(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년03월31일
(11) 등록번호 10-1608102
(24) 등록일자 2016년03월25일

(51) 국제특허분류(Int. Cl.)
G06F 21/79 (2013.01) *G06F 21/30* (2013.01)
(21) 출원번호 10-2010-7028858
(22) 출원일자(국제) 2009년05월20일
심사청구일자 2014년04월18일
(85) 번역문제출일자 2010년12월22일
(65) 공개번호 10-2011-0038633
(43) 공개일자 2011년04월14일
(86) 국제출원번호 PCT/US2009/044655
(87) 국제공개번호 WO 2009/158082
국제공개일자 2009년12월30일
(30) 우선권주장
12/146,066 2008년06월25일 미국(US)

(56) 선행기술조사문헌
임시 저장 장치의 호스트 어태치먼트 인증에 대한 IEEE 표준 프로토콜, "IEEE Standard Protocol for Authentication in Host Attachments of Transient Storage Devices", 2006년, pp.1-59, ISBN: 978-0-7381-5314-8*
Donald Rich, 임시 저장 장치의 인증 "Authentication in transient storage device attachments", 2007년 4월, 미국 캘리포니아 로스 알라모스, IEEE 서비스 센터, 컴퓨터 논문집 제40권 제4호, 2007.04., pp.102-104, ISSN: 0018-9162*
US20070250915 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
마이크로소프트 테크놀로지 라이센싱, 엘엘씨
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
보비, 제임스
미국 98052-6399 워싱턴주 레드몬드 원 마이크로소프트 웨이 마이크로소프트 코포레이션 내
(74) 대리인
제일특허법인

전체 청구항 수 : 총 20 항 심사관 : 박미정

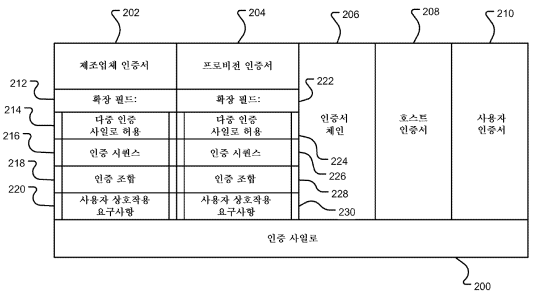
(54) 발명의 명칭 **다수의 인증 사일로를 갖는 임시 저장 장치의 허가**

(57) 요 약

다수의 인증 사일로(302, 304, 306, 308, 310)를 갖는 TSD(transient storage device) 장치(100)에서, TSD(100)에 연결된 호스트 컴퓨팅 장치는 사일로 내의 다양한 유형의 인증 정보를 발견하고 그에 따라 동작하도록 TSD(100)에 의해 구성된다. 연관된 저장 영역에의 액세스를 허용하기 위해 인증 사일로의 하나 이상의 논리적

(뒷면에 계속)

대 표 도



조합이 인증된 상태로 전환된다(406). 인증 사일로의 특정의 정렬(408)이 인증 사일로의 유효한 조합을 달성하는 데 필요할 수 있고(418), TSD 내의 구성 정보에 의해 제안될 수 있으며, 주어진 인증 사일로를 인증하는 데 사용자 입력이 요구되는지(412) 여부, TSD의 사용 환경 또는 가장 신뢰할 수 있는 인증 사일로부터 가장 신뢰할 수 없는 인증 사일로까지의 계층구조에 기초할 수 있다. 이 정보를 사용하여, 호스트는 저장 영역에의 액세스 허용을 가져오는 가장 효율적인 인증 시퀀스를 시작한다(410).

명 세 서

청구범위

청구항 1

컴퓨터 프로세스를 수행하기 위한 컴퓨터 실행가능 명령어들을 저장하는 컴퓨터 판독가능 저장 장치로서,

상기 명령어들은

하나 이상의 인증 사일로 조합을 포함하는 논리식(logical expression)을 생성하기 위해 저장 영역에 대응하는 제1 인증 사일로에 대한 제1 인증 요건 및 상기 저장 영역에 대응하는 제2 인증 사일로에 대한 제2 인증 요건을 조정하는 조정 오퍼레이션 - 상기 논리식은 상기 제1 인증 사일로 및 상기 제2 인증 사일로를 명시하고, 상기 논리식은 제조업체 인증서 또는 프로비전 인증서 중 적어도 하나의 하나 이상의 확장 필드 내의 상기 제1 인증 사일로 및 상기 제2 인증 사일로에 대한 구성가능 설정에 기초함 - 과,

상기 제1 인증 사일로 및 상기 제2 인증 사일로의 하나 이상의 인증 상태가 상기 저장 영역에 액세스하기 위한 상기 논리식의 유효한 인증 사일로 조합이 되는지 판정하는 판정 오퍼레이션과,

상기 유효한 인증 사일로 조합을 판정하는 것에 기초하여 호스트 장치에 의한 상기 저장 영역으로의 액세스를 허가하는 허가 오퍼레이션을 포함하는

컴퓨터 판독가능 저장 장치.

청구항 2

제1항에 있어서,

상기 명령어들은 상기 제1 인증 사일로 및 상기 제2 인증 사일로를 생성하는 생성 오퍼레이션을 포함하는

컴퓨터 판독가능 저장 장치.

청구항 3

제2항에 있어서,

상기 생성 오퍼레이션은

상기 저장 영역의 구성가능 설정을 위한 값을 인증서의 하나 이상의 확장 필드에 설정하는 오퍼레이션과,

상기 인증서를 상기 저장 장치상에 설치하는 오퍼레이션을 포함하는

컴퓨터 판독가능 저장 장치.

청구항 4

제1항에 있어서,

상기 조정 오퍼레이션은

적어도 하나의 인증 사일로의 인증이 사용자 입력을 이용하는지 판정하는 오퍼레이션과,

인증 요건을 충족시키는 사용자 입력을 요청하는 오퍼레이션을 포함하는

컴퓨터 판독가능 저장 장치.

청구항 5

제1항에 있어서,

상기 조정 오퍼레이션은 인증서를 심문하는(interrogate) 오퍼레이션을 포함하는

컴퓨터 판독가능 저장 장치.

청구항 6

제1항에 있어서,

상기 조정 오퍼레이션은 인증 상태의 조합이 상기 논리식 내의 인증 사일로 조합에 의해 명시되는지 여부를 발견하는 오퍼레이션을 포함하고,

상기 판정 오퍼레이션은 상기 조합이 충족되는지 여부를 계산하는 오퍼레이션을 포함하는

컴퓨터 판독가능 저장 장치.

청구항 7

제6항에 있어서,

상기 계산하는 오퍼레이션은 상기 인증 상태의 MaxTerm/MinTerm 값을 계산하는 오퍼레이션을 포함하는

컴퓨터 판독가능 저장 장치.

청구항 8

처리 장치에 의해 구현되는 방법으로서,

하나 이상의 인증 사일로 조합을 포함하는 논리식(logical expression)을 생성하기 위해 저장 영역에 대응하는 제1 인증 사일로에 대한 제1 인증 요건 및 상기 저장 영역에 대응하는 제2 인증 사일로에 대한 제2 인증 요건을 조정하는 단계 - 상기 논리식은 상기 제1 인증 사일로 및 상기 제2 인증 사일로를 명시하고, 상기 논리식은 제조업체 인증서 또는 프로비전 인증서 중 적어도 하나의 하나 이상의 확장 필드 내의 상기 제1 인증 사일로 및 상기 제2 인증 사일로에 대한 구성가능 설정에 기초함 - 과,

상기 제1 인증 사일로 및 상기 제2 인증 사일로의 하나 이상의 인증 상태가 상기 저장 영역에 액세스하기 위한 상기 논리식의 유효한 인증 사일로 조합이 되는지 판정하는 단계와,

상기 유효한 인증 사일로 조합을 판정하는 것에 기초하여 호스트 장치에 의한 상기 저장 영역으로의 액세스를 허가하는 단계

를 포함하는 방법.

청구항 9

제8항에 있어서,

상기 제1 인증 사일로 및 상기 제2 인증 사일로를 생성하는 단계

를 포함하는 방법.

청구항 10

제9항에 있어서,

상기 생성하는 단계는

상기 저장 영역의 구성가능 설정을 위한 값을 인증서의 하나 이상의 확장 필드에 설정하는 단계와,

상기 인증서를 상기 저장 장치상에 설치하는 단계를 포함하는

방법.

청구항 11

제8항에 있어서,

상기 조정하는 단계는

적어도 하나의 인증 사일로의 인증이 사용자 입력을 이용하는지 판정하는 단계와,

인증 요건을 충족시키는 사용자 입력을 요청하는 단계를 포함하는

방법.

청구항 12

제8항에 있어서,

상기 조정하는 단계는 인증서를 심문하는(interrogate) 단계를 포함하는

방법.

청구항 13

제8항에 있어서,

상기 조정하는 단계는 인증 상태의 조합이 상기 논리식 내의 인증 사일로 조합에 의해 명시되는지 여부를 발견하는 단계를 포함하고,

상기 판정하는 단계는 상기 조합이 충족되는지 여부를 계산하는 단계를 포함하는

방법.

청구항 14

제13항에 있어서,

상기 계산하는 단계는 상기 인증 상태의 MaxTerm/MinTerm 값을 계산하는 단계를 포함하는

방법.

청구항 15

하나 이상의 처리 장치와 컴퓨터 실행가능 명령어들을 저장하는 메모리를 포함하는 시스템으로서,

상기 컴퓨터 실행가능 명령어들은 상기 하나 이상의 처리 장치 중 적어도 하나에 의해 실행될 경우,

하나 이상의 인증 사일로 조합을 포함하는 논리식(logical expression)을 생성하기 위해 저장 영역에 대응하는 제1 인증 사일로에 대한 제1 인증 요건 및 상기 저장 영역에 대응하는 제2 인증 사일로에 대한 제2 인증 요건을 조정하는 조정 오퍼레이션 - 상기 논리식은 상기 제1 인증 사일로 및 상기 제2 인증 사일로를 명시하고, 상기 논리식은 제조업체 인증서 또는 프로비전 인증서 중 적어도 하나의 하나 이상의 확장 필드 내의 상기 제1 인증 사일로 및 상기 제2 인증 사일로에 대한 구성가능 설정에 기초함 - 과,

상기 제1 인증 사일로 및 상기 제2 인증 사일로의 하나 이상의 인증 상태가 상기 저장 영역에 액세스하기 위한 상기 논리식의 유효한 인증 사일로 조합이 되는지 판정하는 판정 오퍼레이션과,

상기 유효한 인증 사일로 조합을 판정하는 것에 기초하여 호스트 장치에 의한 상기 저장 영역으로의 액세스를 허가하는 허가 오퍼레이션을 수행하는

시스템.

