값에 기초하여 제2 KPK를 획득
S1322
제2 KPK에 기초하여 복호화된 제1 KEK를 암호화
S1324
암호화된 제1 KEK를 저장
S1326
종료

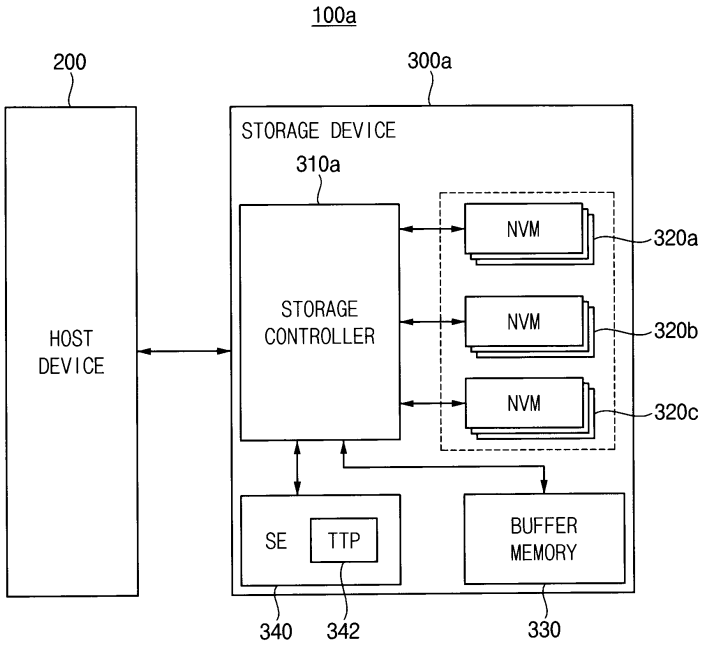
도면20


USER2
610
USR2
TTP
SKTTP
PKTTP
CertTTP
1120
Salt1
KDF
PWDU2
KPKU2
KSR1
KSR2
1210
KEKR1
DEC
WKEKR1"
WDHSKU1
DHPKU1
DHCertU1
CertTTP
WDHSKU2
DHPKU2
DHCertU2
CertTTP
1220
MEKR1
DEC
WMEKR1
1230
DATAR1
DEC
E_DATAR1
CKU1U2
1110
1130
WKEKR1'
DEC
ENC
KEKR1

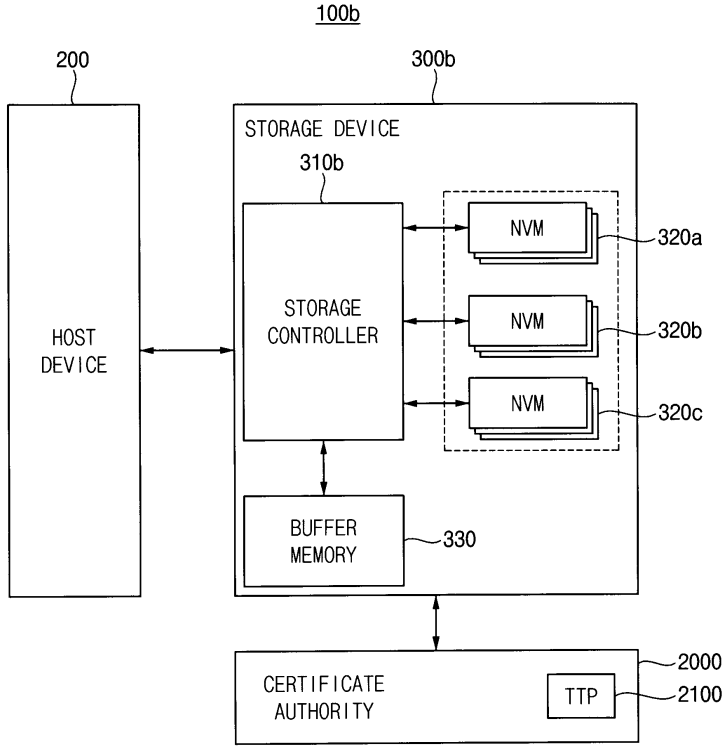
도면21


시작
제1 사용자 ID와 제2 사용자 ID 사이에 키 교환 동작을 수행
S1100
제1 사용자 ID에 의해 액세스된 상태에서, 키 교환 동작에 의해 획득된 사이퍼링 키에 기초하여 제1 KEK를 암호화하여 저장
S1200
제2 사용자 ID에 의해 액세스된 상태에서, 사이퍼링 키에 기초하여 암호화된 제1 KEK를 복호화하여 저장
S1300
제1 KEK를 획득
S2100
제1 KEK에 기초하여 제1 MEK를 획득
S2200
제1 MEK에 기초하여 제1 저장 영역에 저장된 제1 데이터를 획득
S2300
종료

