(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2007-0104393
(43) 공개일자 2007년10월25일

(51) Int. Cl.
G06F 21/20(2006.01) *H04L 9/32*(2006.01)
H04L 9/32(2006.01)
(21) 출원번호 10-2007-7018101
(22) 출원일자 2007년08월06일
심사청구일자 2007년08월06일
번역문제출일자 2007년08월06일
(86) 국제출원번호 PCT/US2005/045040
국제출원일자 2005년12월13일
(87) 국제공개번호 WO 2006/073702
국제공개일자 2006년07월13일
(30) 우선권주장
11/051,499 2005년02월03일 미국(US)
60/642,340 2005년01월07일 미국(US)

(71) 출원인
애플 인크.
미합중국, 95014 캘리포니아, 쿠퍼티노, 인피니트 루프 1
(72) 발명자
루빈스타인, 조나단, 제이크
미국 94111 캘리포니아주, 샌프란시스코 워싱턴 스트리트 611
패델, 안토니, 엠.
미국 94028 캘리포니아주 포톨라 밸리 사우쓰 발 사민 웨이 290
(뒷면에 계속)
(74) 대리인
양영준, 백만기

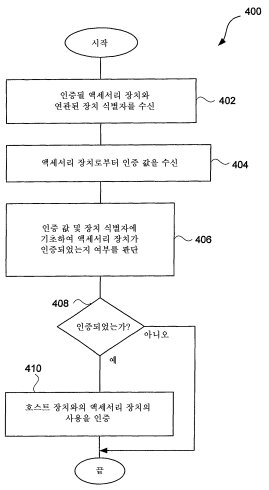
전체 청구항 수 : 총 52 항

(54) 전자 장치에 대한 액세서리 인증

(57) 요 약

전자 장치와 액세서리 장치의 활용을 제어하는 개선된 기술이 개시되어 있다. 개선된 기술은 암호 방법을 이용하여 전자 장치들 즉, 서로 상호접속하고 통신하는 전자 장치들을 인증할 수 있다. 한 가지 특성은, 액세서리 장치와 같은, 전자 장치를 인증하는 기술에 관한 것이다. 또 다른 특징은 전자 장치(예컨대, 호스트 장치)에 의해 또는 전자 장치를 위해 소프트웨어 특징(예컨대, 기능)을 제공하는 것에 관한 것이다. 다른 전자 장치들은 예컨대, 여러 인증 정도 또는 레벨에 따라, 또는 제조자 또는 제품 기반에 따라 다르게 공급될 수 있다. 또 다른 특징은 액세서리(또는 어댑터)를 이용하여 주변 장치(예컨대, USB)를 호스트 장치(예컨대, USB 호스트)로 전환하는 것이다. 개선된 기술은 특히 액세서리 장치를 수신할 수 있는, 이를테면 미디어 장치와 같은, 전자 장치에 대해 적합할 수 있다. 매체 장치의 일 예는 매체 아이템(또는 매체 자산)을 나타낼 수 있는(예컨대, 플레이할 수 있는) 손에 쥐는 매체 플레이어(예컨대, 음악 플레이어)와 같은 매체 플레이어이다.

대표도 - 도4a



(72) 발명자

도로구스키, 제쎄, 엘.

미국 94025 캘리포니아주 멘로 파크 엘-205 샤론 파크 드라이브350

아들러, 미첼

미국 95014 캘리포니아주 쿠퍼티노 파사데나 애비뉴 넘버비310090

아치밸드, 존, 웨슬리

미국 94086 캘리포니아주 서니배일 사우쓰 베이뷰 애비뉴 넘버큐275

특허청구의 범위

청구항 1

휴대용 전자 장치(portable electronic device)로서,

하나 이상의 매체 아이템들(media items)에 대한 매체 콘텐츠(media content)를 저장하는 매체 저장 장치;

상기 매체 저장 장치로부터 매체 아이템들 중 적어도 하나에 대한 매체 콘텐츠를 검색하고 상기 매체 콘텐츠가 상기 휴대용 전자 장치의 사용자에게 보여지도록 하는 매체 표시 모듈(media presentation module);

상기 휴대용 전자 장치와 결합 및 상호작용하도록 인증되는 다양한 액세서리 장치들에 대한 인증 정보(authentication information)를 저장하는 인증 테이블; 및

상기 인증 테이블에 저장된 인증 정보의 적어도 일부에 기초하여 상기 휴대용 전자 장치에 결합된 특정 액세서리 장치가 상기 휴대용 전자 장치와 상호동작하도록 인증되었는지 여부를 판단하는 인증 모듈(authentication module)

을 포함하는 휴대용 전자 장치.

청구항 2

제1항에 있어서,

상기 인증 모듈이 상기 특정 액세서리 장치가 상호동작하도록 인증되지 않았다고 판단하는 경우, 상기 휴대용 전자 장치는 상기 특정 액세서리 장치와 상기 휴대용 전자 장치의 상호동작성(interoperability)을 제한하는 휴대용 전자 장치.

청구항 3

제1항에 있어서,

상기 인증 모듈이 상기 액세서리 장치가 상호동작하도록 인증되지 않았다고 판단하는 경우, 상기 휴대용 전자 장치는 상기 액세서리 장치와 상기 휴대용 전자 장치의 상호동작성을 금지하는 휴대용 전자 장치.

청구항 4

제1항에 있어서,

상기 매체 표시 모듈은 컴퓨터 코드를 포함하고, 상기 인증 모듈도 컴퓨터 코드를 포함하며,

상기 휴대용 전자 장치는 상기 매체 표시 모듈 및 상기 인증 모듈의 컴퓨터 코드를 실행하는 프로세서를 더 포함하는 휴대용 전자 장치.

청구항 5

제4항에 있어서,

상기 인증 모듈의 컴퓨터 코드는 인증 알고리즘을 수행하기 위한 컴퓨터 코드를 포함하는 휴대용 전자 장치.

청구항 6

제1항 내지 제5항 중 어느 한 항에 있어서,

상기 인증 정보는 상기 다양한 액세서리 장치들의 각각이 상기 휴대용 전자 장치와 어떻게 또는 어느 정도 또는 어떻게 및 어느 정도 상호동작할 수 있는지를 표시하는 인증 정보를 적어도 포함하는 휴대용 전자 장치.

청구항 7

제1항 내지 제5항에 있어서,

상기 인증 정보는 상기 다양한 액세서리 장치들의 각각에 대하여 적어도 인증 키(authentication key) 및 장치 식별자(device identifier)를 포함하는 휴대용 전자 장치.

청구항 8

제7항에 있어서,

상기 특정 액세서리 장치는 대응 인증 키(counterpart authentication key) 및 장치 식별자를 포함하고,

상기 인증 모듈은 상기 대응 인증 키 및 상기 장치 식별자에 기초하여 상기 액세서리 장치가 상기 휴대용 전자 장치와 상호동작하도록 인증되었는지 여부를 판단하는 휴대용 전자 장치.

청구항 9

제8항에 있어서,

상기 인증 모듈이 상기 액세서리 장치가 상호동작하도록 인증되지 않았다고 판단하는 경우, 상기 휴대용 전자 장치는 상기 특정 액세서리 장치와 상기 휴대용 전자 장치의 상호동작성을 제한하는 휴대용 전자 장치.

청구항 10

제1항 내지 제9항 중 어느 한 항에 있어서,

상기 휴대용 전자 장치는 매체 플레이어인 휴대용 전자 장치.

청구항 11

제10항에 있어서,

상기 매체 아이템은 음악과 관련되고 상기 매체 플레이어는 음악 플레이어인 휴대용 전자 장치.

청구항 12

휴대용 전자 장치에 대한 액세서리 장치로서,

상기 휴대용 전자 장치와 상호작용하기 위한 입력/출력 포트;

인증 알고리즘;

상기 액세서리 장치와 연관된 인증 키;

적어도 상기 인증 알고리즘 및 상기 인증 키를 이용하여 인증 동작들을 수행하기 위해, 상기 입력/출력 포트로 접속되는 인증 컨트롤러; 및

상기 액세서리 장치와 연관된 동작들을 수행하는 액세서리 회로

를 포함하는 액세서리 장치.

청구항 13

제12항에 있어서,

상기 인증 동작들은 상기 휴대용 전자 장치에 대해 상기 액세서리 장치를 인증하는 일을 하는 액세서리 장치.

청구항 14

제13항에 있어서,

상기 액세서리 장치는,

상기 액세서리 장치와 연관된 장치 식별자

를 더 포함하는 액세서리 장치.

청구항 15

제12항에 있어서,

적어도 상기 인증 키, 상기 인증 알고리즘 및 상기 인증 컨트롤러는 단일 집적 회로 칩 내에 있는 액세서리 장

치.

청구항 16

제12항 내지 제15항 중 어느 한 항에 있어서,

상기 인증 키는 비밀 키(private key)이고, 상기 인증 컨트롤러는 상기 비밀 키를 이용하여 값을 암호화하는 액세서리 장치.

청구항 17

제16항에 있어서,

상기 암호화된 값은 상기 입력/출력 포트 통해 상기 휴대용 전자 장치로 제공되는 액세서리 장치.

청구항 18

제16항에 있어서,

상기 암호화된 값은 디지털 서명인 액세서리 장치.

청구항 19

제12항 내지 제15항 중 어느 한 항에 있어서,

상기 액세서리 장치는 주변 어댑터(peripheral adapter)이고,

상기 액세서리 회로는 제1 전압 레벨을 수신하고 제2 전압 레벨을 출력하는 전압 부스터(voltage booster)를 적어도 포함하고, 상기 제1 전압 레벨은 상기 액세서리 장치가 상기 휴대용 전자 장치에 접속되는 경우 상기 휴대용 전자 장치로부터 수신되며, 상기 제2 전압 레벨은 상기 액세서리 장치가 상기 휴대용 전자 장치에 의해 인증되었을 경우에 출력되는 액세서리 장치.

청구항 20

제12항 내지 제15항 중 어느 한 항에 있어서,

상기 액세서리 장치는 상기 휴대용 전자 장치에 대한 주변 장치인 액세서리 장치.

청구항 21

제12항 내지 제15항 중 어느 한 항에 있어서,

상기 액세서리 장치는 상기 휴대용 전자 장치와 사용하는 스피커 시스템 또는 매체 장치인 액세서리 장치.

청구항 22

제12항 내지 제15항 중 어느 한 항에 있어서,

상기 휴대용 전자 장치는 매체 아이템을 저장 및 플레이할 수 있는 매체 플레이어인 액세서리 장치.

청구항 23

제22항에 있어서,

상기 매체 아이템은 음악과 관련되고 상기 매체 플레이어는 음악 플레이어인 액세서리 장치.

청구항 24

액세서리 장치를 매체 플레이어로 접속하기 위한 커넥터(connector)로서,

커넥터 몸체;

상기 커넥터 몸체 내에 부착되고 상기 액세서리 장치와 상기 매체 플레이어간의 전기적 접속을 제공하는 역할을 하는 복수의 전기적 접촉부(electrical contacts); 및

상기 커넥터 몸체에 배치되고 상기 액세서리 장치가 상기 매체 플레이어에 의해 인증될 수 있도록 하는 인증

키를 제공하는 컨트롤러

를 포함하는 커넥터.

청구항 25

제24항에 있어서,

상기 컨트롤러는 상기 액세서리 장치가 인증되었다고 상기 컨트롤러가 판단는 경우 상기 액세서리 장치에 의해 사용되는 상기 매체 플레이어의 적어도 하나의 특정 기능을 인에이블하는 커넥터.

청구항 26

전자 장치와 함께 사용하기 위한 액세서리 장치를 인증하는 방법으로서,

(a) 상기 액세서리 장치로부터 장치 식별자를 수신하는 단계;

(b) 상기 액세서리 장치로부터 인증 값을 수신하는 단계;

(c) 상기 인증 값에 기초하여 상기 액세서리 장치가 인증되는지 여부를 판단하는 단계; 및

(d) 상기 판단하는 단계(c)에서 상기 액세서리 장치가 인증되었다고 판단하는 경우 상기 전자 장치와의 상기 액세서리 장치의 사용을 인증하는 단계

를 포함하는 액세서리 장치 인증 방법.

청구항 27

제26항에 있어서,

상기 인증하는 단계(d)는 상기 판단하는 단계(c)가 액세서리 장치가 인증되었다고 판단하는 경우에만 상기 전자 장치의 하나 이상의 특징들의 사용에 대해 상기 액세서리 장치를 인증하는 액세서리 장치 인증 방법.

청구항 28

제27항에 있어서,

상기 전자 장치의 하나 이상의 특징들은 상기 장치 식별자에 기초하여 결정되는 액세서리 장치 인증 방법.

청구항 29

제27항에 있어서,

상기 전자 장치의 하나 이상의 특징들은 상기 전자 장치에서 이용할 수 있는 명령들 또는 명령들의 그룹들인 액세서리 장치 인증 방법.

청구항 30

제27항에 있어서,

상기 인증하는 단계(d)는 특정 인터페이스 메커니즘을 통해서만 상기 전자 장치와 상기 액세서리의 하나 이상의 특징들의 사용을 인증하는 액세서리 장치 인증 방법.

청구항 31

제26항에 있어서,

상기 인증 값은 디지털 서명(digital signature)인 액세서리 장치 인증 방법.

청구항 32

제26항 내지 제31항 중 어느 한 항에 있어서,

(e) 상기 액세서리 장치가 상기 전자 장치로부터 분리되는 경우 뒤이어 상기 액세서리 장치의 상기 전자 장치와의 사용을 인증하지 않는(deauthorize) 단계

를 더 포함하는 액세서리 장치 인증 방법.

청구항 33

전자 장치와 함께 사용하는 액세서리 장치를 인증하는 방법으로서,

(a) 상기 전자 장치와 상기 액세서리 장치의 부착(attachment)을 탐지하는 단계;

(b) 상기 탐지하는 단계(a)가 상기 액세서리 장치의 부착을 탐지한 후 난수(random number)를 상기 액세서리 장치로 보내는 단계;

(c) 상기 액세서리 장치로부터 인코딩된 값을 연이어 수신하는 단계;

(d) 상기 액세서리 장치로부터 장치 식별자를 수신하는 단계;

(e) 상기 장치 식별자에 기초하여 암호 키를 얻는 단계;

(f) 상기 암호 키를 이용하여 디코딩된 값을 만들도록 상기 인코딩된 값을 디코딩하는 단계;

(g) 상기 디코딩된 값이 상기 난수에 대응하는지 여부를 판단하는 단계; 및

(h) 상기 판단하는 단계(g)가 상기 디코딩된 값이 상기 난수에 대응한다고 표시하는 경우 상기 전자 장치와의 상기 액세서리 장치의 사용을 인증하는 단계

를 포함하는 액세서리 장치 인증 방법.

청구항 34

제33항에 있어서,

상기 인증하는 단계(h)는 상기 전자 장치의 특징들의 결정된 세트(determined set)의 사용에 대하여 상기 액세서리 장치를 인증하는 액세서리 장치 인증 방법.

청구항 35

제34항에 있어서,

상기 전자 장치의 특징들의 결정된 세트는 상기 장치 식별자에 기초하여 결정되는 액세서리 장치 인증 방법.

청구항 36

제35항에 있어서,

상기 특징들의 결정된 세트는 특정 인터페이스 메커니즘을 통해서만 사용에 대하여 인증되는 액세서리 장치 인증 방법.

청구항 37

제33항 내지 제36항에 있어서,

(i) 상기 액세서리 장치가 상기 전자 장치로부터 분리되었는지 여부를 연이어 판단하는 단계; 및

(j) 상기 판단하는 단계(i)가 상기 액세서리 장치가 상기 전자 장치로부터 분리되었다고 판단하는 경우 상기 전자 장치와의 상기 액세서리 장치의 사용을 디스에이블(disable)하는 단계

를 더 포함하는 액세서리 장치 인증 방법.

청구항 38

전자 장치와 함께 사용하는 액세서리 장치를 인증하는 방법으로서,

(a) 상기 전자 장치와 상기 액세서리 장치의 부착(attachment)을 탐지하는 단계;

(b) 상기 탐지하는 단계(a)가 상기 액세서리 장치의 부착을 탐지한 후 적어도 하나의 난수를 포함하는 인증 요청을 상기 액세서리 장치로 보내는 단계;

(c) 연이어 상기 액세서리 장치로부터 인증 응답을 수신하는 단계로서, 상기 인증 응답은 상기 인증 요청에 대한 응답으로서 적어도 인코딩된 값 및 상기 액세서리 장치에 대한 장치 식별자를 포함하는 단계;

(d) 상기 장치 식별자에 기초하여 암호 키를 얻는 단계;

(e) 상기 암호 키를 이용하여 디코딩된 값을 만들도록 상기 인코딩된 값을 디코딩하는 단계;

(f) 상기 디코딩된 값 및 난수 간의 대응에 기초하여 상기 전자 장치와의 상기 액세서리의 사용을 인증하는 단계

를 포함하는 액세서리 장치 인증 방법.

청구항 39

제38항에 있어서,

상기 인증하는 단계(f)는,

(f1) 상기 디코딩된 값을 상기 난수와 비교하는 단계; 및

(f2) 상기 비교하는 단계(f1)가 상기 디코딩된 값이 상기 난수에 매치된다고 표시하는 경우 상기 전자 장치와의 상기 액세서리 장치의 사용을 인증하는 단계

를 포함하는 액세서리 장치 인증 방법.

청구항 40

제38항에 있어서,

상기 인증하는 단계(g)는 상기 전자 장치의 특징들의 결정된 세트의 사용에 대하여 상기 액세서리 장치를 인증하는 액세서리 장치 인증 방법.

청구항 41

제40항에 있어서,

상기 특징들의 결정된 세트 중 적어도 하나는 특정 인터페이스를 통해서만 사용에 대하여 인증되는 액세서리 장치 인증 방법.

청구항 42

제40항에 있어서,

상기 전자 장치의 특징들의 상기 결정된 세트는 상기 장치 식별자에 기초하여 결정되는 액세서리 장치 인증 방법.

청구항 43

제40항에 있어서,

(h) 상기 액세서리 장치가 상기 전자 장치로부터 분리되었는지 여부를 연이어 판단하는 단계; 및

(i) 상기 판단하는 단계(h)가 상기 액세서리 장치가 상기 전자 장치로부터 분리되었다고 판단하는 경우 상기 전자 장치와의 상기 액세서리 장치의 사용을 디스에이블하는 단계

를 더 포함하는 액세서리 장치 인증 방법.