청구항 16

제15항에 있어서,

상기 명령어들은 상기 제1 인증 사일로 및 상기 제2 인증 사일로를 생성하는 생성 오퍼레이션을 포함하는

시스템.

청구항 17

제16항에 있어서,

상기 생성 오퍼레이션은

상기 저장 영역의 구성가능 설정을 위한 값을 인증서의 하나 이상의 확장 필드에 설정하는 오퍼레이션과,

상기 인증서를 상기 저장 장치상에 설치하는 오퍼레이션을 포함하는

시스템.

청구항 18

제15항에 있어서,

상기 조정 오퍼레이션은

적어도 하나의 인증 사일로의 인증이 사용자 입력을 이용하는지 여부를 판정하는 오퍼레이션과,

인증 요건을 충족시키는 사용자 입력을 요청하는 오퍼레이션을 포함하는

시스템.

청구항 19

제15항에 있어서,

상기 조정 오퍼레이션은 인증서를 심문하는(interrogate) 오퍼레이션을 포함하는

시스템.

청구항 20

제15항에 있어서,

상기 조정 오퍼레이션은 인증 상태의 조합이 상기 논리식 내의 인증 사일로 조합에 의해 명시되는지 여부를 발견하는 오퍼레이션을 포함하고,

상기 판정 오퍼레이션은 상기 조합이 충족되는지 여부를 계산하는 오퍼레이션을 포함하는

시스템.

발명의 설명

배 경 기 술

[0001] TSD(transient storage device)가 최근에 휴대용 컴퓨터 데이터 저장에 널리 사용되고 있다. TSD는 휴대폰, 디지털 카메라, PDA(personal digital assistant), 디지털 음악 플레이어(예를 들어, MP3 플레이어) 및 기타 휴대용 장치의 USB 플래시 드라이브 및 메모리 카드 그리고 "스틱"의 형태를 취할 수 있다. TSD의 대규모 저장 용량 및 TSD로/로부터의 고속의 데이터 전송으로 인해, TSD가 연결될 수 있는 호스트 장치로/로부터의 데이터 전송의 보안은 인식된 문제이다. TSD에 대한 IEEE(Institute of Electrical and Electronics Engineers) 1667 표준은 인증서(authentication certificate)의 저장 및 TSD 상의 사용자 데이터에 대한 차후의 액세스 허가를 위한 인증 데이터 구조("사일로")의 정의를 포함시킴으로써 이 문제를 해결한다.

[0002] IEEE 1667 표준은 장치가 다수의 인증 사일로를 가질 수 있게 하며, 이들 인증 사일로는, 함께 모여, TSD 저장소 볼륨 상의 하나의 데이터 저장 영역[ACT(addressable command target)]에의 액세스에 대한 허가를 제어한다. 그러나, 현재 이 표준은 인증서에 대해 한 유형의 인증 사일로만을 정의하고 있고 어떤 다른 유형의 인증 사일로가 사용될 수 있는지를 제안하고 있지 않다. 이 표준은 ACT에 대해 2개 이상의 인증 사일로가 존재하는 상황에서 어느 인증 사일로를 사용해야 하는지 또는 서로 다른 사용 환경과 관련하여 어떤 지침도 제공하지 않고 있다. 게다가, 이 표준은 다수의 사일로에서 사용하기 위한 일반적인 인증 구성 메커니즘이 없다. 현재의 IEEE 1667 표준의 제약조건 내에서 사일로 계층구조 및 구성을 구현하는 것은 복잡한데, 그 이유는 그 사양이 인증서 사일로에 의해 구현되는 인증 및 인증서 저장소 관리 오퍼레이션의 제한된 세트를 제공하기 때문이다. 그러나, 어떤 구성 해결책이라도 현재의 IEEE 1667 표준 사양의 매개변수 및 요구사항 내에서 동작할 필요가 있을 것이다.

발명의 내용

[0003] 요약

[0004] 다수의 인증 사일로를 갖는 TSD 장치에서, TSD에 연결된 호스트 컴퓨팅 장치는 사일로 내의 다양한 유형의 인증 정보를 발견하고 그에 따라 동작하도록 구성되어 있다. ACT에의 액세스를 허용하기 위해, 인증 사일로들의 하나 이상의 논리적 조합이 인증된 상태로 전환되어야만 한다. 호스트는 TSD에의 호스트 액세스를 허가할 수 있는 인증 사일로들의 논리적 조합의 세트가 있는지 TSD를 검사한다. 인증 사일로들의 유효한 조합을 달성하기 위해, 인증 사일로들의 특정의 정렬이 필요하게 될 수도 있다. 정렬은 TSD 내의 구성 정보에 의해 제안될 수 있다. 정렬은 또한, 예를 들어, 주어진 인증 사일로를 인증하는 데 사용자 입력이 필요한지 여부, TSD의 사용 환경, 또는 가장 신뢰할 수 있는 인증 사일로부터 가장 신뢰할 수 없는 인증 사일로까지의 계층구조에 기초할 수 있다.

[0005] 이 정보를 사용하여, 호스트는 이어서 ACT에의 액세스 허용을 가져오는 가장 효율적인 인증 시퀀스를 시작할 수 있다. 또한, 호스트는, 예를 들어, 가능하다면 사용자에 확인하는 것보다 자동 인증(silent authentication)(사용자 입력 없음)을 우선시하도록 그의 거동을 최적화할 수 있다. 호스트는 또한 이전의 조합이 실패할 때 대안의 인증 사일로 조합을 시도할 수 있다. 게다가, 호스트는 이 정보를 사용하여, 모든 인증 조합을 다 사용한 경우 언제 인증이 가능하지 않은지를 판정할 수 있다.

[0006] TSD의 인증 사일로 내의 제조업체 인증서 및/또는 프로비전 인증서 내의 확장 필드가 현재의 IEEE 1667 표준의 제약조건 내에서 동작하면서 TSD의 특정의 ACT에의 액세스에 대한 인증 요건을 제공하는 데 사용된다. 일 구현에서, TSD의 구성가능 설정에 대한 값들이 제조업체 인증서 및/또는 프로비전 인증서의 확장 필드에 설정되어 있다. 이 방법은 IEEE 1667 인증서 사일로 사양 및 ITU-T X.509 인증서 사양에 고유한 특성들을 고유한 방식으로 이용한다. 장치 구성에 대한 보안 요구사항을 만족시키고 기존의 표준 정의를 수정 없이 있는 그대로 이용하면서 이 방법이 구현된다. 그 중에서도 특히, 이 방법은 TSD 펌웨어에 존재하는 특정의 특징들을 사용가능하거나 사용불가능하도록 할 수 있다.

[0007] 본 명세서의 목적상, "TSD(transient storage device)"라는 용어는 IEEE 1667 표준이 적용될 수 있는 모든 장치는 물론 확장 필드를 지원하는 제조업체 인증서 및/또는 프로비전 인증서와 동등한 것을 마찬가지로 받아들일 수 있는 모든 저장 장치, 예를 들어, ATA(advanced technology attachment) 장치를 포함한다.

[0008] 이 요약은 이하에서 상세한 설명에 더 기술되는 일련의 개념들을 간략화된 형태로 소개하기 위해 제공된 것이다. 이 요약은 청구된 발명 대상의 주요 특징들 또는 필수적인 특징들을 확인하기 위한 것이 아니며, 청구된 발명 대상의 범위를 제한하는 데 사용되기 위한 것도 아니다. 청구된 요지의 다른 특징, 상세, 효용 및 이점이 첨부 도면에 더 예시되고 첨부된 특허청구범위에서 한정되는 다양한 실시예 및 구현에 대한 이하의 상세한 설명으로부터 명백하게 될 것이다.

도면의 간단한 설명

[0009] 도 1은 임시 저장 장치의 가능한 구성의 일 구현을 나타내는 임시 저장 장치의 몇개의 프로토콜 계층의 개략도이다.

도 2는 임시 저장 장치의 인증 사일로 및 임시 저장 장치를 구성하기 위해 제조업체 인증서 또는 프로비전 인증서 내의 확장 필드를 사용하는 구현의 개략도이다.

도 3a 내지 도 3d는 임시 저장 장치 상의 인증 사일로의 예시적인 구현과 임시 저장 장치에 액세스하도록 허가하기 위한 계층구조 및 요구된 인증 조합을 결정하는 선택적인 방법을 나타낸 개략도이다.

도 4는 다수의 인증 사일로를 갖는 임시 저장 장치에 액세스하는 데 필요한 허가 방식을 결정하는 절차의 일 구현의 흐름도이다.

도 5는 임시 저장 장치에 대한 호스트 장치로서 동작할 수 있는 범용 컴퓨터 시스템의 개략도이다.

발명을 실시하기 위한 구체적인 내용

[0010] IEEE 1667 표준이 장치가 다수의 인증 사일로(authentication silo)를 가질 수 있게 하지만, 현재 구현되는 유일한 인증 사일로는 인증서 사일로(certificate silo)이다. 특정의 ACT에 대한 다수의 인증 사일로는, 함께 모여, 하나의 데이터 저장 영역에의 액세스 허가를 제어한다. 장래에, 임시 저장 장치(TSD) 상에 부가의 인증 사일로가 제공되는 경우, 다수의 경쟁할 수도 있는 인증 사일로들 간의 충돌 및 우선순위를 관리하는 방식이 요구

된다.

[0011] 임시 저장 장치(TSD)(100)는 도 1에 나타낸 바와 같이 기능상 몇개의 서로 다른 컴포넌트로 나누어진다. TSD(100)는 TSD(100)가 호스트 장치와 연결되어 통신할 수 있게 하는 물리적 인터페이스(102)를 갖는다. 예를 들어, USB(universal serial bus) 플래시 드라이브(UFD)는 일반적으로 절연체 상에 위치하고 직사각형 접점으로 둘러싸인 4개의 부가의 접촉 배선을 갖는 박스형 접촉 인터페이스를 갖는다. TSD(100)는 데이터 전달, 호스트-장치 상호 인증, 및 TSD(100)의 기타 기능을 실행하는 내장된 펌웨어(106)의 제어 하에서 동작하는 프로세서(104)를 더 포함하고 있다. 각각의 TSD(100)는, 기타 저장 시스템에서의 "논리 단위"와 개념이 유사한, 각각이 "ACT(addressable command target)" 계층을 통해 액세스되는, 적어도 하나, 어쩌면 그 이상의 개별적으로 인증되는 데이터 저장 영역(116)을 가질 수 있다. 도 1은 제1 ACT(108a) 및 제2 ACT(108b)를 갖는 TSD(100)를 나타낸 것이다.

