(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년12월24일
(11) 등록번호 10-1213118
(24) 등록일자 2012년12월11일

(51) 국제특허분류(Int. Cl.)
G06F 21/00 (2006.01) *G06F 21/24* (2006.01)
G06F 21/22 (2006.01)
(21) 출원번호 10-2009-7026878(분할)
(22) 출원일자(국제) 2005년12월21일
심사청구일자 2010년12월10일
(85) 번역문제출일자 2009년12월23일
(65) 공개번호 10-2010-0017907
(43) 공개일자 2010년02월16일
(62) 원출원 특허 10-2007-7016643
원출원일자(국제) 2005년12월21일
(86) 국제출원번호 PCT/US2005/046478
(87) 국제공개번호 WO 2006/069194
국제공개일자 2006년06월29일
(30) 우선권주장
11/314,410 2005년12월20일 미국(US)
(뒷면에 계속)
(56) 선행기술조사문헌
US06026402 A
US20030061504 A1
US20040139021 A1
전체 청구항 수 : 총 34 항

(73) 특허권자
디스크레틱스 테크놀로지스 엘티디.
이스라엘 델타 빌딩 크파르 네터 그랜드 네터 인더스티리얼 존 (우편번호: 40593)
샌디스크 코포레이션
미국 캘리포니아 95035 밀피타스 맥카시 블러바드 601
(72) 발명자
조공쿨롱 파브리스
미국 캘리포니아 94070 산카를로스 855 버클랜드 애비뉴
홀츠만 마이클
미국 캘리포니아 95014 쿠퍼티노 7602 반하트 플레이스
(뒷면에 계속)
(74) 대리인
김용인, 박영복

심사관 : 박진아

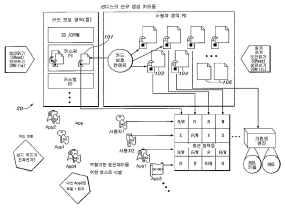
(54) 발명의 명칭 **다기능 컨텐츠 제어가 가능한 메모리 시스템**

(57) 요 약

본 발명은 다기능 컨텐트 제어가 가능한 메모리 시스템에 관한 것이다.

독점적인 이권의 소유자는, 암호화-복호화 키가 매체 자체에 저장되거나 실질적으로 외부장치들이 접근할 수 없다면 상기 매체내의 암호화된 컨텐트에 대한 접근을 제어하기에 더 좋은 위치에 있게 된다. 적절한 크리덴셜을 가진 호스트 장치들만이 상기 키에 접근하는 것이 가능하다. 상기 매체에 저장된 데이터에 접근하기 위한 서로 다른 권한들(예를 들어 서로 다른 승인된 실체들에게)을 부여하는 접근 정책이 저장될 수 있다. 상술한 두 개의 특징들의 조합을 통합하는 시스템이 보다 유리하다. 한편, 컨텐트 소유자 또는 독점권자는 외부 장치들이 실질적으로 접근불가능한 키들을 이용하여 상기 컨텐트로의 접근을 제어할 수 있고, 동시에 상기 매체의 컨텐트에 접근하기 위한 서로 다른 권한들을 부여할 수 있다. 따라서 외부 장치들이 접근에 성공하더라도, 그들의 접근은 여전히 상기 저장매체에 기록된 상기 컨텐트 소유자 또는 독점권자에 의해 설정된 상기 다른 권한들의 집합에 의해 지배를 받을 수 있다. 플래시 메모리에 구현될 때, 상술한 특징들은 특히 컨텐트 보호를 위한 유용한 매체가 된다. 많은 저장장치들은, 많은 컴퓨터 호스트 장치들이 파일형태로 데이터를 읽고 쓰는 동안 파일시스템을 인식하지 않는다. 상기 호스트 장치는, 상기 저장시스템이 상기 키 ID와 결합된 응답에서 키 값을 생성하는 동안 키 참조 또는 ID를 제공하는데, 상기 키 ID는, 호스트가 파일들의 제어를 유지하는 동안 상기 메모리가 암호화 프로세스들을 위한 키 값의 생성 및 이용에 대한 완전하고 독점적인 제어를 유지하는 핸들로서 이용된다.

대 표 도



(72) 발명자

커와미 바먼

미국 캘리포니아 95138 산호세 5899 킬라니 서클

바질라이 론

이스라엘 25147 크파르 브라딤 67 메론 스트리트

하가이 바렐

이스라엘 76574 레호보트 드루얀 4

(30) 우선권주장

11/314,411 2005년12월20일 미국(US)

60/638,804 2004년12월21일 미국(US)

특허청구의 범위

청구항 1

저장 장치와 통신하도록 구성된 인터페이스; 및

상기 인터페이스와 통신하는 제어기를 포함하는 호스트 장치에 있어서,

상기 제어기는,

상기 저장 장치에 키 ID를 포함하는 키(key) 생성 요청을 송신하고,

상기 키의 사용에 적용할 수 있는 하나 이상의 정책들을, 저장을 위하여 상기 저장 장치에 송신하도록 동작하며,

상기 저장 장치에서 상기 키의 생성은 상기 키 ID와 독립적으로 수행되고, 상기 키는 상기 저장 장치 내에서 내부적으로만 접근가능하며,

상기 하나 이상의 정책들은 상기 저장 장치 내의 데이터의 암호화 및/또는 복호화를 위하여 상기 키의 사용을 요청하기 위한, 상기 저장 장치에 의해 인증된 실체들에게 주어진 서로 다른 권한들에 관한 것이며,

상기 저장 장치로 송신된 요청은 상기 하나 이상의 정책들에 근거하여 허용되거나 거절될 수 있으며, 상기 저장 장치에 의해 수신된 요청은 각각 상기 저장 장치에 대한 데이터의 기록 또는 판독에 대응하는 암호화 또는 복호화를 수행할 때 상기 키를 사용하기 위하여 상기 키 ID를 포함하도록 한, 호스트 장치.

청구항 2

제 1 항에 있어서,

상기 하나 이상의 정책들은 실체들의 집합 중 하나 이상의 실체들이 상기 저장 장치에 저장된 동일한 데이터에 접근하기 위한 키를 사용하도록 허가하고, 상기 집합에 속하지 않는 실체들이 상기 저장 장치에 저장된 데이터에 접근하기 위한 키를 사용하지 못하도록 하는 호스트 장치.

청구항 3

제 1 항에 있어서,

상기 하나 이상의 정책들은 하나 이상의 실체들의 제1 집합이 데이터를 암호화 및/또는 복호화하고 상기 저장 장치로부터 데이터를 기록하고 판독하기 위해 상기 키를 사용하도록 허가하고, 하나 이상의 실체들의 제2 집합이 상기 저장 장치 내의 데이터를 복호화하고 상기 복호화된 데이터를 판독하기 위해서만 상기 키를 사용하도록 허가하는 호스트 장치.

청구항 4

제 1 항에 있어서,

상기 하나 이상의 정책들은 하나 이상의 실체들의 집합이 데이터를 암호화하고 상기 암호화된 데이터를 상기 저장 장치에 기록하는 경우에만, 상기 저장 장치 내의 데이터를 복호화하고 상기 복호화된 데이터를 판독하는 경우에만, 또는 양자 모두의 경우에 상기 키를 사용하도록 허가하는 호스트 장치.

청구항 5

제 1 항에 있어서,

상기 하나 이상의 정책들은 한 실체가 다른 실체의 상기 저장 장치로의 접근 권한들을 삭제하거나, 또는 상기 키를 이용하기 위해 다른 실체에 의한 접근을 금지하기 위해 상기 하나 이상의 정책들을 변경하는 것을 허가하며, 상기 다른 실체는 변경 이전에 그러한 접근이 허가되는 호스트 장치.

청구항 6

제 1 항에 있어서,

상기 하나 이상의 정책들은 한 실체가 다른 실체에게 상기 키에 대한 접근 권한들을 위임하거나, 또는 그러한 위임을 허가하기 위해 상기 하나 이상의 정책들을 변경하는 것을 허가하는 호스트 장치.

청구항 7

제 1 항에 있어서,

상기 하나 이상의 정책들은 상기 저장 장치 또는 상기 키에 접근하기 위해 적어도 하나의 실체를 위한 보안 채널의 형성을 요구하는 호스트 장치.

청구항 8

제 1 항에 있어서,

상기 하나 이상의 정책들은 상기 저장 장치 또는 상기 키에 접근하기 위한 보안 채널의 형성을 요구하는 호스트 장치.

청구항 9

제 1 항에 있어서,

상기 하나 이상의 정책들은 제한된 수의 실체에 의해서만 상기 저장 장치 또는 상기 키로의 접근을 허가하는 호스트 장치.

청구항 10

제 1 항에 있어서,

상기 하나 이상의 정책들은 실체가 인증되었는지에 상관없이, 제한된 수의 실체에 의해서만 상기 저장 장치 또는 상기 키로의 접근을 허가하는 호스트 장치.

청구항 11

제 1 항에 있어서,

상기 하나 이상의 정책들은 상기 저장 장치 또는 상기 키에 접근하기 위해 적어도 하나의 실체를 위한 보안 채널의 형성을 요구하지 않는 호스트 장치.

청구항 12

제 1 항에 있어서,

상기 제어기는 상기 저장 장치에,

상기 키의 사용을 위해 적용할 수 있는 추가 정책; 및

추가 키의 생성을 위한 요청 중 적어도 하나를 송신하도록 더 동작하는 호스트 장치.

청구항 13

제 1 항에 있어서,

상기 하나 이상의 정책들은 실체들의 서로 다른 집합들이 상기 키를 서로 다르게 사용하고 데이터로의 서로 다른 접근 권한들을 갖도록 허가하며, 상기 키의 서로 다른 사용은 암호화 및 복호화 중 하나 또는 모두를 포함하고, 상기 서로 다른 접근 권한들을 데이터의 판독 및 기록 중 하나 또는 모두를 포함하는 호스트 장치.

청구항 14

제 1 항에 있어서,

상기 제어기는 상기 저장 장치로, 상기 키와 상기 키로 암호화되어 상기 저장 장치에 저장된 파일을 연결한 조합을 송신하도록 더 동작하는 호스트 장치.

청구항 15

제 14 항에 있어서,

상기 제어기는 상기 저장 장치로, 상기 키의 참조 이름 및 상기 파일을 판독하기 위한 요청을 송신하도록 더 동작하는 호스트 장치.

청구항 16

제 1 항에 있어서,

상기 제어기는 상기 저장 장치로, 각각 하나의 실체에 의한 상기 저장 장치 내의 데이터로의 접근을 제어하기 위한 인증 요구 및 권한(들)을 포함하는 두 개 이상의 레코드들을 송신하도록 더 동작하며, 상기 수신된 두 개 이상의 레코드들은 인증 요구(들) 및 권한(들) 중 적어도 하나에서 서로 다른 호스트 장치.

청구항 17

제 16 항에 있어서,

상기 두 개 이상의 레코드들 각각은 대응하는 실체에 의한 상기 저장 장치의 파티션들(partitions)에 접근하기 위한 권한(들)을 포함하며, 파티션들에 접근하기 위한 적어도 두 개의 대응하는 실체들의 레코드 내의 권한(들)은 완전히 동일하지 않은 호스트 장치.

청구항 18

저장 장치와 통신하는 호스트 장치에 의해 수행되는, 저장 장치에 저장된 데이터 보호 방법에 관한 것으로,

키(key)의 생성을 위하여 상기 키의 키 ID를 포함하는 요청을 상기 저장 장치에 송신하는 단계; 및

상기 키의 사용에 적용할 수 있는 하나 이상의 정책들을 저장을 위하여 상기 저장 장치에 송신하는 단계를 포함하며,

상기 저장 장치에서 상기 키의 생성은 상기 키 ID와 독립적으로 수행되고, 상기 키는 상기 저장 장치 내에서 내부적으로만 접근가능하고,

상기 하나 이상의 정책들은 상기 저장 장치에서 데이터의 암호화 및/또는 복호화를 위하여 상기 키의 사용을 상기 저장 장치에 요청하기 위한, 상기 저장 장치에 의해 인증된 실체들에게 부여된 서로 다른 권한들에 관한 것이며,

상기 저장 장치로 송신된 요청은 상기 저장 장치에 의해 상기 하나 이상의 정책들에 근거하여 허용 또는 거절될 수 있으며, 상기 요청은 각각 상기 저장 장치에 기록 또는 판독된 데이터의 암호화 또는 복호화에 상기 키를 사용하기 위하여 상기 키 ID를 포함하는, 저장 장치에 저장된 데이터 보호 방법.

청구항 19

제 18 항에 있어서,

상기 하나 이상의 정책들은 실체들의 집합 중 하나 이상의 실체들이 상기 저장 장치에 저장된 동일한 데이터에 접근하기 위한 키를 사용하도록 허가하고, 상기 집합에 속하지 않는 실체들이 상기 저장 장치에 저장된 데이터에 접근하기 위한 키를 사용하지 못하도록 하는 데이터 보호 방법.

청구항 20

제 18 항에 있어서,

상기 하나 이상의 정책들은 하나 이상의 실체들의 제1 집합이 데이터를 암호화 및/또는 복호화하고 상기 저장 장치로부터 데이터를 기록하고 판독하기 위해 상기 키를 사용하도록 허가하고, 하나 이상의 실체들의 제2 집합이 상기 저장 장치 내의 데이터를 복호화하고 상기 복호화된 데이터를 판독하기 위해서만 상기 키를 사용하도록 허가하는 데이터 보호 방법.

청구항 21

제 18 항에 있어서,

상기 하나 이상의 정책들은 하나 이상의 실체들의 집합이 데이터를 암호화하고 상기 암호화된 데이터를 상기 저장 장치에 기록하는 경우에만, 상기 저장 장치 내의 데이터를 복호화하고 상기 복호화된 자료를 판독하는 경우에만, 또는 양자 모두의 경우에 상기 키를 사용하도록 허가하는 데이터 보호 방법.

청구항 22

제 18 항에 있어서,

상기 하나 이상의 정책들은 한 실체가 다른 실체의 상기 저장 장치로의 접근 권한들을 삭제하거나, 또는 상기 키를 이용하기 위한 다른 실체에 의한 접근을 금지하기 위해 상기 하나 이상의 정책들을 변경하는 것을 허가하며, 상기 다른 실체는 변경 이전에 그러한 접근이 허가되는 데이터 보호 방법.

청구항 23

제 18 항에 있어서,

상기 하나 이상의 정책들은 한 실체가 다른 실체에게 상기 키에 대한 접근 권한들을 위임하거나, 그러한 위임을 허가하기 위해 상기 하나 이상의 정책들을 변경하는 것을 허가하는 데이터 보호 방법.

청구항 24

제 18 항에 있어서,

상기 하나 이상의 정책들은 상기 저장 장치 또는 상기 키에 접근하기 위해 적어도 하나의 실체를 위한 보안 채널의 형성을 요구하는 데이터 보호 방법.

청구항 25

제 18 항에 있어서,

상기 하나 이상의 정책들은 상기 저장 장치 또는 상기 키에 접근하기 위한 보안 채널의 형성을 요구하는 데이터 보호 방법.

청구항 26

제 18 항에 있어서,

상기 하나 이상의 정책들은 제한된 수의 실체에 의해서만 상기 저장 장치 또는 상기 키로의 접근을 허가하는 데이터 보호 방법.

청구항 27

제 18 항에 있어서,

상기 하나 이상의 정책들은 실체가 인증되었는지에 상관없이, 제한된 수의 실체에 의해서만 상기 저장 장치 또는 상기 키로의 접근을 허가하는 데이터 보호 방법.

청구항 28

제 18 항에 있어서,

상기 하나 이상의 정책들은 상기 저장 장치 또는 상기 키에 접근하기 위해 적어도 하나의 실체를 위한 보안 채널의 형성을 요구하지 않는 데이터 보호 방법.

청구항 29

제 18 항에 있어서,

상기 저장 장치에,

상기 키의 사용을 위해 적용할 수 있는 추가 정책; 및

추가 키의 생성을 위한 요청 중 적어도 하나를 송신하는 단계를 더 포함하는 데이터 보호 방법.

청구항 30

제 18 항에 있어서,

상기 하나 이상의 정책들은 실체들의 서로 다른 집합들이 상기 키를 서로 다르게 사용하고 데이터로의 서로 다른 접근 권한들을 갖도록 허가하며, 상기 키의 서로 다른 사용은 암호화 및 복호화 중 하나 또는 모두를 포함하고, 상기 서로 다른 접근 권한들을 데이터의 판독 및 기록 중 하나 또는 모두를 포함하는 데이터 보호 방법.

청구항 31

제 18 항에 있어서,

상기 저장 장치로 상기 키와 상기 키로 암호화되어 상기 저장 장치에 저장된 파일을 연결한 조합을 송신하는 단계를 더 포함하는 데이터 보호 방법.

청구항 32

제 31 항에 있어서,

상기 저장 장치로 상기 키의 참조 이름 및 상기 파일을 판독하기 위한 요청을 송신하는 단계를 더 포함하는 데이터 보호 방법.

청구항 33

제 18 항에 있어서,

상기 저장 장치에, 하나의 실체에 의해 상기 저장 장치 내의 데이터로의 접근을 제어하기 위한 인증 요구 및 권한(들)을 각각 포함하는 두 개 이상의 레코드들을 송신하는 단계를 더 포함하며, 상기 두 개 이상의 레코드들은 인증 요구(들) 및 권한(들) 중 적어도 하나에서 서로 다른, 데이터 보호 방법.

청구항 34

제 33 항에 있어서,

상기 두 개 이상의 레코드들 각각은 대응하는 실체에 의해 상기 저장 장치의 파티션들(partitions)에 접근하기 위한 권한(들)을 포함하며, 파티션들에 접근하기 위한 적어도 두 개의 대응하는 실체들의 레코드 내의 권한(들)은 완전히 동일하지 않은 데이터 보호 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 일반적으로 메모리 시스템들에 관한 것으로, 특히 다기능 컨텐츠 제어가 가능한 메모리 시스템에 관한 것이다.

배 경 기 술

[0002] 컴퓨팅 장치 시장은 보다 많은 데이터의 교환을 야기함으로써 평균 수익을 증가시키기 위해 이동식 저장장치들의 컨텐츠 저장을 포함하는 방향으로 발전하고 있다. 이것은 이동식 저장 매체의 컨텐츠가 컴퓨팅 장치에서 사용될 때 보호되어야만 함을 의미한다. 컨텐츠는 가치 있는 데이터를 포함하는데, 상기 데이터들은 상기 저장장치를 제조하고 판매하는 자 이외의 다른 관계자에 의해 소유되는 데이터일 수 있다.

발명의 내용

해결 하고자하는 과제

[0003] 암호화 기능이 있는 저장장치의 일 예가 미국특허 번호 제6,457,126호에 개시되어 있다. 그러나 상기 장치에

의해 제공되는 기능은 상당히 제한적이다. 그러므로 보다 다기능의 컨텐츠 제어 특징들을 가진 메모리 시스템이 제공되는 것이 바람직하다.

과제 해결수단

[0004] 이동식 저장매체에서 컨텐츠의 보호는 상기 매체에서 데이터의 암호화와 관련되어 있어, 오직 승인된 사용자들 또는 애플리케이션들만이 상기 매체에 저장된 데이터를 암호화하기 위해 사용되는 키들에 접근할 수 있다. 일부 종래 시스템에서는, 데이터 암호화 및 복호화에 사용되는 키가 이동식 저장매체의 외부 장치들에 저장된다. 이러한 환경에서는 상기 컨텐츠에 독점적인 이권을 소유한 회사 또는 개인이 상기 매체의 컨텐츠의 사용을 많은 부분 제어하지 못할 것이다. 상기 매체의 데이터를 암호화하는데 사용되는 키가 상기 매체 외부에 존재하기 때문에, 이 키는 상기 컨텐츠 독점권자에 의해 제어되지 않는 방식으로 한 장치에서 다른 장치로 건네질 수 있다. 상기 독점적인 이권의 소유자는, 본 발명의 일 특징과 같이 상기 암호화-복호화 키가 매체 자체에 저장되거나 실질적으로 외부장치들이 접근할 수 없다면 상기 매체내의 컨텐츠에 대한 접근을 제어하기에 더 좋은 위치에 있게 될 것이다.

[0005] 상기 매체의 외부로부터 본질적으로 접근 불가능한 키를 생성함으로써, 이 특징은 보안된 컨텐츠에 휴대성(portability)을 제공한다. 따라서, 그러한 키로 암호화되어 보안된 컨텐츠를 포함하는 저장 장치는 상기 장치가 키에 대한 접근을 독점적으로 제어하기 때문에, 보안성 침해의 위험 없이 다양한 호스트 장치들에 의한 접근을 위해 사용될 수 있다. 적절한 크리덴셜들(credentials)을 가진 호스트 장치들만이 상기 키에 접근하는 것이 가능하다.

[0006] 이동식 저장매체에 저장된 컨텐츠의 상업적인 가치를 증가시키기 위해, 상기 컨텐츠의 독점적인 이권의 소유자는 상기 컨텐츠에 접근하기 위한 다른 실체(entity)들에게 서로 다른 권한들을 부여할 수 있도록 하는 것이 바람직하다. 그러므로 본 발명의 다른 특징은 상기 매체에 저장된 데이터에 접근하기 위한 서로 다른 권한들(예를 들어 서로 다른 승인된 실체들에게)을 부여하는 접근 정책이 저장될 수 있다는 인식에 기초한다. 상술한 두 개의 특징들의 조합을 통합하는 시스템이 보다 유리하다. 한편, 컨텐츠 소유자 또는 독점권자는 외부 장치들이 실질적으로 접근불가능한 키들을 이용하여 상기 컨텐츠로의 접근을 제어할 수 있고, 동시에 상기 매체의 컨텐츠에 접근하기 위한 다른 권한들을 부여할 수 있다. 따라서 외부 장치들이 접근에 성공하더라도, 그들의 접근은 여전히 상기 저장매체에 기록된 상기 컨텐츠 소유자 또는 독점권자에 의해 설정된 상기 다른 권한들의 집합에 의해 지배를 받을 수 있다.

[0007] 또한 다른 특징은 상술한 서로 다른 권한들이 서로 다른 승인된 실체들에게 부여된다는 정책이 플래시 메모리에 구현될 때, 이것은 특히 컨텐츠 보호를 위한 유용한 매체가 된다는 인식에 기초한다.

[0008] 많은 저장장치들은, 많은 컴퓨터 호스트 장치들이 파일형태로 데이터를 읽고 쓰는 동안 파일시스템을 인식하지 않는다. 다른 특징에 따라 상기 호스트 장치는, 상기 저장시스템이 상기 키 ID와 결합된 응답(response)에서 키 값을 생성하는 동안 키 참조 또는 ID를 제공한다. 여기서 상기 키 값은 상기 키 ID와 결합된 파일에서 데이터를 암호적으로 처리하는데 이용된다. 상기 호스트는 상기 키 ID와 상기 메모리 시스템에 의해 암호적으로 처리되는 상기 파일을 결합시킨다. 따라서 상기 키 ID는, 호스트가 파일들의 제어를 유지하는 동안 상기 메모리가 암호화 프로세스들을 위한 키 값의 생성 및 이용에 대한 완전하고 독점적인 제어를 유지하는 핸들로서 컴퓨팅 장치 및 메모리에 의해 이용된다.

[0009] 스마트카드와 같은 일부 이동식 저장장치들에서, 상기 카드 컨트롤러는 파일 시스템을 관리한다. 플래시 메모리, 자기 또는 광학 디스크와 같은 이동식 저장장치들의 많은 다른 유형들에서, 상기 장치 컨트롤러는 파일 시스템을 인식하지 않는 대신, 상기 장치 컨트롤러는 상기 파일 시스템을 관리하기 위해 호스트 장치(예를 들어 개인용 컴퓨터, 디지털 카메라, MP3플레이어, 개인휴대단말기(PDA), 휴대폰)에 의존한다. 본 발명의 다양한 측면들은 상기 장치 컨트롤러가 파일 시스템을 인식하지 않는 이런 유형의 저장장치들과 쉽게 통합될 수 있다. 이것은, 그러한 장치들에서 상기 장치 컨트롤러가 파일 시스템을 인식하고 관리하도록 만들기 위해, 본 발명의 다양한 측면들이 그러한 장치들을 재 디자인(re-design)할 필요 없이 널리 다양하게 존재하는 이동식 저장장치들에 적용될 수 있음을 의미한다.

[0010] 저장 매체에 저장된 트리 구조는 접근에 성공한 후에도 실체가 할 수 있는 것에 대한 제어가 가능하게 한다. 상기 트리의 각 노드들은 상기 트리의 그러한 노드를 통해 진입이 이루어진 실체에 의한 권한들을 특정한다. 일부 트리들은 서로 다른 레벨들을 갖는데, 상기 트리의 어느 한 노드에서의 상기 권한 또는 권한들은 동일 트리에서 더 높거나 더 낮거나 동일한 레벨의 다른 노드에서의 권한 또는 권한들과 미리 정해진 관계를 가진다. 상기 노

드들 각각에 특정된 권한들에 따를 것을 실체들에게 요구함으로써, 본 출원의 상기 트리의 특징은 상기 트리가 서로 다른 레벨을 갖는 것과 무관하게 컨텐츠 소유자가 어느 실체가 액션(action)할 수 있는지 및 각 실체들이 취할 수 있는 액션들을 제어할 수 있게 한다.

[0011] 이동식 저장매체에 의해 제공될 수 있는 상업적 가치를 높이기 위해, 이동식 저장장치가 동시에 하나 이상의 애플리케이션을 지원할 수 있는 것이 바람직하다. 두 개 이상의 애플리케이션들이 동시에 이동식 저장장치에 접근하고자 할 때, 그들이 여기서 크로스토크(crosstalk)로 언급되는 현상에서 서로 저촉하지 않도록 상기 두 개 이상의 애플리케이션들의 동작들을 분리할 수 있는 것이 중요할 수 있다. 그러므로 본 발명의 다른 특징은 바람직하게는 계층적인 두 개 이상의 트리들이 상기 메모리로의 접근을 제어하기 위해 제공될 수 있다는 인식에 기초한다. 각각의 트리는, 실체들의 대응하는 집합에 의해 데이터에 접근하는 것을 제어하기 위한 서로 다른 레벨들을 가진 노드들을 포함하는데, 각 트리의 어느 한 노드는 상기 대응하는 실체 또는 실체들의 메모리 데이터에 대한 접근의 권한 또는 권한들을 특정한다. 상기 트리들 각각의 한 노드에서의 권한 또는 권한들은 동일 트리에서 더 높거나 더 낮은 레벨의 다른 노드에서의 권한 또는 권한들과 미리 정해진 관계를 가진다. 상기 두 개 이상의 트리들 사이에서 크로스토크는 없는 것이 바람직하다.

[0012] 이상으로부터, 트리들이 컨텐츠 보안을 위해 사용될 수 있는 강력한 구조들임이 명백하게 될 것이다. 제공되는 중요한 제어들 중의 하나는 트리의 생성에 대한 제어이다. 따라서, 본 발명의 다른 특징에 따른, 상기 이동식 저장장치는 대응하는 실체들에 의해 상기 메모리에 저장된 데이터로의 접근을 제어하기 위한 서로 다른 레벨들에서의 노드들을 포함하는 적어도 하나 이상의 계층적 트리를 생성할 수 있는 시스템 에이전트가 구비될 수 있다. 상기 트리의 각 노드는 메모리 데이터를 접근하기 위한 대응하는 실체 또는 실체들의 권한 또는 권한들을 특정한다. 상기 트리들 각각의 노드에서의 권한 또는 권한들은 동일한 트리에서 더 높거나 더 낮거나 동일한 레벨에서의 노드들의 권한 또는 권한들과 미리 정해진 관계를 갖는다. 따라서, 상기 장치들의 구매자가 본인이 의도하는 애플리케이션에 적합한 계층적 트리들을 자유재량으로 생성하도록, 상기 이동식 저장 장치들은 어떤 트리도 미리 생성됨 없이 배포될 수 있다. 대안적으로, 구매자가 상기 트리들을 생성하는 수고를 겪지 않도록, 상기 이동식 저장장치들은 또한 미리 생성된 트리들을 가진 상태로 배포될 수 있다. 상기 양 경우에서, 그들이 더 이상 변화되거나 변경될 수 없도록, 상기 트리들의 특정 기능성들이 상기 장치들이 제조된 후에 고정될 수 있도록 하는 것이 바람직하다. 이것으로 상기 컨텐츠 소유자에 의한 장치들의 컨텐츠로의 접근에 대한 더 우수한 제어들이 가능하게 된다. 따라서, 일 실시예에서 추가적인 트리들이 생성될 수 없도록, 상기 시스템 에이전트는 불능(디세이블)하게 될 수 있는 것이 바람직하다.

[0013] 일부 이동식 저장 장치들에서는, 컨텐츠 보호가 보호된 영역들에 대한 접근이 사전 인증을 요구하는 분리된 영역들로 상기 메모리를 구분함으로써 이루어진다. 그러한 특징에 의해 일부 보호가 가능한 반면, 불법적인 수단으로 패스워드를 얻어낸 사용자에 대해서는 보호가 되지 않는다. 따라서 본 발명의 다른 측면은, 메모리를 파티션들(partitions)로 구분하는 메커니즘 또는 구조가 제공될 것이고, 그럼으로써 상기 파티션들 내의 적어도 일부 데이터는 키로 암호화될 것이며, 상기 파티션들의 일부에 접근하기 위해 요구되는 인증에 부가하여 하나 이상의 키들에 대한 접근이 그러한 파티션들에서 상기 암호화된 데이터를 복호화하기 위해 요구될 수 있다는 인식에 기초한다.