청구항 44

전자 장치와 함께 사용하는 액세서리 장치를 인증하는 방법으로서,

(a) 상기 전자 장치로부터 난수를 수신하는 단계;

(b) 상기 액세서리 장치 내에서 제공된 적어도 하나의 암호 키를 이용하여 상기 난수를 인코딩하여, 인코딩된 값을 만드는 단계; 및

(c) 상기 인코딩된 값 및 장치 식별자를 상기 전자 장치로 보내는 단계

를 포함하는 액세서리 장치 인증 방법.

청구항 45

제44항에 있어서,

(d) 상기 인코딩된 값에 기초하여 상기 액세서리 장치가 상기 전자 장치에 의해 인증되면, 상기 전자 장치의 하나 이상의 특징에 관하여 상기 전자 장치와 동작하도록 상기 액세서리 장치를 인증하는 단계

를 더 포함하는 액세서리 장치 인증 방법.

청구항 46

제44항에 있어서,

(d) 상기 액세서리 장치가 상기 전자 장치에 의해 인증되지 않은 경우 제한된 방법으로 상기 전자 장치와의 상기 액세서리 장치를 동작시키는 단계

를 더 포함하는 액세서리 장치 인증 방법.

청구항 47

제44항에 있어서,

상기 전자 장치는 휴대용 전자 장치인 액세서리 장치 인증 방법.

청구항 48

제44항에 있어서,

상기 휴대용 전자 장치는 매체 플레이어인 액세서리 장치 인증 방법.

청구항 49

매체 플레이어와 액세서리 장치 사이의 상호작용을 제어하기 위한 방법으로서,

상기 액세서리 장치의 분류(classification)를 판단하는 단계;

상기 액세서리 장치에 대한 인증 레벨을 식별하는 단계; 및

상기 액세서리 장치의 상기 분류 및 인증 레벨에 기초하여 상기 액세서리 장치와 함께 사용될 수 있는 매체 장치의 특징들을 선택적으로 활성화하는 단계

를 포함하는 상호작용 제어 방법.

청구항 50

매체 콘텐츠를 저장하고 복수의 사전결정된 기능들을 지원하는 매체 플레이어; 및

상기 매체 플레이어로 접속할 수 있는 액세서리 장치

를 포함하는 매체 플레이어 시스템으로서,

상기 매체 플레이어 및 상기 액세서리 장치는 인증 프로세스를 수행하도록 상호작용하고,

상기 인증 프로세스에 기초하여, 상기 매체 장치의 특정 기능들이 선택적으로 활성화되어 상기 액세서리 장치에 의해 사용가능할 수 있게 되는 매체 플레이어 시스템.

청구항 51

제50항에 있어서,

상기 매체 프로세스는 암호 키를 상기 매체 플레이어 제공하고, 상기 매체 플레이어는 상기 암호 키를 이용하여 상기 액세서리 장치의 활성 레벨(activation levle)을 결정하는 매체 플레이어 시스템.

청구항 52

제51항에 있어서,

활성화된 상기 매체 장치의 특정 기능들은 상기 액세서리 장치의 상기 인증 레벨에 기초하는 미디어 플레이어 시스템.

명 세 서

기 술 분 야

<1> 본 발명은 전자 장치들에 관한 것이고, 특히, 액세서리 장치들을 수신하는, 이른바 매체 플레이어(media players)와 같은 전자 장치들에 관한 것이다.

배 경 기 술

<2> 매체 플레이어는, 이 매체 플레이어에서 플레이되거나 디스플레이될 수 있는, 오디오 트랙 또는 사진과 같은 매체 자산(media assets)을 저장한다. 매체 플레이어의 한 예는 캘리포니아 쿠페르티노(Cupertino, CA)에 위치한 애플 컴퓨터 유한 책임회사(Apple Computer, Inc.)로부터 입수가능한 iPod® 매체 플레이어이다. 종종, 매체 플레이어는 사용자가 매체 자산을 관리할 수 있도록 도움을 주는 호스트 컴퓨터로부터 자신의 매체 자산을 얻는다. 예를 들어, 호스트 컴퓨터는 매체 자산을 관리하기 위해 매체 관리 애플리케이션을 실행할 수 있다. 매체 관리 애플리케이션의 한 예는 애플 컴퓨터사가 제작한 iTunes®이다.

<3> 매체 플레이어는 일반적으로 매체 플레이어와 인터페이스하는데 사용될 수 있는 하나 이상의 커넥터(connectors) 또는 포트를 포함할 수 있다. 예를 들어, 커넥터 또는 포트는 매체 플레이어가 호스트 컴퓨터로 연결되도록 하거나, 도킹 시스템(docking system)으로 삽입되도록 하거나, 액세서리 장치를 수신하도록 할 수 있다. 오늘날 매체 플레이어와 상호 접속할 수 있는 많은 여러 종류의 액세서리 장치들이 있다. 예를 들어, 사용자가 원격으로 매체 플레이어를 제어하도록 원격 제어부(remote control)가 커넥터 또는 포트로 접속될 수 있다. 또 다른 예로, 자동차가 커넥터를 포함할 수 있고 매체 플레이어는 이 커넥터에 삽입되어 자동차 매체 시스템이 매체 플레이어와 상호작용할 수 있고, 따라서 매체 플레이어 상의 매체 콘텐츠가 자동차 내에서 플레이될 수 있다.

<4> 현재, 매체 플레이어의 커넥터 또는 포트는 호환성이 있는 커넥터 또는 포트가 활용되는 한 공개적으로 사용된다. 결과적으로, 많은 제3자가 다른 제조업자들의 매체 플레이어와 함께 사용하기 위한 액세서리 장치들을 개발해왔다. 한 가지 문제점은 매체 플레이어의 제조업자가, 매체 플레이어로 접속될 수 있는 여러 다른 액세서리 장치들에 대해 제어할 수 없다는 점이다. 이는 제3자 액세서리 장치들이 열등하거나, 에러가 나기 쉽거나, 부서지거나(예컨대, 자원 누수(resource draining)), 또는 심지어 매체 플레이어 자체에 손상을 입힐 수 있기 때문에 문제가 된다. 또 다른 문제는 매체 장치의 제조자에 의해 인증되지 않은 제3자 액세서리 장치들이 바람직하지 않거나 원하지 않는 방법으로 매체 장치의 특성을 활용하려고 하는 점이다.

<5> 따라서, 전자 장치들의 제조자가 액세서리 장치들이 전자 장치들과 함께 활용될 수 범위 및 특성을 제어할 수 있는 향상된 기술이 필요하다.

발명의 상세한 설명

<6> 넓게 말해서, 본 발명은 전자 장치들과 액세서리 장치들의 활용을 제어하는 개선된 기술과 관련이 있다. 개선된 기술은 암호 방법을 이용하여 전자 장치들, 즉 서로 상호접속하고 통신하는 전자 장치들을 인증할 수 있다.

<7> 본 발명의 일 특징은 액세서리 장치와 같은 전자 장치를 인증하는 기술에 관한 것이다. 본 발명의 또 다른 특징은 전자 장치(예컨대, 호스트 장치)에 의해 또는 전자 장치를 위해 소프트웨어 특징(software feature)(예컨대, 기능)을 제공하는 것에 관한 것이다. 다른 전자 장치들은, 예컨대, 다른 여러 정도 또는 레벨에 따라, 또는 제조자 또는 제품 기초에 따라 다르게 공급될 수 있다. 또 다른 특징은 액세서리(또는 어댑터)를 이용하여 주변 장치(예컨대, USB)를 호스트 장치(예컨대, USB 호스트)로 전환하는 것이다. 본 발명의 실시예들은 본 명세서에 개시된 하나 이상의 상기 특징들 또는 다른 특징들에 관한 것일 수 있다.

<8> 본 발명은 메쏘드(method), 시스템, 장치, (그래픽 사용자 인터페이스를 포함하는) 기구, 또는 컴퓨터 판독가능 매체를 비롯한 여러 방법으로 구현될 수 있다. 본 발명의 여러 실시예들은 아래에서 논의된다.

<9> 휴대용 전자 장치로서, 본 발명의 일 실시예는 적어도 하나 이상의 매체 아이템들(media items)에 대한 매체 콘텐츠(media content)를 저장하는 매체 저장 장치; 상기 매체 저장 장치로부터 매체 아이템들 중 적어도 하나에 대한 매체 콘텐츠를 검색하고 상기 매체 콘텐츠가 상기 휴대용 전자 장치의 사용자에게 보여지도록 하는 매체 표시 모듈(media presentation module); 상기 휴대용 전자 장치와 결합 및 상호작용하도록 인증되는 다양한 액세서리 장치들에 대한 인증 정보(authentication information)를 저장하는 인증 테이블; 및 상기 인증 테이블에 저장된 인증 정보의 적어도 일부에 기초하여 상기 휴대용 전자 장치에 결합된 특정 액세서리 장치가 상기 휴대용 전자 장치와 상호동작하도록 인증되었는지 여부를 판단하는 인증 모듈(authentication module)을 포함한다.

<10> 휴대용 전자 장치에 대한 액세서리 장치로서, 본 발명의 일 실시예는 적어도 상기 휴대용 전자 장치와 상호작용하기 위한 입력/출력 포트; 인증 알고리즘; 상기 액세서리 장치와 연관된 인증 키; 적어도 상기 인증 알고리즘 및 상기 인증 키를 이용하여 인증 동작들을 수행하기 위해, 상기 입력/출력 포트로 작용적으로 접속되는 인증 컨트롤러; 및 상기 액세서리 장치와 연관된 동작들을 수행하는 액세서리 회로를 포함한다.

<11> 액세서리 장치를 매체 플레이어로 접속하기 위한 커넥터로서, 본 발명의 일 실시예는 적어도 커넥터 몸체; 상기 커넥터 몸체 내에 부착되고 상기 액세서리 장치와 상기 매체 플레이어간의 전기적 접속을 제공하는 역할을 하는 복수의 전기적 접촉부(electrical contacts); 및 상기 커넥터 몸체에 배치되고 상기 액세서리 장치가 상기 매체 플레이어에 의해 인증될 수 있도록 하는 인증 키를 제공하는 컨트롤러를 포함한다.

<12> 전자 장치와 함께 사용하는 액세서리 장치를 인증하는 방법으로서, 본 발명의 일 실시예는 적어도 상기 액세서리 장치로부터 장치 식별자를 수신하는 단계; 상기 액세서리 장치로부터 인증 값을 수신하는 단계; 상기 인증 값에 기초하여 상기 액세서리 장치가 인증되는지 여부를 판단하는 단계; 및 상기 액세서리 장치가 인증되었다고 판단된 경우 상기 전자 장치와의 상기 액세서리 장치의 사용을 인증하는 단계를 포함한다.

<13> 전자 장치와 함께 사용하는 액세서리 장치를 인증하는 방법으로서, 본 발명의 또 다른 실시예는 적어도 상기 전자 장치와 상기 액세서리 장치의 부착(attachment)을 탐지하는 단계; 상기 액세서리 장치의 부착을 탐지한 후 난수(random number)를 상기 액세서리 장치로 보내는 단계; 상기 액세서리 장치로부터 인코딩된 값을 연이어 수신하는 단계; 상기 액세서리 장치로부터 장치 식별자를 수신하는 단계; 상기 장치 식별자에 기초하여 암호 키를 얻는 단계; 상기 암호 키를 이용하여 디코딩된 값을 만들도록 상기 인코딩된 값을 디코딩하는 단계; 상기 디코딩된 값이 상기 난수에 대응하는지 여부를 판단하는 단계; 및 상기 디코딩된 값이 상기 난수에 대응한다고 판단된 경우 상기 전자 장치와의 상기 액세서리 장치의 사용을 인증하는 단계를 포함한다.

<14> 전자 장치와 함께 사용하는 액세서리 장치를 인증하는 방법으로서, 본 발명의 또 다른 실시예는 적어도 상기 전자 장치와 상기 액세서리 장치의 부착(attachment)을 탐지하는 단계; 상기 액세서리 장치의 부착이 탐지된 후 적어도 하나의 난수를 포함하는 인증 요청을 상기 액세서리 장치로 보내는 단계; 상기 액세서리 장치로부터 인증 응답을 연이어 수신하는 단계로서, 상기 인증 응답은 상기 인증 요청에 응답하고, 상기 인증 응답은 적어도 인코딩된 값 및 상기 액세서리 장치에 대한 장치 식별자를 포함하는 단계; 상기 장치 식별자에 기초하여 암호 키를 얻는 단계; 상기 암호 키를 이용하여 디코딩된 값을 만들도록 상기 인코딩된 값을 디코딩하는 단계; 상기 디코딩된 값 및 난수 간의 대응에 기초하여 상기 전자 장치와의 상기 액세서리의 사용을 인증하는 단계를 포함한다.

<15> 전자 장치와 함께 사용하는 액세서리 장치를 인증하는 방법으로서, 본 발명의 또 다른 실시예는 적어도 상기 전자 장치로부터 난수를 수신하는 단계; 상기 액세서리 장치 내에서 제공된 적어도 하나의 암호 키를 이용하여 상기 난수를 인코딩하여, 인코딩된 값을 만드는 단계; 및 상기 인코딩된 값 및 장치 식별자를 상기 전자 장치로 보내는 단계를 포함한다.

<16> 매체 플레이어와 액세서리 장치 사이의 상호작용을 제어하는 방법으로서, 본 발명의 일 실시예는 적어도 상기 액세서리 장치의 분류(classification)를 판단하는 단계; 상기 액세서리 장치에 대한 인증 레벨을 식별하는 단계; 및 상기 액세서리 장치의 상기 분류 및 인증 레벨에 기초하여 상기 액세서리 장치와 함께 사용될 수 있는 매체 장치의 특징들을 선택적으로 활성화하는 단계를 포함한다.

<17> 매체 플레이어 시스템으로서, 본 발명의 일 실시예는 적어도 매체 콘텐츠를 저장하고 복수의 사전결정된 기능들을 지원하는 매체 플레이어; 및 상기 매체 플레이어로 접속할 수 있는 액세서리 장치를 포함한다. 상기 매체 플레이어 및 상기 액세서리 장치는 인증 프로세스를 수행하도록 상호작용하고, 상기 인증 프로세스에 기초하여, 상기 매체 장치의 특정 기능들이 선택적으로 활성화되어 상기 액세서리 장치에 의해 사용가능할 수 있게 된다.

<18> 본 발명의 다른 특징 및 장점들은, 예를 통해 본 발명의 원리를 설명하는 첨부된 도면과 함께 다음의 상세한 설명으로부터 명확하게 알 수 있을 것이다.

실 시 예

<37> 본 발명은 전자 장치들과 함께 액세서리 장치들의 활용을 제어하는 향상된 기술에 관한 것이다. 향상된 기술은 전자 장치들, 즉, 서로 상호접속하고 통신하는 전자 장치들을 인증하는데 암호 방법(cryptographic approaches)을 이용할 수 있다.

<38> 향상된 기술들은 특히 이를테면 액세서리 장치들을 수신할 수 있는 매체 장치와 같은 전자 장치들에 매우 적합하다. 매체 장치의 일 예는, 매체 아이템(또는 매체 자산)을 나타낼 수(예컨대, 플레이할 수) 있는, 손안에 드는 매체 플레이어(예를 들어, 음악 플레이어)와 같은 매체 플레이어이다. 매체 장치에 대한 액세서리들의 예는 보이스 리코더(voice recorder), FM 트랜시버(transceivers), 주변 버스 장치(예컨대, FireWire® 장치들 또는 USB 장치들), 매체 장치(예컨대, 매체 리더, 디스플레이, 카메라 등), 전력 유닛(예컨대, 전력 어댑터, 배터리 팩 등), 스피커(헤드폰 또는 스피커 시스템), 원격 제어 장치, 네트워크 장치, 또는 자동차 통합 유닛을 포함한다.

<39> 본 발명의 한가지 특징은 액세서리 장치와 같은 전자 장치를 인증하는 기술에 관한 것이다. 본 발명의 또 다른 특징은 전자 장치(예컨대, 호스트 장치)에 의해 또는 전자 장치를 위해 소프트웨어 특징(예컨대, 기능)을 공급하는 것과 관련된다. 예를 들어, 여러 전자 장치들은 여러 인증 레벨 또는 정도에 따라 또는 제조자 또는 제품 기반(product basis)에 따라 다르게 공급될 수 있다. 본 발명의 또 다른 특징은 액세서리(또는 어댑터)를 이용하여 주변 장치(예컨대, USB 장치)를 호스트 장치(예컨대, USB 호스트)로 변환하는 점이다. 본 발명의 실시예들은 본 명세서에서 설명된 하나 이상의 이러한 특징 또는 다른 특징에 관련될 수 있다.

<40> 본 발명의 실시예들은 아래의 도 1-12와 함께 논의된다. 그러나, 당업자라면 발명이 이 제한된 실시예들 범위를 넘어설 수 있기 때문에 이 도면들에 관하여 주어진 상세한 설명이 예시적인 목적을 위한 것이라는 것을 알 것이다.

<41> 도 1a는 본 발명의 일 실시예에 따른 액세서리 인증 시스템(100)의 블록도이다. 액세서리 인증 시스템(100)은 모바일 연산 장치(mobile computing device, 112)를 포함한다. 모바일 연산 장치(102)는 호스트 장치로 또한 불리울 수 있다. 추가적으로, 모바일 연산 장치(102)는 예를 들어, 매체 플레이어, 개인용 디지털 보조기, 또는 모바일 텔레폰에 관한 것일 수 있다. 모바일 연산 장치(102)는 커넥터를 받아들이기 위한 커넥터 포트(104)를 포함한다.

<42> 액세서리 인증 시스템(100)은 또한 커넥터(108) 및 커넥터 포트(110)를 가지는 인증 장치(106)를 포함한다. 인증 장치(106)는 모바일 연산 장치(102)에 부착될 수 있다. 특히, 인증 장치(106)가 모바일 연산 장치(102)에 부착되는 경우, 인증 장치(106)의 커넥터(108)는 모바일 연산 장치(102)의 커넥터 포트(104)에 의해 수신된다. 커넥터(108)가 커넥터 포트(104)로 결합된 경우, 인증 장치(106)는 물리적으로 및 전자적으로 모바일 연산 장치(102)에 접속된다.