[0012] 각각의 ACT(108a, 108b)는 적어도 프로브 사일로(110a, 110b) 및 인증 사일로(112a, 112b)를 비롯한, IEEE 1667 사양에서 "사일로"라고 불리는 몇개의 기능 단위를 구현한다. 각각의 ACT(108a, 108b)는 부가의 제조업체 또는 사용자 정의 사일로(114a, 114b)를 구현할 수 있다. ACT(108a 또는 108b) 및 대응하는 사일로는 TSD(100) 상의 116a 또는 116b에 대응하는 LUN0 또는 LUN1로서 어드레싱되는 구성 및 인증 제어 개별 데이터 저장 영역을 제공한다.

[0013] 프로브 사일로(110a, 110b)는 물리적 인터페이스(102)를 통해 연결된 호스트에서 ACT(108a, 108b)를 검사하고 이용가능한 기능 단위를 식별하는 데 사용된다. TSD(100) 내의 프로브 사일로(110a, 110b)는 호스트 장치 상에서 실행되거나 호스트 장치에 존재하는 IEEE 1667 버전 및 운영 체제의 ID(identification)를 수신한다. 프로브 사일로(110a, 110b)는 각각의 ACT(108a, 108b)에 구현된 사일로의 수, 유형 및 버전을 반환한다. 프로브 사일로(110a, 110b)의 검사는 임의의 다른 사일로에 대해 임의의 추가의 동작이 취해질 수 있기 전에 행해진다.

[0014] 프로브 사일로(110a, 110b)가 필요한 장치 정보를 수신하고 반환하면, 각각의 ACT(108a, 108b)에 대한 인증 사일로(112a, 112b)는 인증서들의 양방향 인증 및 관리에 필요한 기능들을 제공한다. 인증 사일로(112a, 112b)는 인증서를 사용하여 호스트 및 각각의 ACT(108a, 108b)를 인증하고 또한 인증서도 관리한다. 프로브 사일로(110a, 110b), 인증 사일로(112a, 112b) 및 기타 사일로(114a, 114b) 각각은 각자의 ACT(108a, 108b)와 관련되어 있다. 일반적으로, 데이터 저장 영역(116)은 IEEE 1667 표준 하에서 처음에 하나의 "논리 단위", 즉 ACT인 것으로 간주되며, 따라서 전체로서 원래의 또는 제1 인증 사일로(112a)에 위치되어 처리되는 제조업체 인증서 또는 프로비전 인증서의 적용을 받는다. 그러나, 제1 인증 사일로(112a)는 데이터 저장 영역(116)을, 도 1에 나타낸 바와 같이 논리 단위 번호(LUN#), 예를 들어, LUN0(116a) 및 LUN1(116b)을 갖는 디스크들의 구성체(construct)에서 편의상 식별되는 개별적으로 액세스가능한 저장 영역을 갖는 다수의 ACT(108a, 108b)로 분할하도록 구성되어 있다. 게다가, 제조업체 인증서, 프로비전 인증서, 또는 둘다가 ACT 또는 TSD(100) 상의 각각의 ACT에 대해 2개 이상의 유형의 인증 사일로를 제공할 수 있다.

[0015] 인증서 사일로(200)의 기능 컴포넌트의 구현에 대한 보다 상세한 설명이 도 2에 나타내어져 있다. IEEE 1667 표준 하에서, 인증서 사일로(200)에 보유하기 위한 5개의 서로 다른 유형의 인증서, 즉 제조업체 인증서(202), 프로비전 인증서(204), 인증서 체인(206), 호스트 인증서(208), 및 사용자 인증서(210)가 정의된다. 제조업체 인증서(202)는 필수적이며, TSD의 ID(identity)를 증명한다. 제조업체 인증서(202)는 TSD의 고유 식별자 및 TSD를 챌린지(challenge)하는 데 사용될 수 있는 공개 키를 포함한다. 각각의 ACT의 인증 사일로(200)는 각각이 고유의 키 쌍으로부터의 고유의 공개 키를 갖는 고유의 제조업체 인증서(202)를 지닐 수 있다. 그러나, 모든 제조업체 인증서가 동일한 직계 부모 제조업체 인증서에 체인(chain)되어 있어야만 한다. TSD 상의 제1 ACT에 대한 제조업체 인증서는 기본 인증서 사일로(200) 이외의 부가의 유형의 인증 사일로를 사용할 수 있게 하는 데 이용될 수 있다. 프로비전 인증서(204)의 확장 필드(212)는 이 새로운 상태의 상세를 명시하는 데 사용될 수 있으며, 이에 대해서는 이하에서 더 기술한다.

[0016] 프로비전 인증서(204)는 인증 사일로(200)에의 관리상 액세스를 허용하고, 관리자에게 나머지 인증서들을 관리할 수 있게 한다. 인증 사일로(200)에 저장된 프로비전 인증서(204)에 의해 서명된 인증서에 액세스할 수 있는 사용자는 호스트 상의 인증서를 추가, 제거 또는 대체할 수만 있다. 초기 ACT에 대한 프로비전 인증서(204)는 변경할 수 없으며, TSD가 초기 프로비전 인증서(204)로 프로비전될 때 다수의 ACT를 포함하는 새로운 상태로 재초기화되는 TSD를 생성하는 데 사용될 수 있다. 제조업체 인증서와 유사하게, TSD 상의 제1 ACT에 대한 초기 프로비전 인증서는 기본 인증서 사일로(200) 이외의 부가의 유형의 인증 사일로를 사용할 수 있게 하는 데 이용될 수 있다. 프로비전 인증서(204)의 확장 필드(212)는 이 새로운 상태의 상세를 명시하는 데 사용될 수 있으

며, 이에 대해서는 이하에서 더 기술한다. 초기 프로비전 인증서(204)에 의해 생성된 부가의 ACT에 관련된 부가의 프로비전 인증서가 제공될 수 있다.

[0017] ACT가 프로비전되면, TSD는 인증 사일로 인증서 체인(206)을 저장할 수 있다. 사용자는 이 체인을 사용하여 동일한 제조업체 및 제품 식별 번호를 갖는 모든 다른 장치와 별개인 개인화된 장치를 생성할 수 있다. 호스트는 인증서 체인(206)의 내용을 사용하여 ACT를 인증하고 ACT에 있는 저장 장치에의 액세스를 허가할 수 있다. 본 명세서에 개시된 기술과 관련하여 인증서 체인(206)을 사용하는 것에 대해 이하에서 더 기술한다.

[0018] 호스트 인증서(208)는 TSD가 연결되어 있을 때 TSD에 대해 호스트를 인증한다. TSD가 인증될 수 있는 다수의 호스트 장치에 대응하는 다수의 호스트 인증서(208)가 TSD에 추가될 수 있다. IEEE 1667 표준 하에서, 호스트 인증서가 인증 사일로(200)에 저장되지 않은 경우, TSD는 자동으로 호스트를 인증된 것으로 취급할 수 있으며, 이는 특정의 호스트에의 액세스를 제한하기 위한 것이 의도되어 있지 않다는 것을 나타낸다. 이것은 제조업체가 데이터 액세스의 선행 조건으로서 호스트 인증을 요구할 때 TSD의 구성을 간단화시켜준다. 호스트가 인증 사일로 내의 호스트 인증서들 중 하나로 서명된 인증서를 제시할 때 ACT가 인증된 상태로 전환될 것이다.

[0019] 사용자 인증서(210)도 역시 인증 사일로에 위치될 수 있다. 사용자 인증서(210)는 인증 사일로(200)에서 관리되지 않는다. IEEE 1667 표준 하에서, 어떤 응용 프로그램이라도 인증 사일로(200)로부터 이들 인증서를 저장하거나 제거할 수 있다. 호스트 또는 사용자 인증서 보유자가 프로비저너(provisioner)에 의해 TSD에 위치된 프로비전 인증서(204)를 사용하여 성공적으로 인증되지 않는 한, 어떤 추가의 호스트 인증서(208) 또는 사용자 인증서(210)도 TSD에 추가될 수 없다.

[0020] IEEE 1667 표준 하에서, TSD가 저장소 볼륨 상의 데이터에의 안전한 액세스를 제공하는 데 사용될 수 있기 전에, TSD는 그를 위해 준비하는 데 오퍼레이션들의 세트를 거쳐야만 한다. IEEE 1667 표준에서는 이 프로세스를 프로비전이라고 한다. TSD의 프로비저너가 반드시 그 TSD의 사용자인 것은 아니다. 프로비저너는 사실상 TSD의 관리자이며, 사용자, 시스템 관리자, 또는 제조업체일 수 있다.

[0021] 실제로, TSD는 제조업체로부터 프로비전되지 않은 상태로 도착하며, 적어도 하나의 ACT, 즉 초기 ACT(0)가 인증 사일로(200)를 포함하고 있다. 이 ACT(0)의 제1 프로비저너는 ACT-관련 설정에 부가하여 TSD에 대한 장치 전역 설정을 지정할 수 있다. 전역 TSD 설정은 제1 프로비전 오퍼레이션 동안에만 구성가능하다. TSD 상에 위치되면, 초기 프로비전 인증서(204)는 유효한 채로 있고, 장치가 명확하게 재초기화(즉, 원래의 제조 상태로 리셋)되지 않는 한 대체될 수 없다. 따라서, 구성 설정은 일단 지정되면, TSD가 제조 상태로 다시 리셋되지 않는 한 결코 변경될 수 없다. 프로비전 인증서(204)의 이러한 리셋은 모든 보호된 데이터를 파괴하며, 따라서 이 데이터가 안전하게 유지되고 임의의 TSD 구성 설정을 제조시와 같이 초기 상태로 다시 리셋시킨다. 성공적인 제1 프로비전 이후에, TSD는 이제 다르게 거동하거나 원래의 것들 이외에 부가의 ACT 및/또는 사일로를 노출시키는 상태에 있을 수 있다. 다른 제조업체 인증서 및 프로비전에 의한 다른 ACT의 추가적인 프로비전은 초기 제조업체 인증서(202) 및 프로비전 인증서(204)에 의해 설정된 TSD의 전역 설정에 결코 영향을 줄 수 없고 ACT-관련 설정에만 영향을 줄 수 있다. 초기의 제조업체 인증서(202) 및 프로비전 인증서(204) 제약조건으로 인해 TSD 및 TSD 상의 ACT가 안전하게 유지된다.