[0014] 일부 애플리케이션들에서는, 사용자가 상기 메모리 시스템에 하나의 애플리케이션을 이용하여 로그인할 수 있고, 그 후 다시 로그인하지 않고 보호된 컨텐츠에 접근하기 위한 다른 애플리케이션들을 이용할 수 있는 것이 보다 편리하다. 그러한 경우에서, 사용자가 이러한 방식으로 접근하기 원하는 모든 컨텐츠는 제 1 어카운트와 결합될 수 있고, 그 결과 모든 그러한 컨텐츠는 여러 번 로그인하지 않고 다른 애플리케이션(예를 들어 뮤직 플레이어, 이메일, 셀룰라 이동통신 등)을 통해 접근될 수 있다. 그 다음 인증 정보의 다른 집합은, 상기 다른 어카운트들이 동일한 사용자 또는 실체를 위한 것인 경우라도 상기 제 1 어카운트와는 다른 어카운트에 있는 보호되는 컨텐츠에 접근하기 위해 로그인 하는데 이용될 수 있다.

[0015] 더 우수한 다기능성 제어 및/또는 컨텐츠 소유자를 위한 보호를 제공하기 위해, 상술한 특징들은 저장시스템에서 개별적으로 또는 임의의 조합으로 결합되어 이용될 수 있다.

효 과

[0016] 매체의 외부로부터 접근불가능한 키로 암호화되어 보안된 컨텐츠를 포함하는 저장 장치는 상기 장치가 키에 대한 접근을 독점적으로 제어하기 때문에, 보안성 침해의 위험 없이 다양한 호스트 장치들에 의한 접근을 위해 사용될 수 있으므로, 적절한 크리덴셜들을 가진 호스트 장치들만이 상기 키에 접근하는 것이 가능하다.

[0017] 컨텐츠의 독점적인 이권의 소유자는 컨텐츠에 접근하기 위한 다른 실체들에서 서로 다른 권한들을 부여하여, 이동식 저장 매체에 저장된 컨텐츠의 상업적인 가치를 증가시킬 수 있게 된다. 또한 이것이 플래시 메모리에 구현되는 경우 컨텐츠 보호를 위해 유용한 매체가 될 수 있다.

[0018] 따라서 더 우수한 다기능성 제어 및/또는 컨텐츠 소유자를 위한 보호를 본 발명을 통해 제공할 수 있으므로, 본 발명은 다기능 컨텐츠 제어 특징을 가진 메모리 시스템을 제공한다.

[0019] 본 발명에 따른 실시예들은 첨부된 도면을 참조하여 이하에서 상세히 설명한다.

발명의 실시를 위한 구체적인 내용

[0020] 본 발명의 다양한 측면들이 구현될 수 있는 예시적인 메모리 시스템이 도 1의 블록 다이어그램에 의해 도시되어 있다. 도 1에 도시된 바와 같이, 상기 메모리 시스템(10)은 중앙처리장치(CPU, 12), 버퍼관리장치(BMU, 14), 호스트 인터페이스 모듈(HIM, 16) 및 플래시 인터페이스 모듈(FIM, 18), 플래시 메모리(20) 및 주변장치 접근 모듈(PAM, 22)을 포함한다. 메모리 시스템(10)은 호스트 인터페이스 버스(26) 및 포트(26a)를 통해 호스트장치(24)와 통신한다. NAND유형이 될 수 있는 상기 플래시메모리(20)는 상기 호스트 장치(24)를 위해 데이터 저장장치를 제공한다. 상기 CPU(12)를 위한 소프트웨어 코드도 또한 플래시메모리(20)에 저장될 수 있다. FIM(18)은 플래시 인터페이스 버스(28) 및 포트(28a)를 통해 상기 플래시메모리(20)와 접속된다. HIM(16)은, 디지털 카메라, 개인용 컴퓨터, 개인휴대단말기(PDA), 디지털 미디어 플레이어, MP-3플레이어, 휴대폰 또는 다른 디지털 장치들과 같은 호스트 시스템과의 접속을 위해 적합하다. 상기 주변장치 접근 모듈(22)은 상기 CUP(12)와 통신을 위해 FIM, HIM 및 BMU와 같은 적절한 컨트롤러모듈을 선택한다. 일 실시예에서, 상기 점선 박스 안에 시스템(10)의 모든 구성요소들이 메모리 카드 또는 스틱(10’)과 같은 하나의 유닛에 포함될 수 있고, 바람직하게는 캡슐화될 수 있다.

[0021] 여기서 본 발명은 플래시 메모리들을 참조하여 도시되기는 하나, 본 발명은 또한 모든 다른 유형의 재기록 가능한 비휘발성 메모리 시스템들뿐만 아니라 자기디스크, 광학 CD들과 같은 다른 유형의 메모리들에도 적용할 수도 있다.

[0022] 상기 버퍼관리장치(14)는 호스트 직접 메모리 접근(HDMA, 32), 플래시 직접 메모리 접근(FDMA, 34), 중재기(36), 버퍼 랜덤 접근 메모리(BRAM,38) 및 크립토-엔진(40)을 포함한다. 상기 중재기(36)는 공유 버스 중재기이고, 그 결과 오직 하나의 마스터 또는 개시자(initiator)[HDMA(32), FDMA(34), 또는 CPU(12)가 될 수 있음]가 일정 시점에서 활성화될 수 있고, 종속장치(slave) 또는 타겟은 BRAM(38)이다. 상기 중재기는 BRAM(38)에 적절한 개시자 요청의 채널링을 책임지고 있다. 상기 HDMA(32) 및 FDMA(34)는 HIM(16), FIM(18) 및 BRAM(38) 또는 CPU 랜덤 접근 메모리(CPU RAM, 12a) 사이에서 송신된 데이터를 책임지고 있다. HDMA(32) 및 FDMA(34)의 동작은 일반적이므로 여기서 상세하게 기술할 필요가 없다. BRAM(38)은 호스트장치(24)와 플래시메모리(20) 사이에서 통과된 데이터를 저장하는데 이용된다. HDMA (32) 및 FDMA (34)는 HIM(16)/FIM(18)와 BRAM(38) 또는 CPU RAM(12a) 사이에서 데이터를 송신하고 섹터 완료(sector completion)를 지시하는 것을 책임지고 있다.

[0023] 메모리(20)에 저장된 컨텐츠의 보안성을 향상시키기 위해, 메모리 시스템(10)은 암호화 및/또는 복호화를 위해 이용되는 키 값(들)을 생성하는데, 이 값(들)은 실질적으로 호스트장치(24)와 같은 외부 장치들이 접근할 수 없다. 그러나 호스트장치가 메모리 시스템(10)에 파일형태로 데이터를 읽고 쓰기 때문에, 암호화 및 복호화는 전형적으로 파일단위로 이루어진다. 많은 다른 유형의 저장장치들과 같이, 메모리 장치(10)는 파일들 또는 파일 시스템들을 인식하지 않는다. 메모리(20)가 파일들의 논리주소들이 식별되는 파일 할당 테이블(FAT)을 저장하는 반면, FAT는 전형적으로 컨트롤러(12)에 의해서가 아니라 호스트장치(24)에 의해서 접근되고 관리된다. 그러므로 특정 파일에서 데이터를 암호화하기 위해, 컨트롤러(12)는 메모리(20)의 파일에 있는 데이터의 논리주소들을 송신하기 위해 호스트장치에 의존해야만 할 것이다. 그 결과 특정 파일의 데이터는 오직 시스템(10)만이 이용할 수 있는 키 값(들)을 이용하여 시스템(10)에 의해 발견되고 암호화 및/또는 복호화될 수 있게 된다.

[0024] 파일들에 있는 데이터를 암호적으로 처리하기 위한 동일 키(들)를 참조하는 호스트장치(24) 및 메모리 시스템(10) 모두를 위한 핸들을 제공하기 위해, 호스트장치는 시스템(10)에 의해 생성된 키 값들 각각에 대한 참조를 제공하는데, 이러한 참조는 단순하게 키 ID일 수 있다. 따라서 호스트(24)는 키 ID와 시스템(10)에 의해 암호적으로 처리된 각각의 파일을 결합시키고, 시스템(10)은 호스트에 의해 제공되는 키 ID와 암호적으로 데이터를 처리하기 위해 이용되는 각각의 키 값을 결합시킨다. 따라서, 호스트가 파일이 암호적으로 처리되는 것을 요청할 때, 메모리(20)로부터 인출(fetch)되거나 메모리(20)에 저장될 데이터의 논리주소들과 함께 키 ID를 가진 요청이 시스템(10)으로 송신될 것이다. 시스템(10)은 키 값을 생성하고, 상기 값과 호스트(24)에 의해 제공되는 키

ID를 결합시켜서, 암호화 처리를 수행한다. 이러한 방식에서, 키 값(들)에 대한 독점적인 접근을 포함하여 키(들)를 이용하는 암호화 처리를 완전히 제어하도록 허용되는 동안 메모리 시스템(10)이 동작되는 방식에서 만들어지는 어떠한 변경도 필요로 하지 않는다. 바꾸어 말하면, 시스템(10)은 암호화 처리를 위해 이용되는 키 값(들)의 생성 및 관리를 위한 독점적인 제어를 유지하는 반면에, 호스트(24)가 FAT의 독점적인 제어를 가지고 파일들을 관리하는 것을 허용한다. 호스트 장치(24)는 데이터의 암호화처리를 위해 이용되는 키 값(들)의 생성 및 관리에 참여하지 않는다.

[0025] 호스트(24)에 의해 제공되는 키 ID 및 메모리 시스템에 의해 생성되는 키 값은 일 실시예들 중 하나에서 "컨텐츠 암호화 키" 또는 CEK로서 하기에서 언급되는 두 개의 양적 속성(attribute of quantity)을 형성한다. 호스트(24)가 하나 이상의 파일들과 각각의 키 ID를 결합시키는 반면, 호스트(24)는 또한 조직화되지 않는 데이터 또는 임의의 방식으로 조직화된 데이터와 각각의 키 ID를 결합시킬 수도 있으며, 완전한 파일들로 조직화되는 데이터로 제한되는 것은 아니다.

[0026] 사용자 또는 애플리케이션이 시스템(10)내의 보호되는 컨텐츠 또는 영역에 접근할 수 있도록 하기 위해, 시스템(10)에 의해 사전등록된 크리덴셜을 이용하여 인증되는 것이 필요할 것이다. 크리덴셜은 그러한 크리덴셜에 의해 특정 사용자 또는 애플리케이션에 부여되는 접근 권한들(access rights)과 관련되어 있다. 사전등록 처리에서, 시스템(10)은 사용자 또는 애플리케이션의 식별자(identity)와 크리덴셜, 및 접근 권한의 레코드를 저장하고, 접근 권한은 사용자 또는 애플리케이션에 의해 결정되고 호스트(24)를 통해 제공되는 그러한 식별자 및 크리덴셜과 결합된다. 사전 등록이 완료된 후에, 사용자 또는 애플리케이션이 메모리(20)에 데이터 쓰기를 요청할 때, 호스트 장치를 통해 그것의 식별자 및 크리덴셜, 데이터를 암호화하기 위한 키 ID, 및 암호화된 데이터가 저장되는 논리주소들이 제공될 필요가 있을 것이다. 시스템(10)은 키 값을 생성하고 호스트장치에 의해 제공된 키 ID와 이 키 값을 결합시키며, 쓰여질 데이터를 암호화하는데 이용된 키 값에 대한 키 ID를 이 사용자 또는 애플리케이션을 위해 그것의 레코드 또는 테이블에 저장한다. 다음 데이터를 암호화하고, 호스트에 의해 지정된 주소들에 생성된 키 값 뿐만 아니라 암호화된 데이터를 저장한다.

[0027] 사용자 또는 애플리케이션이 메모리(20)로부터 암호화된 데이터를 읽기를 요청할 때, 그것의 식별자 및 크리덴셜, 요청된 데이터를 암호화하는데 이전에 이용된 키에 대한 키 ID 및 암호화된 데이터가 저장된 논리주소들이 제공될 필요가 있다. 다음 시스템(10)은 호스트에 의해 제공된 사용자 또는 애플리케이션의 식별자 및 크리덴셜과, 시스템의 레코드에 저장된 것들이 일치하는지 대조할 것이다. 일치되면, 그 다음 시스템(10)은 메모리로부터 사용자 또는 애플리케이션에 의해 제공된 키 ID에 결합되는 키 값을 인출하고, 키 값을 이용하여 호스트 장치에 의해 지정된 주소들에 저장된 데이터를 복호화하여, 사용자 또는 애플리케이션으로 복호화된 데이터를 송신하게 된다.

[0028] 암호화 처리에 이용되는 키들의 관리와 크리덴셜을 분리함으로써, 크리덴셜들의 공유없이 데이터에 접근하는 권한들을 공유하는 것이 가능해진다. 따라서 다른 크리덴셜을 가진 사용자들 또는 애플리케이션들의 한 그룹이 동일 데이터에 접근하기 위한 동일 키들에 접근할 수 있다. 반면, 이 그룹에 속하지 않는 사용자들은 접근할 수 없다. 한 그룹내의 모든 사용자들 또는 애플리케이션들이 동일 데이터에 접근할 수 있지만, 그들은 여전히 다른 권한들을 가질 수 있다. 따라서 일부는 읽기만 가능한 접근을 갖고, 반면 다른 사람들은 쓰기만 가능한 접근을 가지거나 다른 사람들은 읽기 및 쓰기가 모두 가능한 접근을 가질 수 있다. 시스템(10)이 사용자들 또는 애플리케이션의 식별자들 및 크리덴셜들, 그들이 접근할 수 있는 키 ID들 및 각각의 키 ID들에 결합되는 접근 권한의 레코드를 유지하기 때문에, 모든 것이 정당하게 인증된 호스트장치에 의해 제어되는 것처럼, 시스템(10)이 키 ID들을 추가 또는 제거하고 특정 사용자들 또는 애플리케이션들을 위한 그러한 키 ID들과 결합된 접근 권한를 변경하는 것이 가능하고, 한 사용자 또는 애플리케이션에서 다른 사용자 또는 애플리케이션으로 접근 권한을 위임하거나 심지어 사용자들 또는 애플리케이션들을 위한 레코드들 또는 테이블들을 제거하거나 추가하는 것이 가능하다. 저장된 레코드는 특정 키들을 접근하는데 보안 채널이 요청되는 것을 특정할 것이다. 인증은 패스워드 뿐 아니라 대칭적 또는 비대칭적 알고리즘을 이용하여 이루어질 것이다.

[0029] 메모리 시스템(10)에서 보안된 컨텐츠의 휴대성(portability)이 특히 중요하다. 키 값이 메모리 시스템에 의해 생성되고 실질적으로 외부 시스템들이 이용할 수 없기 때문에, 메모리 시스템 또는 상기 시스템과 통합된 저장 장치가 한 외부시스템에서 다른 외부시스템으로 송신될 때, 그 안에 저장된 컨텐츠의 보안성이 유지되고, 외부 시스템들은 그들이 메모리 시스템에 의해 완전히 제어되는 방식으로 인증되지 않는다면 그러한 컨텐츠에 접근할 수 없다. 심지어 그러한 인증 후에도 접근은 전적으로 메모리 시스템에 의해 제어되고 외부 시스템들은 메모리 시스템의 사전설정된 레코드들에 따라 제어되는 방식으로만 접근할 수 있다. 만약 요청이 그러한 레코드들에 따

르지 않으면 요청은 거부될 것이다.

[0030] 보호되는 컨텐츠에서 더 우수한 융통성을 제공하기 위하여, 하기에서 파티션들로서 언급되는 메모리의 특정영역은 정당하게 인증된 사용자들 또는 애플리케이션들만이 접근할 수 있는 것으로 계획된다. 키 기반 데이터 암호화의 상술한 특징들이 결합될 때, 시스템(10)은 더 우수한 데이터 보호기능을 제공한다. 도 2에 도시된 바와 같이 플래시메모리(20)는 복수의 파티션들, 즉 사용자 영역 또는 파티션 및 커스텀 파티션들(custom partitions)로 구분된 저장용량을 가질 수 있다. 사용자 영역 또는 파티션들 P0는 모든 사용자들 및 애플리케이션들이 인증없이 접근할 수 있다. 사용자 영역에 저장된 데이터 모든 비트 값들은 임의의 애플리케이션 또는 사용자에 의해 읽거나 쓰여질 수 있는 반면, 읽혀진 데이터가 암호화되면, 복호화에 대한 승인이 없는 사용자 또는 애플리케이션은 사용자 영역에 저장된 비트 값들에 의해 표현되는 정보에 접근할 수 없다. 예를 들어, 이것은 사용자 영역 P0에 저장된 파일들 102 및 104에 의해 도시된다. 또한 모든 애플리케이션들 또는 사용자들에 의해 읽혀지고 이해될 수 있는 106과 같은 암호화되지 않은 파일들은 사용자 영역에 저장된다. 따라서 파일들 102 및 104와 같은 암호화된 파일들은 상징적으로 관련되는 자물쇠와 함께 도시되어 있다.

[0031] 사용자 영역 P0의 암호화된 파일은 인증되지 않은 애플리케이션들 또는 사용자들에 의해 이해될 수 없지만, 그러한 애플리케이션들 또는 사용자들은 여전히 파일을 제거 또는 손상시킬 수 있는데, 이것은 일부 애플리케이션들에 바람직하지 않다. 이를 방지할 목적을 위해, 메모리(20)는 또한 사전 인증 없이 접근할 수 없는 파티션들 P1 및 P2와 같은 보호되는 커스텀 파티션들을 포함한다. 이 출원의 실시예에서 허가되는 인증 처리는 후술한다.

[0032] 또한 도 2에 도시된 바와 같이, 다양한 사용자들 또는 애플리케이션들이 메모리(20)의 파일들에 접근할 것이다. 따라서 사용자 1 및 2 및 (장치들 상에서 실행되는) 애플리케이션 1 내지 4가 도 2에 도시된다. 이들 실체들이 메모리(20)의 보호된 컨텐츠에 접근하는 것이 허락되기 전에, 그들은 먼저 후술하는 방식으로 인증 프로세스에 의해 인증된다. 이 프로세스에서, 접근을 요청하는 실체는 역할 기반 접근 제어를 위해 호스트 측에서 식별될 필요가 있다. 따라서 접근을 요청하는 실체는 먼저 "나는 애플리케이션 2 이고 파일1을 읽기 원하다"와 같은 정보를 제공함으로써 실체 자체를 식별시킨다. 컨트롤러(12)는 그 후 식별자, 인증정보 및 요청을 메모리(20) 또는 컨트롤러(12)에 저장된 레코드와 일치여부를 대조한다. 모든 요구조건이 충족되면, 상기 실체에 대해 접근이 승인된다. 도 2에 도시된 바와 같이, 사용자1은 파티션P1의 파일 101을 읽고 쓸 수 있도록 허락되었으나, 파일 102 및 104는 읽기만 할 수 있고, 또한 P0의 파일들 106은 읽고 쓸 수 있는 무제한적인 권한들을 갖는다. 반면 사용자2는 파일101 및 104에 접근이 허용되지 않지만, 파일102는 읽고 쓸 수 있게 접근이 가능하다. 도 2에서 나타난 바와 같이, 사용자1 및 2는 동일한 로그인 알고리즘(AES)을 갖지만, 애플리케이션 1 및 3은 다른 로그인 알고리즘(예를 들어 RSA 및 001001)을 갖는데, 이것은 사용자1 및 2의 알고리즘들과도 다르다.

[0033] 보안 저장 애플리케이션(SSA)은 메모리 시스템(10)의 보안성 애플리케이션이고, 본 발명의 일 실시예를 보여주는데, 이것은 상기에서 명백해진 많은 특징들을 구현하는데 사용될 수 있다. SSA는 메모리(20) 또는 CPU(12)의 비휘발성 메모리(미도시)에 저장되는 데이터베이스를 갖는 소프트웨어 또는 컴퓨터코드로서 구체화될 수 있고, RAM(12a)으로 읽혀져 CPU(12)에 의해 실행된다. SSA와 관련되어 이용되는 두문자어들이 하기 테이블에서 설명된다.

[0034] 정의, 두문자어 및 약어

[0035]

ACR	접근 제어 레코드 (Access Control Records)
AGP	ACR 그룹 (ACR Group)
CBC	체인 블록 암호문 (Chain Block Cipher)
CEK	컨텐츠 암호화 키 (Content Encryption Key)
ECB	전자 코드북 (Electric Codebook)
ACAM	ACR 속성 관리 (ACR Attributes Management)
PCR	권한 제어 레코드 (Permissions Control Record)
SSA	보안 저장장치 애플리케이션 (Secure Storage Application)
실체(Entity)	상기 SSA에 로그인 되고 그 기능성을 이용하는 실제하고 개별적인 존재(호스트 측)를 갖는 임의의 것

[0036] **SSA 시스템 설명**

[0037] 데이터 보안성, 무결성 및 접근 제어는 SSA의 주요한 역할이다. 데이터는 일정 종류의 대량-저장 장치에 다른 방법으로 평이하게 저장되는 파일들이다. SSA 시스템은 저장시스템의 맨 위에 위치하고, 저장된 호스트 파일들

을 위한 보안성 계층들을 추가한다.

[0038] SSA의 주된 임무는 메모리에 저장된(그리고 보안된) 컨텐츠와 결합되는 다른 권한들을 관리하는 것이다. 메모리 애플리케이션은 다양한 사용자들 및 저장된 다양한 컨텐츠에 대한 접근 권한들을 관리하는 것이 필요하다. 호스트 애플리케이션들은 그들 측에서 그러한 애플리케이션들에게 보여지는 드라이브들 및 파티션들과, 저장장치상의 저장된 파일들의 위치들을 관리하고 표시하는 파일 할당 테이블들(FATs)을 참조한다.

[0039] 이 경우 저장 장치는 파티션들로 구분된 NAND 플래시 칩을 사용하지만, 다른 이동식 저장 장치들 또한 본 발명의 범위 내에서 사용될 수 있다. 이들 파티션들은 논리주소들의 연속적 스레드이고, 시작 주소 및 종료 주소는 그들의 경계를 정의한다. 그러므로 숨겨진 파티션들로의 접근에 필요하다면 소프트웨어[메모리(20)에 저장되는 소프트웨어와 같은]에 의한 제한들이 부과될 수 있는데, 그 소프트웨어는 그러한 제한들을 경계 내의 주소들과 결합시킨다. 파티션들은 SSA에 의해 관리되는 그들의 논리주소 경계들에 의해, SSA에 완전히 인식된다. SSA 시스템은 승인되지 않은 호스트 애플리케이션들로부터 데이터를 물리적으로 보안하기 위해 파티션들을 사용한다. 호스트에게 파티션들은 데이터 파일들을 저장하기 위한 독점적인 공간을 정의하는 메커니즘이다. 이들 파티션들은 공용(public)이거나 전용 또는 숨겨진(private or hidden) 것일 수 있는데, 공용 파티션은 저장장치에 접근한 누구나 볼 수 있고 장치상에 파티션들의 존재를 인식할 수 있는 파티션이고, 전용 또는 숨겨진 파티션은 선택된 호스트 애플리케이션들만이 접근하고 저장장치 상의 그들의 존재를 인식할 수 있는 파티션이다.

[0040] 도 3은 메모리의 파티션들, P0, P1, P2 및 P3(4보다 더 적거나 더 많은 파티션들이 채택될 수 있는 것은 명백하다)을 도시한 메모리의 개략도이다. 여기서 P0는 인증 없이 어느 실체에 의해서도 접근될 수 있는 공용 파티션이다.

[0041] 전용 파티션(P1, P2 또는 P3과 같은)은 그 안의 파일들로의 접근을 숨긴다. 호스트가 파티션에 접근하는 것을 방해함으로써, 플래시 장치(예를 들어 플래시 카드)는 파티션 내부의 데이터 파일들을 보호한다. 그러나, 이러한 종류의 보호는 파티션 안에서 논리주소들에 저장된 데이터로의 접근에 대해 제한들을 부과함으로써, 숨겨진 파티션 내에 위치한 모든 파일들을 감싼다. 바꿔 말하면, 제한들은 일련의 논리주소들과 결합된다. 상기 파티션에 접근한 모든 사용자들/호스트들은 내부의 파일들 모두에 무제한적으로 접근할 수 있게 될 것이다. 다른 파일들 또는 파일들의 그룹들을 서로 분리하기 위해, SSA 시스템은 키들 및 키 참조들 또는 키 ID들을 이용하여, 파일마다 또는 파일들의 그룹마다 서로 다른 수준의 보안성 및 무결성을 제공한다. 다른 메모리 주소들에서 데이터를 암호화하기 위해 사용되는 특정 키 값의 키 참조 또는 키 ID는, 암호화된 데이터를 포함하는 컨테이너 또는 도메인과 유사하다. 이러한 이유로 도 4에서 키 참조들 또는 키 ID들(예를 들어 “키 1” 및 “키 2”)이 키 ID들과 결합되는 키 값들을 이용하여 암호화된 파일들을 둘러싸는 영역들로서 도식적으로 보여진다.

[0042] 도 4를 참조하면, 예를 들어 파일 A가 어떤 키 ID에 의해서도 둘러싸이지 않도록 도시되어 있기 때문에, 어떤 인증 없이도 모든 실체들이 접근할 수 있는 것이다. 심지어 공용 파티션내의 파일 B는 모든 실체들에 의해 읽거나 덮어쓰는 것이 가능함에도 불구하고, ID "키 1"을 가진 키로 암호화된 데이터를 포함한다. 그 결과 파일 B에 포함된 정보는 실체가 상기 키에 접근할 수 없다면, 해당 실체가 접근할 수 없다. 이러한 방식으로 키 값들 및 키 참조들 또는 키 ID들을 이용하는 것은 상술한 파티션에 의해 제공되는 유형의 보호와는 반대로 논리적인 보호만을 제공한다. 그러므로, 파티션(공용 또는 전용)에 접근할 수 있는 어떤 호스트도 암호화된 데이터를 포함하여 모든 파티션내의 데이터를 읽거나 쓸 수 있다. 하지만 데이터가 암호화되기 때문에 승인되지 않은 사용자들은 그것에 오류를 일으킬 수만 있다. 바람직하게는 그들이 발견되지 않고 데이터를 변경하거나 사용할 수 없는 것이다. 암호화 및/또는 복호화 키들로의 접근을 제한함으로써, 이 특징은 승인된 실체들만이 데이터를 이용하는 것을 허용할 수 있다. 또한 P0에서 파일B 및 C도 키 ID "키 2"를 갖는 키를 사용하여 암호화된다.

[0043] 데이터 기밀성 및 무결성은, 컨텐츠 암호화키들(CEK), CEK 당 하나를 이용하는 대칭적 암호화 방법들을 통해 제공될 수 있다. SSA 실시예에서, CEK들이 플래시 장치(예를 들어 플래시 카드)에 의해 생성되고, 내부적으로만 사용되며, 외부에 대해서는 비밀로서 유지된다. 또한 암호화되거나 암호문으로 쓰여진 데이터는 데이터 무결성을 보장하기 위해 해시(hashed)되거나 체인 블록화(Chain blocked)된다.

[0044] 파티션내의 데이터 모두가 다른 키들에 의해 암호화되고 다른 키 ID들과 결합되는 것은 아니다. 공용 또는 사용자 파일들 또는 동작 시스템 영역(즉, FAT) 중 어느 하나의 특정 논리주소들이 임의의 키 또는 키 참조와 결합되지 않고, 따라서 파티션 자체에 접근할 수 있는 임의의 실체가 이용할 수 있다.

[0045] 그들로부터 데이터를 읽고 쓰거나 키들을 이용할 뿐만 아니라 키들 및 파티션들을 생성하는 능력을 요구하는 실체는, 접근제어레코드(ACR)를 통해 SSA 시스템에 로그인해야 한다. SSA 시스템 내에서 ACR의 특권들은 액션들

(Actions)로 불린다. 모든 ACR은 다음 3개의 범주의 액션들, 즉 파티션들 및 키들/키 ID들의 생성, 파티션들 및 키들로의 접근 및 다른 ACR들의 생성/업데이팅의 액션들을 수행하기 위한 권한들을 가질 수 있다.

[0046] ACR들은 ACR 그룹들 또는 AGP들로 불리는 그룹들로 조직화된다. 일단 ACR이 성공적으로 인증되면, SSA 시스템은 ACR의 액션들 중 어느 하나가 실행될 수 있도록 세션(Session)을 개방한다.

[0047] 사용자 파티션(들)

[0048] SSA 시스템은 사용자 파티션(들)로도 언급되는 하나 이상의 공용 파티션들을 관리한다. 이 파티션은 저장장치에 존재하고, 저장장치의 표준적인 읽기 쓰기 명령들을 통해 접근될 수 있는 파티션 또는 파티션들이다. 장치에서 그것의 존재뿐만 아니라 파티션(들)의 크기에 관한 정보를 얻는 것이 호스트 시스템으로부터 숨겨질 수 없는 것이 바람직하다.

[0049] SSA 시스템은 표준적인 읽기 쓰기 명령들 또는 SSA 명령들 중 어느 하나를 통해 이 파티션(들)에 접근하는 것을 가능하게 한다. 그러므로 바람직하게는 이 파티션으로의 접근이 특정 ACR들에 대해 제한될 수 없다. 하지만 SSA 시스템은 호스트 장치들이 사용자 파티션에 대해 접근하는 것을 제한할 수 있다. 읽기 및 쓰기 접근은 개별적으로 가능할 수도 있고 불가능할 수도 있다. 4개의 조합들(예를 들어 쓰기만, 읽기만(쓰기 보호), 읽기 및 쓰기, 및 접근 불가) 모두가 허용된다.