<43> 액세서리 인증 시스템(100)은 액세서리 장치(112)를 더 포함한다. 액세서리 장치(112)는, 액세서리 장치(112)가 인증 장치(106)를 통해 모바일 연산 장치(102)와 상호접속된 경우 특정 기능성(functionality)을 모바일 연산 장치(102)에 제공한다. 이러한 상호접속을 돕기 위해, 액세서리 장치(112)는 커넥터(114) 및 케이블(116)을 포함한다. 케이블(116)은 커넥터(114)를 액세서리(112)로 접속시킨다. 커넥터(114)는 인증 장치(106)의 커넥터 포트(110)로 결합될 수 있다. 이러한 접속이 이루어진 경우, 액세서리 장치(112)는 인증 장치(106)를 통해 모바일 연산 장치(102)와 전기적으로 통신한다.

<44> 액세서리 인증 시스템(100)이 커넥터(114) 및 케이블(116)의 말단을 포함하지만, 커넥터(114)는 액세서리 장치(112)에 통합될 수 있다. 즉, 또 다른 실시예에서, 케이블(116)은 필요없다.

<45> 본 발명의 일 특징에 따르면, 인증 장치(106)는 자신을 모바일 연산 장치(102)로 인증하는 일을 한다. 인증된 장치는 모바일 연산 장치(102)와 상호작용하도록 인증된 것으로 간주된다. 또한, 일단 인증되면, 인증된 장치(106)(또는 액세서리 장치(102)) 및 모바일 연산 장치(102) 사이의 상호작용(interaction)의 특성 및 정도가 제어될 수 있다. 결과적으로, 일단 인증되면, 모바일 연산 장치(102)는 인증 장치(106)를, 모바일 연산 장치(102)의 기능, 특징 또는 동작을 액세스하도록 허용되는 신뢰 파트너(trusted partner)로 간주할 수 있다. 반면, 만약 모바일 연산 장치(102)가 인증 장치(106)가 신뢰 파트너와 연관되지 않다고 판단하면, 모바일 연산 장

치(102)는 인증 장치(106)나 액세서리 장치(112)와의 상호작용을 막거나 제한할 수 있다. 인증 장치(106)는 또한 그 자체로 모바일 연산 장치(102)에 대한 액세서리 장치로 고려될 수 있다.

<46> 일 실시예에서 인증 장치(106)는 USB 또는 FireWire® 어댑터와 같은 버스 인터페이스 어댑터로 작동한다. 이 실시예에서, 인증 장치(106)는 모바일 연산 장치(102)를 버스 호스트 장치(예컨대, USB 또는 FireWire® 호스트)에 적합하도록 작동한다. 그 후 액세서리 장치(112)는 유리하게 버스 주변 장치(예컨대, USB 또는 FireWire® 장치)로만 동작할 필요가 있다.

<47> 도 1b는 본 발명의 또 다른 실시예에 따른 액세서리 인증 시스템(150)의 블록도이다. 액세서리 인증 시스템(150)은 커넥터 포트(154)를 가지는 모바일 연산 장치(152)를 포함한다. 모바일 연산 장치(152)는 호스트 장치로 언급될 수도 있다. 추가적으로, 모바일 연산 장치(152)는 예를 들어, 매체 플레이어, 개인용 디지털 보조기, 또는 모바일 텔레폰에 관한 것일 수 있다.

<48> 액세서리 인증 시스템(150)은 또한 액세서리 장치(156)를 포함한다. 액세서리 장치(156)는 커넥터(158) 및 인증 장치(160)를 포함한다. 이 실시예에서, 인증 장치(160)는 액세서리 장치(156)의 내부에 있다. 액세서리 장치(156)는 커넥터(158)를 커넥터 포트(154)에 삽입하여 모바일 연산 장치(152)로 결합될 수 있다. 이러한 접속이 이루어지면, 액세서리 장치(156)는 모바일 연산 장치(152)에 전기적으로 접속된다. 하지만, 모바일 연산 장치(152)는 자신이 액세서리 장치(156)를 인증할 수 있도록 인증 장치(160)와 상호작용할 수 있다. 인증된 경우, 액세서리 장치(156)는 모바일 연산 장치(152)와 상호작용하도록 인증된 것으로 간주된다. 일단 인증되면, 액세서리 장치(156) 및 모바일 연산 장치(152) 사이의 상호작용의 특성 및 정도가 제어될 수 있다. 결과적으로, 일단 인증되면, 모바일 연산 장치(152)는 액세서리 장치(156)를, 모바일 연산 장치(152)의 기능, 특징 또는 동작을 액세스하도록 허용되는 신뢰 파트너(또는 신뢰 파트너와 관련된 것)로 간주할 수 있다. 반면, 만약 모바일 연산 장치(152)가 액세서리 장치(156)가 신뢰 파트너(또는 신뢰 파트너와 관련된 것)가 아니라고 판단하면, 모바일 연산 장치(152)는 액세서리 장치(156)와의 상호작용을 막거나 제한할 수 있다.

<49> 도 1c는 본 발명의 또 다른 실시예에 따른 액세서리 인증 시스템(170)의 블록도이다. 액세서리 인증 시스템(170)은 커넥터 포트(174)를 가지는 모바일 연산 장치(172)를 포함한다. 모바일 연산 장치(172)는 또한 호스트 장치로 불리울 수 있다. 모바일 연산 장치(172)는 예를 들어, 매체 플레이어, 개인용 디지털 보조기, 또는 모바일 텔레폰에 관한 것일 수 있다. 액세서리 인증 시스템(170)은 또한 액세서리 장치(176)를 포함한다. 액세서리 장치(176)는 커넥터(178) 및 인증 장치(180)를 포함한다. 이 실시예에서, 인증 장치(180)는 커넥터(178)에 결합되거나 통합된다. 인증 장치는 상대적으로 작고 따라서 커넥터(178)에 결합되거나 통합된다. 인증 장치(180)를 커넥터(178)에 제공함으로써, 액세서리 장치는 인증 성능(authenticaiton capabilities)을 제공하도록 쉽게 제작될 수 있다.

<50> 액세서리 장치(176)는 커넥터(178)를 커넥터 포트(174)로 삽입하여 모바일 연산 장치(172)에 결합될 수 있다. 이러한 결합이 이루어지면, 액세서리 장치(176)는 모바일 연산 장치(172)에 전기적으로 결합된다. 하지만, 모바일 연산 장치(172)는 자신이 액세서리 장치(176)를 인증할 수 있도록 하기 위해 인증 장치(180)와 상호작용할 수 있다. 인증이 된 경우, 액세서리 장치(176)는 모바일 연산 장치(172)와 상호작용하도록 인증된 것으로 간주된다. 일단 인증되면, 액세서리 장치(176) 및 모바일 연산 장치(172) 사이의 상호작용의 특성 및 정도가 제어될 수 있다. 결과적으로, 일단 인증 되면, 모바일 연산 장치(172)는 액세서리 장치(176)를, 모바일 연산 장치(152)의 기능, 특징 또는 동작을 액세스하도록 허용되는 신뢰 파트너(또는 신뢰 파트너와 관련된 것)로 간주할 수 있다. 반면, 만약 모바일 연산 장치(172)가 액세서리 장치(176)가 신뢰 파트너(또는 신뢰 파트너와 관련된 것)가 아니라고 판단하면, 모바일 연산 장치(172)는 액세서리 장치(176)와의 상호작용을 막거나 제한할 수 있다.

<51> 추가적으로, 비록 도 1a-1c 참조 인증 장치들이 모바일 연산 장치에 대하여 액세서리 장치를 인증하도록 활용되지만, 이러한 인증 장치들은 이와 달리 액세서리 장치에 대하여 모바일 연산 장치를 인증하는데 사용될 수 있다. 어느 경우에서도, 수행되는 인증은, 이른바 암호 기술(cryptographic techniques)을 이용하여, 보안 방식으로 이루어진다. 암호 기술은 실질적으로 위조 액세서리 장치가 사용되는 것을 막을 뿐만 아니라, "스푸핑(spoofing)" 기회가 줄어들도록 한다. 일 실시예에서, 암호 기술은 공개-비밀 키 세트(public-private key set)를 이용하여 유효 디지털 서명(valid digital signature)을 형성한다.

<52> 도 2a는 본 발명의 일 실시예에 따른 인증 컨트롤러(200)의 블록도이다. 인증 컨트롤러(200)는 프로세서(202), 랜덤 액세스 메모리(RAM, 204) 및 리드-온니 메모리(ROM, 206)를 포함한다. ROM(206)은 비밀 키(208) 및 인증 알고리즘(210)을 포함한다. 인증 컨트롤러(200)는 또한 전력 라인(212) 및 통신 버스(링크)(214)를 수신한다.

예를 들어, 전력 라인(212) 및 통신 버스(214)는 이를테면 도 1a에 도시된 커넥터(108), 도 1b에 도시된 커넥터(158), 도 1c에 도시된 커넥터(178)와 같은 인증 컨트롤러(200)의 커넥터에 의해 제공될 수 있다.

<53> 프로세서(202)는 일반적으로 액세서리 장치(또는 인증 장치)를 인증하기 위해 (통신 버스(214)를 통해) 모바일 연산 장치와 상호작용한다. 인증 프로세스 동안, 프로세서(202)는 인증 컨트롤러(200) 내에 저장된 비밀 키(208) 뿐만 아니라 인증 알고리즘(210)을 이용한다. 인증 알고리즘(210)은 여러 구현에 따라 변할 수 있고, 적합한 인증 알고리즘들은 당업자에게 알려져 있다.

<54> 도 2a에 나타나 있지는 않지만, 인증 컨트롤러(200), 또는 인증 컨트롤러(200)를 포함하거나 활용하는 인증 장치 또는 액세서리 장치는 장치 식별자 및 추가적인 회로를 더 포함할 수 있다. 장치 식별자는, 예컨대, 제품 식별자(product identifier) 및/또는 제조자 식별자에 관한 것일 수 있다. 추가적인 회로는 구현에 따라 변할 수 있다. 추가적인 회로가 액세서리 장치 내에 있는 경우, 추가적인 회로는 액세서리 장치로 불리울 수 있다.

<55> 일 실시예에서, 인증 컨트롤러(200)는 단일 집적회로(즉, 단일 칩) 상에서 구현된다. 인증 컨트롤러(200)를 단일 집적회로에 제공함으로써, 비밀 키(208) 및 인증 알고리즘(210)으로의 외부 액세스가 실질적으로 차단된다. 결과적으로, 인증 프로세스는 암호로 보호될 뿐만 아니라 제한된 물리적 액세스에 의해 물리적으로도 보호된다.

<56> 도 2b는 본 발명의 일 실시예에 따른 인증 매니저(250)의 블록도이다. 인증 매니저(205)는, 예컨대, 도 1a에 도시된 모바일 연산 장치(102), 도 1b에 도시된 모바일 연산 장치(152), 또는 도 1c에 도시된 모바일 연산 장치(172)와 같은 전자 장치 내에 제공된다. 이 실시예에서, 전자 장치의 인증 매니저(250)는 액세서리 장치(또는 인증 장치)를 인증한다.

<57> 인증 매니저(250)는 인증 모듈(252), 인증 테이블(254), 및 포트 인터페이스(256)를 포함한다. 인증 모듈(252)은 포트 인터페이스(256)에 결합한 특정 액세서리 장치(또는 인증 장치)가 인증되어 전자 장치와 상호동작하도록 허용되는지 여부를 평가하도록 동작한다. 포트 인터페이스(256)는 전력 및 통신 버스(258)를 액세서리 장치(또는 인증 장치)로 제공할 수 있다. 인증 테이블(254)은 특정 액세서리 장치들(또는 인증 장치들)이 인증되었는지 여부를 평가하기 위해 인증 모듈(252)에 의해 활용되는 인증 정보를 저장한다. 상기 기재된 바와 같이, 인증 매니저(250)는 호스트 장치로 불리울 수 있는 전자 장치 내에 제공된다.

<58> 전자 장치(또는 호스트 장치)는 일반적으로 호출되거나 활용될 수 있는 다양한 동작 특징들(operating features)을 가진다. 일 실시예에서, 인증 매니저(250)에 의해 인증되는 액세서리 장치는 전자 장치(또는 호스트 장치)에서 이용할 수 있는 모든 특징들에 완전히 액세스할 수 있다. 또 다른 실시예에서, 인증 테이블(254)은 액세서리 장치가 이용할 수 있게 된 전자 장치 또는 호스트 장치의 특징들의 방식을 제어할 수 있다. 예를 들어, 만약 전자 장치(또는 호스트 장치)가 활용될 수 있는 복수의 다른 특징들을 제공하면, 인증 테이블(254)은 이러한 이용가능한 특징들 중 어느 것이 특정 액세서리 장치에 의해 활용되도록 허용되는지에 관한 표시를 포함할 수 있다. 예를 들어, 인증은 레벨 또는 클래스로 분류될 수 있는데, 이들 각각은 다른 인증들을 갖는다. 인증은 또한 사용하기 위한 여러 특징들이 인증되는 방식을 기술할 수 있다. 그러므로, 사용하기 위한 특징들은 제한된 방법으로 인증될 수 있다. 예를 들어, 사용하기 위한 특징은 전자 장치와의 빠른 통신 인터페이스(fast communication interface, FireWire® 또는 USB)를 통해서가 아니 전자 장치와의 느린 통신 인터페이스(예를 들어, 직렬)를 통해 인증될 수 있다. 즉, 이 예에서, 사용하기 위한 특징은 특정 인터페이스 메커니즘만을 통해서만 인증될 수 있다.

<59> 도 3은 본 발명의 일 실시예에 따른 인증 장치(300)의 블록도이다. 이 실시예에서, 인증 장치(300)는 자신 또는 여기에 결합된 액세서리 장치의 인증을 위한 회로를 포함할 뿐만 아니라, 인증 장치(300)에 의한 다른 기능들을 제공하기 위한 추가적인 회로를 포함한다. 특히, 인증 장치(300)는 전자 장치 뿐만 아니라 액세서리 장치에 결합되도록 설계된다. 도 3에 나타난 바와 같이, 인증 장치(300)는 메모리(304)를 포함하는 컨트롤러(302)를 포함한다. 예로서, 컨트롤러(302)는 도 2a에 도시된 인증 컨트롤러(200)와 관련될 수 있다. 컨트롤러(302)는 전자 장치로 접속할 수 있는 포트 커넥터(306)에 결합할 수 있다. 포트 커넥터(306)는 전력 라인(P_{IN})을 통해 전자 장치로부터 컨트롤러(302) 및 부스트 컨버터(boost converter, 308)로 전력을 공급할 수 있다. 추가적으로, 컨트롤러(302)는 송신 및 수신 통신 라인(TX, RX)을 거쳐 포트 커넥터(306)를 통해 전자 장치와 통신할 수 있다. 이러한 통신을 통해, 전자 장치는 인증 장치(300)가 전자 장치와 사용되도록 인증되었는지 여부를 판단할 수 있다. 만약 전자 장치가, 인증 장치(300)가 인증되었다고 판단하면, 컨트롤러(302)는 인에이블 신호(EN)를 이용하여 부스트 컨버터(308)를 인에이블할 수 있다. 일단 인에이블되면, 포트 커넥터(306)로부터 전력 라인(P_{IN})을 통해 입력 전압을 수신하는, 부스트 컨버터(308)는 USB 커넥터(310)에 전력 라인(P_{OUT})을 통해 부스

팅된 출력 전압을 출력할 수 있다. 예를 들어, 입력 전압은 3.3볼트가 될 수 있고 부스팅된 출력 전압은 5.0볼트가 될 수 있다. USB 커넥터(310)는 또한 포트 커넥터(306)로부터 한 쌍의 차동 데이터 라인(differential data lines, D+, D-)을 수신하여 USB 커넥터(310)에 결합될 수 있는 액세서리 장치와 전자 장치 사이의 데이터 전송을 가능하게 한다.

<60> 이 실시예에서, 인증 장치(300)는 전자 장치를 호스트 장치, 이를 테면 USB 호스트로 전환시키도록 동작할 수 있다. 일반적으로, 전자 장치는 USB 장치이고 호스트 장치가 아니지만, 인증 장치(300)를 전자 장치에 부착시켜서 전자 장치를 호스트 장치로 전환할 수 있다. 호스트 장치는 임의의 USB 장치가 USB 커넥터(310)로 접속될 수 있도록 USB 컴플라이언트(compliant)가 될 수 있다. 어느 경우에서도, USB 포트를 가지는 액세서리는 인증 장치(300)를 통해 전자 장치와 접속할 수 있다.

<61> 본 발명에 의해 활용되는 인증 기술들은 호스트 장치가 액세서리 장치를 인증할 수 있도록 활용될 수 있거나, 액세서리 장치가 호스트 장치를 인증하도록 할 수 있다. 호스트 장치와 액세서리 장치 사이의 인증 프로세스는 인증 장치와 호스트 장치가 결합되고 있는 동안의 임의의 시점에 개시될 수 있다. 예를 들어, 인증 프로세스는 액세서리 장치가 호스트 장치에 결합되는 때, 제한된 특징의 첫번째 사용 때, 또는 주기적으로 개시될 수 있다.

<62> 도 4a는 본 발명의 일 실시예에 따른 호스트 인증 프로세스(400)의 흐름도이다. 호스트 인증 프로세스(400)는 예컨대 호스트 장치에 의해 수행된다.

<63> 우선 호스트 인증 프로세스(400)는 인증될 액세서리 장치와 연관된 장치 식별자를 수신한다(402). 추가적으로, 인증 값은 액세서리 장치로부터 수신된다(404). 여기서, 호스트 장치는 인증 프로세스를 수행하고 있고, 따라서 액세서리 장치는 인증 값을 호스트 장치에 제공한다. 일 실시예에서, 인증 값을 결정하는 데에 있어서, 액세서리 장치는 난수(random number) 및 비밀 키를 활용한다. 난수는 호스트 장치에 의해 액세서리 장치로 제공될 수 있거나, 액세서리 장치로부터 입수가능할 수 있다.

<64> 다음으로, 호스트 인증 프로세스(400)는 인증 값 및 장치 식별자에 기초하여 액세서리 장치가 인증되었는지 여부를 판단한다(406). 그 후 블록(406)에서 이루어진 판단에 기초하여 액세서리 장치가 인증되었는지 여부를 판단(408)한다. 액세서리 장치가 인증된 것으로 결정되었다고 판단(408)하면, 호스트 장치와의 액세서리 장치의 사용(usage)이 인증된다(410). 인증되고 있는 사용(410)의 특성은 구현에 따라 변화할 수 있다. 예를 들어 인증된 사용(410)은 액세서리 장치의 완전 사용을 가능하게 하거나 액세서리 장치의 제한적 사용을 가능하게 할 수 있다.