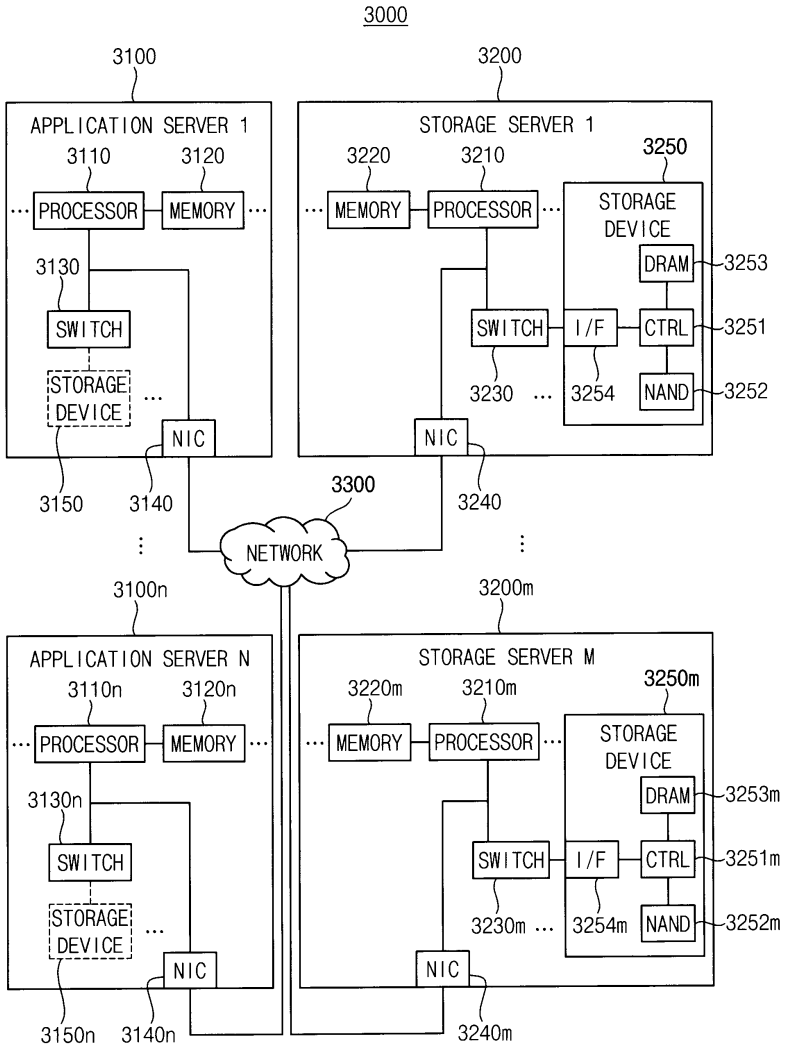
도면22


100a
200
300a
HOST DEVICE
STORAGE DEVICE
310a
STORAGE CONTROLLER
NVM
NVM
NVM
320a
320b
320c
SE
TTP
BUFFER MEMORY
340
342
330

도면23


100b
200
300b
STORAGE DEVICE
310b
HOST DEVICE
STORAGE CONTROLLER
NVM
NVM
NVM
320a
320b
320c
BUFFER MEMORY
330
CERTIFICATE AUTHORITY
TTP
2000
2100

도면24


3000
3100
APPLICATION SERVER 1
3110
3120
PROCESSOR
MEMORY
3130
SWITCH
STORAGE DEVICE
NIC
3150
3140
3200
STORAGE SERVER 1
3220
3210
3250
MEMORY
PROCESSOR
STORAGE DEVICE
DRAM
3253
SWITCH
I/F
CTRL
3251
3230
3254
NAND
3252
NIC
3240
3300
NETWORK
3100n
APPLICATION SERVER N
3110n
3120n
3130n
3150n
3140n
3200m
STORAGE SERVER M
3220m
3210m
3250m
3253m
3251m
3230m
3254m
3252m
3240m