[0050] SSA 시스템은 ACR들이 사용자 파티션 내에서 파일들과 키 ID들을 결합시키고 그러한 키 ID들과 결합된 키들을 이용하여 개별적인 파일들을 암호화시킬 수 있다. 파티션들로의 접근 권한을 설정하는 것뿐만 아니라 사용자 파티션들 내에서 암호화된 파일에 접근하는 것은, SSA 명령어 집합(SSA 명령들의 상세한 설명은 첨부A를 참조-상기 첨부 내에서 키 ID는 "도메인"으로 언급된다)을 사용하여 이루어질 것이다. 또한 상술한 특징들은 파일들로 조직화되지 않은 데이터에도 적용된다.

[0051] SSA 파티션들

[0052] 이들은 SSA 명령들을 통해서만 접근될 수 있는 (호스트 운영체제 또는 OS로부터) 숨겨진 파티션들이다. SSA 시스템은 호스트 장치가 ACR로 로그온 함으로써 형성되는 세션(후술함)을 통하는 것이 아닌 다른 세션으로 SSA 파티션에 접근하는 것을 허용하지 않는 것이 바람직하다. 유사하게 이 요청이 형성된 세션을 통해 오지 않는 한, SSA는 SSA 파티션의 존재, 크기 및 접근 권한에 관한 정보를 제공하지 않는 것이 바람직하다.

[0053] 파티션들로의 접근 권한들은 ACR 권한들로부터 도출된다. 일단 ACR이 SSA 시스템에 로그인되면, 다른 ACR들(후술함)과 파티션을 공유할 수 있다. 파티션이 생성된 때, 호스트는 상기 파티션을 위한 참조이름 또는 ID(예를 들면 도 3 및 도 4의 P0-P3)를 제공한다. 이 참조가 또한 파티션에 읽기 및 쓰기 명령들에 사용된다.

[0054] 저장장치의 파티션닝(partitioning)

[0055] 장치의 이용가능한 모든 저장 용량은, 사용자 파티션 및 현재 구성된 SSA 파티션들로 할당되는 것이 바람직하다. 그러므로 임의의 재파티션 동작은 기존 파티션들의 재구성과 연관될 수 있다. 장치 용량(모든 파티션들의 크기들의 총합)의 실질적인 변화는 없다. 장치 메모리 공간 내의 파티션들의 ID들은 호스트 시스템에 의해 정의된다.

[0056] 호스트 시스템은 존재하는 파티션들을 2개의 더 작은 것들로 재파티션하거나 존재하는 2개의 파티션들(인접하거나 인접하지 않을 수 있음)을 하나로 병합할 수 있다. 나누어지거나 병합된 파티션들 내의 데이터는 호스트의 재량으로 지워지거나 손상 없이 남겨질 수 있다.

[0057] 저장장치의 재파티션이 데이터의 손실(저장장치의 논리주소 공간 주변에서 지워졌거나 이동되었기 때문에)을 야기할 수 있기 때문에, 재파티션에 대한 엄격한 제한들이 SSA 시스템에 의해 실시된다. 루트 AGP(root AGP, 후술함)에 있는 ACR만이 재파티션 명령을 발하는 것이 허용되고, 그것에 의해 소유된 파티션들만 참조할 수 있다. SSA 시스템은, 데이터가 파티션들 내에서 어떻게 조직화되었는지(FAT 또는 다른 파일 시스템구조)를 인식하지 못하기 때문에, 장치가 재파티션될 때마다 이들 구조들을 재구성하는 것은 호스트의 책임이다.

[0058] 사용자 파티션의 재파티션은 호스트 OS에 의해 인지된 이 파티션의 크기 및 다른 속성들을 변화시킬 것이다.

[0059] 재파티션 후에, SSA 시스템내의 어떤 ACR도 존재하지 않은 파티션들을 참조하지 않도록 보장하는 것이 호스트 시스템의 책임이다. 만약 이들 ACR들이 적절하게 제거되거나 업데이트되지 않는다면, 이들 ACR들을 위하여 존재하지 않은 파티션들에 대해 접근하기 위한 나중의 시도들은 시스템에 의해 발견되고 거절될 것이다. 유사한 관리가 제거된 키들 및 키 ID들에 관해서도 취해진다.

[0060] 키들, 키 ID들 및 논리적 보호

[0061] 파일이 특정 숨겨진 파티션에 쓰여진 때, 그것은 일반적인 대중으로부터 숨겨진다. 그러나 일단 실체(적대적이거나 아닌)가 이 파티션에 대한 지식 및 접근을 얻게 되면, 파일은 이용가능하게 되고 용이하게 인지된다. 보다 파일을 보안하기 위해, SSA는 숨겨진 파티션 내의 파일을 암호화할 수 있다. 여기서, 파일을 복호화하기 위한 키에 접근하기 위한 크리덴셜들이 파티션에 접근하기 위한 것들과 다른 것이 바람직하다. 파일들이 SSA가 인식할 수 있는(전적으로 호스트에 의해 제어되고 관리되는) 것이 아니라는 사실 때문에, 파일과 CEK를 결합시키는 것이 문제이다. 파일을 SSA가 인식하는 것-키 ID-과 관련시키는 것으로 이것을 해결할 수 있다. 따라서 키가 SSA에 의해 생성될 때, 호스트는 이 키를 위한 키 ID와 SSA에 의해 생성된 키를 이용하여 암호화된 데이터를 결합시킨다.

[0062] 키 값 및 키 ID는 논리적 보안성을 제공한다. 그것의 위치와 상관없이, 부여된 키ID와 결합된 모든 데이터는, 그것의 참조이름 또는 키ID 가 호스트 애플리케이션에 의해 생성될 때 독특하게 제공되는 동일한 컨텐츠 암호화 키(CEK)에 의해 암호화된다. 실체가 숨겨진 파티션로의 접근이 허용되고(ACR을 통해 인증됨으로써), 이 파티션 내의 암호화된 파일을 읽거나 쓰는 어느 하나를 원하게 되면, 상기 파일과 결합된 키 ID에 접근해야만 한다. 이 키 ID를 위한 키로의 접근을 부여 받을 때, SSA는 이 키 ID와 결합된 CEK내의 키값을 로드하고 그것을 호스트에 보내기 전에 데이터를 복호화하거나 플래시 메모리(20)에 그것을 쓰기 전에 암호화한다. 키 ID와 결합되는 CEK 내의 키 값은 SSA 시스템에 의해 무작위로 한번 생성되면, 그것에 의해 유지된다. SSA 시스템 외부의 어떤 것도 CEK내의 이 키 값에 대해 알거나 접근할 수 없다. 외부 세계는 CEK내의 키 값이 아니라 참조 또는 키 ID만을 제공하고 이용할 뿐이다. 키 값은 전적으로 SSA에 의해서만 관리되고 접근될 수 있다.

[0063] SSA 시스템은 후술하는 암호 모드들(CEK들 내의 키 값들뿐만 아니라 사용되는 실질적인 암호화 알고리즘이 외부 세계에 드러나지 않고 제어되는 시스템이다.)의 임의 것(사용자가 정의함)을 이용하여 키 ID와 결합된 데이터를 보호한다.

[0064] 블록 모드(Block mode)- 데이터가 블록들로 구분되고, 이들 각각이 개별적으로 암호화된다. 이 모드는 일반적으로 덜 보안적이고 사전적인 공격들을 받기 쉽다. 그러나 사용자들에게 임의로 데이터 블록들 중 어느 것이라도 접근하는 것을 허락하다.

[0065] 체인 모드(Chained mode) - 데이터가 블록들로 구분되는데, 이 블록들은 암호화 처리 동안 체인화 된다. 모든 블록이 다음 것의 암호화 처리에 입력들 중 하나로 사용된다. 이 모드는 보다 보안성이 있다고 여겨지지만 데이터가 항상 시작부터 종료까지 순차적으로 쓰여지고 읽혀야 하는 것을 요구하므로, 사용자들이 항상 받아들일 수 없는 오버헤드(overhead)를 생성한다.

[0066] 해시드-체인 모드(Hashed-Chain mode)- 데이터 무결성을 검증하게 하기 위해 사용될 수 있는 데이터 축약(digest)의 추가적인 생성을 갖는다.

[0067] ACR들 및 접근 제어

[0068] SSA는, 이들 각각이 시스템 데이터베이스내의 노드들의 트리로서 표현되는 다수의 애플리케이션을 처리하도록 고안된다. 애플리케이션들 간의 상호적인 배제가 트리 브랜치들 사이의 크로스토크(cross-talk)가 없도록 보장함으로써 달성된다.

[0069] SSA 시스템에 접근하기 위해, 실체는 시스템의 ACR들 중 하나를 통해 접속을 확립할 필요가 있다. 로그인 절차들은, 사용자가 접속하기 위해 선택한 ACR 내에 내장된 정의들에 따라 SSA 시스템에 의해 관리된다.

[0070] ACR은 SSA 시스템의 개별적인 로그인 포인트이다. ACR은 로그인 크리덴셜 및 인증방법을 보유한다. 또한 레코드 내에 있는 것은 읽기 및 쓰기 특권들을 포함하는 SSA 시스템 내의 로그인 권한들이다. 이것은 도 5에 도시되는데, 동일한 AGP 내에 n개의 ACR들이 도시된다. 이것은 n개의 ACR들 중 적어도 일부는 동일한 키에 대한 접근을

공유할 것임을 의미한다. 따라서, ACR#1 및 ACR#n은 키 ID "키 3"을 가진 키에 대한 접근을 공유하는데, ACR#1 및 ACR#n은 ACR ID들이고, "키 3"은 "키 3"과 결합된 데이터를 암호화하는데 이용되는 키를 위한 키 ID이다. 동일한 키가 또한 다수의 파일들 또는 다수의 데이터 집합들을 암호화 및/또는 복호화하기 위해 사용될 수 있다.

[0071] SSA 시스템은 알고리즘 및 사용자 크리덴셜이 다른 시스템에 대한 로그인의 여러 유형을 지원하는데, 일단 성공적으로 로그인되면 시스템 내에서 사용자의 특권들을 가질 수 있다. 도 5는 또한 다른 로그인 알고리즘 및 크리덴셜을 도시한다. ACR#1은 패스워드 로그인 알고리즘 및 크리덴셜로서 패스워드를 요구하는 반면, ACR#2는 PKI(공개 키 기반구조) 로그인 알고리즘과 크리덴셜로서 공개 키를 요구한다. 따라서 로그인하기 위해, 실체는 올바른 로그인 알고리즘 및 크리덴셜뿐만 아니라 유효한 ACR ID를 제시할 필요가 있다.

[0072] 일단 실체가 SSA 시스템의 ACR에 로그인 되면, 그것의 권한들-SSA 명령들을 사용하기 위한 권한들-이 ACR과 결합된 권한 제어 레코드(Permissions Control Record : PCR)에 정의된다. 도 5에서 ACR#1은 "키 3"과 결합된 데이터에 대해 읽기 권한만이 부여되고, ACR#2는 도시된 PCR에 따라 "키 5"와 결합된 데이터에 대해 읽기 및 쓰기의 권한이 부여된다.

[0073] 다른 ACR들은 읽기 및 쓰기를 가진 키들과 같은 시스템 내의 공통 이권(interests) 및 특권들을 공유한다. 이것을 달성하기 위해, 공통된 어떤 것을 가진 ACR들이 AGP들로 그룹화되어 ACR 그룹들이 된다. 따라서 ACR#1 및 ACR#n은 키 ID "키 3"을 가진 키로의 접근을 공유한다.

[0074] AGP들 및 그 안의 ACR들은 계층적 트리로 조직화되고, 민감한 데이터 보안을 유지하는 보안 키들을 생성하는 외에, ACR은 또한 키 ID/파티션들에 대응하는 다른 ACR 엔트리들을 생성하는 것이 바람직하다. 이들 자식 ACR(ACR children)은 부모(father) 즉 생성자와 동일하거나 더 낮은 권한들을 가지며, 부모 ACR 자체의 생성된 키들을 위한 권한들이 주어질 것이다. 부가할 필요 없이, 자식 ACR들은 그들이 생성한 임의의 키에 대한 접근 권한들을 얻는다. 이것이 도 6에 도시된다. 따라서 AGP 120에서 모든 ACR들은 ACR 122에 의해 생성되었고, 그러한 ACR들의 두 개는 "키 3"과 결합된 데이터의 접근에 대한 권한(들)을 ACR 122로부터 상속받는다.

[0075] AGP

[0076] SSA 시스템에 로그온하는 것은 AGP 및 AGP 내의 ACR을 특정함으로써 이루어진다.

[0077] 모든 AGP는 고유의 ID(참조이름)을 갖는데, 이것은 SSA 데이터베이스에서 그것의 엔트리에 대한 색인으로 사용된다. AGP 이름이 AGP가 생성될 때 SSA 시스템에 제공된다. 제공된 AGP 이름이 이미 시스템 내에 존재한다면, SSA는 생성동작을 거절할 것이다.

[0078] AGP들은 접근 및 다음 부분들에 기술될 관리 권한들의 위임에 대한 제한들을 관리하는데 사용된다. 도 6에서 두 개의 트리들에 의해 제공되는 기능들 중 하나는, 두 개의 다른 애플리케이션들 또는 두 명의 다른 컴퓨터 사용자들과 같은 완전히 분리된 실체들에 의한 접근을 관리하는 것이다. 이러한 목적들을 위하여, 두 개의 접근 프로세스들이 심지어 두 개가 동시에 일어남에도 불구하고 실질적으로 서로 독립적으로 되는 것(즉 실질적으로 크로스-토크가 없음)이 중요하다. 이것은 각 트리에서 추가적인 ACR들 및 AGP들의 생성뿐만 아니라 인증, 권한들이 다른 트리의 것들과 연결되지 않고 의존되지 않는다는 것을 의미한다. 그러므로 SSA 시스템이 메모리(10)에서 사용되면, 이것은 메모리 시스템(10)이 다수의 애플리케이션들에 동시에 제공되는 것을 허락한다. 또한 두 개의 애플리케이션들이 서로 독립적으로 두 개의 분리된 데이터 집합들(예를 들어 사진들의 집합 및 노래들의 집합)에 접근하는 것을 허락한다. 이것은 도 6에 도시된다. 따라서, 도 6의 상부에서 트리 내의 노드들(ACR들)을 통해 접근하는 애플리케이션 또는 사용자를 위한 "키 3", "키 X", 및 "키 Z"와 결합된 데이터는 사진들을 포함할 것이다. 도 6의 하부에서 트리의 노드들(ACR들)을 통해 접근하는 애플리케이션 또는 사용자를 위한 "키 5", "키 Y"와 결합된 데이터는 노래들을 포함할 것이다. AGP를 생성한 ACR은 상기 AGP의 ACR 엔트리들이 비었을 때만 그것을 제거하는 것에 대한 권한을 갖는다.

[0079] 실체의 SSA 엔트리 포인트: 접근 제어 레코드(ACR)

[0080] SSA 시스템내의 ACR은 실체가 시스템에 로그인 하는 것이 허가되는 방식을 설명한다. 실체가 SSA 시스템에 로그인할 때, 바로 수행하려는 인증 프로세스에 대응하는 ACR를 특정하는 것이 필요하다. ACR은 일단 도 5에 도시된 바와 같이 ACR에 정의된 대로 인증되면, 사용자가 실행할 수 있는 부여된 액션들을 설명하는 권한들 제어 레코

드(PCR)를 포함한다. 호스트 측 실체는 모든 ACR 데이터 필드들을 제공한다.

[0081] 실체가 성공적으로 ACR로 로그온 된 때, 실체가 ACR의 파티션 및 키 접근 권한들 및 ACAM 권한들(후술함) 모두에 대해 질의할 수 있다.

[0082] ACR ID

[0083] SSA 시스템 실체가 로그인 프로세스를 시작할 때, 상기 로그인 방법에 대응하는 ACR ID(ACR이 생성되었을 때 호스트에 의해 제공되는 것)가 특정될 필요가 있고, 그 결과 모든 로그인 요구조건들이 충족될 때 SSA가 정확한 알고리즘을 설정할 수 있고 정확한 PCR을 선택할 수 있다. 상기 ACR ID 는 ACR 이 생성될 때, SSA 시스템에게 제공된다.

[0084] 로그인/인증 알고리즘

[0085] 인증 알고리즘은 실체에 의해 사용될 로그인 프로시저의 종류 및 사용자의 식별자 증명을 제공하기 위해 필요로 되는 크리덴셜들의 종류를 특정한다. SSA 시스템은 아무 절차 없는 것(및 크리덴셜 없음)과 패스워드 기반 프로시저에서 대칭적 또는 비대칭적 암호화 중 어느 하나에 기초한 두 가지 방식의 인증 프로토콜까지 여러 표준 로그인 알고리즘들을 지원한다.

[0086] 크리덴셜들

[0087] 실체의 크리덴셜들은 로그인 알고리즘에 대응하고, SSA에 의해 사용자를 검증하고 인증하기 위해 사용된다. 크리덴셜을 위한 일 예는 패스워드/패스워드 인증을 위한 PIN-번호, AES 인증을 위한 AES-키 등이 될 수 있다. 크리덴셜들의 유형/포맷(즉 PIN, 대칭 키, 등)은 사전정의되고 인증모드로부터 유래된다. 그들은 ACR이 생성된 때 SSA 시스템에 제공된다. 장치(예를 들어 플래시 카드)가 RSA 키 쌍을 생성하기 위해 사용될 수 있고 공개 키가 인증서 생성을 위해 보내지는 PKI 기반 인증을 제외하면, SSA 시스템은 이들 크리덴셜들을 정의하고 분배하고, 관리하는데 관여하지 않는다.

[0088] 권한 제어 레코드(PCR)

[0089] PCR은 SSA 시스템에 로그인 되고 ACR의 인증 처리가 성공적으로 통과된 후 실체에 부여되는 것들을 보여준다. 다음의 3가지 유형의 권한 범주들이 존재한다: 파티션 및 키들을 위한 생성 권한들, 파티션들 및 키들에 대한 접근 권한들 및 실체-ACR 속성들을 위한 관리 권한들.

[0090] 파티션들에 대한 접근

[0091] 이 PCR의 부분은 실체가 성공적으로 ACR 단계를 완료하여 접근할 수 있는 파티션들의 리스트(SSA 시스템에 제공되는 그들의 ID들을 이용하여)를 포함한다. 각 파티션을 위한 접근 유형은 쓰기만 또는 읽기만으로 제한되거나 완전한 읽기/쓰기 접근 권한들로 특정될 수 있다. 따라서 도 5에서 ACR#1은 파티션#2에 접근할 수 있고, 파티션#1에는 접근할 수 없다. PCR에 특정된 제한들은 SSA 파티션들 및 공용 파티션에 적용된다.

[0092] 공용 파티션은 SSA 시스템을 호스팅하는 장치(예를 들어 플래시 카드)에 대한 규칙적인 읽기 및 쓰기 명령 또는 SSA 명령들 중 어느 하나에 의해 접근될 수 있다. 루트 ACR(후술함)이 공용 파티션을 제한하는 권한을 가지도록 생성될 때, 그것을 자신의 자식에게 보낼 수 있다. ACR이 공용 파티션에 접근하는 것이 규칙적인 읽기 및 쓰기 명령들만으로 제한될 수 있는 것이 바람직하다. SSA 시스템 내의 ACR들은 바람직하게는 그들의 생성에 의해서만 제한될 수 있다. 일단 ACR이 공용 파티션로부터/로 읽기/쓰기에 대한 권한을 가지면, 제거될 수 없는 것이 바람직하다.

[0093] 키 ID들에 대한 접근

[0094] PCR의 이 부분은 ACR 정책들이 실체의 로그인 프로세스에 의해 충족될 때 실체가 접근할 수 있는 키 ID들(호스트에 의해 SSA 시스템에 제공됨)의 리스트와 결합되는 데이터를 포함한다. 특정된 키 ID는 PCR에 나타나는 파티션 내에 있는 파일/파일들과 결합된다. 키 ID들이 장치(예를 들어 플래시 카드)내의 논리주소들과 결합되지 않기 때문에, 하나 이상의 파티션이 특정 ACR과 결합될 때, 상기 파일들은 파티션들 중 어느 하나에만 있을 수 있다. PCR 내의 특정된 키 ID들은 각각 다른 접근 권한의 집합을 가진다. 키 ID들에 의해 지정된 데이터에 대한 접근은 쓰기만 또는 읽기만으로 제한될 수 있거나 완전한 읽기/쓰기 접근 권한로 특정될 수도 있다.

[0095] ACR 속성들의 관리(ACAM)

[0096] 이 부분은 특정 경우에서 ACR의 시스템 속성들이 변경될 수 있는 방법을 설명한다.

[0097] SSA 시스템 내에서 허가될 수 있는 ACAM 액션은 다음과 같다:

[0098] AGP들 및 ACR의 생성/제거/업데이트.

[0099] 파티션들 및 키들의 생성/제거.

[0100] 키들 및 파티션들에 대한 접근권의 위임.

[0101] 부모 ACR이 ACAM 권한들을 편집할 수 없는 것이 바람직하다. 이것은 바람직하게는 ACR의 제거 및 재생성을 요구할 것이다. 또한 ACR에 의해 생성된 키 ID에 대한 접근 권한은 제거될 수 없는 것이 바람직하다.

[0102] AGP들 및 ACR의 생성/제거/업데이트

[0103] ACR은 다른 ACR들 및 AGP들을 생성하기 위한 능력을 가질 수도 있다. ACR들을 생성하는 것은 또한 그들에게 그들의 생성자에 의해 소유된 ACAM 권한들의 일부 또는 전부가 위임되는 것을 의미할 것이다. ACR들을 생성하기 위한 권한을 갖는 것은 다음의 액션들을 위한 권한을 갖는 것을 의미한다:

[0104] 1. 자식의 크리덴셜들을 정의하고 편집한다 -인증 방법은 일단 생성한 ACR에 의해 설정되면 편집될 수 없는 것이 바람직하다. 크리덴셜들은 자식을 위해 이미 정의된 인증 알고리즘의 범위 안에서 변경될 수 있을 것이다.

[0105] 2. ACR를 제거한다.

[0106] 3. 생성 권한을 자식 ACR에게 위임한다(따라서 손자를 갖게 된다).

[0107] 다른 ACR들의 생성에 대한 권한들을 가진 ACR은 (그것이 ACR들을 차단해제(unblocking) 권한을 갖지 않음에도 불구하고) 차단해제 권한을 자신이 생성한 ACR들에게 위임하는 권한을 갖는다. 부모 ACR은 자식 안에 자신의 언블록커(unblocker)에 대한 ACR 참조를 둘 것이다.

[0108] 부모 ACR은 본인의 자식 ACR의 제거에 대한 권한을 갖는 유일한 ACR이다. ACR이 자신이 생성한 더 낮은 레벨의 ACR을 제거할 때, 이 더 낮은 레벨 ACR에 의해 생성된 모든 ACR들이 또한 자동적으로 제거된다. ACR이 제거되고 그 후 그것이 생성한 모든 키 ID들 및 파티션들이 제거된다.

[0109] ACR이 자신의 고유 레코드를 업데이트할 수 있는 두 가지 예외들이 있다:

[0110] 생성자 ACR에 의해 설정되었음에도 불구하고 패스워드들/PIN들은 그들을 포함하는 ACR에 의해서만 업데이트 될 수 있다.

[0111] 루트 ACR은 그 자체와 그것이 존재하는 AGP를 제거할 수 있다.

[0112] 키들 및 파티션들에 대한 접근 권한의 위임

[0113] ACR들 및 그들의 AGP들은 루트 AGP 및 그 안의 ACR들이 트리의 정상에 있는(예를 들어 도 6의 루트 AGP들인 130 및 132) 계층적 트리들로 조립된다. 그들이 완전히 서로 분리됨에도 불구하고 SSA 시스템 내에는 여러 AGP 트리들이 있을 수 있다. AGP 내에서 한 ACR은 그것의 키들에 대한 접근 권한들을 그것이 속한 동일한 AGP 내에 있는 모든 ACR들 및 그들에 의해 생성된 모든 ACR들에게 위임할 수 있다. 바람직하게는, 키들을 생성하기 위한 권한은 키들을 사용하기 위한 접근 권한들의 위임에 대한 권한을 포함한다.

[0114] 키들에 대한 권한들은 3개의 범주로 구분된다:

[0115] 1. 접근-이것은 키를 위한 접근 권한들 즉 읽기, 쓰기를 정의한다.

[0116] 2. 소유권-키를 생성했던 ACR이 그것의 소유자로 정의된다. 이 소유권은 한 ACR에서 다른 ACR(그들이 동일한 AGP 또는 자식 AGP 내에 있다는 조건 하에)로 위임될 수 있다. 키의 소유권은 그것에 대한 권한들의 위임뿐만 아니라 그것의 제거에 대한 권한을 제공한다.

[0117] 3. 접근 권한들 위임- 이 권한은 ACR이 자신이 보유한 권한들을 위임할 수 있게 한다.

[0118] ACR은 접근 권한들을 자신이 접근 권한들을 갖는 다른 파티션들뿐만 아니라 자신이 생성했던 파티션들에 위임할 수 있다.

[0119] 권한 위임은 파티션들 및 키 ID들의 이름들을 위임된 ACR의 PCR에 부가함에 의해 이루어진다. 키 접근 권한들을 위임하는 것은, 키 ID에 의해 또는 접근 권한이 위임하는 ACR의 생성된 키들 모두를 위한 것임을 나타내므로써 이루어질 수 있다.

[0120] ACR들의 차단 및 차단 해제

[0121] ACR은 시스템에 의한 실체의 ACR 인증 프로세스가 실패할 때 증가되는 차단 카운터를 가진다. 실패한 인증들이 특정한 최대 수(MAX)에 도달할 때, ACR이 SSA 시스템에 의해 차단될 것이다.

[0122] 차단된 ACR은 상기 차단된 ACR에 의해 참조되는 다른 ACR에 의해 차단 해제될 수 있다. 상기 차단 해제 ACR에 대한 참조는 그것의 생성자에 의해서 설정된다. 차단 해제된 ACR은 차단된 ACR의 생성자와 동일한 AGP 내에 있고 "차단 해제" 권한을 갖는 것이 바람직하다.

[0123] 시스템 내의 다른 ACR은 차단된 ACR를 차단 해제할 수 없다. ACR은 차단 해체 ACR 없이 오직 차단 카운터로 구성될 것이다. 이 경우 이 ACR이 차단되면 그것은 차단 해제될 수 없다.

[0124] 루트 AGP - 애플리케이션 데이터베이스 생성

[0125] SSA 시스템은 다수의 애플리케이션들을 처리하고 그들 각각의 데이터를 분리하도록 고안된다. AGP시스템의 트리 구조는 애플리케이션 특정 데이터를 식별하고 분리하기 위해 사용되는 주된 도구이다. 루트 AGP는 애플리케이션 SSA 데이터베이스의 첨단에 있고, 다소간 다른 행동 규칙들을 고수한다. 여러 루트 AGP들은 SSA 시스템에 구성될 수 있다. 두 개의 루트 AGP들 130과 132가 도 6 5에 도시된다. 더 적거나 더 많은 AGP들이 이용되고 본 발명의 범위 안에 있다는 것이 명백하다.

[0126] 신규 애플리케이션에 대한 장치(예를 들어 플래시 카드)를 등록하는 것 및/또는 장치에 대한 신규 애플리케이션의 크리덴셜을 발행하는 것이 신규 AGP/ACR 트리를 장치에 추가하는 프로세스를 통해 이루어진다.

[0127] SSA 시스템은 (루트 AGP의 모든 ACR들 및 그들의 권한들 뿐만 아니라) 루트 AGP생성을 위한 다음 3개의 다른 모드들을 지원한다:

[0128] 1. 개방(Open): 어떠한 종류의 인증도 필요 없는 임의의 사용자 또는 실체 또는 시스템 ACR을 통해 인증된 사용자들/실체들이, 신규 루트 AGP를 생성할 수 있다(후술함). 개방 모드는, 모든 데이터 송신이 개방채널(즉 발행 에이전시의 보안 환경에서)에서 이루어지는 동안 임의의 보안성 수단 없이 또는 시스템 ACR 인증[즉 오버 디 에어(OTA)] 및 후 발행(post issuance) 절차들을 통해 확립된 보안채널을 통해서 루트 AGP들의 생성을 가능하게 한다.

[0129] 시스템 ACR이 구성되지 않고(이것은 선택적인 특징이다), 루트 AGP 생성 모드가 개방으로 설정되면, 오직 개방 채널 옵션만이 이용될 수 있다.

[0130] 2. 제어(Controlled): 시스템 ACR을 통해 인증된 실체들만이 신규 루트 AGP를 생성할 수 있다. SSA 시스템은 시스템 ACR이 구성되지 않으면, 이 모드에 설정될 수 없다.

[0131] 3. 잠금(Locked): 루트 AGP들의 생성가능하지 않고 추가적인 루트 AGP들이 시스템에 추가될 수 없다.

[0132] 두 개의 SSA 명령들은 이 특징을 제어한다(이들 명령들은 인증 없이 임의의 사용자/실체가 이용할 수 있다):

[0133] 1. 방법 구성 명령(Method configuration command) - 세 개의 AGP 생성 모드들 중 하나를 사용하기 위해 SSA 시스템을 구성하기 위해 사용됨. 다음의 모드 변경들만이 허락된다 : 개방→제어됨, 제어됨→잠금(즉 SSA 시스템이 현재 제어됨으로 구성되면, 오직 잠금으로만 변경될 수 있다.)

[0134] 2. 방법 구성 잠금 명령(Method configuration lock command) - 방법 구성 명령을 실행할 수 없고 영구적으로 현재 선택된 방법으로 잠그기 위해 사용됨.

[0135] 루트 AGP가 생성될 때, 그것은 그것의 ACR들의 생성 및 구성이 가능한(루트 AGP의 생성에 적용되는 동일한 접근 제한들을 이용하여) 특별한 초기화 모드에 있다. 루트 AGP 구성 프로세스의 종료 시, 실체가 명백히 그것을 동작 모드로 변경할 때, 존재하는 ACR들은 더 이상 업데이트될 수 없고, 추가적인 ACR들은 더 이상 생성될 수 없다.