<65> 반면, 판단(408)이 액세서리 장치가 인증되지 않았다고 판단하는 경우, 블록(410)을 우회하고 액세서리 장치는 호스트 장치와 사용되도록 인증되지 않는다. 이 경우, 액세서리 장치는 인증된 것으로 판단되지 않기 때문에, 호스트 장치와의 액세서리 장치의 사용은 실질적으로 제한되거나 금지된다. 블록(410) 다음에, 또는 이를 우회하여, 호스트 인증 프로세스(400)는 완료되고 종료된다.

<66> 도 4b는 본 발명의 일 실시예에 따른 액세서리 인증 프로세스(450)의 흐름도이다. 액세서리 인증 프로세스(450)는 예컨대, 액세서리 장치에 의해 수행된다.

<67> 액세서리 인증 프로세스(450)는 액세서리 장치와 연관된 비밀 키 식별자를 호스트 장치로 보낸다(452). 액세서리 장치로 보내지는 인증 값(authentication value)을 만드는데 있어서 호스트 장치에 의해 사용되는 적절한 비밀 키를 얻기 위해 이 비밀 키 식별자는 호스트 장치에 의해 사용된다. 액세서리 장치는 호스트 장치로부터 인증 값을 수신할 것이다(454).

<68> 다음으로, 액세서리 인증 프로세스(450)는 인증 값 및 공개 키에 기초하여 호스트 장치가 인증되었는지 여부를 판단한다(456). 일반적으로, 공개 키는 액세서리 장치 내부에 제공된다. 그 후 호스트 장치가 인증되었는지 여부를 판단하는 결정이 이루어진다(458). 호스트 장치가 인증된 것으로 간주되었다고 판단이 이루어지는 경우(458), 액세서리 장치와의 호스트 장치의 사용(usage)이 인증된다(460). 인증된 사용(460)의 특성은 구현에 따라 변화할 수 있다. 예를 들어, 인증된 사용(460)은 호스트 장치의 완전한 사용을 허용하거나 호스트 장치의 제한된 사용을 허용할 수 있다.

<69> 반면, 호스트 장치가 인증되지 않았다고 결정된 경우(458), 블록(460)은 우회되고, 액세서리 장치와 함께 호스트 장치의 사용은 실질적으로 제한되거나 금지된다. 블록(460) 후에, 또는 이를 우회한 후, 액세서리 인증 프로세스(450)는 완료되고 종결된다.

<70> 도 5a 및 5b는 본 발명의 일 실시예에 따른 호스트 장치 프로세싱(500)의 흐름도이다. 호스트 장치 프로세싱

(500)은, 예컨대, 도 1a에 도시된 연산 장치(102), 도 1b에 도시된 모바일 연산 장치(152), 또는 도 1c에 도시된 모바일 연산 장치(172)와 같은 전자 장치에 의해 수행된다.

<71> 호스트 장치 프로세싱(500)은 인증 정보가 액세서리 장치로부터 수신되었는지 여부를 판단하는 것으로 시작한다(502). 인증 정보가 수신되지 않았다고 판단되는 경우(520), 호스트 장치 프로세싱(500)은 인증 정보의 수신을 기다린다. 인증 정보가 호스트 장치에서 수신되었다고 판단하면(502), 호스트 장치 프로세싱(500)은 계속된다. 즉, 호스트 장치에서 난수가 생성된다(504). 일반적으로, 난수는 난수 발생기를 사용하는 것과 같은 랜덤 방식으로 호스트 장치에서 생성된다. 다음으로, 인증 요청(authentication request)이 액세서리 장치로 보내진다(506). 여기서, 인증 요청은 적어도 하나의 난수를 포함한다.

<72> 인증 응답이 액세서리 장치로부터 수신되었는지 여부를 판단한다(508). 인증 응답이 아직 수신되지 않았다고 판단하는 경우, 호스트 장치 프로세싱(500)은 이러한 인증 응답의 수신을 기다린다. 인증 응답이 수신되었다고 판단하면(508), 인코딩된 숫자 및 장치 식별자(device identifier)가 인증 응답으로부터 추출된다(510).

<73> 그 후, 장치 식별자를 사용하여, 공개 키가 얻어질 수 있다(512). 일 실시예에서, 호스트 장치는 다양한 여러 액세서리 장치들로 지정된 복수의 공개 키를 포함한다. 이 실시예에서, 장치 식별자는 특정 액세서리 장치를 지정하는데 활용될 수 있고, 따라서 공개 키들 중 적절한 하나의 선택을 가능하게 한다. 다음으로, 인코딩된 숫자는 디코딩된 숫자를 만들기 위해 공개 키를 이용하여 암호적으로 디코딩된다. 그 후 디코딩된 숫자는 난수와 비교된다(516). 즉, 액세서리 장치로부터 인증 응답에서 수신된 인코딩된 숫자로부터 나온 디코딩된 숫자는, 인증 요청에서 미리 액세서리 장치로 보내진 난수와 비교된다(516). 그 후 디코딩된 숫자가 난수와 매치하는지 여부를 판단한다(518). 디코딩된 숫자가 난수와 매치하지 않는다고 판단하는 경우(518), 사용자는 액세서리 장치가 인증되지 않았다고 선택에 따라(optionally) 통지받을 수 있다(520). 이러한 통지는 비주얼 수단 또는 오디오 수단에 의해 이루어질 수 있다. 예를 들어, 비주얼 통지는 호스트 장치 또는 액세서리 장치와 관련된 디스플레이 장치에 표시될 수 있다.

<74> 반면, 디코딩된 숫자가 난수와 매치한다고 판단하는 경우(518), 장치 식별자와 연관된 인증된 특징이 얻어진다(522). 그 후, 인증된 특징의 활용이 가능해진다(524). 다음으로, 액세서리 장치가 호스트 장치로부터 제거(또는 분리)되었는지 여부를 판단할 수 있다(526). 액세서리 장치가 제거되지 않았다고 판단하는 경우(526), 호스트 장치 프로세싱(500)은 인증된 특징의 활용을 계속해서 허용할 수 있다. 그러나, 액세서리 장치가 제거되었다고 판단하게 되면(526), 호스트 장치의 모든 특징의 활용은 디스에이블될 수 있다(528). 즉, 예로서, 인증된 특징들은 세션(session) 동안 활용가능한 것으로 간주될 수 있다. 이 세션은 액세서리 장치가 호스트 장치에 부착되어 있는 한 유효하게 남아 있을 수 있다. 일단 분리되면, 세션은 종료되고 추후의 재부착(re-attachment)은 재인증을 필요로 한다. 동작(528) 및 동작(520) 다음으로 호스트 장치 프로세싱(500)은 완결되고 종료된다.

<75> 도 6a 및 6b는 본 발명의 일 실시예에 따른 액세서리 장치 프로세싱(600)의 흐름도이다. 액세서리 장치 프로세싱(600)은 예컨대, 도 1a에 도시된 액세서리 장치(112), 도 1b에 도시된 액세서리 장치(156), 또는 도 1c에 도시된 액세서리 장치(176)와 같은 액세서리 장치에 의해 수행된다. 액세서리 장치 프로세싱(600)은 도 5a 및 5b에 도시된 호스트 장치 프로세싱(500)의 대응 프로세싱을 나타낸다.

<76> 액세서리 장치 프로세싱(600)은 전력이 액세서리 장치에 공급되었는지 여부를 판단하는 것(602)으로 시작된다. 전력이 액세서리 장치에 공급되지 않았다고 판단하는 경우, 액세서리 장치 프로세싱(600)은 이용가능한 전력을 기다린다. 일반적으로, 액세서리 장치가 호스트 장치에 접속되면 전력이 액세서리 장치로 공급된다. 따라서, 판단(602)은 다른 방법으로 액세서리 장치가 호스트 장치로 접속하였는지를 판단할 수 있다.

<77> 일단 전력이 액세서리 장치로 공급되었다고 판단하면(602), 인증 정보가 호스트 장치로 보내질 수 있다(604). 일 실시예에서, 인증 정보는 지원되는 하나 이상의 인증 버전을 표시하는 정보를 포함할 수 있다. 그 후 인증 요청이 수신되었는지 여부를 판단한다(606). 인증 요청이 수신되지 않았다고 판단(606)하는 경우, 액세서리 장치 프로세싱(600)은 이러한 요청을 기다린다. 일단 인증 요청이 수신되었다고 판단하면(606), 인증 요청에 제공된 난수가 추출된다(608). 비밀 키가 인증 장치로부터 얻어진다(610). 보안상의 이유로, 비밀 키는 인증 장치 내부에 저장될 수 있고 인증 장치 밖에서는 쉽게 접근할 수 없게 된다. 다음으로, 난수는 인코딩된 숫자를 만들기 위해 비밀 키를 이용하여 암호적으로 인코딩된다(612).

<78> 그 후, 인증 응답은 호스트 장치로 보내진다(614). 여기서, 인증 응답은 적어도 인코딩된 숫자 및 장치 식별자를 포함한다. 인증 응답이 보내진 후에(614), 호스트 장치의 특징으로의 액세스가 인증되었는지 여부를 판단한

다(616). 판단(616)은 능동적으로 또는 수동적으로 이루어질 수 있다. 예를 들어, 호스트 장치는 호스트 장치의 하나 이상의 특징들로의 액세스에 대하여 인증되었다고 액세서리 장치에 통지할 수 있다. 또 다른 예로, 호스트 장치는 액세서리 장치에 통지하지 않고 대신 액세서리 장치로 하여금 인증된 호스트 장치의 하나 이상의 특징들을 액세스하도록 할 수 있다. 어느 경우에서도, 호스트 장치의 특정 특징으로의 액세스가 인증되지 않았다고 판단하는 경우(616), 액세서리 장치의 동작(620)은 호스트 장치의 특정 특징을 사용하는 것이 금지된다. 확실히, 일 실시예에서, 호스트 장치는 액세서리 장치의 임의의 동작을 막을 수 있다. 예로서, 호스트 장치는 액세서리 장치와의 통신 금지하고/하거나 액세서리 장치로의 전력 공급을 중단할 수 있다.

<79> 반면, 호스트 장치의 특정 특징으로의 액세스가 인증되었다고 판단하는 경우(616), 액세서리 장치는 인증된 특징과 함께 동작될 수 있다(618). 즉, 인증되었다면, 액세서리 장치는 호스트 장치와 상호작용하여 호스트 장치에 의해 지원된 특정 특징을 활용할 수 있다.

<80> 동작(618 및 620) 후에, 액세서리 장치가 제거되었는지, 즉 액세서리 장치가 호스트 장치로부터 분리되었는지 여부를 판단한다(622). 액세서리 장치가 호스트 장치에 접속되거나 부착된 상태로 남아있다고 판단하면(622), 적절한 동작(618 또는 620)이 계속할 수 있다. 이와 달리 액세서리 장치가 제거되었다고 판단하면(622), 액세서리 장치는 더 이상 호스트 장치와 상호작용하도록 인증되지 않고 따라서 호스트 장치에 의해 지원된 사전에 인증된 특징을 더 이상 활용할 수 없다. 이 경우에, 액세서리 장치 프로세싱(600)은 종료된다. 그러나, 액세서리 장치는 다시 액세서리 장치 프로세싱(600)을 수행함으로써 추후에 재인증될 수 있다.

<81> 액세서리 장치 프로세싱(600)에서, 장치 식별자는 인증 응답을 제공받는다. 또 다른 실시예에서, 장치 식별자는 다르게 호스트 장치로 제공될 수 있는데, 이를테면 인증 정보와 함께 제공될 수 있다. 장치 식별자는 또한 별개로 호스트 장치로 제공될 수 있다.

<82> 도 6c는 본 발명의 일 실시에에 따른 인증 테이블(650)의 다이어그램이다. 인증 테이블은 예컨대, 도 2b에 나타나 인증 테이블(254)과 같이 사용하기에 적합하다. 일반적으로, 인증 테이블(650)은 해당 액세서리 장치의 인증 특징을 판단하는데 사용될 수 있다. 인증 테이블(650)은 장치 식별자 열(652), 공개 키 열(654), 및 인증된 특징 열(656)을 포함한다. 인증 테이블(650)은 장치 식별자, 공개 키 및 인증된 특징을 연관시킨다. 장치 식별자를 이용하여, 호스트 장치는 특정 장치 식별자를 이용하여 식별된 액세서리 장치가 인증될 수 있는지 여부를 판단하는 경우 사용되는 적절한 공개 키를 결정할 수 있다. 액세서리 장치의 인증이 성공적인 경우, 장치 식별자와 관련된 인증된 특징은 인증된 특징 열(656)에서 식별될 수 있다.

<83> 본 발명의 일 특징에 따르면, 호스트 장치는 호스트 장치에 결합되고 있는 액세서리 장치를 인증하도록 동작할 수 있다. 인증될 수 있는 액세서리 장치들은 좀 더 많이 호스트 장치와 상호 동작하도록 허용될 수 있다. 호스트 장치는 따라서 액세서리 장치들이 호스트 장치와 상호동작할 수 있는 특성 및 정도를 제어할 수 있다. 예를 들어, 호스트 장치는 액세서리 장치가 인증될 수 없는 경우 액세서리 장치가 호스트 장치와 상호동작하는 것을 제한하거나, 제지하거나, 금지시킬 수 있다. 이와 달리, 호스트 장치는 액세서리 장치가 인증된 경우 호스트 장치와의 보다 많은 상호작용을 가능하게 할 수 있다.

<84> 도 7a 및 7b는 본 발명의 일 실시예에 따른 액세서리 장치 프로세싱(700)의 흐름도이다. 도 8a-8c는 본 발명의 일 실시예에 따른 호스트 장치 프로세스(800)의 흐름도이다. 액세서리 장치 프로세스(700)는 호스트 장치와의 인증 프로세스 동안 액세서리 장치에 의해 수행된다. 호스트 장치 프로세스(800)는 액세서리 장치와의 인증 프로세스 동안 호스트 장치에 의해 수행된다. 호스트 장치 프로세스(800)는 액세서리 장치 프로세스(700)에 대응하는 프로세스이다. 즉, 인증 프로세스 동안, 호스트 장치와 액세서리 장치 사이에 정보 교환이 있다. 따라서, 인증 프로세스의 일 실시예 동안, 도 7a 및 7b는 액세서리 장치에 의해 수행되는 프로세싱을 나타내고, 도 8a-8c는 호스트 장치에 의해 수행되는 프로세싱을 나타낸다. 상기 도면들에서 묘사된 인증 프로세스가 실질적으로 순차적인 것으로 도시되어 있지만, 인증 프로세스는 일반적으로 인증 뿐만 아니라 추후의 동작에 대한 정보를 교환하기 위한 액세서리 장치 및 호스트 장치에 의해 활용되는 프로토콜로 간주될 수 있다. 일 실시예에서, 이러한 프로토콜은, 클라이언트-서버(client-server) 또는 마스터-슬레이브(master-slave) 구현에서와 같이, 실질적으로 병렬(parallel)로 고려될 수 있다.

<85> 도 7a 및 7b는 본 발명의 일 실시예에 따른 액세서리 장치 프로세스(700)의 흐름도이다. 액세서리 장치 프로세스(700)는 판단(702)으로 시작한다. 판단(702)은 액세서리 장치가 호스트 장치에 접속하는지 여부를 판단한다. 일반적으로, 판단(702)은 액세서리 장치의 커넥터를 통한 호스트 장치로의 최근 접속을 감지한다. 어느 경우에서도, 액세서리 장치가 호스트 장치에 접속되지 않았다고 판단하는 경우(702), 액세서리 장치 프로세싱(700)은 유효하게 이러한 접속을 기다릴 수 있다. 즉, 액세서리 장치 프로세스(700)는 액세서리 장치가 호스트 장치로

접속한 경우 호출되는 것으로 생각될 수 있다.

<86> 일단 액세서리 장치가 호스트 장치로 접속되었다고 판단하는 경우(702), 액세서리 장치 프로세스(700)는 계속된다. 액세서리 장치 프로세스(700)가 계속되는 경우, 인증 제어 정보가 액세서리 장치로부터 호스트 장치로 보내진다(704). 예로서, 인증 제어 정보는 액세서리 장치의 유형, 인증이 지원되는지 여부, 언제 인증되는지, 및/또는 액세서리 장치의 요구 전력을 기재할 수 있다. 액세서리 장치 유형의 특정 예들로 마이크로폰, 단순 원격(simple remote), 디스플레이 원격, 원격 사용자 인터페이스, RF 송신기, 및 USB 제어 호스트가 있다. 액세서리 장치의 인증 상태는 자발적으로 또는 호스트 장치로부터의 명령 또는 확인에 응답하여 지워진다(706). 여기서, 액세서리 장치가 접속될 때마다 인증 상태를 지움으로써(706), 액세서리 장치는 자신이 호스트 장치와 인증되어야 한다는 것을 알 수 있다.

<87> 다음으로, 장치 인증 정보 요청이 수신되었는지 여부를 판단한다(710). 여기서, 장치 인증 정보 요청은 호스트 장치에 의해 액세서리 장치로 보내진다. 장치 인증 정보 요청은 인증 프로세스 동안 호스트 장치에 의해 활용되게 되는 특정 정보를 액세서리 장치로부터 요청하는 일을 한다. 장치 인증 정보 요청이 아직 수신되지 않았다고 판단(710)하는 경우, 액세서리 장치 프로세스(700)는 이러한 요청을 기다린다. 일단 장치 인증 정보 요청이 수신되었다고 판단(710)하면, 장치 인증 정보가 액세서리 장치로부터 얻어진다(712). 예로서, 장치 인증 정보는 장치 식별자 및 버전 표시자(version indicator)를 포함할 수 있다. 장치 식별자는 벤더 식별자(vendor identifier), 제품 식별자, 또는 이 둘 모두에 관한 것일 수 있다. 버전 표시자는 지원되는 프로토콜 버전에 관한 것일 수 있다. 그 후 장치 인증 정보는 호스트 장치로 보내진다(714).