[0022] ITU(International Telecommunication Union)의 ITU-T X.509 표준에 따라 인증서를 표현하는 데 사용되는 ASN(autonomous system number)의 ASN.1 데이터 형식이 이하에 제시된다. 이것은 IEEE 1667 표준에 따라 TSD 장치의 제조업체 인증서(202) 및 프로비전 인증서(204)에 대해 사용되는 포맷이다. 살펴본 바와 같이, 데이터 형식은 인증서의 끝 부근에서 확장 필드를 사용하는 것을 제공한다. 그러나, 이 확장은 선택적인 것으로 생각되며, 더 이상 정의하지 않는다. 유의할 점은, 인증서에 확장 필드가 존재할 수 있도록 하기 위해, 버전 필드가 버전 3(v3)으로 설정되어야만 한다는 것이다.

```
Certificate ::= SIGNED { SEQUENCE {
        version [0] Version DEFAULT v1,
        serialNumber CertificateSerialNumber,
        signature AlgorithmIdentifier,
        issuer Name,
        validity Validity,
        subject Name,
        subjectPublicKeyInfo SubjectPublicKeyInfo,
        issuerUniqueIdentifier [1] IMPLICIT UniqueIdentifier OPTIONAL,
                                    -- if present, version shall be v2 or v3
        subjectUniqueIdentifier [2] IMPLICIT UniqueIdentifier OPTIONAL,
                                    -- if present, version shall be v2 or v3
        extensions [3] Extensions OPTIONAL
                                    -- If present, version shall be v3 -- } }

        Version ::= INTEGER { v1(0), v2(1), v3(2) }
        CertificateSerialNumber ::= INTEGER
AlgorithmIdentifier ::= SEQUENCE {
        algorithm ALGORITHM.&id ({SupportedAlgorithms}),
```

[0023]

```
        parameters ALGORITHM.&Type ({SupportedAlgorithms}{ @algorithm})
    OPTIONAL }
        -- Definition of the following information object set is deferred, perhaps to
    standardized
        -- profiles or to protocol implementation conformance statements. The set is
    required to
        -- specify a table constraint on the parameters component of AlgorithmIdentifier.
        -- SupportedAlgorithms ALGORITHM ::= { ... }
    Validity ::= SEQUENCE {
        notBefore Time,
        notAfter Time }
    SubjectPublicKeyInfo ::= SEQUENCE {
        algorithm AlgorithmIdentifier,
        subjectPublicKey BIT STRING }
    Time ::= CHOICE {
        utcTime UTCTime,
        generalizedTime GeneralizedTime }
    Extensions ::= SEQUENCE OF Extension
    Extension ::= SEQUENCE {
        extnId EXTENSION.&id ({ExtensionSet}),
        critical BOOLEAN DEFAULT FALSE,
        extnValue OCTET STRING
        -- contains a DER encoding of a value of type &ExtnType
        -- for the extension object identified by extnId -- }
    ExtensionSet EXTENSION ::= { ... }
```

[0024]

[0025] 본 기술은 제조업체 인증서(202) 내의 선택적인 확장 필드(212) 및/또는 프로비전 인증서(204) 내의 확장 필드(222)를 이용하여 인증서 사일로 이외의 부가적인 유형의 인증 사일로를 제공한다. TSD를 프로비전하는 동안, 제조업체 또는 프로비저너는 TSD의 거동 및 성능을 제어하는 다양한 장치 설정을 사용할 수 있거나 사용할 수 없도록 선택할 수 있다. 제조업체 또는 프로비저너는 이들 설정을 초기 제조업체 인증서(202) 내의 ITU-T X.509 인증서 확장 필드(212) 및/또는 초기 프로비전 인증서(204) 내의 확장 필드(222)를 통해 전달한다. ACT는 인증서 설정 명령 동안에 이들 설정을 수신한다. 이들 설정의 신뢰성은 위조가 있는 경우 예상된 값과 일치하지 않게 될 인증서 서명 필드에 의해 TSD 상에서 검증될 수 있다.

[0026] 프로비저너는 제조업체 인증서(202)를 검색함으로써 이용가능한 지원되는 TSD 구성 설정을 발견할 수 있다. 제조업체 인증서(202)는 그 인증서의 확장 필드(212)에 허용가능한 구성 설정의 세트를 나타내고 있다. 프로비저너는, TSD 상에 프로비전 인증서(204)를 배치시키는 동안, 있는 경우, 어느 것을 프로비전 인증서(204)의 확장 필드(222)에 포함시켜야 하는지를 결정하기 위해 이들 설정을 파싱할 수 있다. 프로비전 인증서(204)의 확장 필드(222) 내의 구성 설정이 제조업체 인증서(202)의 확장 필드(212) 내의 임의의 기본 설정보다 우선할 것이다. 확장 필드(212, 222) 내의 구성 설정은, 모든 데이터 및 인증서가 TSD로부터 삭제되게 하는, 제조업체 인증서(202) 또는 초기 프로비전 인증서(204)의 제거에 의하는 것을 제외하고는 변경될 수 없다는 점에서, 변경할 수 없는 값이다.

[0027] 제조업체 인증서(202)의 확장 필드(212)에 배치될 수 있는 예시적인 구성 설정에 대해 이제부터 기술한다. 먼저, 부가의 유형의 인증 사일로의 생성을 제공하기 위해, 다중 인증 사일로 확장 설정(multiple authentication silo extension setting)(214)이 확장 필드(212)에 위치될 수 있다. 이 확장 설정(214)은 제조업체 또는 프로비저너에 의해 기본 인증서 인증 사일로(200) 이외의 부가의 인증 사일로가 TSD 상의 ACT 내에 배치될 수 있도

록 TSD를 구성하는 데 사용될 수 있다. 부가의 인증 사일로 유형은 비밀번호 사일로 및 생체 ID(bio identification) 사일로를 포함할 수 있다. ACT 상의 다수의 인증 사일로가 제조업체 인증서(202)의 확장 필드(212)를 사용하는 상황에 부딪칠 때 성공적인 인증을 위해 요구되는 논리 조합, 정렬 선호도, 및 사용자 인터페이스 요구사항을 나타내기 위한 예시적인 다중 인증 사일로 확장 설정(214)은 다음과 같을 수 있으며,

extnid = urn:oid:2.25.329800735698586629295641978511506172922

critical = 00

extnValue = 01, 02, 00, 02, 03, 00, 00, 02, 04, 00, 00, 00, 01, 02, 03, 04, 00,

02, 03, 00

[0028]

[0029] 여기서 영이 아닌 항들의 제1 문자열은 사일로 인덱스 값들의 논리적 "MinTerm" AND 결합을 나타낸다. (값 00은, 정의에 의해 비인증 사일로인 프로브를 위해 예약되어 있기 때문에, 구분 기호로서 사용될 수 있다.) 이 항은 00 이후에 그 다음에 나오는 "MinTerm" 조합과 OR 결합된다.

[0030] 상기 예에서, 제1 조합 항은 (01 AND 02) OR (02 AND 03)이다. 00, 00의 출현은 한 조합의 끝을 나타낸다. 이것 이후에, 그 다음 조합이 시작된다. 상기 예에서, 그 다음 조합은 (02 AND 04)이다. 00, 00, 00의 문자열은 일련의 조합의 끝을 나타낸다. 이것 다음에는 선호도의 오름차순으로 나타낸 사일로 인덱스의 목록이 온다. 첫번째로 나오는 00은 이 목록을 종료시키고, 이 목록 상에 사용자 입력을 필요로 하는 사일로 인덱스가 열거되며 다시 00으로 종료된다. 사용자 입력이 필요하지 않은 ACT의 경우에, 당연히 시퀀스 00, 00가 사일로 선호도 목록 바로 다음에 온다. 유의할 점은, 이 기능을 구성하는 제조업체 인증서(202) 대신에, 프로비전 인증서(204)의 확장 필드(222)가 TSD의 상태를 변경시키는 다중 인증 사일로 확장 설정(224)을 포함할 수 있다는 것이다.

[0031] 인증 시퀀스 확장 설정(216)은 특정의 ACT에 액세스하는 허가를 가장 효율적으로 설정하기 위해 다수의 인증 사일로로부터의 인증 챌린지를 검사 또는 답변하도록 TSD 또는 호스트 장치의 논리적 순서를 구성하는 데 사용될 수 있다. 다수의 인증 사일로들 간의 인증 옵션을 시도하는 시퀀스가 호스트 장치의 ID 또는 운영 환경의 다른 양태들에 따라 동일하거나 변할 수 있다. 유의할 점은, 제조업체 인증서(202)가 이 기능을 구성하는 대신에, 프로비전 인증서(204)의 확장 필드(222)가 TSD의 상태를 변경시키는 인증 시퀀스 확장 설정(226)을 포함할 수 있다는 것이다.

[0032] 제공될 수 있는 다른 설정은 인증 조합 확장 설정(218)이다. 다수의 인증 사일로가 사용될 때, 연관된 ACT에 사용자가 액세스하는 것을 허용하기 위해 어느 사일로가 인증된 상태로 있어야만 하는지를 지정하는 것이 중요할 수 있다. 예를 들어, 일 구현에서, 몇개의 인증 사일로가 제공되거나 지원될 수 있지만, 이들 중 어느 하나의 인증이 액세스를 허용하게 될 것이다. 이 예를 계속하면, 사용자는 TSD를 즉각 인증하고 허가하는 올바른 인증서를 자신의 개인 호스트 컴퓨터 상에 가질 수 있지만, 사용자는 대응하는 인증서 없이 공중 호스트 컴퓨터 상에서 TSD를 사용하기를 원하고 별도의 비밀번호 사일로를 인증하기 위해 비밀번호를 입력함으로써 TSD에 액세스할 수 있다. TSD가 인증서 또는 비밀번호를 받아들이도록 구성되어 있는 경우, 올바른 비밀번호를 갖는 사용자에의 액세스가 허용될 것이다. 대안의 예에서, TSD가 액세스를 허용하기 위해 호스트로부터의 인증서 및 사용자로부터의 비밀번호 둘다의 조합을 필요로 하도록 구성되어 있는 경우, 상기 시나리오에서, 사용자는 공중 호스트 컴퓨터 상에서 TSD에의 액세스를 허용받지 못할 것이며, 그 이유는 허가를 받는 데 필요한 인증 조합이 이용가능하지 않았기 때문이다. 유의할 점은, 이 기능을 구성하는 제조업체 인증서(202) 대신에, 프로비전 인증서(204)의 확장 필드(222)가 TSD의 상태를 변경시키는 인증 조합 확장 설정(228)을 포함할 수 있다는 것이다.