[0136] 일단 루트 AGP가 표준 모드에 놓여지면, 그것은 루트 AGP를 제거하기 위한 권한이 부여된 그것의 ACR들 중 하나를 통해 시스템에 로그인함에 의해서만 제거될 수 있다. 이것은 상기 특별한 초기화 모드에 추가하여 루트 AGP의 또 다른 예외이며, 그것은 바람직하게는 다음 트리 레벨에서 AGP들에 대립되는 것과 같은 본인 소유 AGP를 제거하기 위한 권한을 가진 ACR을 포함할 수 있는 유일한 AGP이다.

[0137] 루트 ACR 과 표준 ACR 사이의 세 번째이고 마지막 차이는, 시스템내의 ACR만이 파티션들을 생성하고 제거하는 것에 대한 권한을 가질 수 있는 것이다.

[0138] SSA 시스템 ACR

[0139] 시스템 ACR은 다음 두 개의 SSA 동작들을 위해 사용될 수 있다:

[0140] 1. 적대적인 환경 안에서 보안된 채널의 보호하에서 ACR/AGP 트리를 생성한다.

[0141] 2. SSA 시스템을 호스팅하는 장치를 식별하고 인증한다.

[0142] SSA내에 한 개의 시스템 ACR만이 있는 것이 바람직하고, 일단 정의되면 변경될 수 없는 것이 바람직하다. 시스템 ACR을 생성할 때 시스템 인증에 대한 필요가 없고, 오직 SSA 명령만이 필요로 된다. 생성-시스템 ACR 특징이 불능해질 수 있다(생성-루트-AGP 특징과 유사하게). 시스템 ACR이 생성된 후에, 바람직하게 오직 하나의 시스템 ACR만이 허락되기 때문에 상기 생성-시스템-ACR 명령은 영향을 미치지 못한다.

[0143] 생성 프로세스 동안 시스템 ACR이 동작하지 않는다. 완료되면 시스템 ACR이 생성되고 나갈 준비가 되도록 지시하는 특별한 명령이 발행될 필요가 있다. 이 시점 이후에 시스템 ACR은 업데이트되거나 대체될 수 없는 것이 바람직하다.

[0144] 시스템 ACR은 SSA에서 루트 ACR/AGP를 생성한다. 그것은 호스트가 그것에 만족하고 그것을 차단하는 시간까지, 루트 레벨을 추가/변경하기 위한 권한을 갖는다. 루트 AGP의 차단은 필수적으로 시스템 ACR과의 연결을 끊고 그것에 템퍼 프루프(temper proof)를 부여한다. 이 시점에서 어떤 것도 루트 AGP 및 그 안의 ACR들을 변경/편집할 수 없다. 이것은 SSA 명령을 통해 이루어진다. 루트 AGP들의 생성 불능은 영구적 효과를 갖고 취소될 수 없다. 상기 시스템 ACR과 관련된 특징들이 도 7에 도시된다. 시스템 ACR은 세 개의 다른 루트 AGP들을 생성하는데 이용된다. 이들이 생성된 후에 특정 시간에서, 시스템 ACR로부터 루트 AGP들을 차단하기 위해 SSA 명령이 호스트로부터 전달된다. 그렇게 함으로써 도 7에서 시스템 ACR과 루트 AGP들을 연결하는 점선에 의해 표시된 바와 같이 생성-루트-AGP 특징을 불능으로 한다. 이것은 세 개의 루트 AGP들에게 템퍼 프루프를 부여한다. 세 개의 루트 AGP들은 루트 AGP들이 차단되기 전 또는 후에 세 개의 분리된 트리를 형성하기 위해 자식 AGP들을 생성하는데 이용될 수 있다.

[0145] 상술한 특징들은 컨텐츠를 가진 보안 제품들을 구성하는데 있어 컨텐츠 소유자에게 매우 큰 융통성을 제공한다. 보안 제품들은 "발행"되는 것이 필요하다. 발행(issuance)은 장치가 호스트를 식별하고 반대로 호스트가 장치를 식별할 수 있는 식별 키들을 넣는 프로세스이다. 장치(예를 들어 플래시 카드)를 식별하는 것은 호스트가 장치에게 비밀을 맡길 수 있는지 여부를 결정할 수 있게 한다. 한편, 호스트를 식별하는 것은 호스트가 허락될 때만 장치가 보안 정책들을 실시하는(특정 호스트 명령을 부여하고 실행함) 것을 가능하게 한다.

[0146] 다수의 애플리케이션들을 제공하도록 디자인된 제품들은 여러 식별 키들을 가질 것이다. 제품은 "사전-발행(pre-issued)"-송신 전에 제조하는 동안 저장된 키들-이거나 "사후-발행(post-issued)"- 신규 키들이 수송 후에 부가됨-일 수 있다. 사후 발행을 위해, 메모리 장치(예를 들어 메모리 카드)는 장치에 애플리케이션들을 추가하

는 것이 허용된 실체들을 식별하기 위해 사용되는 몇 가지 종류의 마스터 또는 장치 레벨 키들을 포함할 필요가 있다.

[0147] 상술한 특징들은 제품이 사후 발행을 가능/불능 하도록 구성되는 것을 가능하게 할 수 있다. 또한 사후 발행 구성은 수송 후에 안전하게 이루어질 수 있다. 장치는 상술한 마스터 또는 장치 레벨 키들에 더하여 그것에 키들이 없는 소매제품으로서 구입 될 수 있고, 그 후 신규 소유자에 의해 사후 발행 애플리케이션들을 가능하게 하거나 그들을 불능하게 구성될 것이다.

[0148] 따라서 시스템 ACR특징은 상술한 목적들을 달성할 수 있는 능력을 제공한다:

[0149] - 시스템 ACR 없는 메모리 장치들은 무제한적이고 제어되지 않는 애플리케이션들의 추가가 허락될 것이다.

[0150] - 시스템 ACR이 없는 메모리 장치들은 시스템 ACR 생성이 불가능하게 구성될 수 있는데, 이것은 신규 애플리케이션들의 추가를 제어하기 위한 방법이 없음을 의미한다(신규 루트 AGP를 생성하기 위한 특징이 또한 불가능하게 되지 않는다면).

[0151] - 시스템 ACR을 가진 메모리 장치들은, 시스템 ACR 크리덴셜을 이용하여 인증 절차를 통해 확립된 보안 채널을 통해서 애플리케이션들의 제어된 추가만이 허락될 것이다.

[0152] - 시스템 ACR을 가진 메모리 장치들은 애플리케이션들이 추가되기 전 또는 후에 애플리케이션 추가 특징이 불가능하도록 구성될 수 있다.

[0153] 키 ID 리스트

[0154] 키 ID들은 특정 ACR 요청마다 생성되지만, 메모리 시스템(10)에서 그들은 SSA 시스템에 의해 유일하게 사용된다. 키 ID가 생성될 때, 다음 데이터가 생성한 ACR에 의해 또는 상기 ACR로 제공된다:

[0155] 1. 키 ID. 상기 ID는 호스트를 통해 실체에 의해 제공되고, 키 및 모든 추가 읽기 또는 쓰기 접근들에서 상기 키를 이용하여 암호화되거나 복호화되는 데이터를 참조하는데 사용된다.

[0156] 2. 키 암호 및 데이터 무결성 모드(상기 및 후술할 블록화, 체인화 및 해시드 모드들).

[0157] 제공된 호스트 속성들에 더하여, 다음의 데이터가 SSA 시스템에 의해 유지된다:

[0158] 1. 키 ID 소유자. 소유자인 ACR의 ID이다. 키 ID가 생성될 때 생성자 ACR은 그것의 소유자가 된다. 하지만 키 ID 소유권은 다른 ACR로 전달될 수 있다. 키 ID 소유자만이 키 ID 소유권의 전달 및 위임을 허락할 수 있는 것이 바람직하다. 결합된 키에 대한 접근 권한의 위임 및 이들 권한들의 취소는 키 ID 소유자 또는 위임 권한들이 할당된 임의의 다른 ACR 중 어느 하나에 의해 관리될 수 있다. 이들 동작들 중 어느 하나가 실행되는 것이 시도될 때마다, SSA 시스템은 요청한 ACR가 승인된 때만 그것을 제공할 것이다.

[0159] 2. CEK. 이것은 키 ID와 결합되거나 지적된 컨텐츠를 암호화하기 위해 이용되는 CEK이다. CEK는 SSA 시스템에 의해 생성된 128 비트 AES 랜덤 키일 것이다.

[0160] 3. MAC 및 IV값들. 체인화 블록 암호(CBC) 암호화 알고리즘들에서 사용되는 동적 정보(메시지 인증 코드들 및 초기 벡터들).

[0161] SSA의 다양한 특징들은 또한 도 8a 내지 도 16의 순서도를 참조하여 설명된다. 여기서 한 단계에서 왼쪽의 'H'는 동작이 호스트에 의해 수행되는 것을 의미하고 'C'는 동작이 카드에 의해 수행됨을 의미한다. 시스템 ACR을 생성하기 위해, 호스트는 메모리 장치(10) 내의 SSA에 시스템 ACR을 생성하는 명령을 발행한다(블록 202). 장치(10)는 시스템 ACR이 이미 존재하는지 여부를 확인하여 응답한다(블록 204, 마름모 206). 이미 존재한다면 장치(10)는 실패를 리턴하고 종료한다(타원형 208). 만약 존재하지 않는다면, 메모리(10)는 시스템 ACR 생성이 허락되는지를 알아보기 위해 확인하고(마름모 210), 허락되지 않는다면 실패상태를 리턴 한다(블록 212). 따라서 요구되는 보안성 특징들이 사전 결정됨으로써 시스템 ACR이 요구되지 않는 경우와 같이, 장치 발행자가 시스템 ACR의 생성을 허락하지 않는 경우들이 있을 수 있다. 만약 이것이 허락된다면, 장치(10)는 OK상태를 리턴하고 시스템 ACR 크리덴셜들을 호스트로부터 기다린다(블록 214). 호스트는 SSA 상태와 장치(10)가 시스템 ACR의 생성이 허락되는 것으로 표시되었는지 여부를 확인한다(블록 216 및 마름모 218). 생성이 허락되지 않거나 시스템 ACR이 이미 존재한다면, 호스트는 종료한다(타원형 220). 장치(10)가 시스템 ACR의 생성이 허락되는 것으로 표시한다면, 호스트는 로그인 크리덴셜을 정의하기 위해 SSA 명령을 발행하고 그것을 장치(10)에 송신한다(블록

222). 장치(10)는 시스템 ACR 레코드를 수신된 크리덴셜로 업데이트하고 OK 상태를 리턴한다(블록 224). 이 상태 신호에 응답하여 호스트는 시스템 ACR이 준비되었음을 표시하는 SSA 명령을 발행한다(블록 226). 장치(10)는 시스템 ACR을 잠금으로써 응답하고, 그 결과 그것은 업데이트 되거나 대체될 수 없다(블록 228). 이것은 시스템 ACR의 특징들 및 장치(10)를 식별하기 위한 그것의 식별자를 호스트에게 잠그는 것이다.

[0162] 신규 트리들(신규 루트 AGP들 및 ACR)을 생성하기 위한 절차는 이들 기능들이 장치에 구성된 방식에 의해 결정된다. 도 9는 절차들을 설명한다. 호스트(24) 및 메모리 시스템(10) 모두 이 절차를 따른다. 신규 루트 AGP를 추가하는 것이 전혀 불가능하다면, 신규 루트 AGP들은 추가될 수 없다(마름모 246). 만약 가능하지만 시스템 ACR을 요구한다면, 호스트는 생성 루트 AGP 명령(블록 254)을 발행하기 전에 시스템 ACR을 통해 인증하고 보안 채널을 형성한다(마름모 250, 블록 252). 만약 시스템 ACR이 요구되지 않는다면(마름모 248), 호스트(24)는 인증 없이 생성 루트 AGP 명령을 발행할 수 있고, 블록 254로 진행한다. 시스템 ACR이 존재한다면, 호스트는 그것이 요구되지 않더라도(흐름도에는 미도시) 그것을 사용할 수 있을 것이다. 장치(예를 들어 플래시 카드)는 그 기능이 불능화되지 않는다면 신규 루트 AGP를 생성하기 위한 어떠한 시도로 거절할 것이고, 만약 시스템 ACR이 요구된다면 인증 없이 신규 루트 AGP를 생성하려는 시도를 거절할 것이다(마름모 246 및 250). 블록 254에서 새롭게 생성된 AGP 및 ACR은, 지금 동작 모드로 전환되고 그 결과 그러한 AGP들 내의 ACR들이 업데이트 또는 다른 변경이 될 수 없고, 어떤 ACR들도 그들에게 추가될 수 없다(블록 256). 그 후 시스템은 선택적으로 잠기고 그 결과 추가적인 루트 AGP들이 생성될 수 없다(블록 258). 점선으로 된 박스 258은 이 단계가 선택적인 단계임을 표시하는 약속이다. 이 출원의 도면들의 순서도에서 점선의 모든 박스들은 선택적인 단계들이다. 이것은 컨텐츠 소유자가, 적법한 컨텐츠를 가진 진정한 메모리 장치를 모방하는 다른 불법적인 목적들을 위해 장치(10)가 사용되는 것을 차단할 수 있도록 한다.

[0163] ACR들(상술한 루트 AGP 내의 ACR들과는 다른)을 생성하기 위해, 도 10에 도시된 바와 같이 ACR을 생성하는 권한을 가진 임의의 ACR을 시작하게 할 것이다(블록 270). 실체는 엔트리 포인트 ACR 식별자 및 그것이 생성하기를 바라는 모든 필요한 속성들을 가진 ACR을 제공함으로써 호스트(24)를 통해 들어가는 것을 시도할 수도 있다(블록 272). SSA는 ACR 식별자가 일치되는 지와 그러한 식별자를 가진 ACR이 ACR을 생성하기 위한 권한을 갖는지를 확인한다(마름모 274). 요청이 승인된 것으로 검증되면, 장치(10)의 SSA는 ACR을 생성한다(블록 276).

[0164] 도 11은 도 10의 방법을 이용하여 보안성 애플리케이션들에서 유용한 트리를 설명하는 두 개의 AGP들을 보여준다. 따라서 마케팅 AGP 내에서 식별자 m1을 가진 ACR은 ACR을 생성하기 위한 권한을 갖는다. 또한 ACR m1은 키 ID "마케팅 정보"와 결합된 데이터 및 키 ID "가격 리스트"와 결합된 데이터를 읽고 쓰기 위한 키를 사용하는 권한을 가진다. 도 10의 방법을 이용하여, 두 개의 ACR들, s1 및 s2를 갖는 세일즈 AGP를 생성하는데, 상기 s1 및 s2은 키 ID "마케팅 정보 “와 결합된 데이터에 접근하기 위해 필요한 키가 아닌, 키 ID "가격 리스트"와 결합된 가격 데이터에 접근하기 위한 키에 대한 읽기 권한만을 가진다. 이러한 방식으로 ACR들 s1 및 s2를 가진 실체들은 가격 데이터를 읽을 수만 있으며 변경할 수는 없고, 마케팅 데이터에 대한 접근은 할 수 없을 것이다. 한편 ACR m2는 ACR들을 생성하기 위한 권한이 없고, 키 ID "가격 리스트" 및 키 ID "마케팅 정보"와 결합된 데이터에 접근하기 위한 키들에 대한 읽기 권한만을 갖는다.

[0165] 따라서, 접근 권한들은 m1이 가격 데이터를 읽을 수 있는 권한을 s1 및 s2에 위임하는 상술한 방식으로 위임될 것이다. 이것은 특히 대규모 마케팅 및 세일즈 그룹들이 관련되는 경우에 유용하다. 하나 또는 소수의 판매자들이 있는 경우에, 도 10의 방법을 사용할 필요는 없을 것이다. 대신에, 도 12에 도시된 바와 같이 접근 권한들은 ACR에 의해 동일한 AGP내에서 더 낮거나 동일한 레벨의 ACR에 위임될 것이다. 먼저 실체는 호스트를 통해 트리 내에서 상술한 방식으로 ACR을 특정함으로써 그러한 AGP를 위한 트리에 진입한다(블록 280). 다음으로 호스트는 ACR 및 위임할 권한을 특정할 것이다. 상기 SSA는 그러한 ACR을 위한 트리(들) 및 특정된 다른 ACR에 권한들을 위임하기 위한 권한을 가진 ACR인지 여부를 확인한다(마름모 282). 만약 그렇다면 권한은 위임되고(블록 284), 그렇지 않다면 종료한다. 결과는 도 13에 도시되어 있다. 이 경우 ACR m1은 ACR s1에 읽기 권한을 위임하기 위한 권한을 가지고, 그 결과 s1은 위임 후에 가격 데이터에 접근하기 위한 키를 사용할 수 있을 것이다. 이것은, m1이 가격데이터에 접근하기 위한 동일하거나 더 우수한 권한들 및 위임을 위한 권한을 가진 경우에 수행될 것이다. 일 실시예에서 m1은 위임 후에도 그것의 접근 권한들을 보유한다. 바람직하게는 접근 권한들은 제한된 시간, 제한된 접근 횟수들 등과 같이 제한된 조건들 하에서(영구적인 것보다는) 위임될 수 있다.

[0166] 키 및 키 ID를 생성하기 위한 프로세스는 도 14에 도시되어 있다. 실체는 ACR을 통해 인증된다(블록 302). 실체는 호스트에 의해 특정된 ID를 가진 키의 생성을 요청한다(블록 304). SSA는 특정된 ACR이 그렇게 행동하는 것에 대한 권한을 갖는지를 확인하고 인지한다(마름모 306). 예를 들어 키가 특정 파티션에 있는 데이터에 접근하기 위해 이용되는 것이면, 상기 SSA는 ACR이 그러한 파티션에 접근할 수 있는지 확인하고 인지할 것이다. 만약

ACR이 승인된 경우라면, 그 후 메모리 장치(10)는 호스트에 의해 제공된 키 ID와 결합되는 키 값을 생성한다(블록 308). 그리고 ACR 내에 키 ID를 저장하고 그것의 메모리(컨트롤러-결합된 메모리 또는 메모리(20) 중 어느 하나)에 키 값을 저장하며, 실체에 의해 제공된 정보에 따라 권한들 및 권한들을 할당하고(블록 310), 그러한 할당된 권한 및 권한들을 가진 ACR의 PCR을 변경한다(블록 312). 따라서, 키의 생성자는 읽기 및 쓰기 권한들, 동일한 AGP내의 다른 ACR들 또는 더 낮은 레벨의 ACR과 공유하고 위임하기 위한 권한들 및 키의 소유권을 이전하는 권한와 같은 모든 이용가능한 권한들을 가진다.

[0167] 도 15에 도시된 바와 같이 ACR은 SSA 시스템내의 다른 ACR의 권한들(또는 존재도 함께)을 변경할 수 있다. 실체는 이전처럼 ACR을 통해 트리에 진입할 것인데, 한 경우 실체는 인증되고 그 후 ACR을 특정한다(블록 330, 332). 그것은 타겟 ACR의 제거 또는 타겟 ACR 내의 권한을 요청한다(블록 334). 만약 특정된 ACR 또는 그 때 활성화된 것이 그렇게 하는 권한을 가진다면(마름모 336), 타겟 ACR은 제거되고, 또는 타겟 ACR의 PCR은 그러한 권한을 제거하기 위해 변경된다(블록 338). 만약 승인되지 않으면 시스템은 종료된다.

[0168] 상술한 프로세스 후에, 타겟은 상기 프로세스 이전에는 가능했던 데이터에 더 이상 접근할 수 없을 것이다. 도 16에 도시된 바와 같이, 실체는 타겟 ACR에 진입하기 위해 시도할 것이고(블록 350), 이전에 존재하는 ACR ID가 SSA 내에 더 이상 존재하지 않기 때문에 인증 프로세스는 실패할 것이고, 권한은 거절된다(마름모 352). ACR ID가 제거되지 않았다고 가정하면, 실체는 ACR를 특정하고(블록 354), 특정 파티션 내의 키 ID 및/ 또는 데이터를 특정하며(블록 356), 그 후 SSA는 키 ID 또는 파티션 접근 요청이 그러한 ACR의 PCR에 따라 허가되었는지를 확인하고 인지한다(마름모 358). 권한이 제거되거나 기간 만료되지 않는다면, 그 후 이 요청은 다시 거절된다. 그렇지 않다면 요청이 승인된다(블록 360).

[0169] 상기 프로세스는 ACR 및 그것의 PCR이 다른 ACR에 의해 방금 변경되었는지 또는 시작하기 위해 구성되었는지 여부와 상관없이, 보호되는 데이터로의 접근이 장치(예를 들어 플래시 카드)에 의해 관리되는 방법을 설명한다.

[0170] 세션들

[0171] SSA 시스템은 동시에 로그인 하는 다수의 사용자들을 처리하도록 고안된다. 이 특징은, SSA에 의해 수신된 모든 명령이 특정 실체와 결합되고, 이 실체를 인증하기 위해 사용된 ACR이 요청된 액션에 대한 권한들을 가질 때만 실행되는 것을 요구한다.

[0172] 다수의 실체들은 세션 컨셉(session concept)을 통해 지원된다. 세션은 인증 프로세스 동안 형성되고 SSA 시스템에 의해 세션-id가 할당된다. 세션-id는 내부적으로 시스템에 로그인 하기 위해 사용된 ACR과 결합되고 모든 추가적인 SSA 명령들에 사용되기 위해 실체에 보내진다.

[0173] SSA 시스템은 두 가지 유형의 세션, 즉 개방 및 보안 세션들을 지원한다. 특정된 인증 프로세스와 결합되는 세션 유형이 ACR 내에서 정의된다. SSA 시스템은 그것이 인증 자체를 실시하는 방식과 유사한 방식으로 세션 형성을 실시할 것이다. ACR이 실체 권한들을 정의하기 때문에, 이 메커니즘은 시스템 디자이너들이 특정 키 ID들에 대한 접근 또는 특정 ACR 관리 동작들(즉 신규 ACR들의 생성 및 크리덴셜들의 설정)의 호출 중 어느 하나와 보안 터널링을 결합시키는 것이 가능하게 한다.

[0174] 개방 세션

[0175] 개방 세션은 버스 암호화 없이 세션-id에 의해 식별된 세션으로, 모든 명령들 및 데이터가 방해 없이 통과된다. 이 동작 모드는 실체들이 위험 모델(threat model)에 속하지 않거나 버스상 도청이 일어나지 않는 다수의 사용자 또는 다수의 실체가 있는 환경에서 사용되는 것이 바람직하다.

[0176] 호스트 측에 있는 애플리케이션들 사이에서 데이터의 송신을 보호하거나 방화벽을 효과적으로 할 수는 없지만, 개방 세션 모드는 SSA 시스템이 현재 인증된 ACR들에게 허락된 정보만을 접근하도록 허락하는 것을 가능하게 한다.

[0177] 또한 개방 세션은 파티션 또는 키가 보호될 필요가 있는 경우에도 사용될 수 있다. 하지만 유효한 인증 프로세스 후에, 호스트 상의 모든 실체들에게 접근이 승인된다. 다양한 호스트 애플리케이션들이 인증된 ACR의 권한들을 얻기 위해 공유할 필요가 있는 유일한 것은 세션-id이다. 이것은 도 17a에 도시되어 있다. 줄 400 상부의 단계들은 호스트(24)에 의해 처리된 것들이다. 실체가 ACR1을 위해 인증(블록402)된 후에 그것은 메모리 장치(10)

내의 키 ID X와 결합된 파일로 접근을 요청한다(블록 404, 406 및 408). 만약 ACR1의 PCR이 그러한 접근을 허락하면, 장치(10)는 요청을 승인한다(마름모 410). 그렇지 않으면, 시스템은 블록 402로 리턴한다. 인증이 완결된 후에, 메모리 시스템(10)은 할당된 세션 id(및 ACR 크리덴셜들이 아님)에 의해서만 명령을 발행하는 실체를 식별한다. 일단 개방 세션에서 ACR1이 그것의 PCR에 있는 키 ID들과 결합된 데이터에 대한 접근이 이루어지면, 임의의 다른 애플리케이션 또는 사용자는 호스트(24)상의 다른 애플리케이션들 사이에서 공유되는 정확한 세션 ID를 특정함으로써 동일한 데이터에 접근할 수 있다. 이 특징은, 사용자가 한번만 로그인 할 수 있고, 그것을 통해 로그인이 다른 애플리케이션들을 위해 수행되는 어카운트에 연결된 모든 데이터에 접근할 수 있어 보다 편리해지는 애플리케이션들에서 유리하다. 따라서 휴대폰 사용자는 여러 번 로그하지 않고도 저장된 이메일들에 접근할 수 있고, 메모리(20)에 저장된 음악을 들을 수 있을 것이다. 한편 ACR1에 의해 처리되지 않는 데이터는 접근할 수 없을 것이다. 따라서, 동일한 휴대폰 사용자는 분리된 어카운트 ACR2를 통해 접근할 수 있는 게임들 및 사진들과 같은 가치 있는 컨텐츠를 가질 수 있다. 비록 그가 제 1 어카운트 ACR1을 통해 이용가능한 데이터에 타인들이 접근하는 것을 꺼려하지 않지만, 이것은 자신의 휴대폰을 빌려간 타인들이 접근하기를 원하지 않는 데이터이다. 개방세션에서 ACR1에 대한 접근을 허락하더라도, 데이터를 두 개의 분리된 어카운트들로 나누어 접근을 분리하는 것은 가치 있는 데이터를 보호할 수 있을 뿐만 아니라 사용을 용이하게 한다.

[0178] 호스트 애플리케이션들 사이에서 세션-id를 공유하는 프로세스를 보다 더 쉽게 하기 위해, ACR이 개방세션을 요청할 때, 세션에 "0" id를 할당할 것을 특히 요청할 수 있다. 이러한 방식으로, 애플리케이션들이 사전 정의된 세션-id를 사용하도록 고안될 수 있다. 명백한 이유들로 세션 0을 요청한 하나의 ACR만이 특정한 시점에서 인증될 수 있다는 것이 유일한 제한이다. 세션 0을 요청한 다른 ACR을 인증하려는 시도는 거절될 것이다.

[0179] 보안 세션

[0180] 보안성 계층을 추가하기 위해, 세션 id가 도 17b에 도시된 바와 같이 사용될 것이다. 또한 그 후 메모리(10)는 활성 세션들의 세션 id들을 저장한다. 도 17b에서, 예를 들어 키 ID X와 결합된 파일에 접근할 수 있기 위해서는, 실체는 그것이 파일에 접근을 허락받기 전에 세션 id "A"와 같은 세션 id가 제공할 필요가 있을 것이다(블록 404, 406, 412 및 414). 이러한 방식으로, 요청하는 실체가 정확한 세션 id를 인식하고 있지 않는다면, 그것은 메모리(10)에 접근할 수 없다. 세션 id는 세션이 끝난 후에 제거되고 각각의 세션을 위해 다를 것이기 때문에, 실체는 그것이 세션 번호를 제공할 수 있을 때만 접근에 성공할 수 있다.

[0181] SSA 시스템은, 세션 번호를 이용하는 것 이외에 명령이 실제로 정확한 인증된 실체로부터 왔는지를 확인할 방법이 없다. 공격자들이 악의적인 명령들을 송신하기 위해 개방채널을 사용하려고 시도할 징후가 있는 애플리케이션들 및 사용 케이스들의 경우에, 호스트 애플리케이션은 보안 세션(보안 채널)을 이용한다.

[0182] 보안 채널을 이용할 때, 모든 명령 뿐만 아니라 세션-id는 보안 채널 암호화(세션) 키에 의해 암호화되고 보안성 수준은 호스트 측 구현만큼 높다.

[0183] 세션 종료

[0184] 다음의 시나리오 중 어느 하나에서 세션은 종료되고, ACR은 로그 오프된다:

[0185] 1. 실체가 명백한 종료 세션 명령을 발행한다.

[0186] 2. 통신 중 타임아웃. 특정 실체가 ACR 파라미터들의 하나로서 정의된 시간 기간 동안 아무런 명령을 발행하지 않았다.

[0187] 3. 장치 (예를 들어 플래시 카드)가 리셋 및/또는 파워 사이클 후에 모든 개방 세션들이 종료된다.

[0188] 데이터 무결성 서비스들

[0189] SSA 시스템은 SSA 데이터베이스(모든 ACR들, PCR들, 등을 포함한다)의 무결성을 검증한다. 또한 데이터 무결성 서비스들은 키 ID 메커니즘을 통해 실체 데이터에 제공된다.

[0190] 만약 키 ID가 그것의 암호화 알고리즘들로서 해시드로 구성된다면, 해시 값들은 CEK레코드에서 CEK 및 IV를 가진 측을 따라 저장된다. 해시 값들은 쓰기 동작 동안 연산되고 저장된다. 해시 값들은 읽기 동작들 동안 다시

연산되고, 이전 쓰기 동작들 동안에 저장된 값들과 비교된다. 실체가 키 ID에 접근할 때마다 추가적인 데이터가 구 데이터(old data)에 (암호화되어)연관되고, 적절한 해시 값(읽기 또는 쓰기를 위한)이 업데이트된다.

[0191] 호스트만이 키 ID와 결합되거나 그것에 의해 지정된 데이터 파일들을 알기 때문에, 호스트는 명백하게 다음의 방식으로 데이터 무결성 기능의 여러 측면들을 관리한다:

[0192] 1. 키 ID와 결합되거나 그것에 지정된 데이터 파일이 시작부터 종료까지 쓰여지고 읽힌다. SSA 시스템이 CBC 암호화 방법을 이용하여 전체 데이터의 해시화된 메시지 축약을 생성하기 때문에, 파일의 부분들에 접근하려는 어떠한 시도도 그것을 혼란 시키지 못 할 것이다.