<88> 그 후 인증 요청이 호스트 장치로부터 수신되었는지 여부를 판단한다(716). 여기서, 인증 요청은 액세서리 장치를 인증하는데 활용되는 디지털 서명을 포함하는 인증 응답을 제공하기 위한 호스트 장치로부터의 요청이다. 인증 요청이 수신되지 않았다고 판단(716)하는 경우, 액세서리 장치 프로세서(700)는 이러한 요청을 기다린다. 일단 인증 요청이 수신되었다고 판단하면(716), 호스트 난수(host random number)가 인증 요청으로부터 추출된다(718). 인증 요청은 인증 프로세스에서 사용되게 될 호스트 난수를 적어도 포함한다.

<89> 그 후 액세서리 장치 내부의 비밀 키가 얻어진다(720). 그 후 적어도 호스트 난수, 비밀 키 및 장치 난수를 이용하여 장치 디지털 서명이 계산될 수 있다(722). 장치 난수는 액세서리 장치 내에서 생성되거나 얻어질 수 있다. 장치 디지털 서명은 액세서리 장치를 인증하기 위해 호스트 장치에 의해 사용되게 될 암호화된 값이다. 그 후 인증 응답이 호스트 장치로 보내진다(724). 인증 응답은 그 자체가 적어도 장치 디지털 서명을 포함하는 식으로 이루어진다.

<90> 그 후 장치 인증 상태(device authentication status)가 호스트 장치로부터 수신되었는지 여부를 판단한다(726). 장치 인증 상태가 수신되지 않았다고 판단(726)하는 경우, 액세서리 장치 프로세스(700)는 이러한 정보를 기다린다. 일단 장치 인증 상태가 수신되었다고 판단하면(726), 장치 인증 상태는 액세서리 장치에 저장될 수 있다(728). 블록(728) 다음에, 액세서리 장치 프로세스(700)는 종료된다.

<91> 도 8a-8c는 본 발명의 일 실시예에 따른 호스트 장치 프로세스(800)의 흐름도이다. 호스트 장치 프로세스(800)는 인증 제어 정보가 액세서리 장치로부터 수신되었는지 여부를 판단(802)하는 것으로 시작한다. 인증 제어 정보가 수신되지 않은 것으로 판단(802)하는 경우, 호스트 장치 프로세스(800)는 이러한 정보를 기다린다. 일단 인증 제어 정보가 수신된 것으로 판단하면(802), 호스트 장치 프로세스(800)는 계속된다. 즉, 호스트 장치 프로세싱(800)은 인증 제어 정보가 수신되면 유효하게 호출된다.

<92> 호스트 장치 프로세스(800)가 계속되는 경우, 장치 인증 상태가 리셋(즉, 지워짐)될 수 있다(804). 따라서, 액세서리 장치는 인증 프로세스가 액세서리 장치를 인증할 수 있을 때까지 인증되지 않은 것으로 간주된다. 이러한 동작은 이를테면, 액세서리 장치가 호스트 장치로부터 분리된 경우, 호스트 장치에서 자동으로 미리 발생될 수 있다.

<93> 그 후 액세서리 장치가 인증 제어 정보에 기초하여 인증을 지원하는지 여부를 판단한다(806). 인증이 액세서리 장치에 의해 지원되지 않는다고 판단(806)하는 경우, 호스트 장치 프로세싱(800)은 액세서리 장치를 인증하지 않고 종료된다. 이 경우, 액세서리 장치는 호스트 장치와 상호작용하는 것이 제한되거나 심지어 금지될 수 있다.

<94> 반면, 인증이 액세서리 장치에 의해 지원된다고 판단(806)하는 경우, 호스트 장치 프로세스(800)는 계속된다. 이 경우, 장치 인증 정보 요청이 액세서리 장치로 보내진다(808). 그 후, 장치 인증 정보가 수신되었는지 여부를 판단한다(810). 장치 인증 정보가 수신되지 않았다고 판단(810)하는 경우, 호스트 장치 프로세스(800)는 이

러한 정보가 수신되기를 기다린다. 장치 인증 정보가 수신되었다고 판단하면(810), 이 시점에서 인증이 수행되어야 하는지 여부를 판단한다(812). 여기서, 호스트 장치 프로세스(800)는 액세서리 장치가 호스트 장치로 접속되는 때 바로 다음에 인증을 수행할 수 있거나, 인증은 추후의 시점, 이를테면 액세서리 장치가 인증된 장치만이 사용할 수 있는 호스트 장치의 확장된 특징을 사용하기를 희망하는(예컨대, 제1 희망(first deseires)) 때까지 정기적으로 연기될 수 있다. 그러므로, 인증을 즉시 필요로 하지 않는다고 판단(812)하는 경우, 호스트 장치 프로세스(800)는 적절한 시간을 기다려 인증 프로세스를 수행할 수 있다. 일단 수행되어야 한다고 판단하면(812), 호스트 난수가 생성된다(814). 다음으로, 인증 요청이 액세서리 장치로 보내진다(816). 인증 요청은 생성된(814) 호스트 난수를 적어도 포함한다.

<95> 인증 응답이 액세서리 장치로부터 수신되었는지 여부를 판단한다(818). 인증 응답이 수신되었다고 판단(818)하는 경우, 장치 디지털 서명이 인증 응답으로부터 추출된다(820). 액세서리 장치와 함께 사용하기 위한 공개 키도 또한 얻어진다(822). 일 실시예에서, 호스트 장치는 여러 장치 식별자들과 연관된 복수의 공개 키들을 포함한다. 따라서, 액세서리 장치로부터의 장치 인증 정보는 액세서리 장치에 대한 장치 식별자를 포함할 수 있다. 장치 식별자는 액세서리 장치와 함께 사용하기 위한 공개키를 얻는데(822) 활용될 수 있다. 예로서, 도 6c에 나타난 인증 테이블(650)과 같은 인증 테이블이 공개 키를 얻는데 사용될 수 있다.

<96> 다음으로, 장치 디지털 서명이 공개 키를 이용하여 유효하게 된다(824). 일 실시예에서, 장치 디지털 서명의 유효화(824)는 또한 호스트 난수를 이용한다. 그 후 장치 디지털 서명이 유효화되었는지 여부를 판단한다(826). 장치 디지털 서명이 유효화되었다고 판단(826)하는 경우, 액세서리 장치는 인증된 것으로 간주된다(828). 그 후 액세서리 장치와 연관된 명령 액세스 허가(command access permissions)는, 액세서리 장치가 인증 장치들에 의해 허용된 상기 명령들을 이용하는 것을 호스트 장치가 허가하도록 업데이트 될 수 있다(830). 반면, 디지털 장치 서명이 유효화되지 않았다고 판단(826)하는 경우, 액세서리 장치는 인증되지 않는 것으로 간주된다(832). 블록(830 및 832) 다음에, 장치 인증 상태가 액세서리 장치로 보내진다(834). 장치 인증 상태는 액세서리 장치에게 호스트 장치가 액세서리 장치를 인증했는지 여부에 대하여 알려주는 일을 한다.

<97> 장치 인증 상태가 액세서리 장치가 인증된 것으로 간주된다고 나타낸다면, 액세서리 장치는 인증된 사용 정도에 따라 호스트 장치와 계속해서 상호작용할 수 있다. 또 다른 예로서, 장치 인증 상태가 액세서리 장치가 인증되지 않은 것으로 간주된다고 나타내는 경우, 액세서리 장치는 호스트 장치와의 상호작용이 제한되거나, 심지어 금지될 수 있다. 어느 경우에서도, 호스트 장치와 액세서리 장치와의 사용의 인증된 정도는 액세서리 장치가 인증되는 때에 더 커진다.

<98> 도 9a-9c는 본 발명의 일 실시예에 따른 액세서리 장치 프로세스(900)의 흐름도이다. 도 10a 및 10b는 본 발명의 일 실시예에 따른 호스트 장치 프로세스(1000)의 흐름도이다. 액세서리 장치 프로세스(900)는 호스트 장치를 인증하려고 하는 인증 프로세스 동안 액세서리 장치에 의해 수행된다. 호스트 장치 프로세스(1000)는 액세서리 프로세스와 함께 인증 프로세스 동안 호스트 장치에 의해 수행된다. 호스트 장치 프로세스(1000)는 액세서리 장치 프로세스(900)에 대응하는 프로세스이다. 즉, 인증 프로세스 동안, 호스트 장치와 액세서리 장치 간에 정보 교환이 있게 된다. 따라서, 인증 프로세스의 일 실시예 동안, 도 9a-9c는 액세서리 장치에 의해 수행되는 프로세싱을 나타내고 도 10a 및 10b는 호스트 장치에 의해 수행되는 프로세싱을 나타낸다. 상기 도면들에서 묘사된 인증 프로세스가 실질적으로 순차적인 것으로 도시되어 있지만, 인증 프로세스는 일반적으로 인증 뿐만 아니라 추후의 동작에 대한 정보를 교환하기 위한 액세서리 장치 및 호스트 장치에 의해 활용되는 프로토콜로 간주될 수 있다. 일 실시예에서, 이러한 프로토콜은, 클라이언트-서버(client-server) 또는 마스터-슬레이브(master-slave) 구현에서와 같이, 실질적으로 병렬(parallel)로 고려될 수 있다.

<99> 도 9a-9c는 본 발명의 일 실시예에 따른 액세서리 장치 프로세스(900)의 흐름도이다. 액세서리 장치 프로세스(900)는 액세서리 장치와 접속된 호스트 장치를 인증하려고 하는 때에 액세서리 장치에 의해 수행된다.

<100> 액세서리 장치 프로세스(900)는 액세서리 장치가 호스트 장치에 접속하는지 여부를 판단(902)하는 것을 시작한다. 액세서리 장치가 호스트 장치에 접속되지 않았다고 판단하는 경우(902), 액세서리 장치 프로세스(900)는 이러한 접속을 기다릴 수 있다. 즉, 액세서리 장치 프로세스(900)는 액세서리 장치가 호스트 장치로 접속되는 경우 유효하게 호출되는 것으로 생각될 수 있다. 일 실시예에서, 액세서리 장치가 최근에 막 호스트 장치로 접속되었다고 판단되면 액세서리 장치 프로세스(900)가 호출된다. 그러나, 다른 실시예에서, 인증 프로세스는 추후에 수행될 수 있다(예컨대, 연기).

<101> 일단 액세서리 장치가 호스트 장치로 접속되었다고 판단하면(902), 인증 제어 정보가 호스트 장치로 보내진다(904). 그 후 인증 제어 정보가 인정(acknowledge)되었는지 여부를 판단한다(906). 인증 제어 정보가 인정되

었다고 판단(906)하는 경우, 액세서리 장치의 인증 상태는 지워질 수 있다(908). 여기서, 인증 상태를 지움으로써(908), 호스트 장치가 접속될 때마다 액세서리 장치에 의해 인증된다.

<102> 다음으로, 호스트 인증 정보 요청이 호스트 장치로 보내진다(910). 그 후 호스트 인증 정보가 호스트 장치로부터 수신되었는지 판단한다(912). 호스트 인증 정보가 호스트 장치로부터 수신되지 않았다고 판단하면(912), 액세서리 장치 프로세스(900)는 이러한 정보를 기다린다.

<103> 호스트 인증 정보가 수신되었다고 판단(912)하면, 이 시점에서 인증이 수행되어야 하는지 여부를 판단한다(914). 여기서, 인증 프로세스는 이를테면 접속이 감지된 후 즉각적으로 수행되거나, 추후의 시점, 이를테면 호스트 장치의 명령 또는 확장된 기능성이 요구되는 때까지 연기될 수 있다. 어느 경우에서도, 이 시점에서 인증이 수행될 필요가 없다고 판단하는 경우, 액세서리 장치 프로세스(900)는 인증을 수행할 적절한 시기를 기다릴 수 있다.

<104> 인증이 수행되어야 한다고 판단(914)하면, 장치 난수가 생성된다(916). 그 후, 인증 요청이 호스트 장치(918)로 보내진다. 인증 요청은 일반적으로 적어도 장치 난수 및 비밀 키 숫자를 포함한다. 비밀 키 숫자는 호스트 장치에서 비밀 키를 선택하는데 사용된다.

<105> 다음으로, 인증 응답이 호스트 장치로부터 수신되었는지를 판단한다(920). 인증 응답이 수신되지 않았다고 판단(920)하는 경우, 액세서리 장치 프로세스(900)는 이러한 응답을 기다린다. 일단 인증 응답이 수신되었다고 판단(920)하면, 호스트 디지털 서명이 인증 응답으로부터 추출된다(922). 또한, 공개 키가 공개 키 인덱스(public key index)에 기초하여 얻어진다(924). 일 실시예에서, 공개 키 인덱스는 호스트 인증 정보와 함께 액세서리 장치로 제공된다. 일 실시예에서, 공개 키는 공개 키 인덱스를 이용하여 액세서리 장치에서 결정된다. 예를 들어, 액세서리 장치는 복수의 다른 공개 키들을 포함할 수 있고, 활용될 공개 키들 중 적절한 하나가 공개 키 인덱스에 의해 식별될 수 있다.

<106> 그 후 호스트 디지털 서명이 공개 키를 이용하여 유효화된다(926). 유효화(926)는 또한 장치 난수를 이용할 수 있다. 그 후, 호스트 디지털 서명이 유효화되었는지 여부를 판단한다(928). 호스트 디지털 서명이 유효화되었다고 판단(928)하는 경우, 호스트 장치는 인증된 것으로 간주된다(930). 결과적으로, 호스트 장치에 의해 사용되는 명령 액세스 허가(command access permissions)가 업데이트된다(932). 예를 들어, 호스트 장치가 유효화되었기 때문에, 적어도 명령 액세스 허가의 정도에 있어서 호스트 장치와 액세서리 장치 사이의 상호작용은 인증된 것으로 간주된다. 이와 달리, 호스트 장치가 유효화되지 않았다고 판단(928)하는 경우, 호스트 장치는 인증되지 않은 것으로 간주된다(934). 블록(932 및 934) 다음에, 호스트 인증 상태가 호스트 장치로 보내질 수 있다(936). 여기서, 호스트 인증 상태는 호스트 장치에게 인증 프로세스의 결과를 알린다. 블록(936) 다음에, 액세서리 장치 프로세스(900)는 완료되고 종료된다.

<107> 도 10a 및 10b는 본 발명의 일 실시예에 따른 호스트 장치 프로세싱(1000)의 흐름도이다. 호스트 장치 프로세싱(1000)은 액세서리 장치와 상호작용하는 동안 호스트 장치에서 수행된다. 호스트 장치 프로세싱(1000)은 인증 프로세스 동안 액세서리 장치 프로세스(900)에 대응하는 프로세싱을 나타낸다.

<108> 호스트 장치 프로세싱(1000)은 액세서리 장치로부터 인증 제어 정보가 수신되었는지 여부를 판단(1002)하는 것으로 시작한다. 인증 제어 정보가 수신되지 않았다고 판단(1002)하는 경우, 호스트 장치 프로세싱(1000)은 이러한 정보를 기다린다. 일단 인증 제어 정보가 수신되었다고 판단(1002)하면, 호스트 장치 프로세싱(1000)은 계속된다. 즉, 호스트 장치 프로세싱(1000)은 인증 제어 정보가 액세서리 장치로부터 수신되면 효과적으로 호출된다.

<109> 호스트 장치 프로세싱(1000)이 계속되는 경우, 호스트 인증 상태가 리셋되고(1004), 이에 따라 이전에 가졌던 임의의 이전 인증 상태를 지운다. 그 후, 호스트 인증 정보 요청이 수신되는지 여부를 판단한다(1006). 호스트 인증 정보 요청이 수신되지 않았다고 판단(1006)하는 경우, 호스트 장치 프로세싱(1000)은 이러한 요청을 기다린다. 호스트 인증 정보 요청이 수신되었다고 판단(1006)하면, 호스트 인증 정보가 호스트 장치에서 얻어진다(1008). 그 후 호스트 인증 정보는 액세서리 장치로 보내진다(1010). 일 실시예에서, 호스트 인증 정보는 적어도 버전 정보 및 공개 키 인덱스를 포함한다.

<110> 다음으로, 인증 요청이 수신되었는지 여부를 판단한다(1012). 인증 요청이 수신되지 않았다고 판단(1012)하는 경우, 호스트 장치 프로세싱(1000)은 이러한 요청을 기다린다. 인증 요청이 수신되었다고 판단(1012)하면, 장치 난수 및 비밀 키 숫자가 인증 요청으로부터 추출된다(1014). 이 실시예에서, 액세서리 장치로부터 수신되는 인증 요청은 호스트 장치에 의해 활용될 수 있는 장치 난수 및 비밀 키 숫자를 적어도 포함한다. 그 후, 비밀

키는 비밀 키 숫자에 기초하여 얻어진다(1016). 여기서, 얻어지는 비밀 키(1016)는 호스트 장치 내부에 있고 비밀 키 숫자의 사용을 통해 식별된다.

<111> 그 후 호스트 디지털 서명은 장치 난수, 비밀 키 및 호스트 난수를 이용하여 계산된다(1018). 호스트 난수는 호스트 장치에서 생성되거나 입수가능할 수 있다. 그 후 호스트 장치 프로세스(1000)는 액세서리 장치에 인증 응답을 보낸다(1020). 인증 응답은 적어도 호스트 디지털 서명을 포함한다.

<112> 그 후, 호스트 인증 상태가 수신되었는지 여부를 판단한다(1022). 호스트 인증 상태가 수신되지 않았다고 판단(1022)하는 경우, 호스트 장치 프로세싱(1000)은 이러한 정보를 기다린다. 호스트 인증 상태가 수신되었다고 판단(1022)하면, 인증 상태는 호스트 장치에 저장된다(1024). 여기서, 호스트 장치는 자신이 액세서리 장치와 함께 있다는 인증 상태를 알고 이에 따라 동작할 수 있다. 블록(1024) 다음에, 호스트 장치 프로세싱(1000)은 완료되고 종료된다.

<113> 본 발명의 또 다른 특징에 따르면, 전자 장치 또는 호스트 장치는 퍼스널 컴퓨터와 같은 호스트 컴퓨터로 또한 접속할 수 있다. 퍼스널 컴퓨터는 매체 아이템을 저장하고 활용하며 관리할 수 있다. 매체 아이템의 관리는 호스트 컴퓨터 뿐만 아니라 전자 장치를 위한 것일 수 있다.