[0033] 제조업체 인증서(202)의 확장 필드(212)에 배치하기 위한 인증 사일로에 관련된 다른 설정은 특정의 사일로에 대한 사용자 상호작용 요구사항을 구성하는 사용자 상호작용 요구사항 확장 설정(220)일 수 있다. 이 설정은 사일로를 인증된 상태로 변경하기 위해 사일로가 단지 TSD와 호스트 간의 인증서 비교보다는 사용자 입력을 필요로 하는지 여부를 나타낼 수 있다. 예를 들어, 인증 사일로는 비밀번호 인증 또는 얼굴 인식 또는 기타 생체-인증을 필요로 할 수 있으며, 이들 모두는 TSD 상에 저장된 대응하는 인증 파일 또는 관련 보안 해시값과 비교하기 위해 호스트 장치에의 사용자 입력을 필요로 할 것이다. 대안으로서, 인증서 인증 사일로는 사용자 입력을 필요로 하지 않을 것이다. 유의할 점은, 제조업체 인증서(202)가 이 기능을 구성하는 대신에, 프로비전 인증서(204)의 확장 필드(222)가 TSD의 상태를 변경시키는 사용자 상호작용 요구사항 확장 설정(230)을 포함할 수 있다는 것이다.

[0034] TSD 자체 또는 호스트 장치 상에서 동작하는 TSD에 대한 소프트웨어 에이전트(예를 들어, 소프트웨어 또는 장치-관련 구성 파일의 형태로 되어 있음) 또는 이 둘의 조합이 제조업체 인증서 또는 프로비전 인증서의 확장 필드에 있는 다수의 인증 사일로에 대한 구성 설정에 기초한 하나 이상의 APE(authorization policy expression)를 지니고 있을 수 있다. APE는 다음과 같은 컴포넌트들 중 하나 이상을 포함할 수 있다.

[0035] · 인증 시퀀스 순서에 따라 순위가 매겨진 사일로 ID의 순서있는 목록을 포함하는 문자열 표현;

[0036] · 대응하는 인증 사일로가 인증된 상태에 있을 때, ACT에의 허가된 액세스가 TSD에 의해 호스트 장치에 허용되도록 되어 있는 인증 조합의 논리식(예를 들어, 이하에 기술되는 MaxTerm/MinTerm으로 이루어짐); 및

[0037] · 어느 인증 사일로가 사용자 상호작용을 필요로 하는지를 나타내는 문자열 표현.

[0038] 호스트 장치는 APE에 있는 정보를 사용하여 ACT를 인증된 상태에 두기 위한 가장 효율적인 경로를 계산한다. 인증 사일로의 임의의 가능한 논리적 조합 및 시퀀스에도 대처할 수 있다. APE는 또한 그룹 정책의 시행을 고려하면서 인증 및 허가 프로세스를 최적화하고 제어하는 안내를 호스트 장치에 제공할 수 있다.

[0039] 일군의 예시적인 인증 사일로가 도 3a에 제시되어 있다. 인증 사일로 A는 기본 인증서 사일로(302)로서 나타내어져 있다. 인증 사일로 B는 호스트 장치로부터 올바른 비밀번호의 사용자 입력을 제시할 때 인증되는 비밀번호 사일로(304)로서 나타내어져 있다. 비밀번호 사일로(304)는 특정의 비밀번호에 상관될 사용자 이름을 요청함으로써 TSD의 다수의 사용자에 대처할 수 있거나, 받아들이도록 구성되어 있는 다수의 비밀번호 중 임의의 비밀번호만 인증할 수 있다.

[0040] 인증 사일로 C는 호스트 장치에 연결된 지문 판독기의 사용자 입력을 제시할 때 인증되는 지문 사일로(306)로서 나타내어져 있다. 인증을 수행하기 위해 입력 지문의 해시가 지문 사일로(306)에 저장된 해시와 비교될 수 있다. 지문 사일로(306)는 특정의 지문 해시에 상관될 사용자 이름을 요청함으로써 TSD의 다수의 사용자에 대처할 수 있거나, 받아들이도록 구성되어 있는 다수의 지문 중 임의의 지문만 인증할 수 있다.

[0041] 인증 사일로 D는 호스트 장치에 연결된 성문 판독기의 사용자 입력을 제시할 때 인증되는 성문 사일로(308)로서 나타내어져 있다. 인증을 수행하기 위해 입력 성문의 해시가 성문 사일로(308)에 저장된 해시와 비교될 수 있다. 성문 사일로(308)는 특정의 성문 해시에 상관될 사용자 이름을 요청함으로써 TSD의 다수의 사용자에 대처할 수 있거나, 받아들이도록 구성되어 있는 다수의 성문 중 임의의 성문만 인증할 수 있다.

[0042] 인증 사일로 E는 호스트 장치에 연결된 광학 판독기에서 망막 스캔의 사용자 입력을 제시할 때 인증되는 광학 스캔 사일로(310)로서 나타내어져 있다. 인증을 수행하기 위해 입력 망막 스캔의 해시가 광학 스캔 사일로(310)에 저장된 해시와 비교될 수 있다. 광학 스캔 사일로(310)는 특정의 망막 스캔 해시에 상관될 사용자 이름을 요청함으로써 TSD의 다수의 사용자에 대처할 수 있거나, 받아들이도록 구성되어 있는 다수의 망막 스캔 중 임의의 망막 스캔만 인증할 수 있다.

[0043] 도 3b는 인증 시퀀스 순서에 따라 순위가 매겨진 사일로 ID의 순서있는 목록을 포함하는 예시적인 문자열 표현을 개략적으로 나타낸 것이다. 사일로 B는 바람직한 인증 방법으로서 첫번째로 순위 지정되어 있다. 따라서, 이 경우에, 호스트 장치는 사일로 B를 먼저 사용하여 인증을 시도하도록 APE에 의해 지시를 받을 것이다. 도 3a의 예에서, 이것은 호스트 장치가 비밀번호 형태의 사용자 입력을 탐색하고 다른 인증 사일로들 중 임의의 인증 사일로를 시도해보기 전에 장치에 대해 호스트를 인증하기 위해 비밀번호를 사일로 B에 제시할 것임을 의미할 것이다. 도시된 바와 같이, 바람직한 인증 시퀀스에서, 사일로 C가 두번째로 순위 지정되고, 사일로 D가 세번째로 순위 지정되며, 사일로 E가 네번째로 순위 지정되고, 사일로 A가 다섯번째로 순위 지정된다. 호스트 장치는 APE에 따라 이 순서로 사일로에 대한 인증을 시도할 것이다. 그러나, 호스트 장치는 (예를 들어, 동작 환경에 기초하여) 인증 프로세스를 신속히 처리하기로 결정할 수 있다. 예를 들어, 특정의 사용자 입력이 이용가능하지 않은 경우(예를 들어, 호스트 장치가 도 3a에서와 같이 키보드 또는 지문 판독기를 구비하고 있지 않은 경우), 호스트 장치는 이 사실을 인식하고 곧바로 인증을 위한 사용자 성문 입력을 요청하는 것으로 건너뛸 수 있다.

[0044] 도 3c는 대응하는 인증 사일로가 인증된 상태에 있을 때, ACT에의 허가된 액세스가 TSD에 의해 호스트 장치에 허용되도록 되어 있는 인증 조합의 논리식의 예시적인 일 구현을 개략적으로 나타낸 것이다. 이 예에서, TSD는 ACT에 액세스 권한 부여를 제공하기 위해 극도로 높은 보안을 요구하는 것으로 이해될 수 있다. 이 경우에, APE는 TSD 상의 ACT에 대한 액세스를 허가하기 위해 인증서 및 비밀번호와 관련하여 인증서(사일로 A) 및 비밀번호(사일로 B) 둘다와 지문 일치(사일로 C) 또는 성문 일치(사일로 D) 중 어느 하나의 조합을 필요로 한다.

대안으로서, (예를 들어, 광학 판독기의 정확성 또는 알려진 환경 보안에서) 광학 망막 스캔(사일로 E)을 더 많이 신뢰하기 때문에, 이 인증만으로 TSD 상의 ACT에 액세스할 수 있을 것이다.

[0045] 도 3d는 대응하는 인증 사일로가 인증된 상태에 있을 때, ACT에의 허가된 액세스가 TSD에 의해 호스트 장치에 허용되도록 MaxTerm/MinTerm 구성체를 사용하여 인증 조합의 논리식의 대안의 예시적인 구현을 개략적으로 나타낸 것이다. 도 3d에 도시된 바와 같이, 인증서 인증(사일로 A)이 비밀번호 인증(사일로 B), 지문 인증(사일로 C), 또는 성문 인증(사일로 D) 중 임의의 것에 수반되는 경우, TSD 상의 ACT에 대한 액세스가 허가될 수 있다. 대안으로서, 광학 스캔 사일로(사일로 E)만을 제공하는 것으로 액세스가 허용될 것이다.

[0046] TSD(또는 APE에 따른 호스트 장치)는 표준 MaxTerm/MinTerm 비교를 수행함으로써 이들 특정의 조합 중 임의의 것이 존재하는지를 판정할 수 있다. 최소항(minimum term)은 사일로 A 및 B, 사일로 A 및 C, 사일로 A 및 D, 그리고 사일로 E의 조합이다. 임의의 사일로가 인증되는 경우, 그의 상태가 1로 표현될 수 있다. 사일로가 인증되지 않은 경우, 그의 상태가 0으로 표현될 수 있다. 이들 상태 값을 MinTerm 연산자에 조합하는 것은 상태 값들을 서로 곱함으로써 수행된다. 따라서, 하나의 상태 항(state term)이 0인 경우, MinTerm은 0일 것이고, 양쪽 상태 항 모두가 1인 경우, 그 조합에 대해 MinTerm은 1일 것이다. 모든 MinTerm 조합의 합인 Maxterm이 0보다 크면, 적절한 인증 및 권한 부여가 있다. 모든 MinTerm이 0인 경우, MaxTerm이 0일 것이고, ACT에의 액세스가 거부될 것이다. 모든 MinTerm이 0보다 큰 경우, MaxTerm이 0보다 클 것이고, ACT에의 액세스가 허용될 것이다.