[0193] 2. 중간 해시 값들이 SSA 시스템에 의해 유지되기 때문에 연속 스트림에서 데이터를 처리할 필요가 없다 [데이터 스트림은 다른 키 ID들의 데이터 스트림들과 상호배치될 수 있고 다수의 세션들로 분리될 수 있다]. 하지만 데이터 스트림이 재시작 된다면, 실체는 SSA 시스템에게 해시 값들을 리셋하라고 명백하게 지시할 필요가 있을 것이다.

[0194] 3. 읽기 동작이 완결될 때, 호스트는 쓰기 동작 동안 연산된 해시 값과 그것을 비교함으로써 읽기 해시를 검증하도록 SSA 시스템에게 명백히 요청해야 한다.

[0195] 4. SSA 시스템은 또한 "더미 읽기" 동작을 제공한다. 이 특징은 암호화 엔진들을 통해 데이터를 스트림하지만 그것을 호스트로 보내지는 않을 것이다. 이 특징은 그것이 실질적으로 장치(예를 들어 플래시 카드)로 읽혀지지 전에 데이터 무결성을 검증하기 위해 사용될 수 있다.

[0196] 난수 생성

[0197] SSA 시스템은 외부 실체들이 내부 난수 생성기를 이용하도록 하고 SSA 시스템의 외부에서 이용되는 난수들을 요청하도록 할 수 있다. 이 서비스는 임의의 호스트가 이용할 수 있고 인증을 요구하지 않는다.

[0198] RSA 키 쌍 생성

[0199] SSA 시스템은 외부 사용자들이 내부 RSA 키 쌍 생성 특징을 이용하도록 하고 SSA 시스템 외부에서 이용되는 RSA 키 쌍을 요청하도록 할 수 있다. 이 서비스는 임의의 호스트가 이용할 수 있고 인증을 요구하지 않는다.

[0200] 대안적인 실시예

[0201] 계층적 방식을 이용하는 대신에, 도 18에 도시된 바와 같은 데이터베이스 방식을 이용하여 유사한 결과들이 얻어질 수 있다.

[0202] 도 18에 도시된 바와 같이, 실체들을 위한 크리덴셜 리스트, 인증 방법들, 실패한 시도들의 최대수, 및 차단해제에 필요한 크리덴셜의 최소 수가, 컨트롤러(12) 또는 메모리(20)에 저장되는 데이터베이스에 기록될 것인데, 이것은 이런 크리덴셜 요구사항들과 메모리(10)의 컨트롤러(12)에 의해 수행되는 데이터베이스 내의 정책들(키들 및 파티션들에 대한 읽기, 쓰기 접근, 보안 채널 요구사항)을 관련시킨다.

[0203] 또한 키들 및 파티션들에 대한 접근의 제약들 및 제한들이 데이터베이스에 저장된다. 따라서 일부 실체들(예를 들어 시스템 관리자)은 화이트 리스트에 있는데, 이것은 이들 실체들이 항상 모든 키들 및 파티션들에 접근할 수 있음을 의미한다. 다른 실체들은 블랙리스트에 있을 수 있는데, 임의의 정보에 접근하기 위한 그들의 시도들은 차단될 것이다. 제한은 전역적일 수 있거나 키 및/또는 파티션에 특정될 수 있다. 이것은 일부 실체들만이 항상 일부 특정된 키들 및 파티션들에 접근할 수 있고, 일부 실체들은 항상 그렇게 할 수 없다는 것을 의미한다. 또한 제약들은 컨텐츠 자체에, 그것이 있는 파티션 또는 그것을 암호화하고 복호화하는데 이용되는 키에 관계없이 놓여질 수 있다. 따라서, 일정 데이터(예를 들면 노래들)는 어느 실체들이 접근했는지와 상관없이 그들이 그들에게 접근하는 처음 다섯 개의 호스트 장치들에 의해서만 접근될 수 있거나 다른 데이터(예를 들어 영화들)는 제한된 횟수만큼만 읽혀질 수 있는 속성들을 가질 것이다.

[0204] **인증**

[0205] 패스워드 보호

[0206] 패스워드-보호는 보호되는 영역을 접근하기 위해 패스워드가 제시될 필요가 있음을 의미한다. 그것이 하나 이상의 패스워드일 수 있다면, 패스워드들은 읽기 접근 또는 읽기/쓰기 접근과 같은 다른 권한와 결합될 수 있다.

[0207] 패스워드 보호는 장치(예를 들어 플래시 카드)가 호스트에 의해 제공된 패스워드를 검증할 수 있는 것 즉 장치는 또한 장치의 관리되고 보안되는 메모리 영역에 저장된 패스워드를 가진다는 것을 의미한다.

[0208] 발행들 및 제한들

[0209] 패스워드들은 재송신 공격을 받기 쉽다. 패스워드가 각각 제시된 후에 변경되지 않기 때문에 그것은 동일하게 재송신될 수 있다. 그것은 보호되는 데이터가 가치 있고 통신 버스가 쉽게 접근가능한 것이라면 패스워드가 사용되어서는 안 됨을 의미한다.

[0210] 패스워드는 저장된 데이터로의 접근을 보호할 수 있는 것이나, 데이터(키가 아님)를 보호하기 위해 이용되어서는 안 된다.

[0211] 패스워드들과 결합된 보안성 수준을 증가시키기 위해, 그들은 마스터 키를 이용하여 다양화될 수 있는데 그럼으로써 하나가 해킹되어도 전체 시스템이 붕괴되지 않는다. 보안 통신 채널에 기초한 세션 키는 패스워드를 보내는데 이용될 수 있다.

[0212] 도 19는 패스워드를 이용하는 인증을 설명하는 순서도이다. 실체는 어카운트 id와 패스워드를 시스템(10)[예를 들어 플래시 메모리 카드]으로 송신한다. 시스템은 패스워드가 그것의 메모리에 있는 것과 일치되는지 여부를 확인한다. 일치되면, 인증된 상태가 리턴된다. 그렇지 않으면 그 어카운트에 대한 에러 카운터가 증가된다. 그리고 실체에 어카운트 id와 패스워드가 재 입력되는 것이 요구된다. 카운터가 오버플로우 되면 시스템은 접근이 거절되는 상태로 리턴된다.

[0213] 시도 응답

[0214] 도 20은 시도/응답 유형의 방법을 이용하는 인증을 설명하는 순서도이다. 실체는 어카운트 id를 보내고 시스템(10)으로부터 시도를 요청한다. 시스템(10)은 난수를 생성하고 그것을 호스트에 제시한다. 호스트는 상기 수로부터 응답을 계산하고 그것을 시스템(10)으로 송신한다. 시스템(10)은 응답과 저장된 값을 비교한다. 나머지 단계들은 접근이 승인되는지 여부를 결정하기 위한 도 19에서의 것들과 유사하다.

[0215] 도 21은 다른 시도/응답 유형의 방법을 이용하는 인증을 설명하는 순서도이다. 도 21은 호스트가 시스템(10)에 의해 인증되는 것이 요구되는 것이 부가된 점과, 시스템(10)이 또한 호스트로부터 시도를 요청하고 호스트에 의해 확인되는 응답을 리턴하는 시도/응답에 의해서 인증되는 것이 요구되는 점에서 도 20과 다르다.

[0216] 도 22는 다른 시도/응답 유형의 방법을 이용하는 인증을 설명하는 순서도이다. 이 경우 시스템(10)만이 인증될 것을 필요로 한다. 여기서 호스트는 시스템(10)에 시도를 보내는데, 이것은 시스템(10)의 레코드와 일치를 위해 호스트에 의해 확인되는 응답을 계산한 것이다.

[0217] 대칭 키

[0218] 대칭 키 알고리즘은 동일한 키가 암호화 및 복호화 양측에 이용됨을 의미한다. 그것은 키가 통신 전에 미리 동의되어야 함을 의미한다. 또한 각 측은 서로의 리버스 알고리즘, 즉 한 측은 암호화 알고리즘을 다른 측은 복호화 알로리즘을 구현해야만 한다. 양 측은 통신을 위한 양 측의 알고리즘들을 구현할 필요가 없다.

[0219] 인증

[0220] 대칭 키 인증은 장치(예를 들어 플래시 카드) 및 호스트가 동일한 키를 공유하고, 동일한 암호화 알고리즘(다이렉트 및 리버스 예를 들어 DES 및 DES-1)을 갖는 것을 의미한다.

[0221] 대칭 키 인증은 시도-응답을 의미한다(재송신 공격에 대해 보호함).

[0222] 보호된 장치는 다른 장치에 대한 시도를 생성하고 양자는 응답을 계산한다. 인증하는 장치는 응답을 반송하고, 보호되는 장치는 응답을 확인하고 그에 따라 인증을 검증한다. 그 후 인증과 결합된 권한이 부여될 수 있다.

[0223] 인증은 하기의 것일 수 있다:

[0224] 외부적: 장치(예를 들어 플래시 카드)는 외부세계를 인증한다. 즉 장치는 주어진 호스트 또는 애플리케이션의 크리덴셜을 검증한다.

[0225] 상호간: 시도는 양 측에서 생성된다.

[0226] 내부적: 호스트 애플리케이션은 장치(예를 들어 플래시 카드)를 인증한다. 즉 호스트는 장치가 그것의 애플리케이션을 위한 진정한 것인지를 확인한다.

[0227] 전체 시스템의 보안성 수준을 높이기 위해(즉 침입자 하나가 전부를 붕괴시키지 못하는),

[0228] 대칭 키는 보통 마스터 키를 이용한 다양화와 통합된다.

[0229] 상호 인증은 시도가 진짜 시도인지 보장하기 위해 양 측으로부터의 시도를 이용한다.

[0230] 암호화

[0231] 또한 대칭 키 암호기법은 그것이 매우 효과적인 알고리즘, 즉 암호기법을 다루기 위해 강력한 CPU가 필요하지 않기 때문에, 암호화를 위해 이용된다.

[0232] 통신 채널을 보안하기 위해 이용될 때 :

[0233] 양 장치들은 채널을 보안하기 위해 이용되는 세션 키를 알아야 한다(즉 나가는 모든 데이터를 암호화하고 들어오는 모든 데이터를 복호화한다). 이 세션 키는 보통 사전 공유되는 비밀 대칭 키 또는 PKI를 이용하여 형성된다.

[0234] 양 장치들은 동일한 암호화 알고리즘들을 알고 구현해야 한다.

[0235] 서명

[0236] 또한 대칭 키는 데이터에 서명하기 위해 이용될 수 있다. 이 경우 서명은 암호화의 부분적인 결과이다. 상기 부분적인 결과를 유지하는 것은 키 값을 노출하지 않고 필요한 수만큼 서명하는 것을 허락한다.

[0237] 발행들 및 제한들

[0238] 대칭적 알고리즘들은 매우 효과적이고 보안되지만 그들은 사전 공유된 비밀에 기초한다. 발행은 동적인 방식으로 이 비밀을 보안적으로 공유하고, 가능하면 그것을 무작위하게 갖는다(세션 키와 같이). 이 아이디어는 공유된 비밀이 장기간 안전성을 유지하기 어렵고 다수의 사람들이 공유하는 것이 거의 불가능한 것이다.

[0239] 이 동작을 용이하게 하기 위해, 공개 키 알고리즘이 그것이 그들을 공유함 없이 비밀들의 교환을 허락하도록 발명되었다.

[0240] 공개 키 암호 기법

[0241] 비대칭 키 알고리즘은 보통 공개 키 암호로 언급된다. 그것은 상당히 복잡하고 보통 CPU 집중적인 수학적 구현이다. 그것은 대칭 키 알고리즘들과 결합된 키 분배의 발행들을 해결하도록 발명되었다. 또한 그것은 데이터 무결성을 보장하기 위해 이용된 서명 능력들을 제공한다.

[0242] 비대칭 키 알고리즘은 각각 개인 키 및 공개 키로서 언급되는 개인 및 공개 엘리먼트들을 갖는 키를 이용한다. 개인 키 및 공개 키 양자는 서로 수학적으로 연결된다. 공개 키는 공유될 수 있는 반면 개인키는 비밀로 남아야만 한다. 키들을 위해, 비대칭적 알고리즘은 랩 및 언랩 또는 서명을 제공하고 검증하기 위해 두 개의 수학 함

수(하나는 개인키를 위한 것이고, 다른 하나는 공개 키를 위한 것임)을 이용한다.

[0243] 키 교환 및 키 분배

[0244] 키 교환은 PK 알고리즘을 이용하면 매우 간단하게 된다. 장치는 그것의 공개 키를 다른 장치에 보낸다. 다른 장치는 공개 키로 그것의 비밀 키를 싸서 제 1 장치로 암호화된 데이터를 리턴한다. 제 1장치는 데이터를 풀고, 양측에 알려지고 데이터 교환에 이용될 수 있는 비밀 키를 검색하기 위해, 그것의 개인키를 이용한다. 대칭 키가 그것을 쉽게 교환시킬 수 있기 때문에 보통 그것은 랜덤키이다.

[0245] 서명

[0246] 그것의 특성 때문에 공개 키 알고리즘은 보통 적은 양의 데이터를 서명하는 데만 이용된다. 데이터 무결성을 보장하기 위해, 그것은 그 후 메시지의 일 방향 풋 프린트(one-way foot print)를 제공하는 해시함수와 통합된다.

[0247] 개인키는 데이터를 서명하는데 이용된다. 공개 키(자유롭게 이용가능한)는 상기 서명을 검증하는 것을 허락한다.

[0248] 인증

[0249] 인증은 보통 서명을 이용한다: 시도는 서명되고 검증을 위해 리턴된다.

[0250] 키의 공개 부분이 검증을 위해 이용된다. 누구나 키 쌍을 생성할 수 있기 때문에, 이것이 정확한 키를 이용하는 정당한 사람임을 입증하기 위해 공개 키의 소유자를 인증할 필요가 있다. 인증기관은 인증을 제공하고 서명된 인증서 내의 공개 키를 포함할 것이다. 인증서는 상기 기관 자체에 의해 서명된다. 그 다음 서명을 검증하기 위한 공개 키의 사용은 그 키를 포함하는 인증서가 발행된 기관이 신뢰할 만하고, 인증서가 해킹되지 않았음을 검증할 수 있는, 즉 기관에 의해 서명된 인증서 해시가 정확하다는 것을 의미한다; 사용자가 기관 공개 키 인증서를 가지며 신뢰한다는 것을 의미함.

[0251] PK 인증을 제공하는 가장 일반적인 방식은 기관 및 최상위 인증서를 신뢰하는 것이고 주어진 기관에 의해 인증된 모든 키 쌍들을 간접적으로 신뢰하는 것이다. 인증하는 것은, 누군가 가진 개인키가 시도를 서명함에 의해 인증서와 일치되는 지를 증명하고 시도 응답, 및 인증서 제공하는 문제이다. 그 다음 인증서는 그것이 해킹되지 않았고 신뢰되는 기관에 의해 서명된 것이 확실한 지 확인된다. 그 후 시도 응답이 검증된다. 인증서가 신뢰되고 시도 응답이 정확하다면 인증은 성공적이다.

[0252] 장치(예를 들면 플래시 카드)에서 인증은 장치가 신뢰되는 최상위 인증서로 로드되고 장치가 해시 서명된 인증서뿐만 아니라 시도 응답을 검증할 수 있음을 의미한다.

[0253] 파일 암호화

[0254] PK 알고리즘은 다량의 데이터를 암호화하는데 이용되지 않는다. 그것이 너무 CPU 집중적이지만 보통 컨텐츠를 암호화하기 위해 생성되는 무작위적인 암호화/복호화 키를 보호하는데 이용되기 때문이다. 예를 들어 SMIME(보안 이메일)는 모든 수령인의 공개 키로 암호화된 키를 생성한다.

[0255] 발행들 및 제한들

[0256] 어떤 것은 키 쌍을 생성할 수 있기 때문에, 그것의 기원을 보장하기 위해 인증되어야만 한다. 키 교환 동안 비밀 키가 정당한 장치에 제공되는지 확인하는 것을 원할 수 있다. 즉 제공된 공개 키의 기원은 확인될 필요가 있을 것이다. 그 다음 크리덴셜 관리는 그것이 키의 정당성 및 키가 철회되었는지 여부를 통지할 수 있기 때문에 보안성의 부분이 된다.

[0257] 본 발명은 다양한 실시예들을 참조하여 상술되었지만, 본 발명의 범위를 벗어나지 않고 변경들 및 변형들이 가능하며, 본 발명의 범위는 첨부되는 청구항들 및 그들의 균등물에 의해서만 정의되는 것으로 이해될 것이다. 여

기서 언급된 모든 참조들은 참조로 추가된다.

[0258] **첨부 A**

[0259] **1. SSA 명령들**

[0260] SSA 시스템 명령들은 표준적인(관련된 폼 팩터 프로토콜을 위한) 쓰기 및 읽기 명령들을 이용하여 메모리 카드로 보내진다. 그러므로 호스트 관점에서 SSA 명령을 보내는 것은, 버퍼 파일로 이용되는 메모리 장치상의 특정 파일에 데이터를 쓰는 것을 실제로 의미한다. SSA 시스템으로부터 정보를 얻는 것은, 버퍼 파일로부터 데이터 읽기를 통해 이루어진다. 호스트 애플리케이션은 데이터가 항상 버퍼 파일의 제 1 LBA로부터 쓰여지고 읽혀지도록 확인해야만 한다. 호스트 OS에서 버퍼 파일들을 관리하는 것은 본 상세한 설명의 범위를 벗어나는 것이다.

[0261] **1.1 SSA 시스템과의 통신**

[0262] 다음 섹션들은 SSA 관련 명령들 및 데이터가 폼 팩터 표준 쓰기/읽기 명령들을 이용하여 SSA 시스템과 통신하는 방식을 정의한다.

[0263] **1.1.1 SSA 시스템에 명령들/데이터 송신**

[0264] 모든 쓰기 명령들의 제 1데이터 블록이 서명을 통해 패스에 대해 정밀 검사된다. 만약 발견된다면, 데이터가 SSA 명령들로서 해석된다. 만약 발견되지 않는다면, 데이터가 지정된 주소에 쓰여진다.

[0265] SSA 애플리케이션 특정 쓰기 명령들은 다중 섹터 송신을 포함할 것이다. 여기서 제 1 섹터는 요구되는 서명들 및 명령의 인수들(arguments)을 보유하고, 데이터 블록들의 나머지는 만약 있다면 관련된 데이터를 보유한다. 표는 SSA 명령의 제 1블록(데이터 블록들은 표준 OS 파일 시스템들에 이용되는 것으로서 항상 512 바이트들이다)의 포맷을 정의한다.

[0266] 표 1은 SSA 명령 인수 LBA 포맷을 나타낸다.

표 1

[0267]

바이트 색인	길이 (바이트)	설명	주석
0-31	32	서명을 통한 애플리케이션 패스	ASCⅡ스트링일 것 : “지원된 모드를 통한 SSTA 패스”
32	4	SSA애플리케이션 ID	0x00000000일 것
36	4	SSA 세션 ID	인증 프로세스를 통해 SSA 시스템에 의해 제공되는 것으로서의 SSA 세션 ID. 세션이 개방되지 않으면, 이 필드는 값 0x00000000을 포함할 것이다. 보안 채널이 이용될 때 명령 인수들(제 1 블록의 a\t 바이트 옵셋 64 시작) 및 데이터 블록들은 세션키로 암호화된다.
40	24	미래 사용을 위해 예비 할당	데이터는 미정의된다.
64	4	SSA 세션ID	SSA 세션 ID의 제 2 카피. 이 필드는 세션키의 유시지(usage)를 검증하는데 이용된다.
68	4	SSA애플리케이션 명령 op-코드	다음 섹션들에서 상세한 SSA 명령 설명으로 정의된 바와 같음
72	4	SSA 애플리케이션데이터 블록들	추가되는 데이터 블록들의 수. 데이터 블록들이 사용되지 않으면 0
76-511	436	SSA 애플리케이션명령 인수들	다음 섹션들에서 상세한 SSA 명령 설명으로 정의된 바와 같음

[0268] **1.1.2 SSA 시스템으로부터 데이터 읽기**

[0269] 읽기 명령들은 두 부분들로 실행될 것이다:

[0270] 1. 읽기 명령의 모든 인수들을 정의하는 하나의 데이터 블록을 가진 쓰기 명령을 첫번째 송신하여 읽기 명령 개시됨

[0271] 2. 쓰기 명령이 송신의 올바른 상태에서 카드 애플리케이션을 설정한 후에, 읽기 명령이 카드로부터 호스트로 실질적인 데이터 송신을 개시하는데 이용된다. 읽기 명령은 이전 쓰기 명령에 이용되는 동일한 LBA 주소를 이용해야만 한다. 이것은 호스트가 이전에 요청된 SSA 데이터를 얻기 위해 시도되는 카드로의 유일한 지시이다.

[0272] 쓰기/읽기 명령 쌍들은 주의 깊게 동기화 되어야만 한다. 다음 세션은 시퀀스 에러들이 처리되고 그로부터 회복되는 방법을 정의한다. 정의된 바와 같이 SSA 시스템은 다수의 호스트 측 사용자들을 지원한다. 이들은 동시적으로 로그온 될 수 있을 것이다. 각 사용자는 독립적으로 및 비동기적으로 쓰기/읽기 명령쌍들을 개시하는 것이 기대되므로, 호스트 OS의 임의의 특정 행동을 요구하지 않는다. 카드 관점에서 이들 개별적인 쌍들이 시퀀스의 도중 쓰기에 이용되는 LBA주소에 의해 식별된다. 호스트 관점에서 그것은 각 사용자가 다른 파일 버퍼를 이용해야만 하는 것을 의미한다.

[0273] **1.1.3 쓰기/읽기 시퀀스 에러들**

[0274] **1.2 명령들의 상세한 설명**

[0275] 표 2는 SSA 명령들의 일반적인 개요를 제공한다.

[0276] 명령 이름 칼럼은 명령들 유시지의 기본적인 설명 및 또한 명령의 상세한 설명에 대한 인덱스를 제공한다. 명령 op-코드는 SSA 명령에 사용되는 실제 값이다. 인수길이(Arg Len) 칼럼은 명령의 인수 필드의 크기를 정의한다(0 값은 인수가 없음을 의미한다)

[0277] 인수들은 명령 특정적이고 상세한 명령 설명에서 특정된다.

[0278] 데이터 길이는 명령들과 결합된 추가적인 데이터 블록들에서 명령 데이터의 크기이다. 0 값은 데이터가 없음을 의미하고, "Var"의 값은 명령이 다양한 데이터 크기들을 갖고 실질적인 크기는 명령 자체에 특정된다. 고정된 크기의 데이터 명령들의 경우 이 칼럼은 데이터 크기의 크기를 저장한다. 데이터 방향은 명령이 데이터를 가지고 있지 않다면(표1에 특정된 바와 같은 명령 인수들 모두가 바이트76과 바이트511사이의 공간에 적합하게 되고, 이것을 넘어서는 명령 섹터와 동반하는 데이터 페이로드가 놓인다는 것을 의미한다) 블랭크, 데이터가 호스트로부터 카드로 이동되면(쓰기 명령의 인수 블록에 첨부된) "쓰기", 또는 데이터가 카드로부터 호스트로 이동되면(상술한 바와 같이 인수들을 제공하는 쓰기 명령에 다음에 오는 읽기 명령에서) "읽기" 중 어느 하나일 수 있다.

[0279] 칼럼들과 관련된 모든 크기는 바이트 단위를 사용한다.

[0280] 표 2는 SSA 명령들을 나타낸다.

표 2

[0281]

Cmd OP-코드	명령이름 (Cmd name)	인수 길이	데이터 길이	데이터 방향	설명			
ACR/AGP 관리 명령들								
1	CREATE_SYSTEM ACR	1	0		SSA데이터베이스에서 시스템ACR엔트리를 생성하고 시스템 ACR구성 시퀀스를 시작한다.			
2	SYS_ACR_CREATION _DONE	0	0		시스템 ACR 구성 시퀀스를 종료하고 시스템 ACR을 활성화한다.			
3	PASSWORD_CREDENT IAL			쓰기	패스워드 인증을 사용한 ACR을 위한 크리덴셜 데이터를 제공한다.			
4	SYMMETRIC_CREDEN TIAL			쓰기	대칭적 인증을 사용한 ACR을 위한 크리덴셜 데이터를 제공한다.			
5	ASYMETRIC_CREDEN TIAL			쓰기	비대칭적 인증을 사용한 ACR을 위한 크리덴셜 데이터를 제공한다.			
6	GET_ACR_PUBLIC_K EY			쓰기	CA에 의한 서명을 위한 ACR의 공개키를 입수한다. ACR이 생성되었을 때 SSA 시스템에서 생성된 ACR RSA 키쌍			

7	SEND_CERTIFICATE			읽기	ACR 공개 키를 서명하기 위한 크리덴셜을 제공한다.			
8	CONFIGURE_ACAM			쓰기	ACR의 ACAM(ACR 관리 권한들)레코드를 설정한다.			
9-15	미래사용을 위해 예비할당							
16	CREATE_ROOT_AGP			쓰기	SSA 시스템 데이터 베이스에서 루트 AGP엔트리 생성한다.			
17	ROOT_AGP_CREATION_DONE	0	0		루트 AGP의 구성 프로세스를 종료하고 그것을 활성화시킨다.			
18	DISBALE_SYSTEM_ACR_CREATION	0	0		시스템 ACR을 생성하고 구성하는 특징을 불능으로 한다.			
19	SET_ROOT_AGP_CREATION_MODE	1			루트 AGP 생성의 모드(개방, 제어됨 또는 차단)를 정의한다.			
20	DISBALE_ROOT_AGP_CHANGE_MODE				루트 AGP의 생성모드를 변경하는 특징을 불능으로 한다.			
21-25	미래사용을 위해 예비할당							
26	CREATE_AGP			쓰기	SSA 시스템 데이터베이스에서 AGP엔트리를 생성한다.			
27	DELETE_AGP			쓰기	SSA 시스템 데이터베이스에서 AGP엔트리를 제거한다.			
28	CREATE_ACR				SSA 시스템 데이터베이스 에서 ACR 엔트리를 생성한다.			
29	CREATE_ACR_DONE	0	0		ACR의 생성 및 구성 프로세스를 종료하고 그것을 활성화시킨다.			
30	DELETE_ACR			쓰기	SSA 시스템 데이터베이스로부터 ACR 엔트리를 제거한다.			
31	UNBLOCK_ACR			쓰기	차단된(인증 실패들로 인해) ACR을 차단 해제한다.			
32-49	미래사용을 위해 예비할당							
파티션 및 도메인 관리 명령들								
50	CREATE_PARTITION						쓰기	이 명령은 주어진 파티션을 두개로 분리한다. 그것은 루트 ACR에 의해서만 발행될 수 있다.

51	UPDATE_PARTITION			쓰기	두 개의 기존 파티션들의 크기를 변경한다. 이들 두 개의 파티션들의 전체 크기에 대한 순 변경은 0이어야 한다.
52	DELETE_PARTITION			쓰기	두 개의 기존 파티션들을 하나로 병합한다.
53	RESTRIC_PUBLIC_PARTITION_ACCESS			쓰기	표준(SSA가 아닌) 명령들을 이용하여 장치의 공용 파티션에 접근하는 ac를 가능케하다/불능케하다.
54-59	미래사용을 위해 예비할당				
60	CREATE_DOMAIN			쓰기	SSA 데이터베이스에서 보안성 도메인을 생성한다.
61	DELET_DOMAIN			쓰기	SSA 데이터베이스에서 보안성 도메인을 제거한다.
62-69	미래사용을 위해 예비할당				

70	DELEGATE_DOMAIN_PERMISSIONS			쓰기	접근 및 도메인의 소유자 권한을 특정 ACR로 위임 한다.
71	DELEGATE_PARTITION_PERMISSION			쓰기	파티션의 접근 권한을 특정 ACR로 위임 한다.
72-99	미래사용을 위해 예비할당				
시스템 로그인 및 인증 명령들					
100	SYSTEM_LOGIN			쓰기	
101	SYSTEM_LOGOUT	0	0	쓰기	
102-109	미래사용을 위해 예비할당				
110	SEND_PASSWORD TO SSA			쓰기	
111-119	미래사용을 위해 예비할당				
121	GET_SYMETRIC_CHALLENGE			읽기	
122	SEND_SYMETRIC_CHALLENGE			쓰기	
123	GET_SYMETRIC_CHALLENGE_RESPONSE			읽기	
124	SEND_SYMETRIC_CHALLENGE_RESPONSE			쓰기	
125-129	미래사용을 위해 예비할당				
130	SEND_ASYMETRIC_CHALLENGE			쓰기	
131	GET_ASYMETRIC_CHALLENGE			읽기	
132	SEND_USER_CERTIFICATE			쓰기	
133	GET_SSA_PRE_MASTER_SECRETE			읽기	
134	GET_ACR_CERTIFICATE			읽기	
135	SEND_HOST_PRE_MASTER_SECRET			쓰기	
136	START_SERSSION			쓰기	
137	AHUTHENTICATION_COMPLETE	0	0	읽기	
138-199	미래사용을 위해 예비할당				
읽기 쓰기 및 상태 명령들					
200	WRITE		Var	쓰기	쓰기 데이터명령
201	READ		Var	읽기	읽기 데이터명령

202	COMMAND_STATUS		Var	읽기	현재 SSA 명령 실행 상태를 입수한다.
203	SYSTEM_QUERY		Var	읽기	ACR 현재 구성 데이터의 요청을 입수한다.

[0282] 1.2.1 시스템 ACR 생성

[0283] 시스템 ACR 생성은 SSA 데이터베이스에서 시스템 ACR 엔트리를 만든다. 일단 엔트리가 생성되면, 크리덴셜들은 특정된 로그인 알고리즘에 따라 구성될 수 있다. 마지막으로 CREATE_SYSTEM_ACR_DONE명령은 시퀀스를 종료하고 시스템 ACR을 활성화시키기 위해 이용된다.