<114> 도 11은 본 발명의 일 실시예에 따른 매체 관리 시스템(1100)의 블록도이다. 매체 관리 시스템(1100)은 호스트 컴퓨터(1102) 및 매체 플레이어(1104)를 포함한다. 호스트 컴퓨터(1102)는 일반적으로 퍼스널 컴퓨터이다. 다른 종래의 구성요소들 가운데, 호스트 컴퓨터는 소프트웨어 모듈인 관리 모듈(1106)을 포함한다. 관리 모듈(1106)은 호스트 컴퓨터(1102) 뿐만 아니라 매체 플레이어(1104) 상에서 매체 아이템(및/또는 플레이리스트(playlists))의 중앙 관리(centralized management)를 제공한다. 특히, 관리 모듈(1106)은 호스트 컴퓨터(1102)와 연관된 매체 저장소(1108)에 저장된 매체 아이템을 관리한다. 관리 모듈(1106)은 매체 저장소(1108)에 저장된 매체 아이템과 연관된 매체 정보를 저장하기 위해 매체 데이터베이스(1110)와 상호작용한다.

<115> 매체 정보는 매체 아이템의 특성 또는 속성과 관계가 있다. 예를 들어, 오디오 또는 오디오비주얼(audiovisual) 매체의 경우, 매체 정보는 하나 이상의: 제목, 앨범, 트랙, 아티스트, 작곡가 및 장르를 포함할 수 있다. 이러한 유형의 매체 정보는 특정 매체 아이템에 특유하다. 또한, 매체 정보는 매체 아이템의 품질 특성과 관계가 있을 수 있다. 매체 아이템의 품질 특성의 예는 비트 전송율(bit rate), 샘플링 비율(sample rate), 이퀄라이저 세팅, 볼륨 조절, 시작/멈춤 및 전체 시간 중 하나 이상을 포함할 수 있다.

<116> 또한, 호스트 컴퓨터(1102)는 플레이 모듈(1112)을 포함한다. 플레이 모듈(1112)은 매체 저장소(1108)에 저장된 특정 매체 아이템을 플레이하는데 활용될 수 있는 소프트웨어 모듈이다. 플레이 모듈(1112)은 또한 매체 데이터베이스(1110)로부터의 매체 정보를 (디스플레이 스크린 상에) 디스플레이하거나 활용할 수도 있다. 일반적으로, 관심있는 매체 정보는 플레이 모듈(1112)에 의해 플레이되는 매체 아이템에 해당한다.

<117> 호스트 컴퓨터(1102)는 또한 매체 플레이어(1104) 내의 대응 통신 모듈(1106)에 결합하는 통신 모듈(1114)을 포함한다. 제거될 수 있는 접속부 또는 링크(1118)는 통신 모듈(1114 및 1116)을 결합한다. 일 실시예에서, 접속부 또는 링크(1118)는 해당 기술 분야에 잘 알려진 FIREWIRE™ 버스 또는 USB 버스와 같은 데이터 버스를 제공하는 케이블이다. 또 다른 실시예에서, 접속부 또는 링크(1118)는 무선 네트워크를 통한 무선 채널 또는 접속부이다. 따라서, 구현에 따라, 통신 모듈(1114 및 1116)은 유선 또는 무선 방식으로 통신할 수 있다.

<118> 매체 플레이어(1104)는 또한 매체 플레이어(1104) 내에 매체 아이템을 저장하는 매체 저장소(1120)를 포함한다. 선택에 따라, 매체 저장소(1120)는 데이터를 저장할 수도 있는데, 즉 비매체 아이템 저장소(non-media item storage)가 된다. 매체 저장소(1120)에 저장되고 있는 매체 아이템은 일반적으로 호스트 컴퓨터(1102)로부터 접속부 또는 링크(1118)를 통해 수신된다. 특히, 관리 모듈(1106)은 매체 저장소(1108)에 있는 매체 아이템의 전부 또는 일부를 접속부 또는 링크(1118)를 통해 매체 플레이어(1104) 내의 매체 저장소(1120)로 보낸다. 추가적으로, 호스트 컴퓨터(1102)로부터 매체 플레이어(1104)로 역시 전달되는 매체 아이템에 대한 대응 매체 정보는 매체 데이터베이스(1122)에 저장될 수 있다. 이 점에서, 호스트 컴퓨터(1102) 내 매체 데이터베이스(1110)로부터의 특정 매체 정보는 접속부 또는 링크(1118)를 통해 매체 플레이어(1104) 내의 매체 데이터베이스(1122)로 보내질 수 있다. 더욱이, 특정 매체 아이템을 식별하는 플레이리스트는 관리 모듈(1106)에 의해 접속부 또는 링크(1118)를 통하여 매체 플레이어(1104) 내의 매체 저장소(1120) 또는 매체 데이터베이스(1122)로 보내질 수 있다.

<119> 또한, 매체 플레이어(1104)는 매체 저장소(1120) 및 매체 데이터베이스(1122)에 결합된 플레이 모듈(1124)을 포함한다. 플레이 모듈(1124)은 매체 저장소(1120)에 저장된 특정 매체 아이템을 플레이하는데 활용될 수 있는

소프트웨어 모듈이다. 플레이 모듈(1124)은 또한 매체 데이터베이스(1122)로부터의 매체 정보를 (디스플레이 스크린 상에) 디스플레이하거나 활용할 수 있다. 일반적으로, 관심있는 매체 정보는 플레이 모듈(1124)에 의해 플레이되는 매체 아이템에 해당한다.

<120> 일 실시예에 따르면, 매체 플레이어(1104) 상에서 인증 프로세스를 지원하기 위해 매체 플레이어(1104)는 인증 모듈(1126) 및 인증 테이블(1128)을 더 포함할 수 있다. 한가지 구현에서, 인증 모듈(1126) 및 인증 테이블(1128)은 각각 도 2b에 관하여 상기 설명된 인증 모듈(252) 및 인증 테이블(254)에 해당할 수 있다.

<121> 상기 기재된 바와 같이, 액세서리 장치는 매체 플레이어에 결합할 수 있다. 따라서, 도 11은 또한 매체 플레이어(1104)에 결합할 수 있는 액세서리 장치(1130)를 도시한다. 일 실시예에 따르면, 액세서리 장치(1130)는 인증 장치(1132)를 더 포함할 수 있다. 인증 장치(1132)는 일 실시예에 따라 매체 플레이어(1104) 상에서 인증 프로세스를 지원하도록 동작한다. 한가지 구현에서, 인증 장치(1132)는 도 2a에 관하여 상기 설명된 인증 컨트롤러(200)에 해당할 수 있다.

<122> 일 실시예에서, 매체 플레이어(1104)는 매체 플레이어(1104) 상의 매체 아이템을 관리할 능력이 없거나 제한된다. 그러나, 호스트 컴퓨터(1102) 내의 관리 모듈(1106)은 매체 플레이어(1104)에 있는 매체 아이템을 간접적으로 관리할 수 있다. 예를 들어, 매체 플레이어(1104)에 매체 아이템을 "추가하기" 위해서, 관리 모듈(1106)은 매체 저장소(1108)로부터 매체 플레이어(1104)에 추가될 매체 아이템을 식별하는 일을 하고 그 후 이 식별된 매체 아이템이 매체 플레이어(1104)로 전달되도록 한다. 또 다른 예로서, 매체 플레이어(1104)로부터 매체 아이템을 "지우기" 위해서, 관리 모듈(1106)은 매체 저장소(1108)로부터 지워질 매체 아이템을 식별하고 그 후 이 식별된 매체 아이템이 매체 플레이어(1104)로부터 지워지도록 한다. 또 다른 예로서, 만약 매체 아이템의 특성에 대한 변화(즉, 변경)가 관리 모듈(1106)을 이용하여 호스트 컴퓨터(1102)에서 이루어지면, 이러한 특성은 매체 플레이어(1104)의 대응 매체 아이템으로 전달될 수 있다. 한가지 구현에서, 추가, 삭제, 및/또는 변경은 매체 플레이어(1104)의 매체 아이템과 호스트 컴퓨터(1102)의 매체 아이템의 동기화 동안 배치 유사 프로세스(batch-like process)로 발생한다.

<123> 또 다른 실시예에서, 매체 플레이어(1104)는 매체 플레이어(1104)의 플레이리스트를 관리하는 능력이 없거나 제한된다. 그러나, 호스트 컴퓨터(1102) 내의 관리 모듈(1106)은 호스트 컴퓨터(1102)에 있는 플레이리스트의 관리를 통해 매체 플레이어(1104)에 있는 플레이리스트를 간접적으로 관리할 수 있다. 이 점에서, 플레이리스트에 대한 추가, 삭제 또는 변경이 호스트 컴퓨터(1102) 상에서 수행될 수 있고 그 후 미디어 플레이어(1104)로 전달된다.

<124> 상기 기재된 바와 같이, 동기화는 매체 관리의 한 형태이다. 자동으로 동기화를 개시하는 능력은 또한 상기에서 미리 논의되었고 상기 기재된 관련 애플리케이션에서도 논의되었다. 그러나, 또한, 장치들 간의 동기화는 호스트 컴퓨터와 매체 플레이어가 서로를 인식하지 못하는 때에 자동 동기화를 막기 위해 제한될 수 있다.

<125> 일 실시예에 따르면, 매체 플레이어가 호스트 컴퓨터로 우선 접속된 경우(또는 더 일반적으로 매칭 식별자(matching identifiers)가 존재하지 않는 경우), 매체 플레이어의 사용자는 자신이 매체 플레이어를 호스트 컴퓨터에 제휴(affiliate), 지정(assign), 또는 잠금(lock)을 원하는지 여부에 관하여 질문받는다. 매체 플레이어의 사용자가 매체 플레이어와 호스트 컴퓨터의 제휴, 지정 또는 잠금을 선택하는 경우, 의사-랜덤 식별자(pseudo-random identifier)가 얻어지고 호스트 컴퓨터 및 매체 플레이어 내의 매체 데이터베이스 또는 파일에 저장된다. 한가지 구현에서, 식별자는 호스트 컴퓨터 또는 이의 관리 모듈과 연관된(예컨대, 호스트 컴퓨터 또는 이의 관리 모듈에 의해 알려지거나 생성된) 식별자이고 이러한 식별자는 매체 플레이어에 보내지고 저장된다. 또 다른 구현에서, 식별자는 매체 플레이어와 연관되고(예컨대, 미디어 플레이어에 의해 알려지거나 생성되고) 호스트 컴퓨터의 파일 또는 매체 데이터베이스로 보내지고 저장된다.

<126> 도 12는 본 발명의 일 실시예에 따른 매체 플레이어(1200)의 블록도이다. 매체 플레이어(1200)는 매체 플레이어(1200)의 전반적 동작을 제어하는 컨트롤러 또는 마이크로프로세서에 해당하는 프로세서(1202)를 포함한다. 매체 플레이어(1200)는 파일 시스템(1204) 및 캐시(1206)의 매체 아이템에 속하는 매체 데이터를 저장한다. 파일 시스템(1204)은 일반적으로 저장 장치이다. 파일 시스템(1204)은 일반적으로 매체 플레이어(1200)에게 대용량 저장 능력을 제공한다. 예를 들어, 저장 장치는, 플래시 메모리와 같은, 반도체 기반 메모리가 될 수 있다. 파일 시스템(1204)은 매체 데이터를 저장할 수 있을 뿐만 아니라 비-매체 데이터(예컨대, 데이터 모드로 동작되는 경우)를 저장할 수 있다. 그러나, 파일 시스템(1204)으로의 액세스 시간이 상대적으로 늘리기 때문에, 매체 플레이어는 캐시(1206)를 또한 포함할 수 있다. 캐시(1206)는, 예컨대, 반도체 메모리에 의해 제공되는 랜덤 액세스 메모리(RAM)이다. 캐시(1206)로의 상대적 액세스 시간은 파일 시스템(1204)에 대하여보다 실질적으로

짧다. 그러나, 캐시(1206)는 파일 시스템(1204)의 큰 저장 용량을 갖지 못한다. 또한, 파일 시스템(1204)은 동작중인 경우 캐시(1206)보다 더 많은 전력을 소비한다. 전력 소비는 매체 플레이어(1200)가 배터리(도시되지 않음)에 의해 전력공급을 받는 휴대용 매체 플레이어인 경우 종종 문제가 된다. 매체 플레이어(1200)는 또한 RAM(1220) 및 리드-온니 메모리(ROM, 1222)를 포함한다. ROM(1222)은 비휘발성 방법으로 수행되는 프로그램, 유틸리티 또는 프로세스를 저장할 수 있다. RAM(1220)은 캐시(1206)와 같은 휘발성 데이터 저장소를 제공한다. 일 실시예에서, ROM(1220) 및 RAM(1222)은 파일 시스템(1204)을 제공하는 저장 장치에 의해 제공될 수 있다.

<127> 매체 플레이어(1200)는 또한 매체 플레이어(1200)의 사용자로 하여금 매체 플레이어(1200)와 상호작용할 수 있게 하는 사용자 입력 장치(1208)를 포함한다. 예를 들어, 사용자 입력 장치(1208)는, 이를테면 버튼, 키패드, 다이얼 등과 같은, 다양한 형태를 취할 수 있다. 또한, 매체 플레이어(1200)는 정보를 사용자에게 디스플레이하기 위한, 프로세서(1202)에 의해 제어될 수 있는, 디스플레이(1210)(스크린 디스플레이)를 포함한다. 사용자 입력 장치(1208) 및 디스플레이(1210)는 도한 터치 스크린의 경우 결합될 수 있다. 데이터 버스(1211)는 적어도 파일 시스템(1204), 캐시(1206), 프로세서(1202) 및 코덱(1212) 간의 데이터 전송을 손쉽게할 수 있다.

<128> 일 실시예에서, 매체 플레이어(1200)는 파일 시스템(1204) 내에 복수의 매체 아이템(예컨대, 노래)을 저장하는 일을 한다. 사용자가 매체 플레이어가 특정 매체 아이템을 플레이하기를 원하는 경우, 이용가능한 매체 아이템의 목록이 디스플레이(1210)에 디스플레이된다. 그 후, 사용자 입력 장치(1202)를 이용하여, 사용자는 이용가능한 매체 아이템 중 하나를 선택할 수 있다. 프로세서(1202)는 특정 매체 아이템의 선택을 수신한 후에, 특정 매체 아이템에 대한 매체 데이터(예컨대, 오디오 파일)를 코더/디코더(CODEC, 1212)로 공급한다. 그 후 CODEC(1212)은 스피커(1214)로 아날로그 출력 신호를 만들어낸다. 스피커(1214)는 매체 플레이어(1200)의 내부 또는 매체 플레이어(1200)의 외부 스피커가 될 수 있다. 예를 들어, 매체 플레이어(1200)로 접속하는 헤드폰 또는 이어폰은 외부 스피커로 고려된다.

<129> 매체 플레이어(1200)는 또한 데이터 링크(1218)에 결합되는 네트워크/버스 인터페이스(1216)를 포함한다. 데이터 링크(1218)는 매체 플레이어(1200)가 호스트 컴퓨터 또는 액세서리 장치에 결합되는 것을 가능하게 한다. 데이터 링크(1218)는 유선 접속 또는 무선 접속을 통해 제공될 수 있다. 무선 접속의 경우, 네트워크/버스 인터페이스(1216)는 무선 송수신기를 포함할 수 있다.

<130> 일 실시예에서, 호스트 컴퓨터는 매체 장치 플레이리스트를 비롯한 플레이리스트에 대한 활용을 허용하고 이에 대한 관리를 제공하기 위해 호스트 컴퓨터에 있는 애플리케이션을 활용할 수 있다. 한가지 이러한 애플리케이션은 캘리포니아 쿠페르티노(Cupertino, CA)에 위치한 애플 컴퓨터 유한 책임회사(Apple Computer, Inc.)에 의해 제작된 iTunes®, 버전 4.2이다.

<131> 매체 아이템(매체 자산)은 하나 이상의 다른 유형의 매체 콘텐츠에 해당할 수 있다. 일 실시예에서, 매체 아이템은 오디오 트랙이다. 또 다른 실시예에서, 매체 아이템은 이미지(예컨대, 사진)이다. 그러나, 다른 실시예에서, 매체 아이템은 오디오, 그래픽 또는 비디오 콘텐츠의 임의의 조합이 될 수 있다.

<132> 상기 논의는 액세서리 장치 또는 호스트 장치를 인증하기 위해 암호 방법으로 사용되는 난수를 참조한다. 상기 논의된 암호 방법은 난수, 공개-비밀 키 쌍 및 인증 알고리즘을 사용할 수 있다. 난수들은 랜덤 다이제스트(random digests)로 불리울 수도 있다. 공개-비밀 키 쌍 및 인증 알고리즘은 공지의 RSA 알고리즘 또는 타원 곡성 암호(Elliptic Curve Cryptography: ECC) 알고리즘과 같은 공개-키 암호 시스템을 활용할 수 있다. RSA 구현에서 일반적인 큰 키(예컨대, 1024 비트)에 비하여 상대적으로 작은 키(예컨대, 160 비트)로 감소된 메모리 소비를 제공하는 ECC 알고리즘을 이용하는 것이 유리할 수 있다. 감소된 메모리 ECC 알고리즘의 예는 "적은 메모리 풋프린트 빠른 타원 암호(SMALL MEMORY FOOTPRINT FAST ELLIPTIC ENCRYPTION)" 제목의 2005년 2월 3일 출원된 미국 특허출원 번호 11/051,441에 기재되어 있으며, 이 내용은 본 명세서에서 참조로 인용된다.

<133> 본 발명의 다양한 태양, 실시예, 구현 또는 특징은 개별적으로 또는 임의의 조합으로 사용될 수 있다.

<134> 본 발명은 소프트웨어, 하드웨어, 또는 소프트웨어 및 하드웨어의 조합에 의해 구현될 수 있다. 본 발명은 또한 컴퓨터 판독가능 매체 상의 컴퓨터 판독가능 코드로 구체화될 수 있다. 컴퓨터 판독가능 매체는 컴퓨터 시스템에 의해 판독될 수 있는 데이터를 저장할 수 있는 임의의 데이터 저장 장치이다. 컴퓨터 판독가능 매체의 예로 리드-온니 메모리(ROM), 랜덤 액세스 메모리(RAM), CD-ROM, DVD, 자기 테이프, 광 데이터 저장 장치, 및 캐리어 웨이브(carrier wave)가 있다. 컴퓨터 판독가능 매체는, 또한 컴퓨터 판독가능 코드가 분배된 방식(distributed fashion)으로 저장되고 실행되도록, 네트워크-결합된 컴퓨터 시스템을 통해 분배될 수 있다.