[0047] 다수의 인증 사일로를 갖는 환경에서 TSD의 사용자에 대한 ACT에의 액세스를 허가하는 예시적인 인증 프로세스(400)가 도 4에 제시되어 있다. 액세스 오퍼레이션(402)에서, 프로브 사일로를 검사하여 사일로의 수, 유형 및 버전을 얻기 위해 TSD 상의 프로브 사일로가 호스트에 의해 액세스된다. 호스트는 이와 동시에 호스트 장치와 관련된 운영 체제 및 IEEE 1667 버전 정보를 제공한다. 사일로 정보를 사용하여, 호스트는 그 다음에 제2 액세스 오퍼레이션(404)에서 프로브 사일로에 의해 제공되는 ID 정보에 기초하여 인증 사일로(들)에 액세스한다. 프로브 사일로가 특정의 ACT에 대해 2개 이상의 인증 사일로가 있다고 나타내는 경우, APE는 인증 프로세스(400)가 인증 요건을 조정하고 인증 사일로의 상태를 보고하여 액세스 허가를 위해 필요한 종합적 상태가 달성되었는지를 판정하는 것을 돕도록 구성될 수 있다. 프로세스(400)는 이어서 APE에 따라 제1 판정 오퍼레이션(406)에서 나타낸 바와 같이 허가를 위해 필요한 인증들의 조합이 있는지를 판정한다. 프로세스(400)는 또한 장치 선호도 또는 오퍼레이션(408)에서의 호스트 최적화 판정에 따라 다수의 사일로의 논리 조합의 인증을 위한 논리 시퀀스 또는 순서를 결정한다. 오퍼레이션(410)에서, 선호도 및/또는 호스트 최적화에 따라 처음으로 나오는 인증 사일로의 논리적 조합이 선택된다.

[0048] APE는 또한 특정의 인증 사일로가 사용자 입력을 필요로 하는지 여부에 관한 정보를 제공할 수 있다. 시퀀스에서 제1 인증 사일로에 대해, 프로세스(400)는, 질의 오퍼레이션(412)에서, 사일로를 인증하는 데 사용자 입력이 필요한지를 질의한다. 사용자 입력이 필요하지 않은 경우, 프로세스는 자동 인증 조합(예를 들어, 호스트 장치에 의해 제공되는 인증서)을 인증하려고 시도하기 위해 인증 오퍼레이션(418)으로 이동한다. 프로세스(400)는 인증들의 조합에 의해 ACT에의 허가된 액세스에 대해 TSD에 의해 요구되는 전체적인 인증이 성공적으로 허용되었는지를 판정하기 위해 질의 오퍼레이션(420)으로 이동한다. 요구된 인증 조합이 충족된 경우, 호스트는 허가되고, 허용 오퍼레이션(422)에서 나타낸 바와 같이, ACT에의 액세스가 허용될 것이다.

[0049] 사용자 입력 질의 오퍼레이션(412)으로 되돌아가서, 사용자 입력(예를 들어, 비밀번호 또는 생체-인증)이 요구되는 경우, 요청 오퍼레이션(414)에서 호스트 장치는 요구된 사용자 입력을 요청할 것이다. 호스트 장치는 이어서, 질의 오퍼레이션(416)에서, 요청된 입력 정보가 이용가능한지 여부를 판정한다. 호스트 장치가 요청된 사용자 입력이 이용가능하지 않은 것으로(예를 들어, 호스트 장치가 특정의 입력 인터페이스 장치에 연결되어 있지 않은 것으로) 또는 적당한 기간 후에 사용자 입력이 공급되지 않은 것으로 판정하는 경우, 프로세스(400)는 질의 오퍼레이션(424)의 일부로서 시도될 수 있는 임의의 추가의 논리 조합이 남아 있는지 여부를 판정한다. 추가의 조합이 남아 있지 않은 경우, 호스트는 오퍼레이션(426)에서 나타낸 바와 같이 임의의 추가의 인증 시도를 종료한다. 그러나, 추가의 조합이 남아 있는 경우, 그 다음 조합이 선택되는데, 그 이유는 프로세스(400)가 그 다음 이용가능한 조합을 선택하기 위해 오퍼레이션(410)으로 되돌아가기 때문이다.

[0050] 대안으로서, 질의 오퍼레이션(416)이 사용자 입력이 이용가능하고 적절하다고 판정하는 경우, 프로세스는 ACT의 논리적 조합을 인증하려고 시도할 때 사용자 입력이 다른 필요한 데이터와 함께 사용되는 오퍼레이션(418)으로 이동한다. 프로세스(400)는 이어서 임의의 요구된 인증 조합이 충족되었는지 여부를 판정하기 위해 질의 오퍼레이션(420)으로 이동한다. 인증 사일로의 인증 상태가 모여서 요구된 인증 조합을 달성하게 되는 경우, 호스

트는 허가되고, 허용 오퍼레이션(420)에서 나타낸 바와 같이, ACT에의 액세스가 허용될 것이다.

[0051] 대안으로서, 질의 오퍼레이션(416)이 인증서 또는 수신된 입력이 유효하지 않은 것으로 판정하거나 질의 오퍼레이션(420)이 인증된 사일로들의 요구된 조합이 충족되지 않은 것으로 판정하는 경우, 프로세스(400)는 질의 오퍼레이션(424)에서 시도되어야 하는 임의의 논리적 조합이 남아 있는지를 판정한다. 남아 있는 조합이 더 이상 없는 경우, 오퍼레이션(426)에 나타낸 바와 같이 ACT에 액세스하기 위한 인증 시도가 더 이상 행해지 않을 것이다. 대안으로서, 이용가능한 조합이 더 있는 경우, 프로세스(400)는 선택 오퍼레이션(410)에 나타낸 바와 같이 시도된 인증에 대한 그 다음 인증 사일로 조합을 선택할 수 있고 앞서 설명한 바와 같이 TSD에 대해 호스트 장치를 인증하려고 시도할 수 있다.

[0052] TSD에 대해 호스트 컴퓨터 장치로서 동작할 수 있는 범용 컴퓨팅 장치(500)의 개략도가 도 5에 도시되어 있다. 호스트 컴퓨팅 장치의 예시적인 하드웨어 및 동작 환경은 처리 장치(502), 시스템 메모리(504), 및 시스템 메모리(504)를 비롯한 각종 시스템 컴포넌트들을 처리 장치(502)에 연결시키는 동작을 하는 시스템 버스(518)를 포함할 수 있다. 컴퓨터(500)의 프로세서가 하나의 중앙 처리 장치(CPU) 또는 복수의 처리 장치(흔히, 병렬 처리 환경이라고 함)를 포함하도록 하나 이상의 처리 장치(502)가 있을 수 있다. 컴퓨터(500)는 종래의 컴퓨터, 분산 컴퓨터, 또는 임의의 다른 유형의 컴퓨터일 수 있다.

[0053] 시스템 버스(518)는 메모리 버스 또는 메모리 컨트롤러, 주변 장치 버스, 스위치 패브릭(switched fabric), 점대점 연결, 및 각종 버스 아키텍처 중 임의의 것을 이용하는 로컬 버스를 비롯한 몇몇 유형의 버스 구조 중 어느 것이라도 될 수 있다. 시스템 메모리(504)는 또한 간단히 메모리라고도 할 수 있으며, 판독 전용 메모리(ROM)(506) 및 랜덤 액세스 메모리(RAM)(505)를 포함한다. 시작 중과 같은 때에, 컴퓨터(500) 내의 구성요소들 사이의 정보 전송을 돕는 기본 루틴을 포함하는 기본 입/출력 시스템(BIOS)(508)은 ROM(506)에 저장되어 있다. 컴퓨터(500)는 하드 디스크(도시 생략)에 기록을 하거나 그로부터 판독을 하는 하드 디스크 드라이브(530), 이동식 자기 디스크(536)에 기록을 하거나 그로부터 판독을 하는 자기 디스크 드라이브(532), 및 CD-ROM 또는 기타 광 매체와 같은 이동식 광 디스크(538)에 기록을 하거나 그로부터 판독을 하는 광 디스크 드라이브(534)를 더 포함한다.

[0054] 하드 디스크 드라이브(530), 자기 디스크 드라이브(532) 및 광 디스크 드라이브(534)는 각각 하드 디스크 드라이브 인터페이스(520), 자기 디스크 드라이브 인터페이스(522), 및 광 디스크 드라이브 인터페이스(524)에 의해 시스템 버스(518)에 접속된다. 이 드라이브들 및 그들과 관련된 컴퓨터-판독가능 매체는 컴퓨터(500)의 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 및 기타 데이터의 비휘발성 저장을 제공한다. 당업자라면 컴퓨터에 의해 액세스될 수 있는 데이터를 저장할 수 있는 임의의 유형의 컴퓨터-판독가능 매체, 예를 들어, 자기 카세트, 플래시 메모리 카드, DVD(digital video disk), RAM, 및 ROM이 예시적인 운영 환경에서 사용될 수 있다는 것을 잘 알 것이다.

[0055] 운영 체제(510), 하나 이상의 응용 프로그램(512), 기타 프로그램 모듈(514) 및 프로그램 데이터(516)를 비롯한 다수의 프로그램 모듈이 하드 디스크(530), 자기 디스크(532), 광 디스크(534), ROM(506) 또는 RAM(505)에 저장될 수 있다. 예시적인 구현에서, TSD와의 통신 및 데이터 전송을 위한 프로그램이 운영 체제(510)[예를 들어, API(application protocol interface)의 일부로서], 응용 프로그램(512), 또는 기타 프로그램 모듈(514)(예를 들어, 인증 프로세스 동안에 APE를 처리하는 모듈)의 일부로서 포함될 수 있다.

[0056] 사용자는 키보드(540) 및 포인팅 장치(542), 예를 들어, 마우스 등의 입력 장치를 통해 퍼스널 컴퓨터(500)에 명령 및 정보를 입력할 수 있다. 기타 입력 장치(도시 생략)는, 예를 들어, 마이크, 조이스틱, 게임 패드, 태블릿, 터치 스크린 장치, 위성 안테나, 스캐너, 팩시밀리 기계, 및 비디오 카메라를 포함할 수 있다. 이들 및 기타 입력 장치는 종종 시스템 버스(518)에 연결된 직렬 포트 인터페이스(526)를 통해 처리 장치(502)에 접속되지만, 병렬 포트, 게임 포트 또는 USB(universal serial bus) 등의 다른 인터페이스에 의해 접속될 수도 있다.