[0284] 시스템 ACR 생성 명령은 ACR 엔트리가 이미 존재하거나 시스템 ACR 생성 특징이 불능화된 경우라면 거절될 것이다. 시스템 ACR은 이용할 수 있는 로그인 모드들(섹션 1.3.2에 상세히 언급)의 하위집합만으로 구성될 것이다. 유효하지 않은 모드가 이용되면, 명령은 거절될 것이다.

[0285] 명령 인수들이 표3에 주어진다. 바이트 옵셋이 명령 인수 LBA(섹션1.1.1참조)의 시작과 관련된다. 인수길이는 바이트단위로 주어진다. 인수이름은 인수의 목적을 정의하며 상세한 인수 설명의 색인으로서 이용될 수 있다.

[0286] 표 3은 시스템 ACR 생성 명령 인수를 나타낸다.

표 3

[0287]

바이트 옵셋	인수 길이	인수 이름	주석
76	1	로그인 알고리즘	시스템 ACR은 다음의 로그인 알고리즘들에 의해서만 구성될 수 있다: ·AES, DES, 3DES, 상호 모드에서만 비대칭적 인증들

[0288] 1.2.2 시스템 ACR 생성 완료

[0289] 이 명령은 시스템 ACR 생성이 시작된 후에만 보내진다. 다른 때에는 명령이 거절될 것이다. 이 명령을 보냄으로써 시스템 ACR생성이 종료되고 현재 구성의 ACR이 영구히 남게 될 것이다.

[0290] 이 명령을 위한 인수들은 없다.

[0291] 1.2.3 패스워드 크리덴셜

[0292] SSA 명령[28]-CREATE_ACR-을 송신한 후에, 그 다음ACR의 크리덴셜들의 송신이 후속된다. 이 경우 그것은 일정 길이의 패스워드이다-최대 길이는 20바이트임.

[0293] 표 4는 패스워드 크리덴셜 명령 인수들을 나타낸다.

표 4

[0294]

바이트 옵셋	인수 길이	인수 이름	주석
76	바이트 인수 필드내의 패스워드 길이에 특정된 바와 같음	패스워드_크리덴셜	패스워드 프레이즈(password phrase) 포맷 및 길이에 관해 섹션 1.3.2 참조

[0295] 1.2.4 대칭적 크리덴셜

[0296] ACR를 위해 대칭적인 로그인 절차를 선택할 때, 그것은 AES, DES 또는 3DES 키 형태로 ACR의 대칭적인 크리덴셜을 보내는 것이 후속될 것이다. 알고리즘의 특징은 바이트로 크리덴셜의 (키)길이를 지시할 것이다. 이 명령은 규칙적인 ACR들 및 시스템 ACR 생성시에 사용될 수 있다.

[0297] 에러! 참조소스가 발견되지 않음. 표 13은 비대칭적인 크리덴셜들의 다른 유형들을 설명한다.

[0298] 표 5는 대칭적 크리덴셜 명령 인수들을 나타낸다.

표 5

[0299]

바이트 옵셋	인수 길이	인수 이름	주석
76	1	크리덴셜 유형	유형 값들 및 기호들을 위해 표13 에러! 참조소스가 발견되지 않음. 참조
78	1	크리덴셜 길이 바이트	
79	바이트 필드내의 크리덴셜 길이에 특정된 바와 같음	대칭적 크리덴셜	

[0300] 1.2.5 비대칭적 크리덴셜

[0301] 비대칭적 로그인 절차를 가진 ACR을 위해, SSA에 패스되어야만 하는 몇 개의 크리덴셜들이 있다. 다음의 표14는 비대칭적 크리덴셜의 다른 유형들을 설명한다:

[0302] 표 6은 비대칭적 크리덴셜 명령 인수들을 나타낸다.

표 6

[0303]

바이트 옵셋	인수 길이	인수 이름	주석
76	1	세션ID	세션 ID는 ACR ID의 필요성을 제거한다. 시스템 ACR생성시 이 필드는 ULL상태이다.
77	1	크리덴셜 유형	유형 값들 및 기호들을 위해 표13 에러! 참조소스가 발견되지 않음. 참조
78	1	크리덴셜 길이 바이트	
79	바이트 필드내의 크리덴셜 길이에 특정된 바와 같음	대칭적 크리덴셜	

[0304] 1.2.6 공개 키 보내기

[0305] 1.2.7 인증서 들여오기

[0306] 1.2.8 구성 아캄(CONFIGURE ACAM)

[0307] 이 명령의 송신은 ACR 관리 권한들을 구성한다. 명령은 ACR 생성 동안에만 송신된다. 명령은 시스템 ACR을 위해서는 유효하지 않다. ACAM 유형들 및 코드들은 표16에 설명된다: 아캄 유형들

[0308] 표 7은 구성 아캄 명령 인수들을 나타낸다.

표 7

[0309]

바이트 옵셋	인수 길이	인수 이름	주석
76	1	세션ID	시스템 ACR로그인 절차 후 이용될 때만 유효함. 그렇지 않으면 NULL로 남음
77	1	AGP 이름/ID 길이 바이트	최대 길이는 20 바이트이다.
78	바이트인수 필드내의 AGP 이름/ID 길이에 특정된 바와 같음	AGP 이름/ID	

[0310] 1.2.9 루트 AGP 생성

[0311] 보안 채널하에서 루트 AGP를 생성하기 위해, 시스템 ACR을 통한 SSA 시스템 로그인이 실행되어야만 한다. 로그인 후에, 세션 ID가 생성될 것이고 생성 시퀀스를 위해 이용될 것이다. 세션 ID는 시스템 ACR 로그인 시퀀스가 완료된 후에 시스템 명령 리턴 상태 권한이 요청된 때 이용될 수 있다. 시스템 ACR에 먼저 로그인 하지 않으면 (보안채널을 가진 루트 AGP를 생성한다) 루트 AGP의 생성은 세션 ID를 요구하지 않는다.

[0312] 표8은 명령들의 인수들을 검토한다. 시스템 ACR을 이용하지 않을 때, 세션 ID필드는 NULL(NA)로 남게 된다. AGP 이름/ID가 그것의 길이의 바이트 수만큼 선행된다.

[0313] 표 8은 루트 AGP 생성 명령 인수들을 나타낸다.

표 8

[0314]

바이트 옵셋	인수 길이	인수 이름	주석
76	1	세션ID	시스템 ACR로그인 절차 후 이용될 때만 유효함. 그렇지 않으면 NULL로 남음
77	1	AGP 이름/ID 길이 바이트	최대 길이는 20 바이트이다.
78	바이트인수 필드내의 AGP 이름/ID 길이에 특정된 바와 같음	AGP 이름/ID	

[0315] **명령 구조**:

[0316] · 명령 이름/OP 코드 - 1 바이트 : SSA_CREATE_ROOT_AGP_CMD [3]

[0317] · 명령 인수들-

[0318] 1. 세션 ID- 그것이 필요로 되는가?

[0319] 2. AGP 이름/ID 길이 바이트- 1 바이트

[0320] 3. AGP 이름/ID-

[0321] 1.2.10 루트 AGP 생성 완료

[0322] 이 명령은 루트 AGP가 완료될 때-AGP내의 모든 ACR들이 생성된 것을 의미함-전달된다. 이 명령은 AGP를 잠그므로 더 이상 ACR들이 생성될 수 없다. 이 명령에 대한 인수들은 없다.

[0323] **명령 구조**:

[0324] · 명령 이름/OP 코드 - 1 바이트 :

[0325] SSA_ROOT_AGP_CREATION_DONE_CMD [4]

[0326] · 명령 인수들-

[0327] 1. 세션 ID- 그것이 필요로 되는가?

[0328] 2. AGP 이름/ID 길이 바이트- 1 바이트

[0329] 3. AGP 이름/ID -

[0330] ### 1.2.11 시스템 ACR 생성 불능

[0331] 이 명령을 송신하면 시스템 ACR을 생성하는 능력이 종료될 것이다.

[0332] 이 명령에 대한 인수들은 없다.

[0333] ### 1.2.12 루트 AGP 생성 모드 설정

[0334] 루트 AGP의 생성을 제어하는 것은, SSA 명령[19] SET _ROOT_AGP_CREATION_MODE에 의해 처리된다.

[0335] 다른 모드들을 위한 코드들은 표9에 설명된다. 이 명령은 SSA에 로그인이 요구되지 않고 따라서 필요로 되는 세션 ID가 없다.

[0336] 표 9는 루트 AGP 생성 모드들을 나타내고, 표 10은 루트 AGP 생성 모드 설정 명령 인수들을 나타낸다.

표 9

[0337]

모드이름	코드	설명
개방(OPEN)	1	루트 AGP 생성이 시스템ACR 또는 정규 개방채널 중 어느 하나를 통해 될 수 있다.
제어(CONTROLLED)	2	시스템 ACR만을 통해서만 루트 AGP 생성
잠금(LOCKED)	3	루트 AGP가 생성되지 않는다.

표 10

[0338]

바이트 옵셋	인수길이	인수이름	주석
76	1	루트AGP 크리덴셜 모드	

[0339] ### 1.2.13 루트 AGP 변경 모드 불능

[0340] 이 명령은 SET_ROOT_AGP_CREATION_MODE 명령이 작동될 수 없게 하고, 그것은 SSA에 의해 거절될 것이다. 이 명령은 인수들을 갖지 않는다.

[0341] ### 1.2.14 AGP 생성

[0342] 표 11은 AGP 명령 인수들을 나타낸다.

표 11

[0343]

바이트 옵셋	인수 길이	인수이름	주석
76	1	세션 ID	
77	1	AGP 이름/ID 길이 바이트	최대 길이는 20 바이트이다.
78	바이트인수 필드내의 AGP 이름/ID 길이에 특정된 바와 같음	AGP 이름/ID	

[0344] **명령 구조**:

[0345] · 명령 이름/OP 코드 - 1 바이트 : SSA_CREATE_AGP_CMD[5]

[0346] · 명령 인수들-

[0347] 1. 세션 ID- 1 바이트

[0348] 2. AGP 이름/ID 길이 바이트- 1 바이트

[0349] 3. AGP 이름/ID-

[0350] 1.2.15 AGP 제거

[0351] 이 명령은 AGP를 생성했던 ACR에 유효하고 ACR들이 비어 있는 ACR들에 부여된다.

[0352] **명령 구조**:

[0353] · 명령 이름/OP 코드 - 1 바이트 : SSA_DELETE_AGP_CMD[6]

[0354] · 명령 인수들-

[0355] 1. 세션 ID- 1바이트

[0356] 2. AGP 이름/ID 길이 바이트- 1 바이트

[0357] 3. AGP 이름/ID ?

[0358] 1.2.16 ACR 생성

[0359] **명령 구조**:

[0360] · 명령 이름/OP 코드 - 1 바이트 : SSA_CREATE_ACR_CMD[7]

[0361] · 명령 인수들-

[0362] 1. AGP 이름/ID-

[0363] 2. ACR 이름/ID-

[0364] 3. 로그인 알고리즘- 1 바이트

[0365] 4. 키 길이

[0366] 5. ACR 이름/ID의 차단해제

[0367] 6. 관리 권한들 (ACAM)의 수-1바이트

[0368] 7. ACAM #1

[0369] 8. ACAM #n

[0370] 1.2.17 ACR 업데이트

[0371] 이 명령은 자식 ACR를 업데이트하기 위해 ACR 생성자에 의해서만 송신될 수 있다. 루트 AGP내에 있는 ACR들은 그들이 부모 ACR을 갖지 않기 때문에 업데이트될 수 없다.

[0372] **명령 구조**:

[0373] · 명령 이름/OP 코드 - 1 바이트 : SSA_UPDATE_ACR_CMD[8]

[0374] · 명령 인수들-

[0375] 1. 세션 ID- 1바이트

[0376] 2. AGP 이름/ID 길이 바이트- 1 바이트

[0377] 3. AGP 이름/ID -

[0378] 4. ACR 이름/ID 길이 바이트- 1 바이트

[0379] 5. ACR 이름/ID-

[0380] 1.2.18 ACR 제거

[0381] 이 명령은 자식 ACR를 제거하기 위해 ACR 생성자에 의해서만 송신될 수 있다. 루트 AGP내에 있는 ACR들은 스스로를 제거할 수 있는 능력을 갖는다.

[0382] **명령 구조**:

[0383] · 명령 이름/OP 코드 - 1 바이트 : SSA_DELETE_ACR_CMD[9]

[0384] · 명령 인수들-

[0385] 1. 세션 ID- 1바이트

[0386] 2. AGP 이름/ID 길이 바이트- 1 바이트

[0387] 3. AGP 이름/ID -

[0388] 4. ACR 이름/ID 길이 바이트- 1 바이트

[0389] 5. ACR 이름/ID-

[0390] 1.2.19 ACR 차단 해제

[0391] 이 명령은 일정 ACR을 차단 해제하는 명시적인 권한을 가진 ACR에 의해서만 송신될 수 있다.

[0392] **명령 구조**:

[0393] · 명령 이름/OP 코드 - 1 바이트 : SSA_UNBLOCK_ACR_CMD[10]

[0394] · 명령 인수들-

[0395] 1. 세션ID- 1바이트

[0396] 2. AGP 이름/ID 길이 바이트- 1 바이트

[0397] 3. AGP 이름/ID -

[0398] 4. ACR 이름/ID 길이 바이트- 1 바이트

[0399] 5. ACR 이름/ID-

[0400] 1.2.20 도메인 권한 위임

[0401] **명령 구조**:

[0402] · 명령 이름/OP 코드 - 1 바이트 :

[0403] SSA_DELEGATE_DOMAIN_PERMISSION_CMD [11]

[0404] · 명령 인수들-

[0405] 1. 세션ID- 1바이트

[0406] 2. 위임하기 위한 권한들의 수- 1 바이트

[0407] 3. 위임된 권한 코드

[0408] 4. 도메인 이름/ID 길이 바이트- 1 바이트

[0409] 5. 도메인 이름/ID

[0410] 1.2.21 **파티션 생성**

[0411] 이 명령은 루트 AGP에 있는 ACR에 의해서만 송신될 수 있다.

[0412] **명령 구조**:

[0413] · 명령 이름/OP 코드- 1 바이트: SSA_CREATE_PARTITION_CMD [12]

[0414] · 명령 인수들-

[0415] 1. 세션ID- 1바이트

[0416] 2. 파티션 이름/ID 길이 바이트- 1 바이트

[0417] 3. 파티션 이름/ID

[0418] 4. 섹터들 [512 바이트] 내에서 파티션 크기 - 4 바이트

[0419] 5. 감소된 파티션 이름/ID 길이 바이트- 1 바이트

[0420] 6. 감소된 파티션 이름/ID

[0421] 1.2.22 **파티션 업데이트**

[0422] 이 명령은 루트 AGP에 있는 ACR에 의해서만 송신될 수 있다.

[0423] **명령 구조**:

[0424] · 명령 이름/OP 코드 -1 바이트 : SSA_UPDATE_PARTITION_CMD [13]

[0425] · 명령 인수들-

[0426] 1. 세션ID- 1바이트

[0427] 2. 파티션 이름/ID 길이 바이트- 1 바이트

[0428] 3. 파티션/ID

[0429] 4. 섹터들 [512 바이트] 내에서 파티션 크기 - 4 바이트

[0430] 5. 감소 파티션 이름/ID 길이 바이트- 1 바이트

[0431] 6. 감소 파티션 이름/ID

[0432] 1.2.23 **파티션 제거**

[0433] 이 명령은 루트 AGP에 있는 ACR에 의해서만 송신될 수 있다.

[0434] **명령 구조**:

[0435] · 명령 이름/OP 코드 - 1바이트 :

[0436] SSA_DELETE_PARTITION_CMD [14]

[0437] · 명령 인수들-

[0438] 6. 세션 ID- 1바이트

[0439] 7. 파티션 이름/ID 길이 바이트- 1 바이트

[0440] 8. 파티션 이름/ID

[0441] 1.2.24 공용 도메인 접근 제한

[0442] 이 명령은 정규 읽기/쓰기 명령들(호스트에 의해 송신된 명령들이고 SSA 명령 프로토콜의 일부가 아님)을 공용 파티션(a.k.a. 사용자 영역)로/로부터 제한할 것이다.

[0443] **명령 구조**:

[0444] · 명령 이름/OP 코드 - 1 바이트 :

[0445] SSA_RESTRICT_PUBLIC_PARTITION_CMD [15]

[0446] · 명령 인수들-

[0447] 1. 세션 ID- 1바이트

[0448] 2. 공용 파티션 제한 코드- 1 바이트

[0449] 1.2.25 도메인 생성

[0450] **명령 구조**:

[0451] · 명령 이름/OP 코드 -1 바이트 :SSA_CREATE_DOMAIN_CMD[16]

[0452] · 명령 인수들-

[0453] 1. 세션 ID- 1바이트

[0454] 2. 파티션 이름/ID 길이 바이트- 1 바이트

[0455] 3. 파티션 이름/ID

[0456] 4. 도메인 이름/ID 길이 바이트- 1 바이트

[0457] 5. 도메인 이름/ID

[0458] 1.2.26 도메인 제거

[0459] 도메인 소유자만이 이 명령을 송신하고 도메인을 제거할 수 있다.

[0460] **명령 구조**:

[0461] · 명령 이름/OP 코드 -1 바이트 :SSA_DELETE_DOMAIN_CMD[17]

[0462] · 명령 인수들-

[0463] 1. 세션 ID- 1바이트

[0464] 2. 파티션 이름/ID 길이 바이트- 1 바이트

[0465] 3. 파티션 이름/ID

[0466] 4. 도메인 이름/ID 길이 바이트- 1 바이트

[0467] 5. 도메인 이름/ID

[0468] 1.2.27 시스템 로그인

[0469] 이 명령은 호스트 사용자가 ACR들 중 하나를 통해 SSA 시스템을 사용하기 원할 때 발행된다. 명령은 로그인/인증 프로세스를 시작할 것이다.

[0470] **명령 구조**:

[0471] · 명령 이름/OP 코드 -1 바이트 : SSA_SYSTEM_LOGIN_CMD[18]

[0472] · 명령 인수들-

[0473] 1. AGP 이름/ID 길이 바이트- 1 바이트

[0474] 2. AGP 이름/ID -

[0475] 3. ACR 이름/ID 길이 바이트- 1 바이트

[0476] 4. ACR 이름/ID-

[0477] 1.2.28 시스템 로그아웃

[0478] 이 명령은 호스트 사용자가 SSA 시스템으로 작업 세션을 종료하기 원할 때 발행된다. 이 명령은 현재 로그인 세션을 위한 모든 사용자 활동을 종결 시킨다. 이 명령 후에 호스트 사용자는 SSA 시스템으로 추가 액션들을 실행할 수 있도록 로그인 프로세스를 다시 시작할 필요가 있을 것이다.

[0479] **명령 구조**:

[0480] · 명령 이름/OP 코드-1 바이트:SSA_SYSTEM_LOGOUT_CMD [19]

[0481] · 명령 인수들-

[0482] 1. AGP 이름/ID 길이 바이트- 1 바이트

[0483] 2. AGP 이름/ID -

[0484] 3. ACR 이름/ID 길이 바이트- 1 바이트

[0485] 4. ACR 이름/ID-

[0486]

[0487] 1.2.29 읽기

[0488] **명령 구조**:

[0489] · 명령 이름/OP 코드 -1 바이트 :SSA_READ_CMD[20]

[0490] · 명령 인수들-

[0491] 1. 세션 ID- 1바이트

[0492] 2. 파티션 이름 길이 바이트- 1 바이트

[0493] 3. 파티션 이름

[0494] 4. 도메인 이름 길이 바이트- 1 바이트

[0495] 5. 도메인 이름

[0496] 6. 파티션 주소 (LBA)-4 바이트

[0497] 7. 읽기를 위한 LBA들의 수 (섹터들-섹터=512바이트)-4바이트

[0498] 1.2.30 쓰기

[0499] **명령 구조**:

[0500] · 명령 이름/OP 코드 -1 바이트 :SSA_WRITE_CMD[21]

[0501] · 명령 인수들-

[0502] 1. 세션ID- 1바이트

[0503] 2. 파티션 이름 길이 바이트- 1 바이트

[0504] 3. 파티션 이름

[0505] 4. 도메인 이름 길이 바이트- 1 바이트

[0506] 5. 도메인 이름

[0507] 6. 파티션 주소 (LBA)-4 바이트

[0508] 7. 읽기를 위한 LBA들의 수 (섹터들-섹터=512바이트)-4바이트

[0509] 1.2.31 명령 상태(Command Status)

[0510] 이 상태 명령은 송신된 이전 명령의 리턴 상태를 입수하고자 할 때 송신된다. 상태는 명령 프로세스 및 SSA 시스템 상태를 다룬다.

[0511] **명령 구조**:

[0512] · 명령 이름/OP 코드 -1 바이트 :SSA_CMD_STATUS_CMD[22]

[0513] · 명령 인수들-

[0514] 1. 세션 ID- 1바이트

[0515] 1.2.32 시스템 질의

[0516] 시스템 질의 명령은 로그인 된 ACR의 범위 내에 있는 SSA정보를 읽는다.

[0517] **명령 구조**:

[0518] 명령 이름/OP 코드 -1 바이트 :SSA_SYS_QUERY_CMD[23]

[0519] 명령 인수들-

[0520] 1. 세션 ID- 1바이트

[0521]

[0522] 1.2.33 패스워드 인증 명령들

[0523] 1.2.33.1 SSA로 패스워드 송신

[0524] 이 명령은 SSA에 의해 검증될 실제 ACR 패스워드를 송신한다. 이 명령 상태 명령(22)를 송신함으로써, 호스트가 명령 상태 및 인증 프로세스의 상태 명령 완료-패스/실패-을 읽을 수 있게 할 것이다.

[0525] **명령 구조**:

[0526] · 명령 이름/OP 코드-1 바이트: SSA_PWD_AUTH_SEND PWD_CMD [24]

[0527] · 명령 인수들-

[0528] 1. 패스워드 길이 바이트- 1바이트

[0529] 2. 패스워드 데이터

[0530] 1.2.34 대칭적 인증 명령들

[0531] 1.2.34.1 SSA로부터 시도 입수

[0532] **명령 구조**:

[0533] · 명령 이름/OP 코드 - 1 바이트 :

[0534] SSA_SYM_AUTH_GET_CHLG_CMD [25]

[0535] · 명령 인수들-

[0536] 1.2.34.2 SSA로 시도 송신

[0537] **명령 구조**:

[0538] · 명령 이름/OP 코드 -1 바이트 :

[0539] SSA_SYM_AUTH_SEND_CHLG_CMD [26]

[0540] · 명령 인수들-

[0541] 1.2.34.3 SSA로부터 시도 응답 입수

[0542] **명령 구조**:

[0543] · 명령 이름/OP 코드 -1 바이트 :

[0544] SSA_SYM_AUTH_GET_CHLG_RES_CMD [27]

[0545] · 명령 인수들-

[0546] 1.2.34.4 SSA로부터 시도 응답 송신

[0547] **명령 구조**:

[0548] · 명령 이름/OP 코드 -1 바이트 :

[0549] SSA_SYM_AUTH_SEND_CHLG_RES_CMD [28]

[0550] · 명령 인수들-

[0551] 1.2.35 비대칭적 인증 명령들

[0552] 1.2.35.1 SSA로 시도 송신

[0553] **명령 구조**:

[0554] · 명령 이름/OP 코드 -1 바이트 :

[0555] SSA_ASYM_AUTH_SEND_CHLG_CMD [29]

[0556] · 명령 인수들- 시도 난수-28바이트

[0557] 1.2.35.2 SSA로부터 시도 입수

[0558] **명령 구조**:

[0559] · 명령 이름/OP 코드 -1 바이트 :

[0560] SSA_ASYM_AUTH_GET_CHLG_CMD [30]

[0561] · 명령 인수들-NA

[0562] 1.2.35.3 SSA로 CA 크리덴셜 송신

[0563] **명령 구조**:

[0564] · 명령 이름/OP 코드 -1 바이트 :

[0565] SSA_ASYM_AUTH_SEND_CA_CERT_CMD [31]

[0566] · 명령 인수들-

[0567] 1.2.35.4 SSA 프리-마스터 비밀 입수

[0568] **명령 구조**:

[0569] · 명령 이름/OP 코드 -1 바이트 :

[0570] SSA_ASYM_AUTH_GET_PRE_MASTER_SECRET_CMD [32]

[0571] · 명령 인수들-

[0572] 1.2.35.5 SSA로부터 ACR 인증서 입수

[0573] **명령 구조**:

[0574] · 명령 이름/OP 코드 -1 바이트 :

[0575] SSA_ASYM_AUTH_GET_CHLG_CMD [33]

[0576] · 명령 인수들-

[0577] 1.2.35.6 SSA로 호스트 프리-마스터 비밀 송신

[0578] **명령 구조**:

[0579] · 명령 이름/OP 코드 -1 바이트 :

[0580] SSA_ASYM_AUTH_SEND_PRE_MASTER_SECRET_CMD[34]

[0581] · 명령 인수들-

[0582] 1.2.35.7 세션 시작 메시지 송신

[0583] **명령 구조**:

[0584] · 명령 이름/OP 코드 -1 바이트 :

[0585] SSA_ASYM_AUTH_SEND_START_SESSION_MSG_CMD [35]

[0586] · 명령 인수들-

[0587] 1. PIN 옵션-

[0588] 2. PIN 길이 바이트-

[0589] 3. PIN 스트링-

[0590] 1.2.35.8 SSA로부터 인증 완료 메시시 입수

[0591] **명령 구조**:

[0592] · 명령 이름/OP 코드 -1 바이트 :

[0593] SSA_SYM_AUTH_GET_CHLG_CMD [36]

[0594] · 명령 인수들-

[0595] 1.3 SSA 명령 인수들

[0596] 1.3.1 해당 사항 없음(Not Applicable)

[0597] 인수 리스트 내에서 해당 사항 없음(NA, 이용불가)으로 정의된 모든 필드들은 0으로 설정되어야 한다.

[0598] ### 1.3.2 패스워드 및 PIN구조

[0599] 패스워드 및 PIN 프레이즈들은 20바이트 길이이고 SSA 시스템에 2진 값이다. 20바이트보다 짧은 프레이즈는 "0"으로 패딩되어야만 한다.

[0600]

'0'의 패딩											프레이즈(phrase)								
MSB19																			LSE 0
00	00	00	00	00	00	00	49	F3	70	15	CC	52	74	A1	EC	2B	00	01	05

[0601] ### 1.3.3 로그인 알고리즘

[0602] 이 인수는 ACR의 로그인 알고리즘을 정의한다. 그것은 1 바이트 길이이다. 이용가능한 값들이 다음 표에서 정의된다:

[0603] 표 12는 로그인 알고리즘 유형들을 나타낸다.

표 12

[0604]

기호	값	설명
NONE	0	인증이 요구되지 않는다. 이 세션은 시스템 로그인 명령이 이 ACR을 위해 발행되자마자 개방된다.
PASSWORD	1	패스워드 기반의 인증
미래사용을 위해 예비할당	2-9	
AES_HOST_AUTH	10	AES 알고리즘을 이용한 일 방향 대칭적 인증. 카드는 인증사용자이다.
AES_HOST_AUTH_SEC	11	AES 알고리즘을 이용한 일 방향 대칭적 인증. 카드는 인증사용자이다. 보안채널이 이 ACR을 위해 형성되고 이용된다.
AES_HOST_AUTH_SEC_PIN	12	AES 알고리즘을 이용한 일 방향 대칭적 인증. 카드는 인증사용자이다. 보안채널이 이 ACR을 위해 형성되고 이용된다. 인증은 추가된 PIN이 제공된 후에 완성된다.
AES_MUTUAL_AUTH	13	AES 알고리즘을 이용한 양방향 대칭적 인증. 카드 및 호스트는 서로 인증한다.
AES_MUTUAL_AUTH_SEC	14	AES 알고리즘을 이용한 양방향 대칭적 인증. 카드 및 호스트는 서로 인증한다. 보안채널이 이 ACR을 위해 형성되고 이용된다.
AES_MUTUAL_AUTH_SEC_PIN	15	AES 알고리즘을 이용한 이중 대칭적 인증. 카드 및 호스트는 서로 인증한다. 보안채널이 이 ACR을 위해 형성되고 이용된다. 인증은 추가된 PIN이 제공된 후에 완료된다.
미래사용을 위해 예비할당	16-19	
DES_HOST_AUTH	20	DES알고리즘이 이용되는 예외를 가진 로그인 모드들의 AES 그룹과 유사
DES_HOST_AUTH-SEC	21	
DES_HOST_AUTH-SEC_PIN	22	
DES_MUTUAL_AUTH	23	
DES_MUTUAL_AUTH-SEC	24	
DES_MUTUAL_AUTH-SEC_PIN	25	
미래사용을 위해 예비할당	26-29	
3DES_HOST_AUTH	30	3DES알고리즘이 이용되는 예외를 가진 로그인 모드들의 AES 그룹과 유사
3DES_HOST_AUTH_SEC	31	
3DES_HOST_AUTH_SEC_PIN	32	
3DES_MUTUAL_AUTH	33	
3DES_MUTUAL_AUTH_SEC	34	

3DES_MUTUAL_AUTH_SEC_PIN	35	
미래사용을 위해 예비할당	36-39	
RSA_HOST_AUTH	40	
RSA_HOST_AUTH_PIN	41	
RSA_MUTUAL_AUTH	42	
RSA_MUTUAL_AUTH_PIN	43	
미래사용을 위해 예비할당	44-225	

[0605] 1.3.4 **대칭적 크리덴셜 기호들**

[0606] 표 13은 대칭적 크리덴셜 유형들을 나타낸다.