<135> 본 발명의 장점은 여러가지이다. 다른 특징, 실시예 또는 구현은 하나 이상의 다음의 장점들을 가져올 수

있다. 본 발명의 한가지 장점은 호스트 장치와 액세서리의 상호작용에 대한 제어가 제어될 수 있다는 점이다. 결과적으로, 전자 장치는 인증된 것으로 간주된 액세서리 장치만이 전자 장치의 특징의 일부 또는 전부를 사용하도록 제한할 수 있다. 본 발명의 또 다른 장점은 호스트 장치와 활용되도록 허가된 액세서리 장치의 품질(quality)을 관리하는 능력을 제공한다는 점이다. 액세서리 장치의 품질을 관리함으로써, 전자 장치의 동작은 하급 액세서리 장치의 부착에 의해 잘 손상되지 않는다. 본 발명의 또 다른 장점은 인증 프로세스가 제조자 또는 장치에 기초하여 전자 장치의 특정 특징으로의 액세스를 제어할 수 있다는 점이다.

<136> 본 발명의 많은 특징 및 장점을 상기 명세서로부터 명확히 알 수 있고, 따라서 첨부된 청구항은 본 발명의 이러한 모든 특징 및 장점을 망라하는 것으로 의도된다. 또한, 다양한 수정 및 변경을 가하는 것이 당업자에게 명확하기 때문에, 발명은 도시되고 설명된 정확한 구조 또는 동작에 한정되어서는 안 된다. 그러므로, 모든 적합한 수정 및 동등물은 발명의 범위 내에 있는 것으로 고려될 수 있다.

도면의 간단한 설명

<19> 본 발명은 첨부된 도면과 함께 다음의 상세한 설명을 통해 쉽게 이해할 수 있을 것이고, 동일한 참조 숫자는 동일한 구조적 요소를 지정한다.

<20> 도 1a는 본 발명의 일 실시예에 따른 액세서리 인증 시스템의 블록도.

<21> 도 1b는 본 발명의 또 다른 실시예에 따른 액세서리 인증 시스템의 블록도.

<22> 도 1c는 본 발명의 또 다른 실시예에 따른 액세서리 인증 시스템의 블록도.

<23> 도 2a는 본 발명의 일 실시예에 따른 인증 컨트롤러의 블록도.

<24> 도 2b는 본 발명의 일 실시예에 따른 인증 관리자의 블록도.

<25> 도 3은 본 발명의 일 실시예에 따른 인증 장치의 블록도.

<26> 도 4a는 본 발명의 일 실시예에 따른 호스트 인증 프로세스의 흐름도.

<27> 도 4b는 본 발명의 일 실시예에 따른 액세서리 인증 프로세스의 흐름도.

<28> 도 5a 및 5b는 본 발명의 일 실시예에 따른 호스트 장치 프로세싱의 흐름도.

<29> 도 6a 및 6b는 본 발명의 일 실시예에 따른 액세서리 장치 프로세싱의 흐름도.

<30> 도 6c는 본 발명의 일 실시예에 따른 인증 테이블의 다이어그램.

<31> 도 7a 및 7b는 본 발명의 일 실시예에 따른 액세서리 장치 프로세스의 흐름도.

<32> 도 8a-8c는 본 발명의 일 실시예에 따른 호스트 장치 프로세스의 흐름도.

<33> 도 9a-9c는 본 발명의 일 실시예에 따른 액세서리 장치 프로세스의 흐름도.

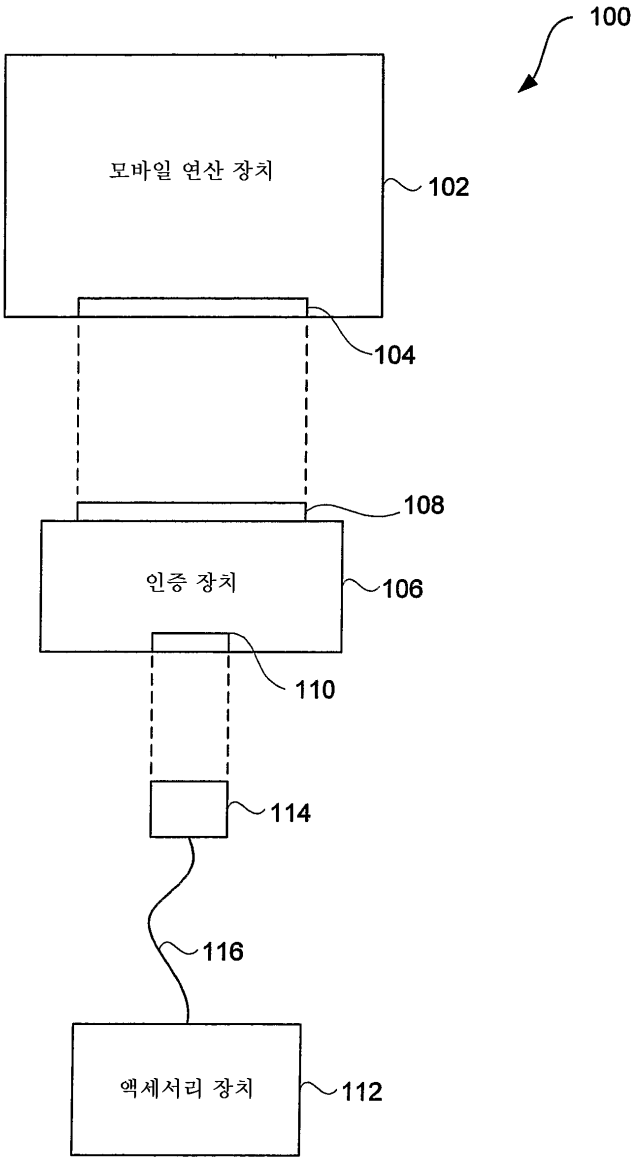
<34> 도 10a 및 10b는 본 발명의 일 실시예에 따른 호스트 장치 프로세스의 흐름도.

<35> 도 11은 본 발명의 일 실시예에 따른 매체 관리 시스템의 블록도.

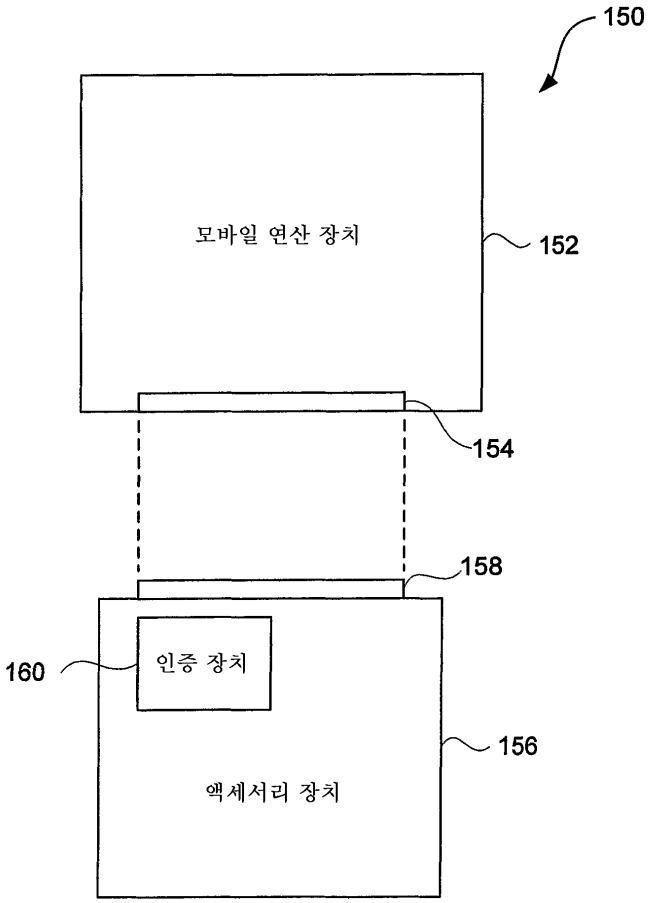
<36> 도 12는 본 발명의 일 실시예에 따른 매체 플레이어의 블록도.

도면

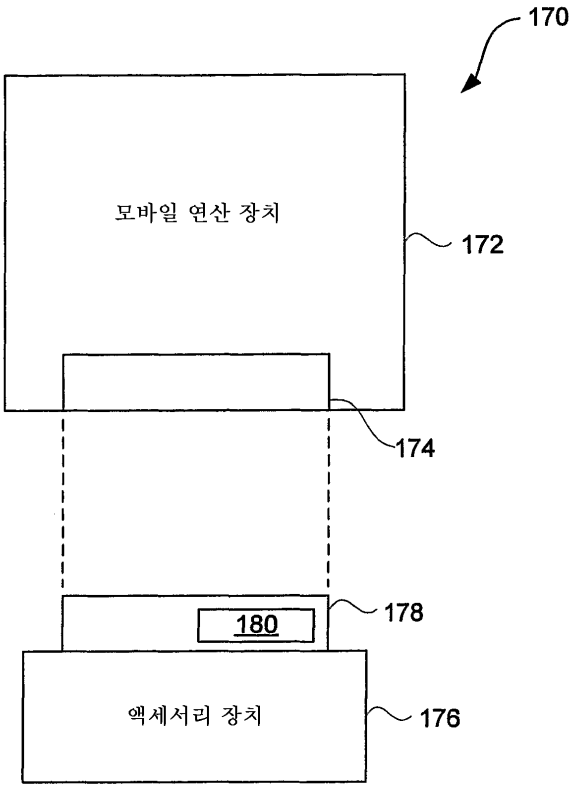
도면1a



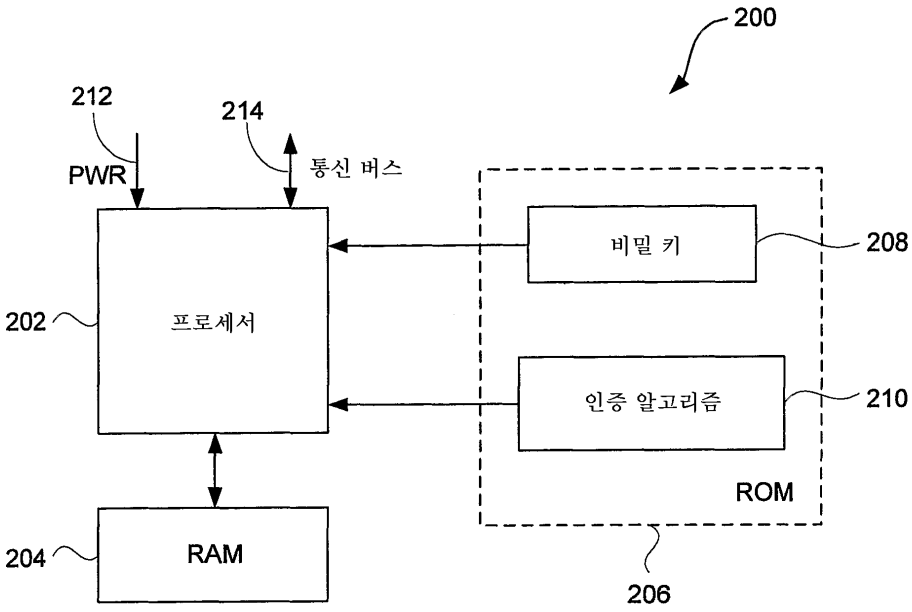
도면1b



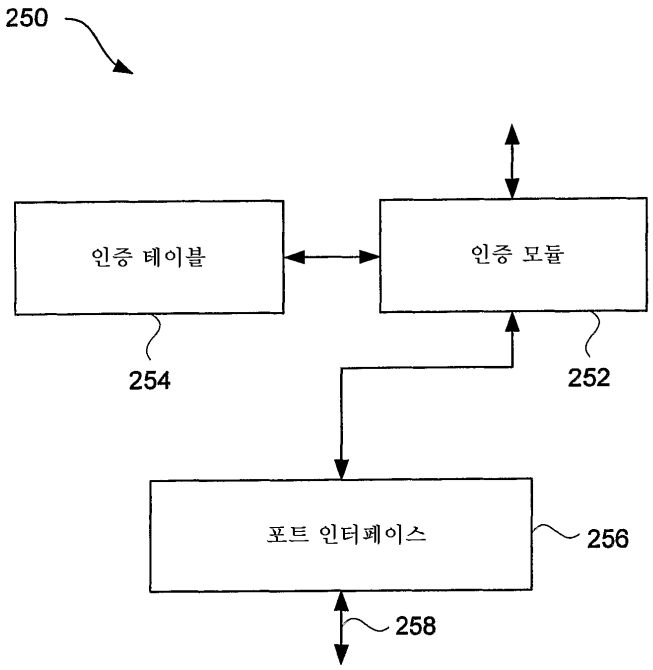
도면1c


170
모바일 연산 장치
172
174
178
180
액세서리 장치
176

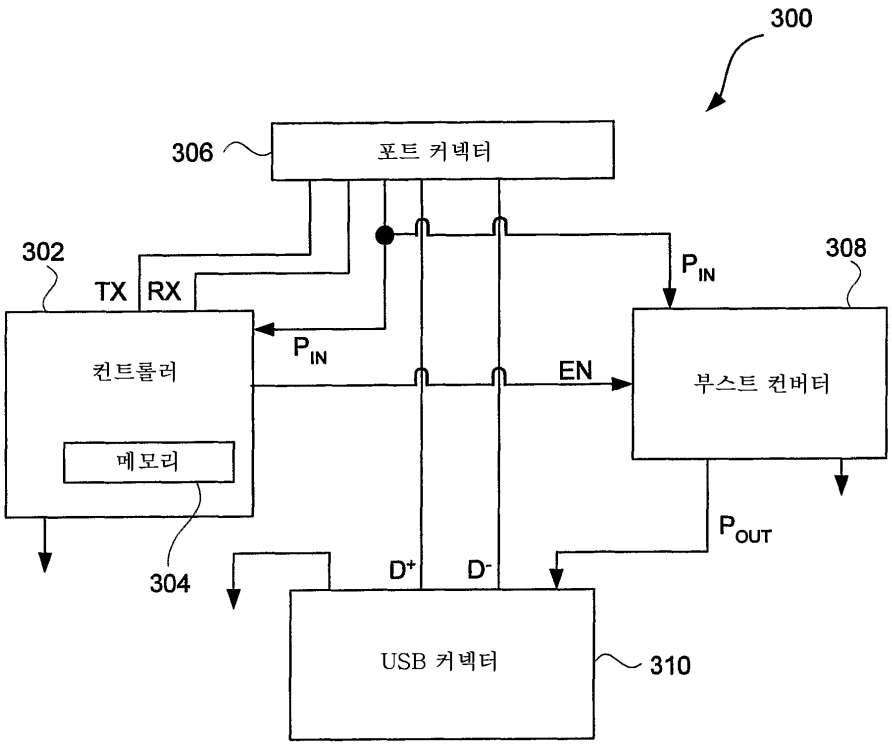
도면2a


200
212
214
PWR
통신 버스
비밀 키
208
202
프로세서
인증 알고리즘
210
ROM
RAM
204
206

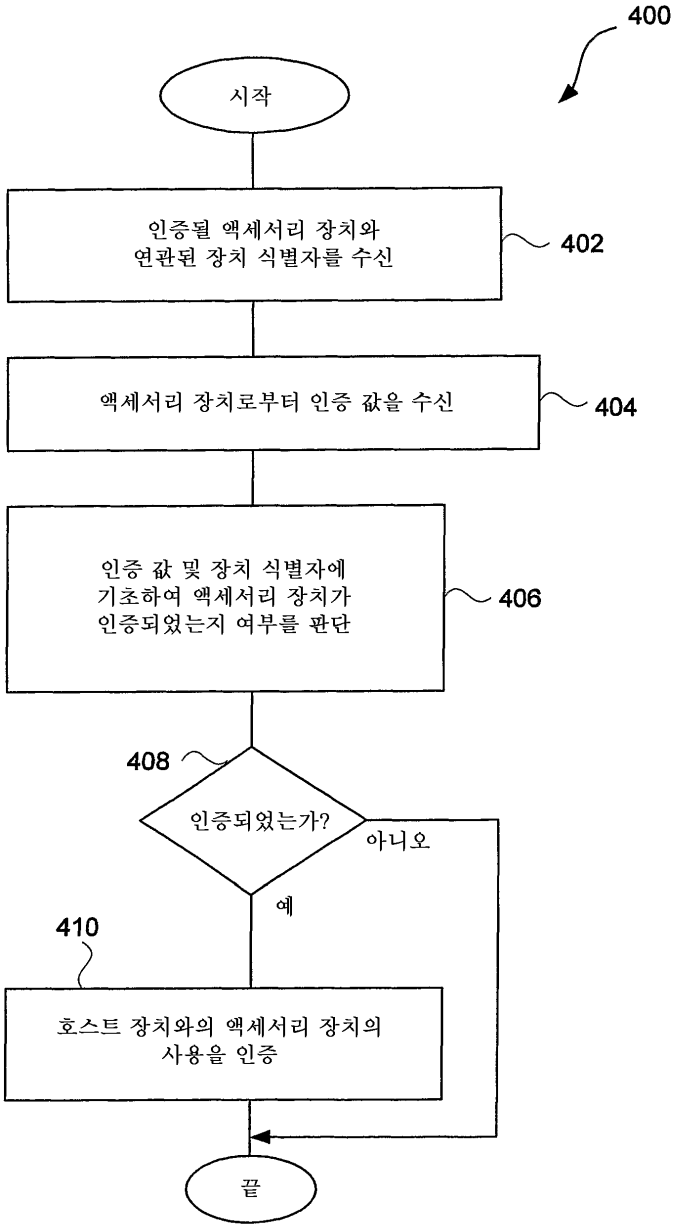
도면2b


250
인증 테이블
인증 모듈
254
252
포트 인터페이스
256
258

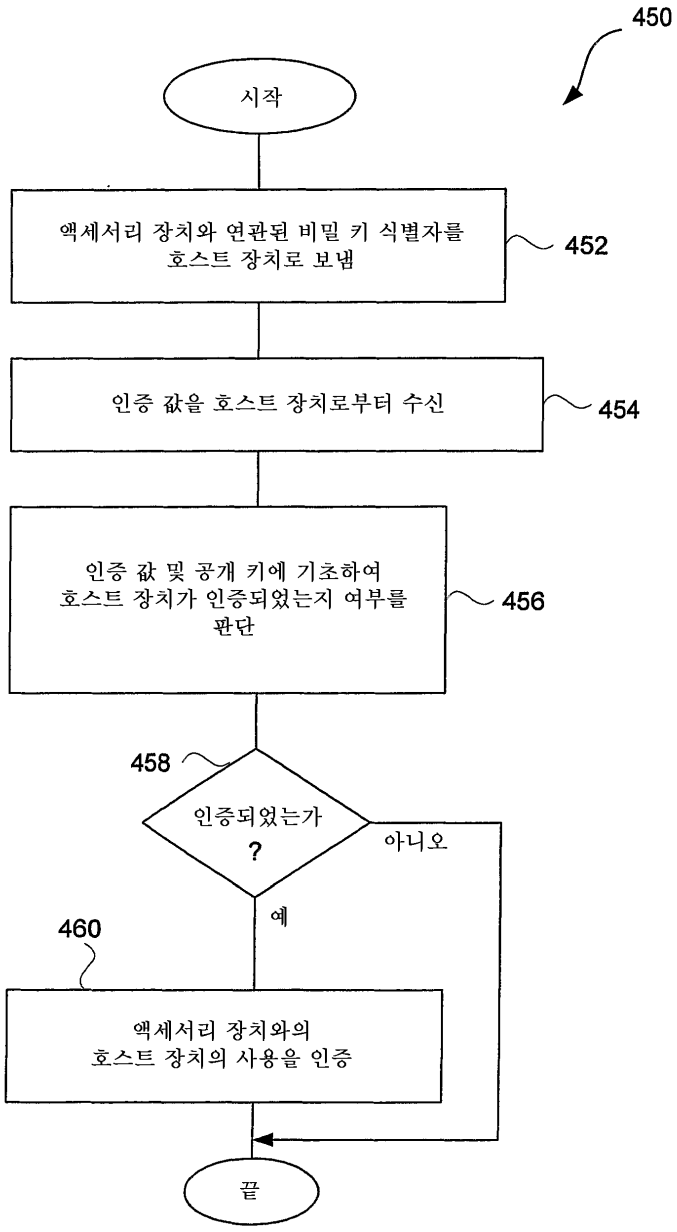
도면3


300
306
포트 커넥터
302
TX
RX
P_{IN}
308
P_{IN}
EN
컨트롤러
부스트 컨버터
메모리
304
P_{OUT}
D^+
D^-
USB 커넥터
310