[0057] 모니터(544) 또는 기타 종류의 디스플레이 장치도 비디오 어댑터(546) 등의 인터페이스를 통해 시스템 버스(518)에 접속되어 있다. 모니터(544) 외에, 컴퓨터는 통상적으로 프린터(558) 및 스피커(도시 생략) 등의 기타 주변 출력 장치를 포함한다. 이들 및 기타 출력 장치는 종종 시스템 버스(518)에 연결된 직렬 포트 인터페이스(526)를 통해 처리 장치(502)에 접속되지만, 병렬 포트, 게임 포트 또는 USB(universal serial bus) 등의 다른 인터페이스에 의해 접속될 수도 있다. 미디어 튜너 모듈(560)도 역시 시스템 버스(518)에 접속되어, 비디오 어댑터(546) 또는 기타 프레젠테이션 출력 모듈을 통해 출력하기 위해 오디오 및 비디오 프로그래밍(예를 들어, TV 프로그래밍)을 튜닝할 수 있다.

[0058] 컴퓨터(500)는 원격 컴퓨터(554)와 같은 하나 이상의 원격 컴퓨터로의 논리적 접속을 사용하여 네트워크화된 환경에서 동작할 수 있다. 이들 논리적 접속은 컴퓨터(500)에 연결되거나 컴퓨터(500)와 통합된 통신 장치에 의해 달성될 수 있으며, 본 발명은 특정의 유형의 통신 장치로 제한되지 않는다. 원격 컴퓨터(554)는 또 하나의 컴퓨터, 서버, 라우터, 네트워크 PC, 클라이언트, 피어 장치 또는 기타 통상의 네트워크 노드일 수 있고, 통상적으로 컴퓨터(500)와 관련하여 상술된 구성요소들의 대부분 또는 그 전부를 포함하지만, 도 5에는 메모리 저장 장치(556)만이 도시되어 있다. 도 5에 도시된 논리적 접속은 LAN(550) 및 WAN(552)을 포함한다. 이러한 네트워킹 환경은 사무실 네트워크, 전사적 컴퓨터 네트워크(enterprise-wide computer network), 인트라넷 및 인터넷에서 일반적인 것이며, 이들은 모든 유형의 네트워크이다.

[0059] LAN(550) 환경에서 사용될 때, 컴퓨터(500)는 네트워크 인터페이스 또는 어댑터(528)(예를 들어, 이더넷 또는 기타 통신 인터페이스)를 통해 LAN(550)에 접속될 수 있다. WAN(552) 환경에서 사용될 때, 컴퓨터(500)는 통상적으로 WAN(552)을 통해 통신을 설정하기 위한 모뎀(548), 네트워크 어댑터, 또는 임의의 다른 유형의 통신 장치를 포함한다. 내장형 또는 외장형일 수 있는 모뎀(548)은 직렬 포트 인터페이스(526)를 통해 시스템 버스(518)에 접속된다. 네트워크화된 환경에서, 퍼스널 컴퓨터(500) 또는 그의 일부와 관련하여 기술된 프로그램 모듈은 원격 메모리 저장 장치에 저장될 수 있다. 도시된 네트워크 연결이 예시적인 것이고 컴퓨터들 간에 통신 링크를 설정하는 기타 수단 및 통신 장치가 사용될 수 있다는 것을 잘 알 것이다.

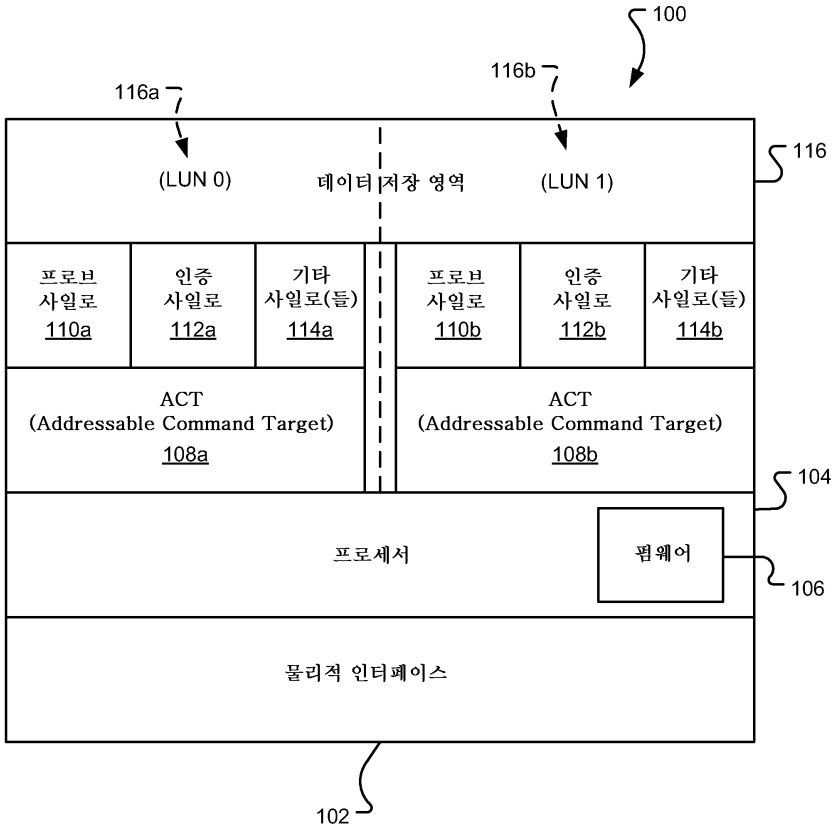
[0060] 본 명세서에 설명된 기술이 하나 이상의 시스템에서 논리 연산 및/또는 모듈로서 구현될 수 있다. 논리 연산은 하나 이상의 컴퓨터 시스템에서 실행되는 일련의 프로세서-구현 단계들로서 또 하나 이상의 컴퓨터 시스템 내의 상호 연결된 기계 또는 회로 모듈로서 구현될 수 있다. 마찬가지로, 다양한 컴포넌트 모듈에 대한 설명이 모듈에 의해 실행되거나 실시되는 오퍼레이션들과 관련하여 제공될 수 있다. 그 결과 얻어지는 구현은 설명된 기술을 구현하는 기반 시스템의 성능 요건에 따른 선택의 문제이다. 그에 따라, 본 명세서에 설명된 기술의 실시예들을 이루고 있는 논리 연산들이 연산, 단계, 개체 또는 모듈로서 여러가지로 지칭된다. 게다가, 명시적으로 달리 청구되지 않거나 특정의 순서가 청구항 문언에 의해 본질적으로 필요로 하지 않는 한, 논리 연산이 임의의 순서로 수행될 수 있다는 것을 잘 알 것이다.

[0061] 일부 구현들에서, 제조 물품이 컴퓨터 프로그램 제품으로서 제공된다. 일 구현에서, 컴퓨터 프로그램 제품이 컴퓨터 시스템에 의해 실행가능한 인코딩된 컴퓨터 프로그램 명령어를 저장하는 컴퓨터-판독가능 매체로서 제공된다. 컴퓨터 프로그램 제품의 다른 구현이 컴퓨팅 시스템에 의해 반송파에 구현된, 컴퓨터 프로그램을 인코딩하는 컴퓨터 데이터 신호로 제공될 수 있다. 다른 구현들도 본 명세서에 설명되고 인용되어 있다.

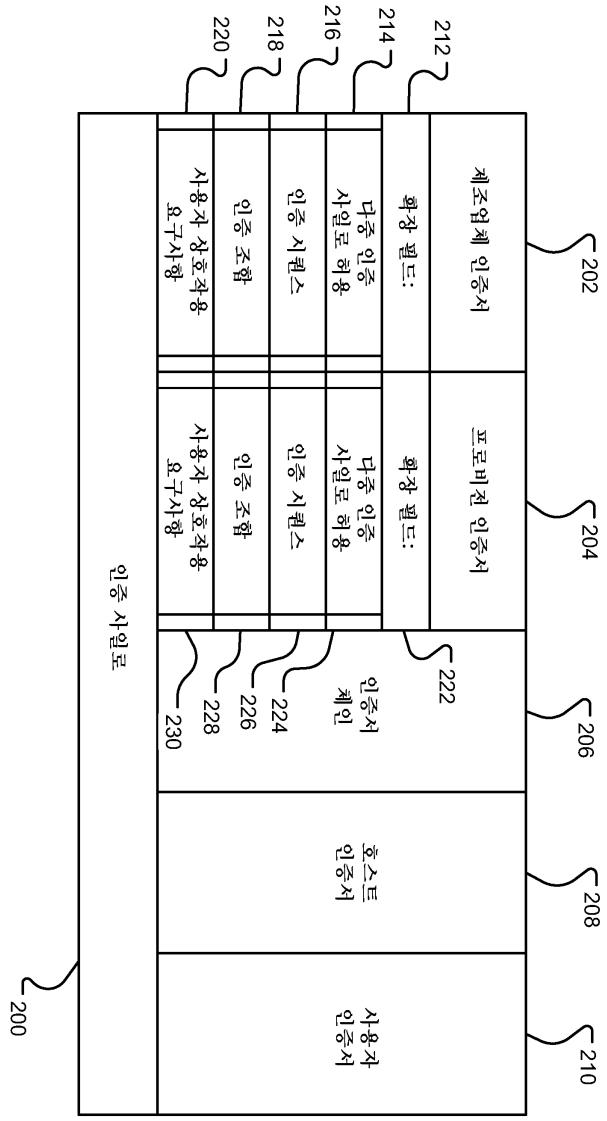
[0062] 이상의 명세서, 예 및 데이터는 본 발명의 예시적인 실시예들의 구조 및 용도에 대한 완전한 설명을 제공한다. 본 발명의 다양한 실시예들이 이상에서 어느 정도 상세히 또는 하나 이상의 개별적인 실시예들을 참조하여 기술되어 있지만, 당업자라면 본 발명의 사상 또는 범위를 벗어나지 않고 개시된 실시예들에 대해 많은 변경들을 할 수 있다. 특히, 설명된 기술이 퍼스널 컴퓨터와 독립적으로 이용될 수 있다는 것을 잘 알 것이다. 따라서, 다른 실시예들이 생각되고 있다. 이상의 설명에 포함되고 첨부 도면에 도시된 모든 내용이 제한하는 것이 아니라 특정의 실시예를 예시한 것에 불과한 것으로 해석되어야만 한다. 이하의 특허청구범위에 한정된 본 발명의 기본적인 구성요소를 벗어나지 않고 상세 또는 구조의 변경이 행해질 수 있다.