표 13

[0607]

기호	값	설명
SYMMETRIC_KEY	1	선택된 대칭적 인증 시퀀스에 대응하는 대칭 키. 선택된 인증 시퀀스는 또한 그 키 길이에 반영될 것이다.
USER_PIN	2	PIN은 최대 20바이트의 2진 값이다.

[0608] 1.3.5 **비대칭적 크리덴셜 유형들**

[0609] 표 14는 비대칭적 크리덴셜 유형들을 나타낸다.

표 14

[0610]

기호	값	설명
CA_ID		
CA_PUBLIC_RSA_KEY	1	
ACR_CRETIFICATE	2	
USER_PIN	4	

[0611] 1.3.6 **파티션 권한들**

[0612]

파티션 권한들 바이트 비트맵							
읽기	쓰기	위임	예비할당	예비할당	예비할당	예비할당	예비할당

[0613] 1.3.7 **도메인 권한들**

표 15

[0614]

도메인 권한들 바이트 비트맵							
읽기	쓰기	위임	예비할당	예비할당	예비할당	예비할당	예비할당

[0615] 1.3.8 **도메인 권한 코드리들**

[0616] 표 16은 도메인 권한 유형들을 나타낸다.

표 16

[0617]

기호	값	설명
READ	1	
WRITE	2	
DOMAIN_PERMISSION_DELEGATION	3	
DOMAIN_OWNERSHIP	4	

[0618] 1.3.9 아캄(ACAM)

[0619] 표 17은 아캄 유형들을 나타낸다.

표 17

[0620]

기호	값	설명
CREATE-AGP	1	
ACAM_CREATE_ACR	2	AGP들 및 ACR의 생성/제거/업데이트
ACAM_CREATE_PARTITION	3	파티션들의 생성/제거
ACAM_CREATE_DOMAIN	4	도메인들의 생성/제거
ACAM_DELEGATE_DOMAIN_RIGHTS	5	도메인에 대한 접근 권한을 위임한다-이것은 도메인마다 이루어진다.
ACAM_DELEGATE_PARTITION_RIGHTS	6	파티션에 대한 접근 권한을 위임한다-이것은 파티션마다 이루어진다.
UNBLOCK_ACR	7	

[0621] 1.3.10 공용 파티션 제한 코드들

[0622] 표 18은 공용 파티션 제한 유형들을 나타낸다.

표 18

[0623]

기호	값	설명
READ_RESTRICTION	1	
WRITE_RESTRICTION	2	
READ_WRITE_RESTRICTION	3	

[0624] 1.3.11 명령 상태

표 19

[0625]

필드이름	컨텐츠	바이트 수
세션ID	ID 번호	1
마지막 명령 OP-코드	유효한 SSA 명령 OP-코드	1
마지막 명령 상태	· 컴플리트_OK_0(COMPLETE_OK_0) · 컴플리트 _에러_1(COMPLETE_ERROR_1) · 비지_2(BUSY_2)	1
에러 코드		1
인증상태	인증 명령들을 위해서만 이용할 수 있음	1
전달된 섹터들의 수	데이터 송신 명령들을 위해서만 이용할 수 있음	

[0626] 1.3.12 SSA 질의

표 20

[0627]

필드이름	컨텐츠	바이트 수
세션ID	ID 번호	1
마지막 명령 OP-코드	유효한 SSA 명령 OP-코드	1
마지막 명령 상태	· 컴플리트_OK_0(COMPLETE_OK_0) · 컴플리트 _에러_1(COMPLETE_ERROR_1) · 비지_2(BUSY_2)	1
에러 코드		1
SSA 버전	버전 번호	1
접근가능한 파티션 리스트	파티션ID, 순 크기 및 접근권한	
접근가능한 도메인 리스트	도메인 ID, 순 크기 및 접근권한	

[0628] 1.3.13 명령 시퀀스들

[0629] 1.3.13.1 상호 대칭적 인증에 의한 SSA 로그인을 위한 명령 시퀀스

[0630]

시퀀스 색인	명령이름 및 Op-코드	인수설명	일반적인 설명
1	SSA_SYSTEM_LOGIN_CMD-[18]	ACR 및 AGP 이름들	로그인 시퀀스 시작. 요청으로만 작동
2	SSA_CMD_STATUS_CMD-[22]	세션ID - NA	CMD18에 대한 상태를 입수한다. CMD18이 실패하면, 그 후 로그인 시퀀스가 종료된다
3	SSA_SYM_AUTH_SEND_CHLG_CMD-[26]	시도#1	시도#1을 SSA에 송신한다
4	SSA_CMD_STATUS_CMD-[22]	세션ID-NA	CMD26에 대한 상태를 입수한다. CMD26이 실패하면, 그 후 로그인 시퀀스가 종료된다
5	SSA_SYM_AUTH_GET_CHLG_RES_CMD-[27]	NA	시도#1에 대한 SSA응답을 읽는다. 호스트는 그 응답이 유효한지 검증한다
6	SSA_CMD_STATUS_CMD-[22]	세션ID-NA	CMD27에 대한 상태를 입수한다. CMD27이 실패하면, 그 후 로그인 시퀀스가 종료된다
7	SSA_SYM_AUTH_GET_CHLG_CMD-[25]	NA	SSA로부터 시도#2을 읽는다
8	SSA_CMD_STATUS_CMD-[22]	세션ID-NA	CMD25에 대한 상태를 입수한다. CMD25가 실패하면, 그 후 로그인 시퀀스가 종료된다
9	SSA_SYM_AUTH_SEND_CHLG_RES_CMD-[28]	시도#2응답	시도#2응답을 SSA에 송신한다
10	SSA_CMD_STATUS_CMD-[22]	세션ID-NA	CMD28에 대한 상태를 입수한다. CMD28이 실패하면, 그 후 로그인 시퀀스가 종료된다. 이 단계에서 명령 상태는 인증 프로세스가 성공적으로 완료되었는지 또는 실패했는지 여부를 보여준다.

[0631] 이 시퀀스가 성공적으로 이루어진 때, SSA의 ACR는 로그인 되고 SSA 동작을 시작할 수 있다.

[0632] 1.3.13.2 루트 AGP를 생성하기 위한 명령 시퀀스

[0633] 루트 AGP는 시스템 ACR(시스템 ACR에 로그인 시퀀스의 실행을 요구하는)을 통해 또는 보안 채널을 무시하고 ACR 인증 프로세스를 건너뛰고 생성될 수 있다. 명령 SSA_CREATE_ROOT_AGP_CMD[3]이 루트 AGP의 식별자와 함께 송신된다.

[0634] SSA가 이 명령을 거절하지 않았고 에러 없이 이루어졌음을 확인하기 위해, 이 명령에 이어서

SSA_CMD_STATUS_CMD[22]가 후속될 수 있다.

[0635] 루트 AGP가 완성되고 루트 AGP를 봉인(seal)하기 위해 그것의 모든 ACR들이 생성된 때, SSA_ROOT_AGP_CREATION_DONE_CMD[4] 명령이 송신될 것이다.

[0636] **1.3.13.3 AGP생성을 위한 명령 시퀀스**

[0637] AGP를 생성하기 위해, 사용자는 1.3.13.1에 보여진 로그인 명령 시퀀스를 실행함으로써 먼저 SSA에 로그인해야 한다. AGP는 ACR들의 신규 그룹을 생성하기 전에 생성되어야만 한다. AGP는 AGP 이름/ID를 가진 명령 SSA_CREATE_AGP_ CMD[5]를 송신함으로써 생성된다.

[0638] CMD[5]가 에러 없이 수신되었고 실행되었는지를 검증하기 위해, 사용자는 SSA_CMD_STATUS_CMD[22]를 송신하고, 이전 송신된 명령의 상태를 읽는다. 사용자가 AGP의 생성을 마친 때 그는 ACR의 생성을 진행할 수 있거나 SSA 시스템으로부터 로그아웃 할 수 있다.

[0639] **1.3.13.4 ACR생성을 위한 명령 시퀀스**

[0640] ACR을 생성하기 위해, 사용자는 1.3.13.1에 보여진 로그인 명령 시퀀스를 실행함으로써 먼저 SSA에 로그인해야 한다. 또한 신규 ACR이 속한 AGP가 있어야 한다. 그 다음 사용자는 신규 ACR의 모든 데이터(이름, AGP, 로그인 방법들..등)를 가진 명령 SSA_CREATE_ACR_CMD[7]을 송신한다. CMD[7]이 에러 없이 수신되었고 실행되었는지를 검증하기 위해, 사용자는 SSA_CMD_STATUS_CMD[22]를 송신하고, 이전 송신된 명령의 상태를 읽는다.

[0641] 사용자가 ACR의 생성을 완료한 때 그는 다른 SSA 동작들을 진행할 수 있거나 SSA 시스템으로부터 로그아웃 할 수 있다.

[0642] **1.4 제품 파라미터들**

[0643] · 모든 실체들의 최대수(MAROs, ARCR, 병렬적인 세션들, 등)

[0644] · 이용할 수 있는 암호화 파라미터, 즉 RSA 키 길이에 대한 정의를 추가한다.

[0645] · 프로토콜들마다 에러 조건들 및 메시지들을 정의할 필요가 있다.

[0646] · 타임아웃 및 비지 핸들링을 정의할 필요가 있다

[0647] · 트리들의 레벨들의 수를 특정한다.

[0648] · 루트 MAROS의 #을 제한한다.

[0649] · 모든 위임 상의 자식들(루트상)의 #을 제한한다.

[0650] · 5-10과 같은 병렬적인 CBC 콘텍스트(contexts)의 수에 대한 제한일 수 있다.

[0651] · 프로토콜 및 제품 버전들

산업이용 가능성

[0652] 본 발명의 상세한 설명에 포함됨.

도면의 간단한 설명

[0653] 도 1은 본 발명을 도시하기에 유용한 호스트장치와 통신하는 메모리 시스템의 블록도이다.

[0654] 도 2는 본 발명의 일 실시예를 도시하기 위한, 메모리의 서로 다른 파티션들과 서로 다른 파티션들에 저장된 암호화되지 않은 또는 암호화된 파일들을 보여주는 개략도로서, 여기서 특정 파티션들 및 암호화된 파일들로의 접근은 접근 정책과 인증절차에 의해 제어된다.

[0655] 도 3은 상기 메모리 내의 상기 다른 파티션들을 보여주는 메모리의 개략도이다.

[0656] 도 4는 본 발명의 일 실시예를 도시하기 위한, 상기 파티션들의 상기 파일들의 일부가 암호화된 도 3에 도시된 상기 메모리의 다른 파티션들을 위한 파일 위치 테이블들의 개략도이다.

[0657] 도 5는 본 발명의 일 실시예를 도시하기 위한, 접근 제어된 레코드 그룹에서의 접근 제어 레코드 및 결합된 키

참조의 개략도이다.

[0658] 도 6은 본 발명의 일 실시예를 도시하기 위한, 접근 제어된 레코드 그룹들 및 접근 제어된 레코드들에 의해 형성된 트리 구조들의 개략도이다.

[0659] 도 7은 상기 트리들의 형성 프로세스를 도시하기 위해, 접근 제어된 레코드 그룹들의 3개의 계층적 트리들을 도시한 트리의 개략도이다.

[0660] 도 8a 및 8b는 시스템 접근 제어 레코드를 생성하고 이용하기 위해, 호스트 장치 및 메모리 카드와 같은 메모리 장치에 의해 수행되는 프로세스들을 도시한 순서도들이다.

[0661] 도 9는 본 발명을 도시하기 위한, 접근 제어된 레코드 그룹을 생성하기 위해 시스템 접근 제어 레코드를 이용하는 프로세스를 도시한 순서도이다.

[0662] 도 10은 접근 제어 레코드를 생성하기 위한 프로세스를 도시한 순서도이다.

[0663] 도 11은 상기 계층적 트리의 특정 응용을 도시하기 위해 유용한 2개의 접근 제어 레코드 그룹들의 개략도이다.

[0664] 도 12는 특정 권한들의 위임을 위한 프로세스를 도시한 순서도이다.

[0665] 도 13은 도 12의 위임 프로세스를 도시하기 위한 접근 제어된 레코드 그룹 및 접근 제어 레코드의 개략도이다.

[0666] 도 14는 암호화 및/또는 복호화 목적을 위한 키를 생성하는 프로세스를 도시한 순서도이다.

[0667] 도 15는 접근되고 제어된 레코드에 따라 데이터 접근을 위한 접근 권한 및/또는 권한(permission)을 제거하는 프로세스를 도시한 순서도이다.

[0668] 도 16은 접근 권한 및/또는 접근에 대한 권한이 삭제 또는 종료되었을 때 접근을 요청하는 프로세스를 도시한 순서도이다.

[0669] 도 17a 및 17b는 본 발명의 다른 실시예를 도시하기 위한, 암호화 키들에 접근을 승인하기 위한 정책들 및 인증을 위한 규칙 구조의 조직화를 도시하는 개략도들이다.

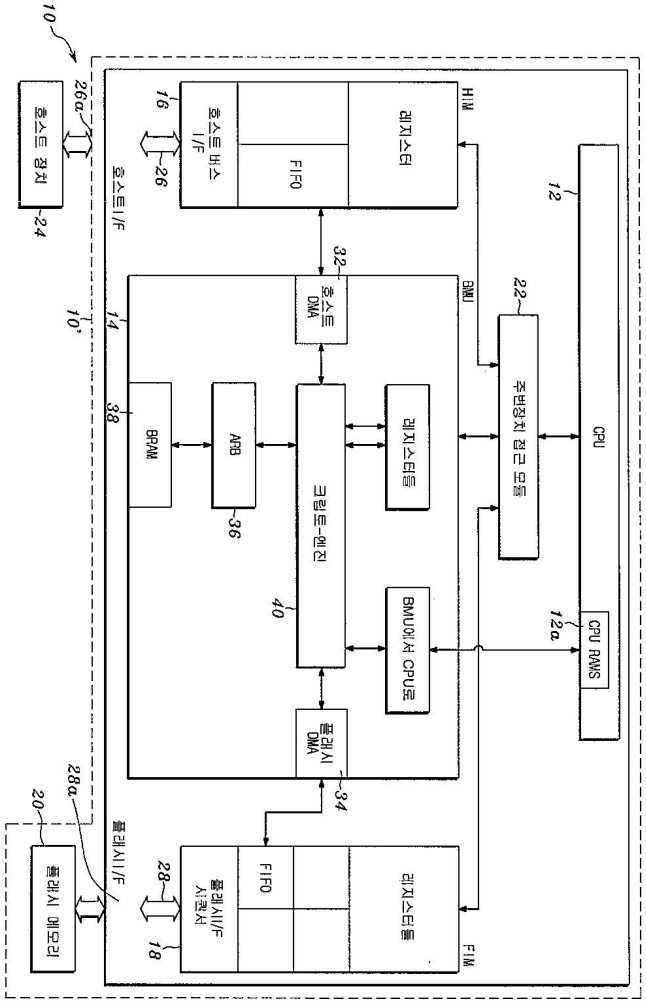
[0670] 도 18은 일부 세션이 개방될 때, 인증 및 접근의 세션들을 도시하는 흐름도이다.

[0671] 도 19 내지 22는 다른 인증 프로세스들을 도시하는 순서도들이다.

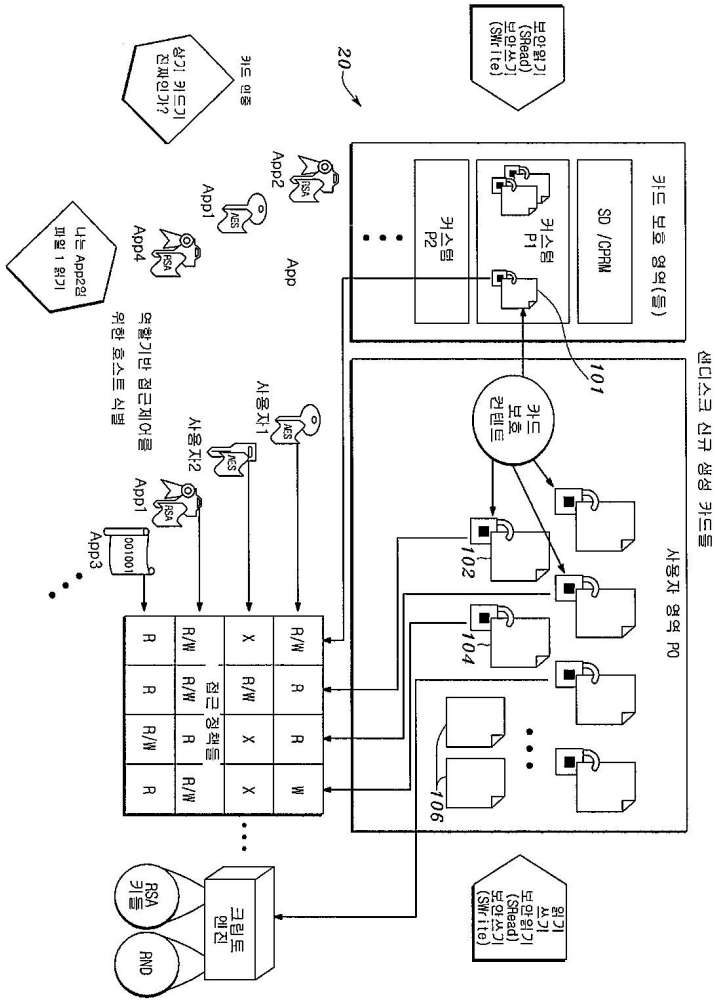
[0672] 설명의 간략화를 위해, 본 출원에서 동일한 구성 요소들은 동일한 번호들로 표시된다.

도면

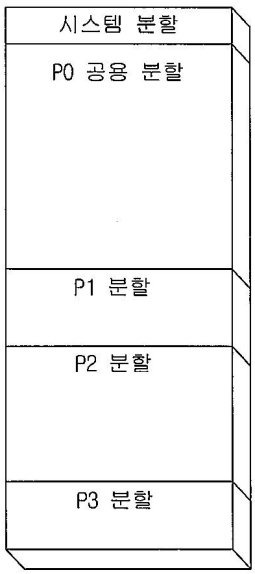
도면1


10
호스트 장치
26a
24
호스트 I/F
16
호스트 버스 I/F
26
FIFO
레지스터
HIM
12
32
호스트 DMA
BMU
22
주변장치 접근 모듈
CPU
10'
14
38
BRAM
ARB
36
크립토-엔진
40
레지스터들
BMU와 CPU로
12a
CPU RAMS
플래시 DMA
34
28a
20
플래시 메모리
플래시 I/F
28
플래시 시퀀서
18
FIFO
레지스터들
FIM

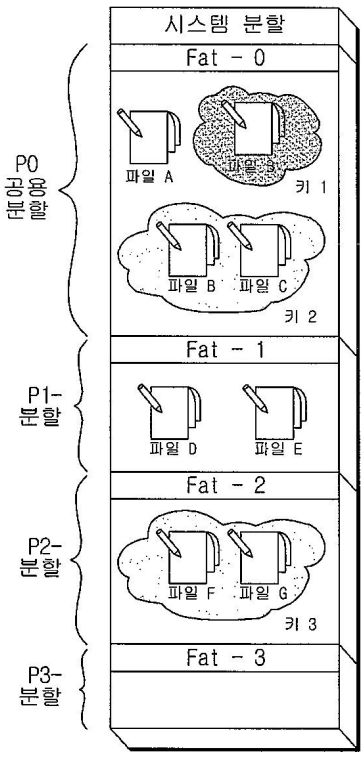
도면2


20
보안읽기
(SRead)
보안쓰기
(SWrite)
카드 인증
장기 카드기
인증인가?
App2
App1
App4
App
나는 App2의
피일 1 읽기
역할기반 접근제어를
위한 호스트 식별
사용자1
사용자2
App1
App3
00100
R
R/W
X
R/W
R
R/W
R
R
R/W
R
X
R
R/W
R/W
R
W
접근 정책들
RSA
키들
RND
크립토
엔진
카드 보호 영역(들)
SD /CPRM
시스템
P2
시스템
P1
카드
보호
컴퍼넌트
101
102
104
106
샌디스크 신규 생성 카드들
사용자 영역 P0
읽기
쓰기
보안읽기
(SRead)
보안쓰기
(SWrite)

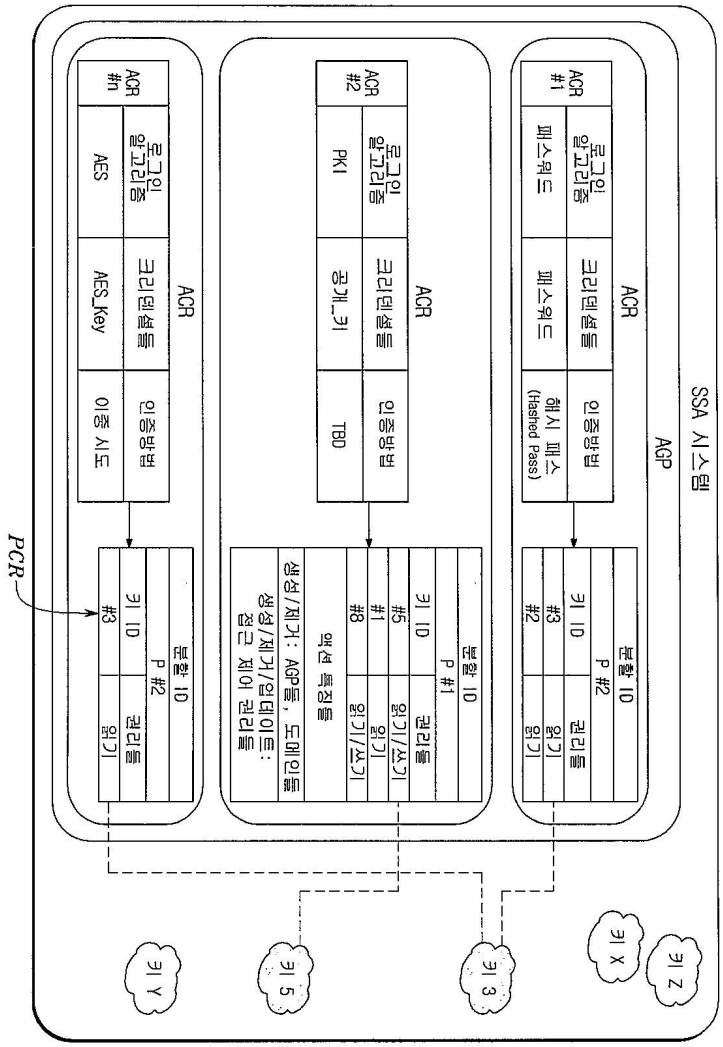
도면3


시스템 분할
P0 공용 분할
P1 분할
P2 분할
P3 분할

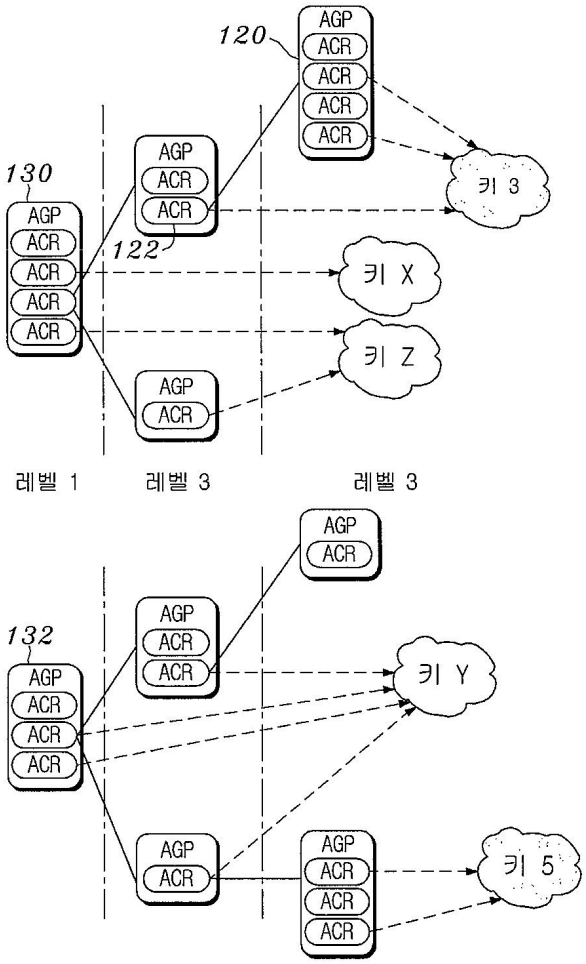
도면4


시스템 분할
Fat - 0
파일 A
파일 I
키 1
파일 B
파일 C
키 2
Fat - 1
파일 D
파일 E
Fat - 2
파일 F
파일 G
키 3
Fat - 3
P0
공용
분할
P1-
분할
P2-
분할
P3-
분할

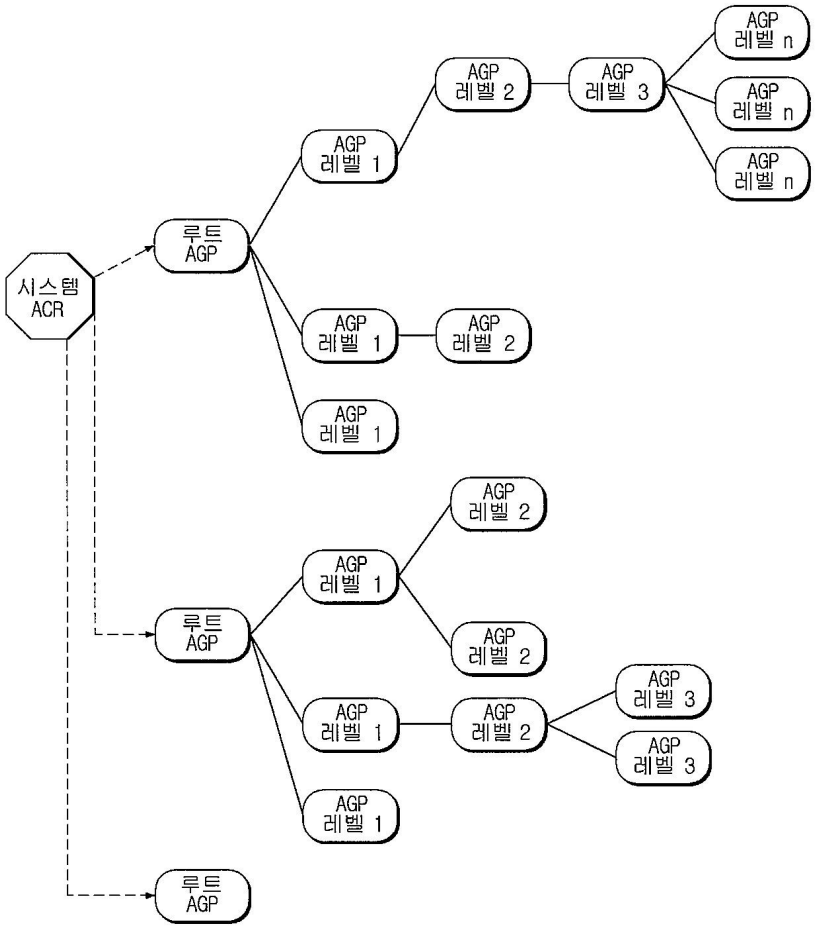
도면5


SSA 시스템
AGP
ACR #1
로그인 알고리즘
패스워드
ACR
크리덴셜들
패스워드
인증방법
해시 패스 (Hashed Pass)
분할 ID
P #2
키 ID
#3
#2
권리들
읽기
읽기
ACR #2
로그인 알고리즘
PKI
공개_키
TBD
ACR
크리덴셜들
인증방법
분할 ID
P #1
키 ID
#5
#1
#8
권리들
읽기/쓰기
읽기
읽기/쓰기
액션 특정들
생성/제거 : AGP들, 도메인들
생성/제거/업데이트 : 접근 제어 권리들
ACR #n
로그인 알고리즘
AES
ACR
크리덴셜들
AES_Key
인증방법
이중 시도
분할 ID
P #2
키 ID
#3
권리들
읽기
PCR
키 X
키 Z
키 3
키 5
키 Y

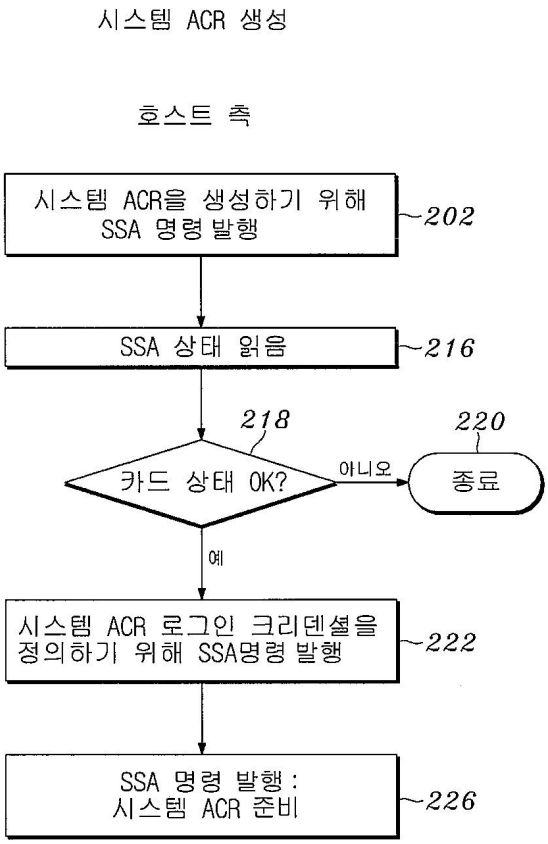
도면6


120
AGP
ACR
ACR
ACR
ACR
키 3
130
AGP
ACR
ACR
ACR
ACR
122
AGP
ACR
ACR
키 X
키 Z
AGP
ACR
레벨 1
레벨 3
레벨 3
132
AGP
ACR
AGP
ACR
ACR
키 Y
AGP
ACR
AGP
ACR
ACR
ACR
키 5

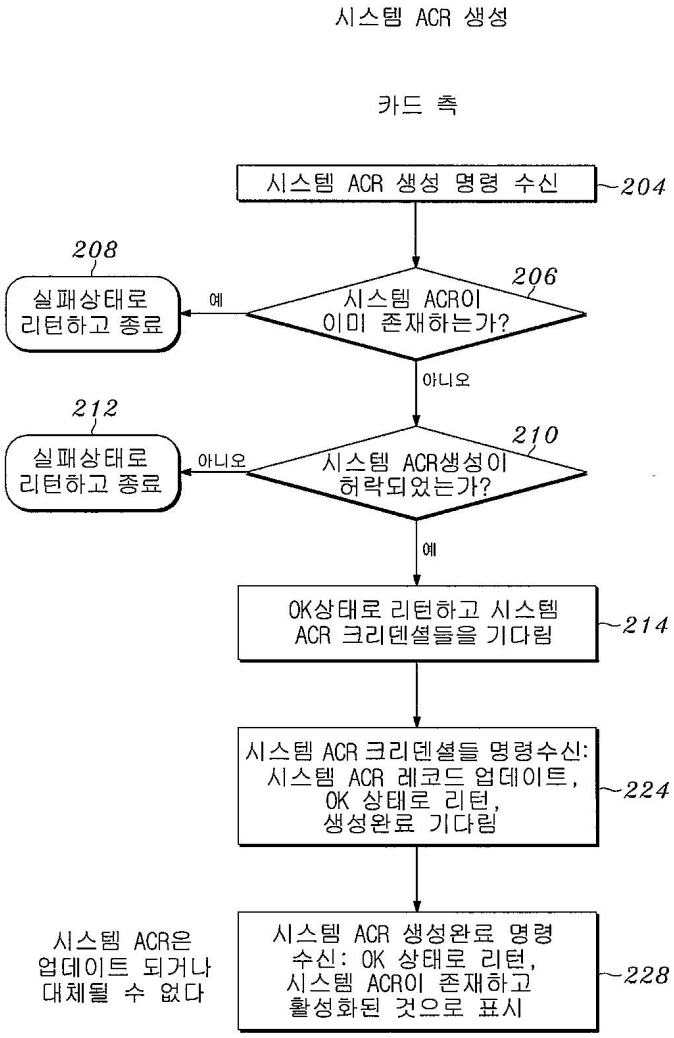
도면7


시스템
ACR
루트
AGP
AGP
레벨 1
AGP
레벨 2
AGP
레벨 3
AGP
레벨 n
AGP
레벨 n
AGP
레벨 n
AGP
레벨 1
AGP
레벨 2
AGP
레벨 1
루트
AGP
AGP
레벨 1
AGP
레벨 2
AGP
레벨 2
AGP
레벨 1
AGP
레벨 2
AGP
레벨 3
AGP
레벨 3
AGP
레벨 1
루트
AGP

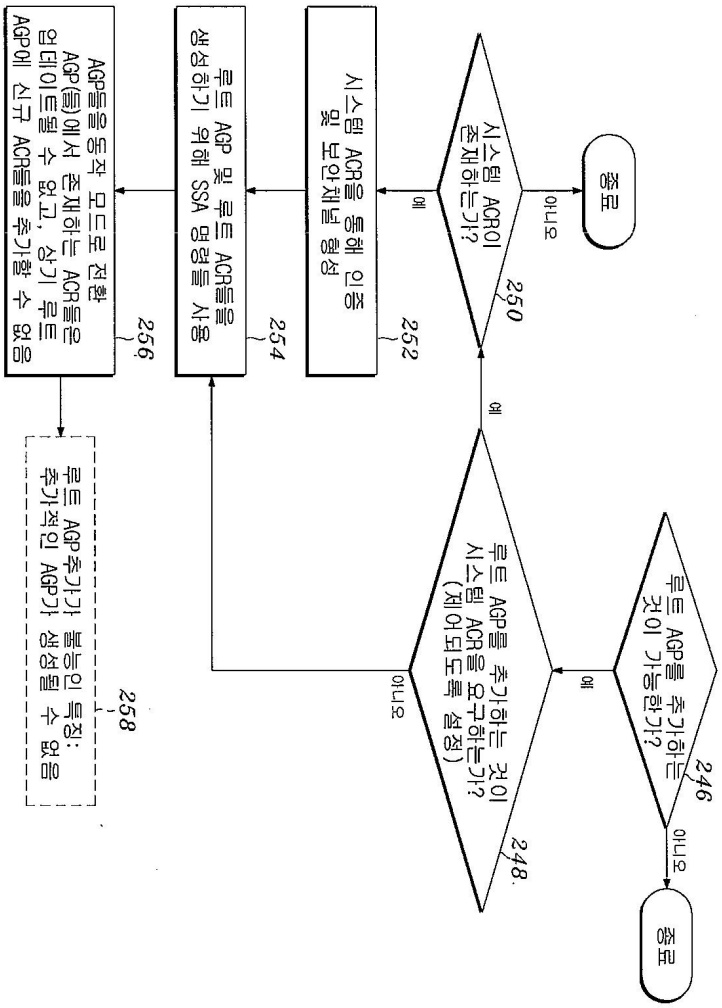
도면8a


시스템 ACR 생성
호스트 측
시스템 ACR을 생성하기 위해 SSA 명령 발행
202
SSA 상태 읽음
216
218
220
카드 상태 OK?
아니오
종료
예
시스템 ACR 로그인 크리덴셜을 정의하기 위해 SSA명령 발행
222
SSA 명령 발행 : 시스템 ACR 준비
226

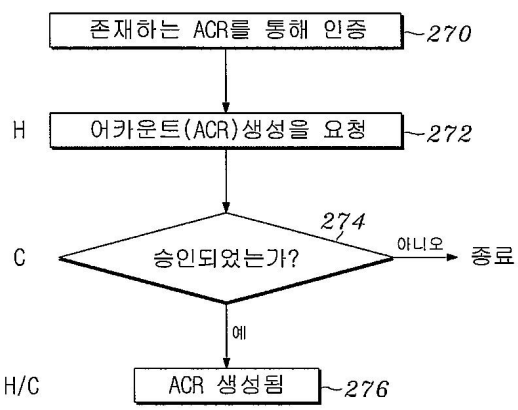
도면8b


시스템 ACR 생성
카드 측
시스템 ACR 생성 명령 수신
204
206
시스템 ACR이 이미 존재하는가?
예
208
실패상태로 리턴하고 종료
아니오
210
시스템 ACR생성이 허락되었는가?
아니오
212
실패상태로 리턴하고 종료
예
OK상태로 리턴하고 시스템 ACR 크리덴셜들을 기다림
214
시스템 ACR 크리덴셜들 명령수신: 시스템 ACR 레코드 업데이트, OK 상태로 리턴, 생성완료 기다림
224
시스템 ACR은 업데이트 되거나 대체될 수 없다
시스템 ACR 생성완료 명령 수신: OK 상태로 리턴, 시스템 ACR이 존재하고 활성화된 것으로 표시
228

도면9

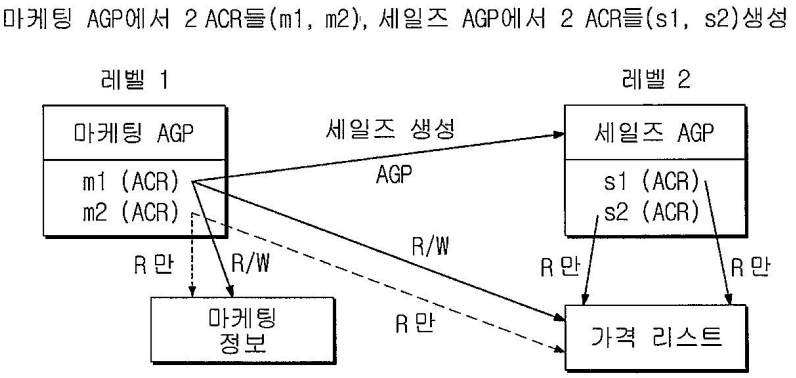


도면10

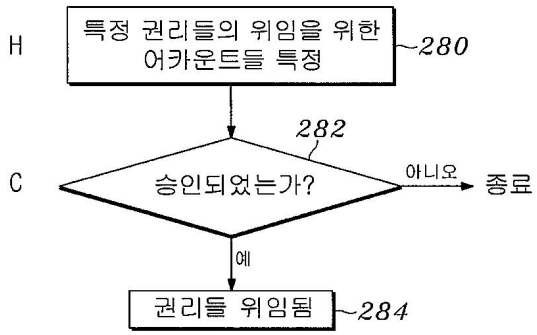


m1, m2, s1, s2를 생성하기 위해 사용되는 프로세스

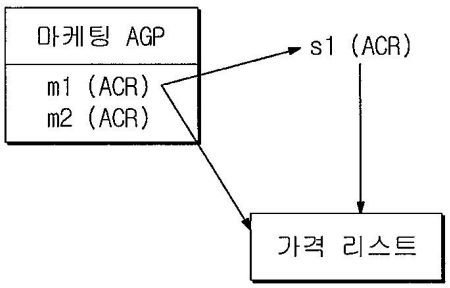
도면11



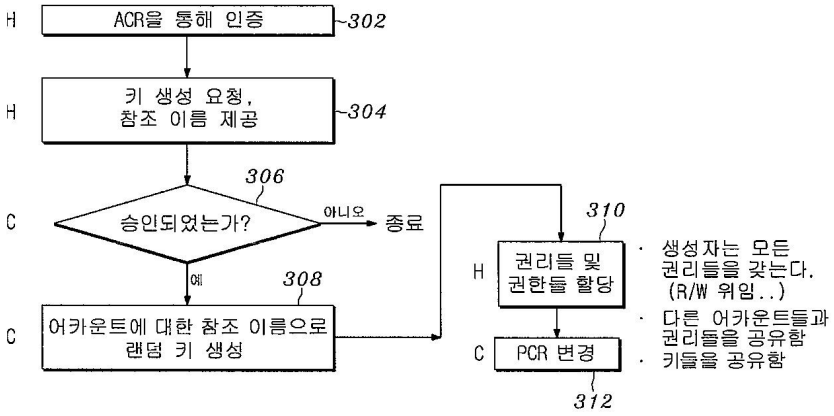
도면12



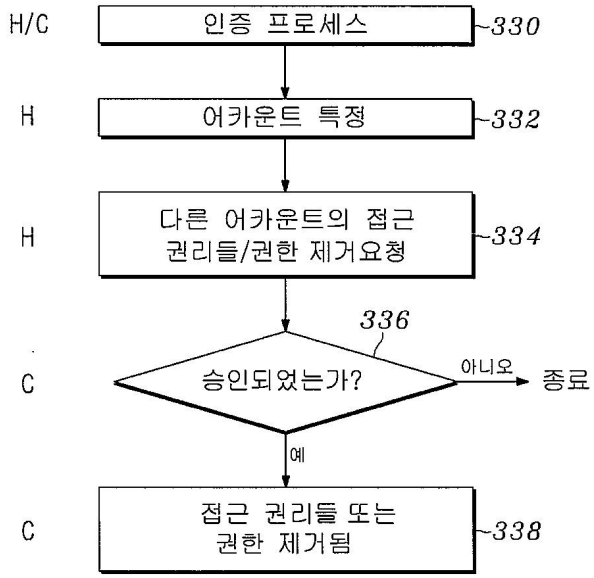
도면13



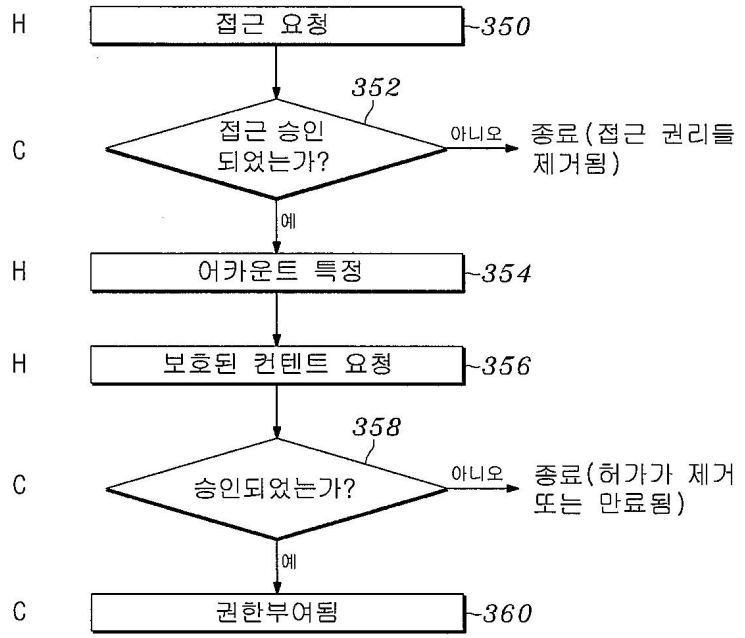
도면14


H
ACR을 통해 인증
302
H
키 생성 요청,
참조 이름 제공
304
306
C
승인되었는가?
아니오
종료
예
308
C
어카운트에 대한 참조 이름으로
랜덤 키 생성
310
H
권리들 및
권한들 할당
· 생성자는 모든
권리들을 갖는다.
(R/W 위임..)
· 다른 어카운트들과
권리들을 공유함
· 키들을 공유함
C
PCR 변경
312

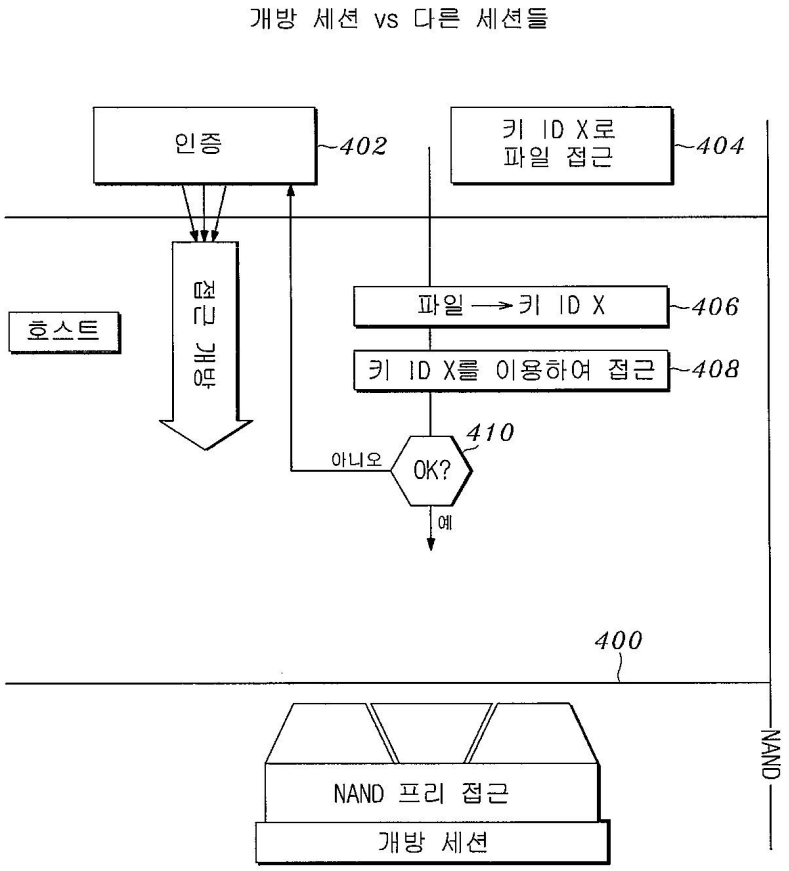
도면15


H/C
인증 프로세스
330
H
어카운트 특정
332
H
다른 어카운트의 접근
권리들/권한 제거요청
334
336
C
승인되었는가?
아니오
종료
예
C
접근 권리들 또는
권한 제거됨
338

도면16

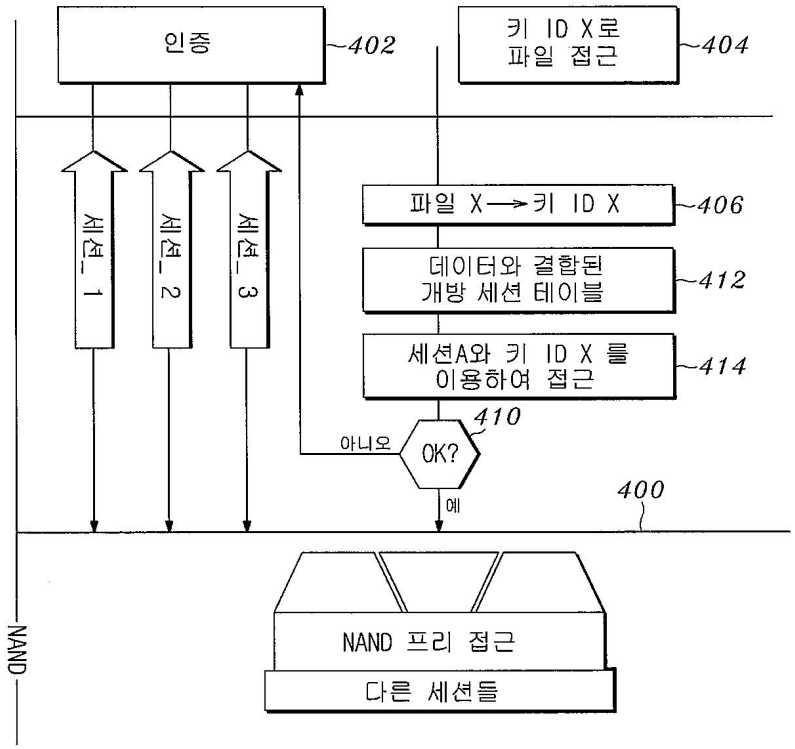

H
접근 요청
350
352
C
접근 승인 되었는가?
아니오
종료(접근 권리들 제거됨)
예
H
어카운트 특정
354
H
보호된 컨텐트 요청
356
358
C
승인되었는가?
아니오
종료(허가가 제거 또는 만료됨)
예
C
권한부여됨
360

도면17a

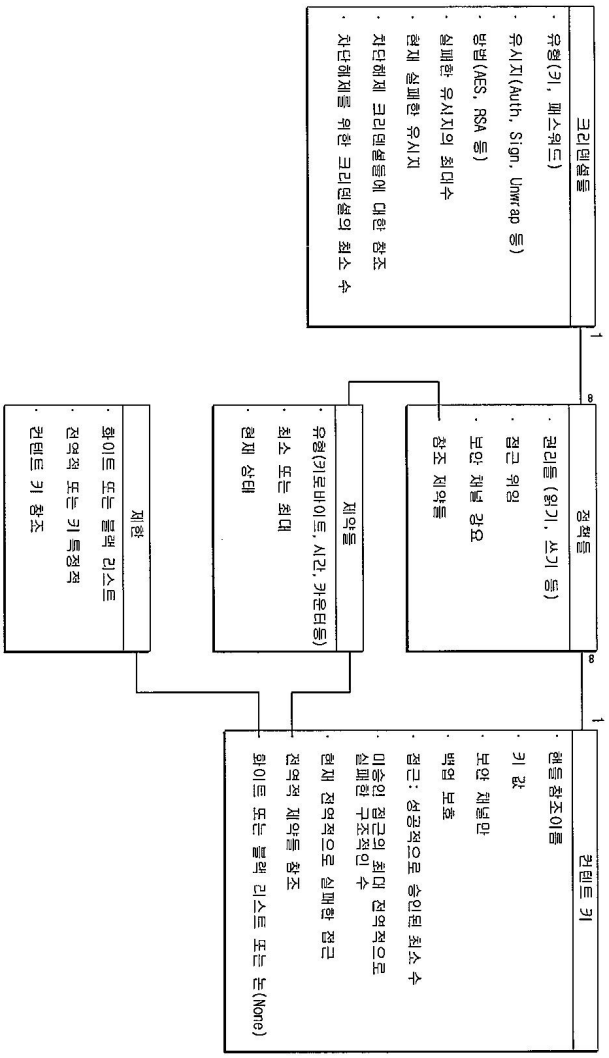

개방 세션 vs 다른 세션들
인증
402
키 ID X로 파일 접근
404
호스트
명령 대기
파일 → 키 ID X
406
키 ID X를 이용하여 접근
408
410
아니오
OK?
예
400
NAND 프리 접근
개방 세션
NAND

도면17b

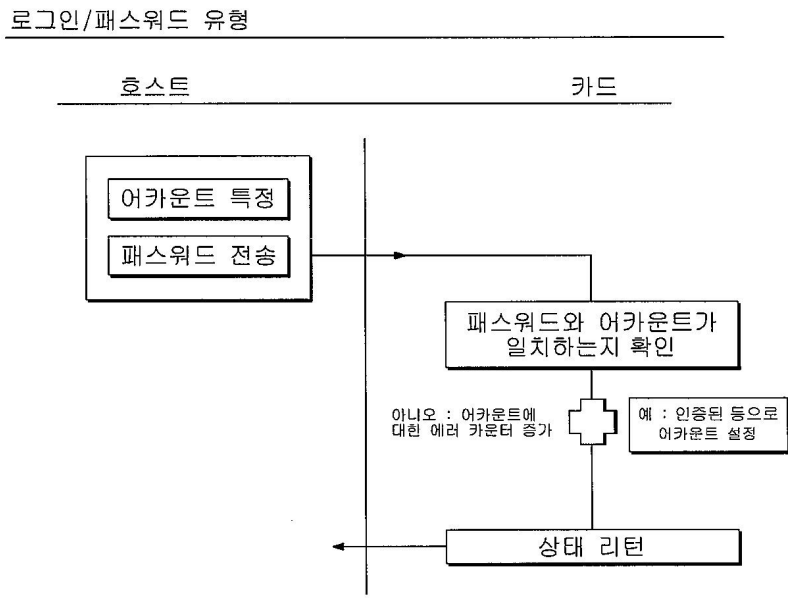
개방 세션 vs 다른 세션들



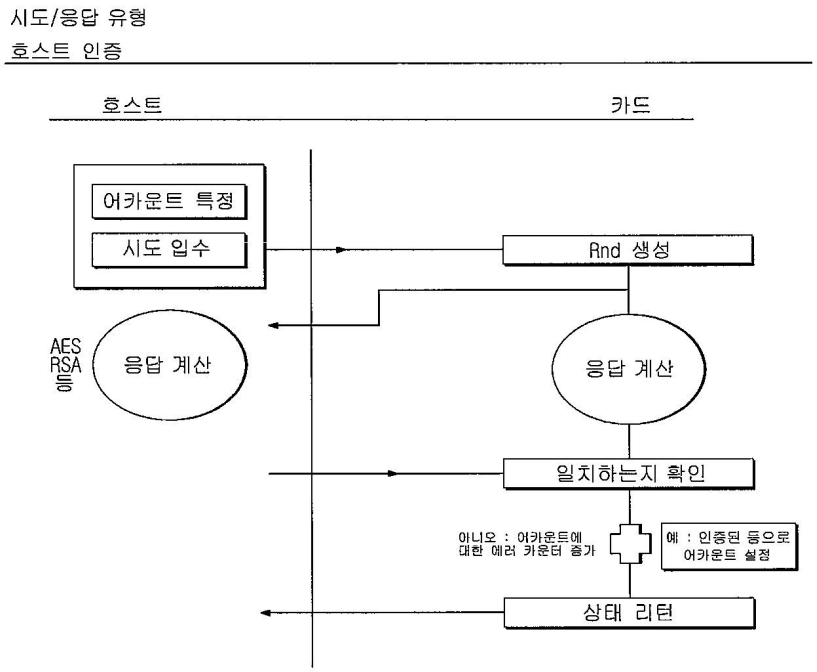
도면18


크리덴셜들
· 유형(키, 패스워드)
· 유시지(Auth, Sign, Unwrap 등)
· 방법(AES, RSA 등)
· 실패한 유시지의 최대수
· 현재 실패한 유시지
· 차단해제 크리덴셜들에 대한 참조
· 차단해제를 위한 크리덴셜의 최소 수
1
정책들
· 권리들 (읽기, 쓰기 등)
· 접근 위임
· 보안 채널 강요
· 참조 제약들
제약들
· 유형(키로바이트, 시간, 카운터등)
· 최소 또는 최대
· 현재 상태
제한
· 화이트 또는 블랙 리스트
· 전역적 또는 키 특정적
· 컨텐트 키 참조
컨텐트 키
· 핸들 참조이름
· 키 값
· 보안 채널만
· 백업 보호
· 접근: 성공적으로 승인된 최소 수
미승인 접근의 최대 전역적으로
실패한 구조적인 수
· 현재 전역적으로 실패한 접근
전역적 제약들 참조
화이트 또는 블랙 리스트 또는 논(None)

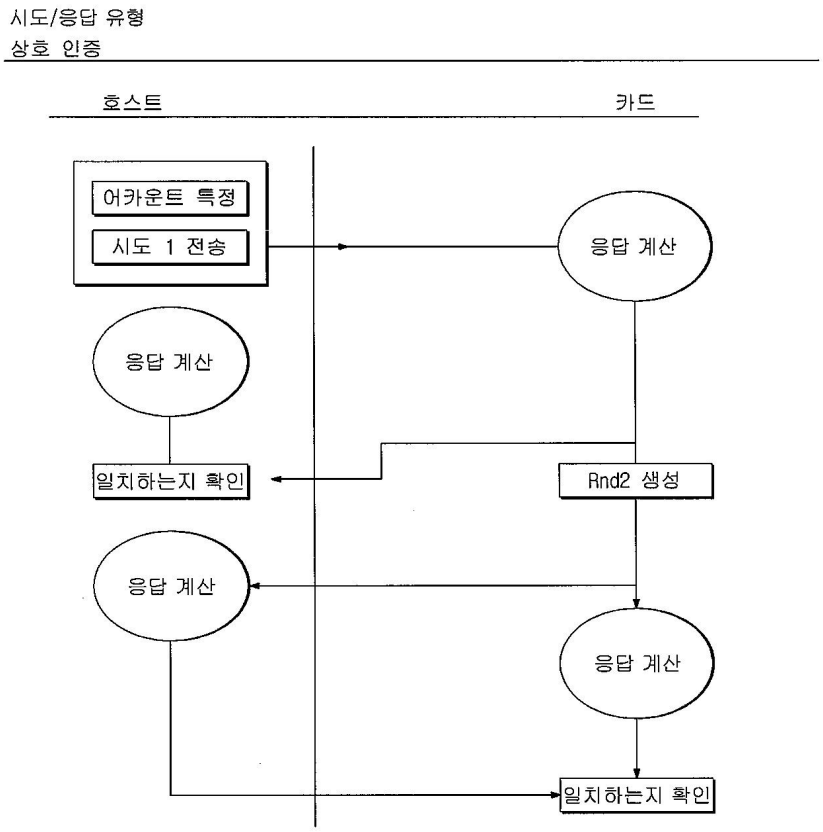
도면19


로그인/패스워드 유형
호스트
카드
어카운트 특정
패스워드 전송
패스워드와 어카운트가 일치하는지 확인
아니오 : 어카운트에 대한 에러 카운터 증가
예 : 인증된 등으로 어카운트 설정
상태 리턴

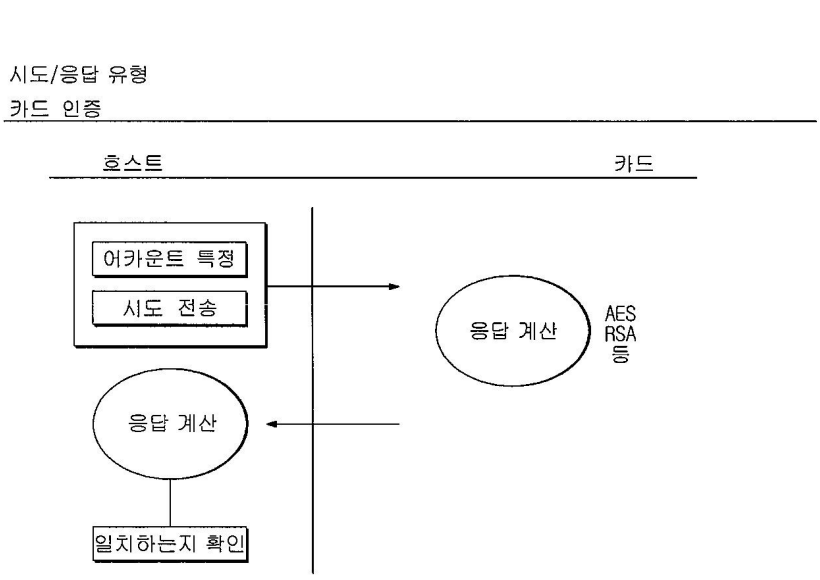
도면20


시도/응답 유형
호스트 인증
호스트
카드
어카운트 특정
시도 입수
Rnd 생성
AES RSA 등
응답 계산
응답 계산
일치하는지 확인
아니오 : 어카운트에 대한 에러 카운터 증가
예 : 인증된 등으로 어카운트 설정
상태 리턴

도면21


시도/응답 유형
상호 인증
호스트
카드
어카운트 특정
시도 1 전송
응답 계산
응답 계산
일치하는지 확인
Rnd2 생성
응답 계산
응답 계산
일치하는지 확인

도면22


시도/응답 유형
카드 인증
호스트
카드
어카운트 특정
시도 전송
응답 계산
AES
RSA
등
응답 계산
일치하는지 확인