도면

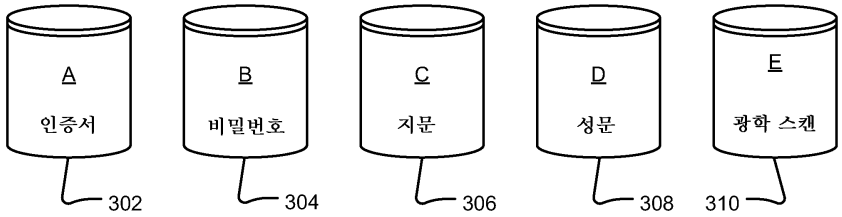
도면1


100
116a
116b
(LUN 0)
데이터 저장 영역
(LUN 1)
116
프로브 사일로 110a
인증 사일로 112a
기타 사일로(들) 114a
프로브 사일로 110b
인증 사일로 112b
기타 사일로(들) 114b
ACT (Addressable Command Target) 108a
ACT (Addressable Command Target) 108b
104
프로세서
펌웨어
106
물리적 인터페이스
102

도면2



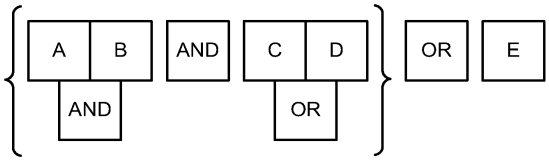
도면3a



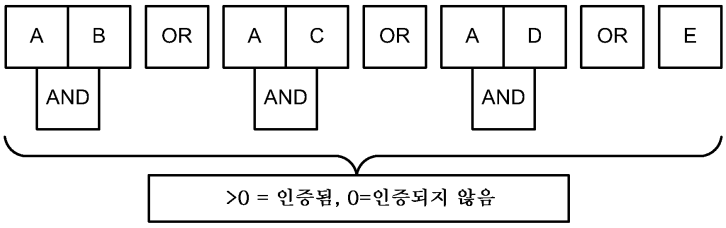
도면3b

A	B	C	D	E
4	1	2	3	5

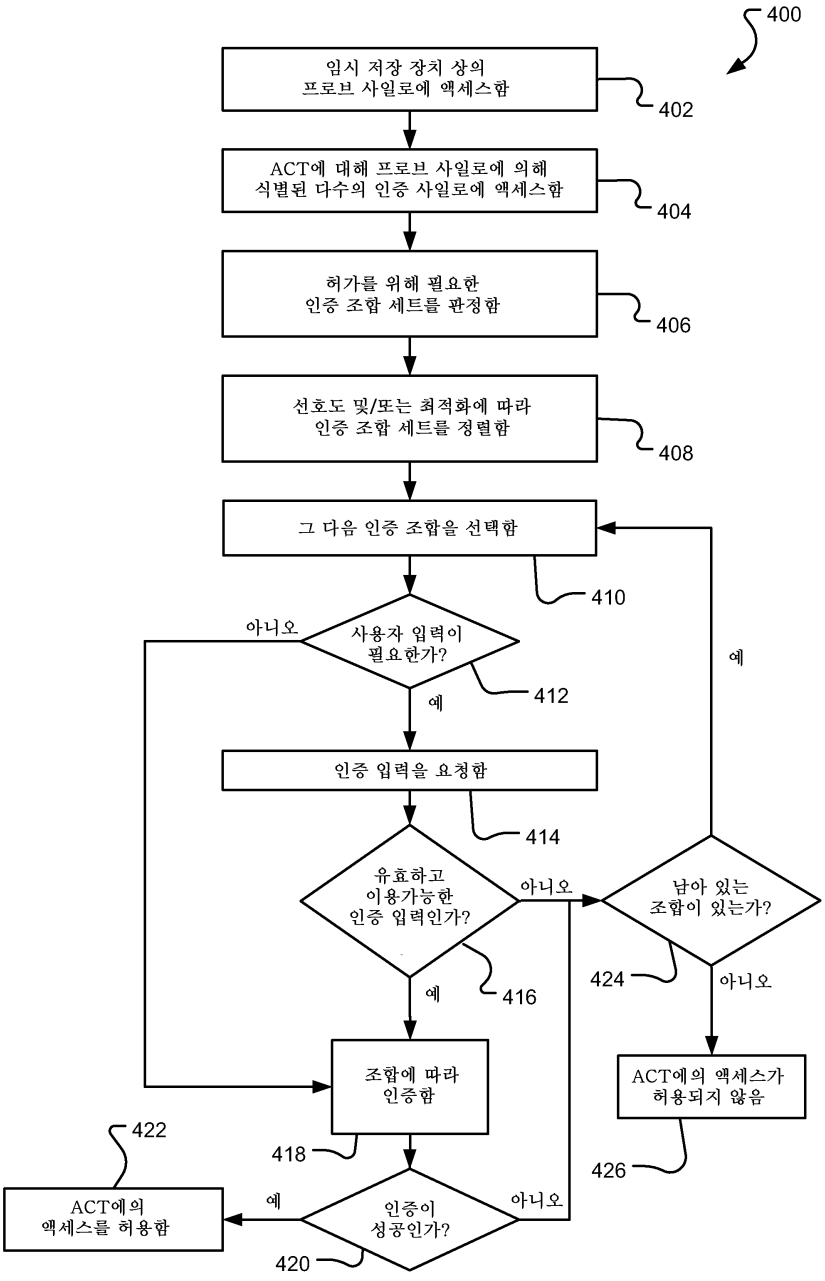
도면3c



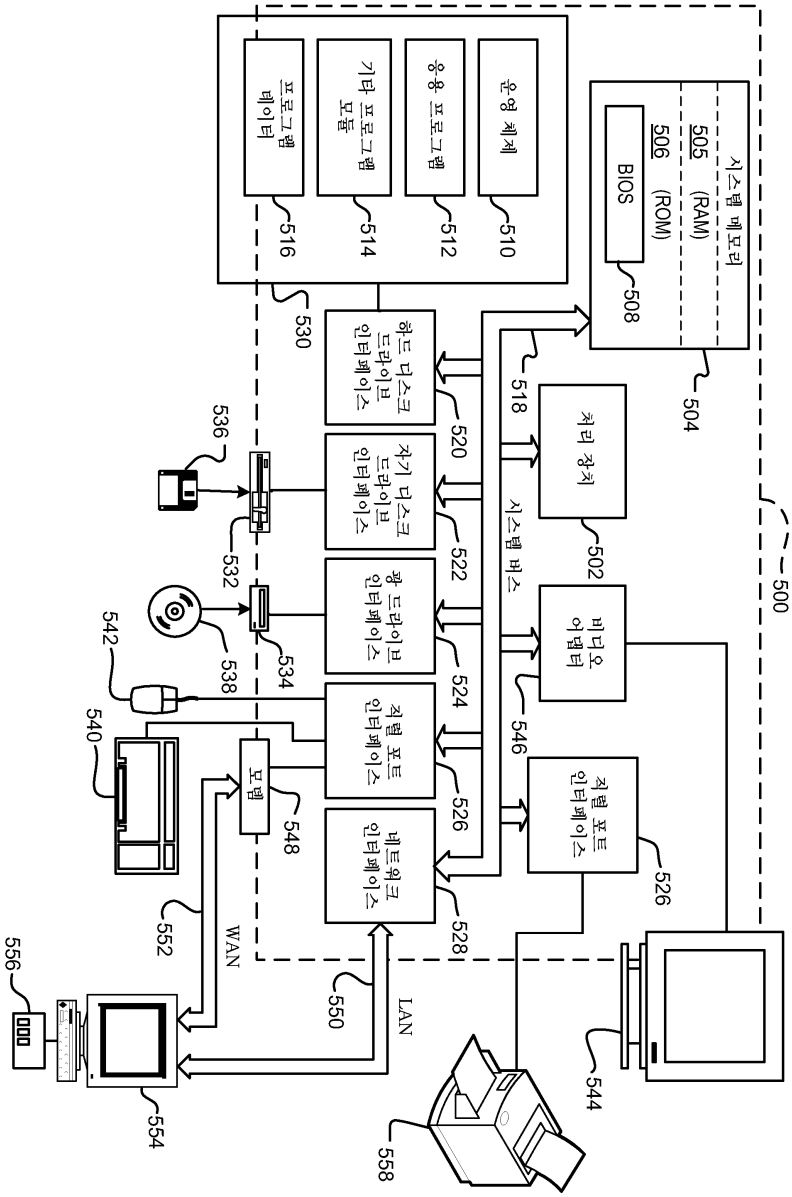
도면3d



도면4


400
임시 저장 장치 상의 프로브 사일로에 액세스함
402
ACT에 대해 프로브 사일로에 의해 식별된 다수의 인증 사일로에 액세스함
404
허가를 위해 필요한 인증 조합 세트를 판정함
406
선호도 및/또는 최적화에 따라 인증 조합 세트를 정렬함
408
그 다음 인증 조합을 선택함
410
사용자 입력이 필요한가?
412
아니오
예
인증 입력을 요청함
414
유효하고 이용가능한 인증 입력인가?
416
아니오
예
남아 있는 조합이 있는가?
424
아니오
예
조합에 따라 인증함
418
ACT에의 액세스가 허용되지 않음
426
인증이 성공인가?
420
아니오
예
ACT에의 액세스를 허용함
422

도면5


500
시스템 메모리
505 (RAM)
506 (ROM)
BIOS
508
504
운영 체제
510
응용 프로그램
512
기타 프로그램 모듈
514
프로그램 데이터
516
530
518
처리 장치
502
시스템 버스
하드 디스크 드라이브 인터페이스
520
자기 디스크 드라이브 인터페이스
522
광 드라이브 인터페이스
524
직렬 포트 인터페이스
526
네트워크 인터페이스
528
비디오 어댑터
546
직렬 포트 인터페이스
526
모뎀
548
536
532
534
538
542
540
552
WAN
550
LAN
556
554
544
558