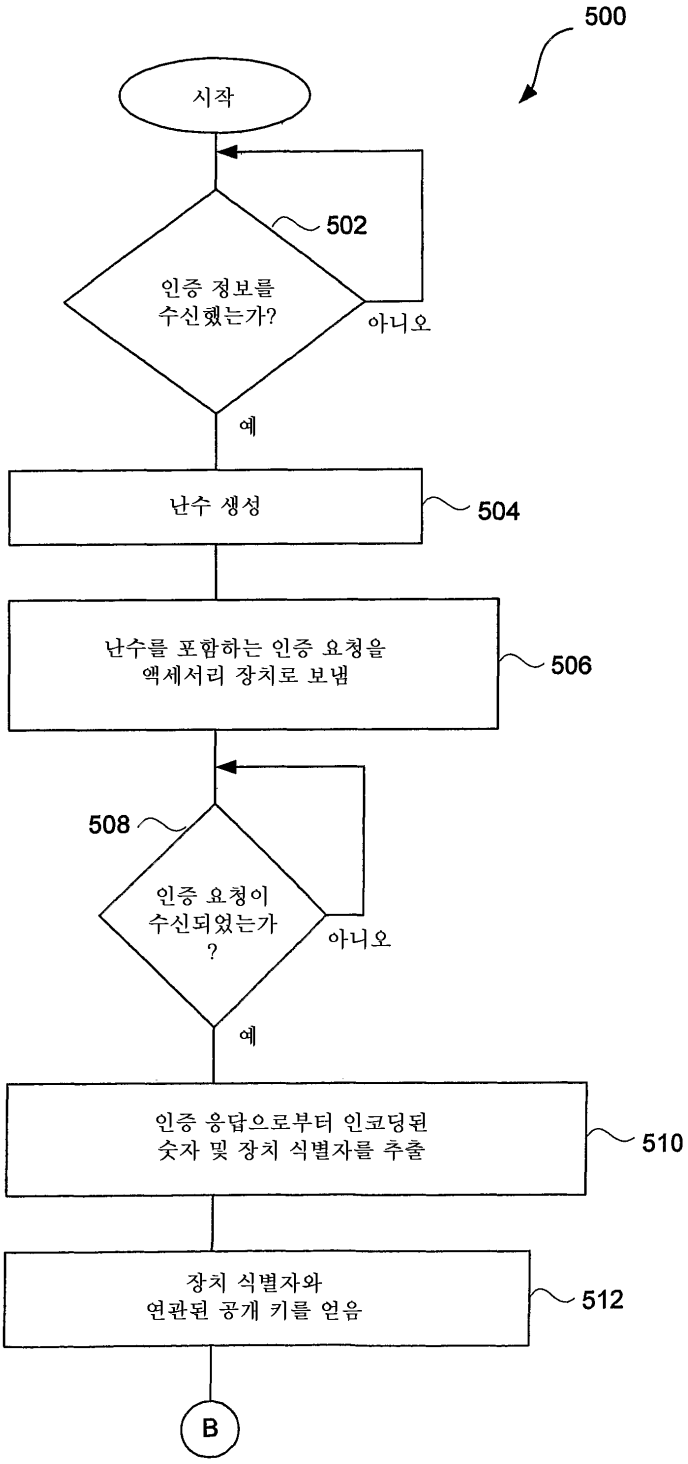
도면4a


400
시작
인증될 액세서리 장치와
연관된 장치 식별자를 수신
402
액세서리 장치로부터 인증 값을 수신
404
인증 값 및 장치 식별자에
기초하여 액세서리 장치가
인증되었는지 여부를 판단
406
408
인증되었는가?
아니오
예
410
호스트 장치와의 액세서리 장치의
사용을 인증
끝

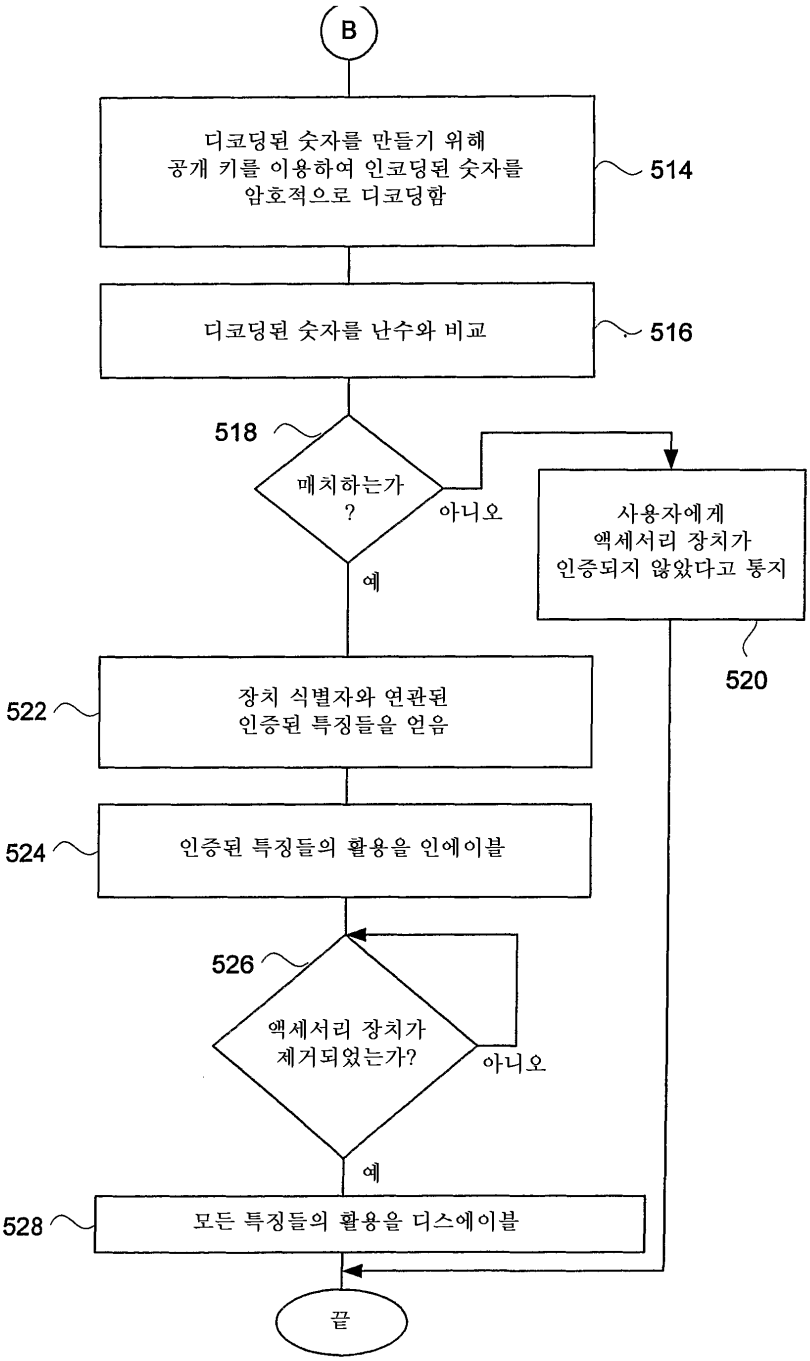
도면4b


450
시작
액세서리 장치와 연관된 비밀 키 식별자를 호스트 장치로 보냄
452
인증 값을 호스트 장치로부터 수신
454
인증 값 및 공개 키에 기초하여 호스트 장치가 인증되었는지 여부를 판단
456
458
인증되었는가 ?
아니오
예
460
액세서리 장치와의 호스트 장치의 사용을 인증
끝

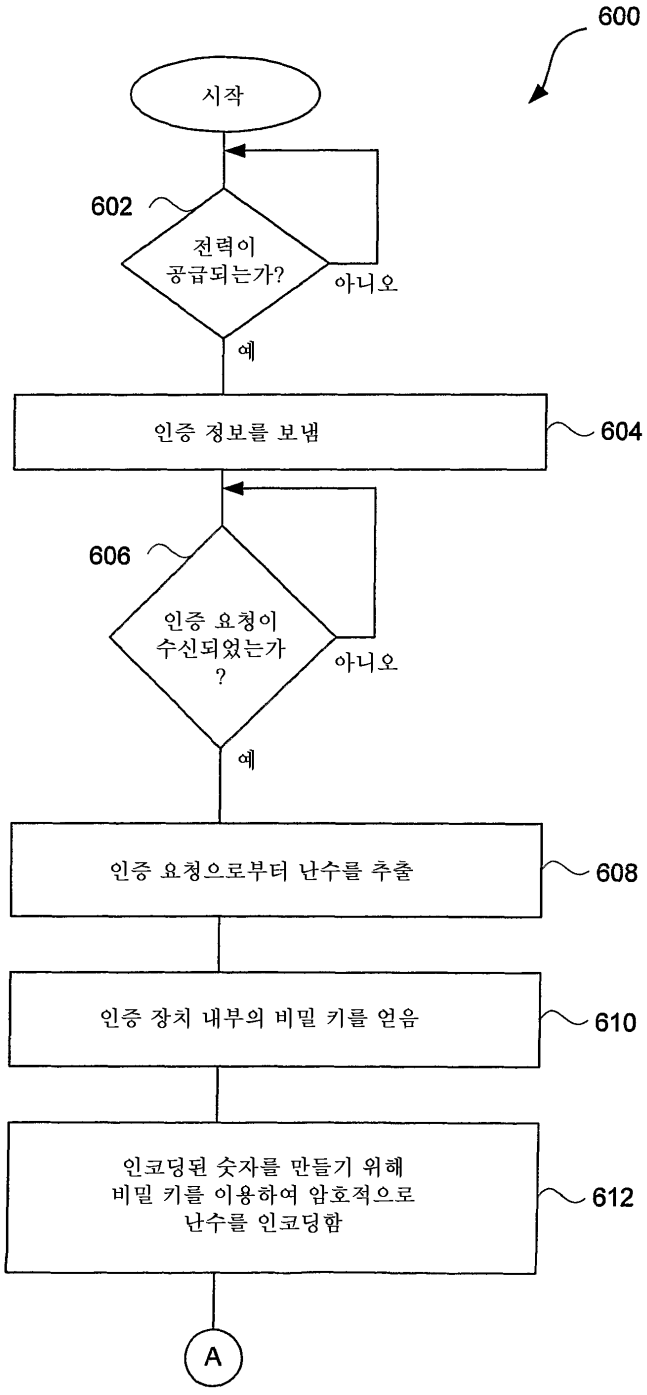
도면5a


500
시작
502
인증 정보를
수신했는가?
아니오
예
난수 생성
504
난수를 포함하는 인증 요청을
액세서리 장치로 보냄
506
508
인증 요청이
수신되었는가
?
아니오
예
인증 응답으로부터 인코딩된
숫자 및 장치 식별자를 추출
510
장치 식별자와
연관된 공개 키를 얻음
512
B

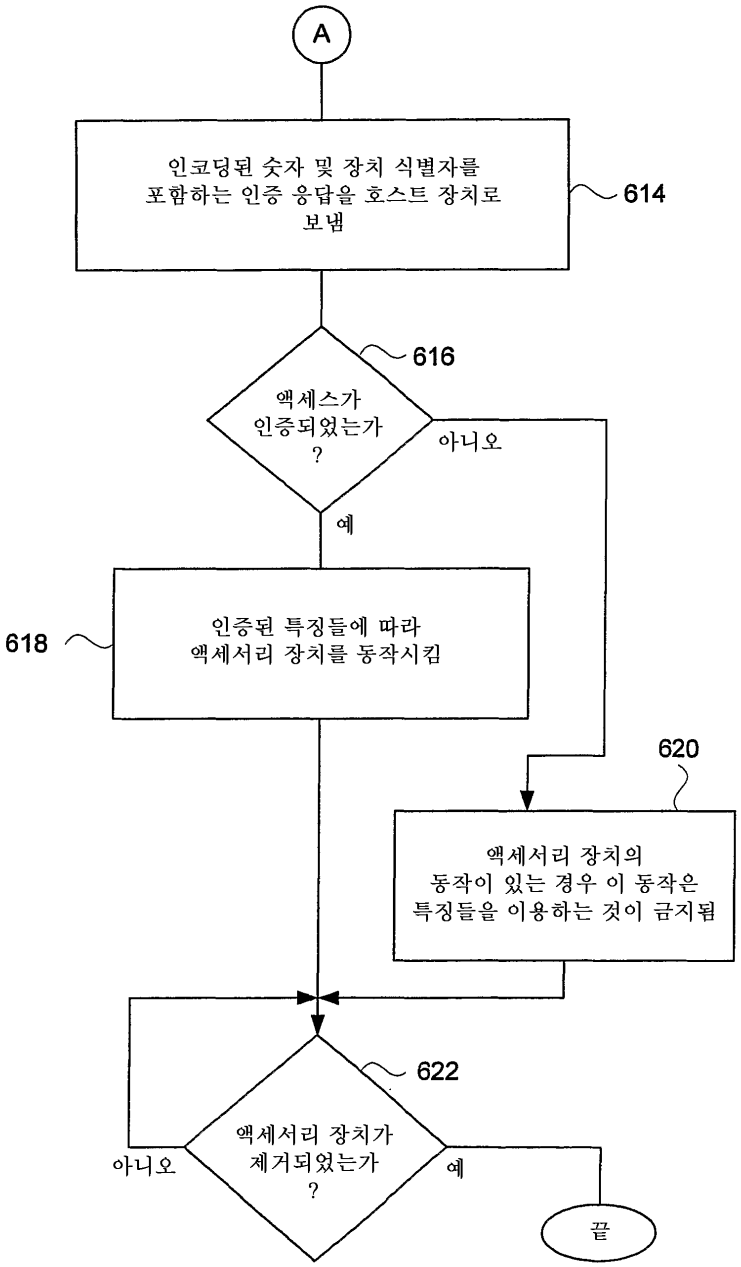
도면5b


B
디코딩된 숫자를 만들기 위해
공개 키를 이용하여 인코딩된 숫자를
암호적으로 디코딩함
514
디코딩된 숫자를 난수와 비교
516
518
매치하는가
?
아니오
예
사용자에게
액세서리 장치가
인증되지 않았다고 통지
520
522
장치 식별자와 연관된
인증된 특징들을 얻음
524
인증된 특징들의 활용을 인에이블
526
액세서리 장치가
제거되었는가?
아니오
예
528
모든 특징들의 활용을 디스에이블
끝

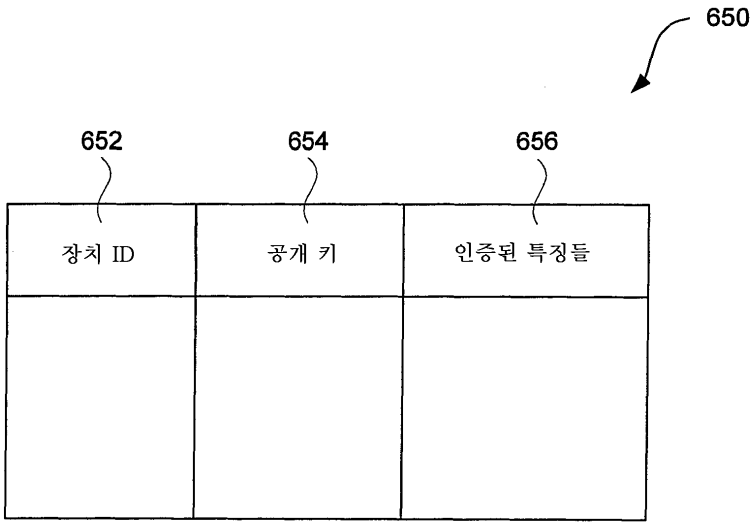
도면6a


600
시작
602
전력이 공급되는가?
아니오
예
인증 정보를 보냄
604
606
인증 요청이 수신되었는가 ?
아니오
예
인증 요청으로부터 난수를 추출
608
인증 장치 내부의 비밀 키를 얻음
610
인코딩된 숫자를 만들기 위해 비밀 키를 이용하여 암호적으로 난수를 인코딩함
612
A

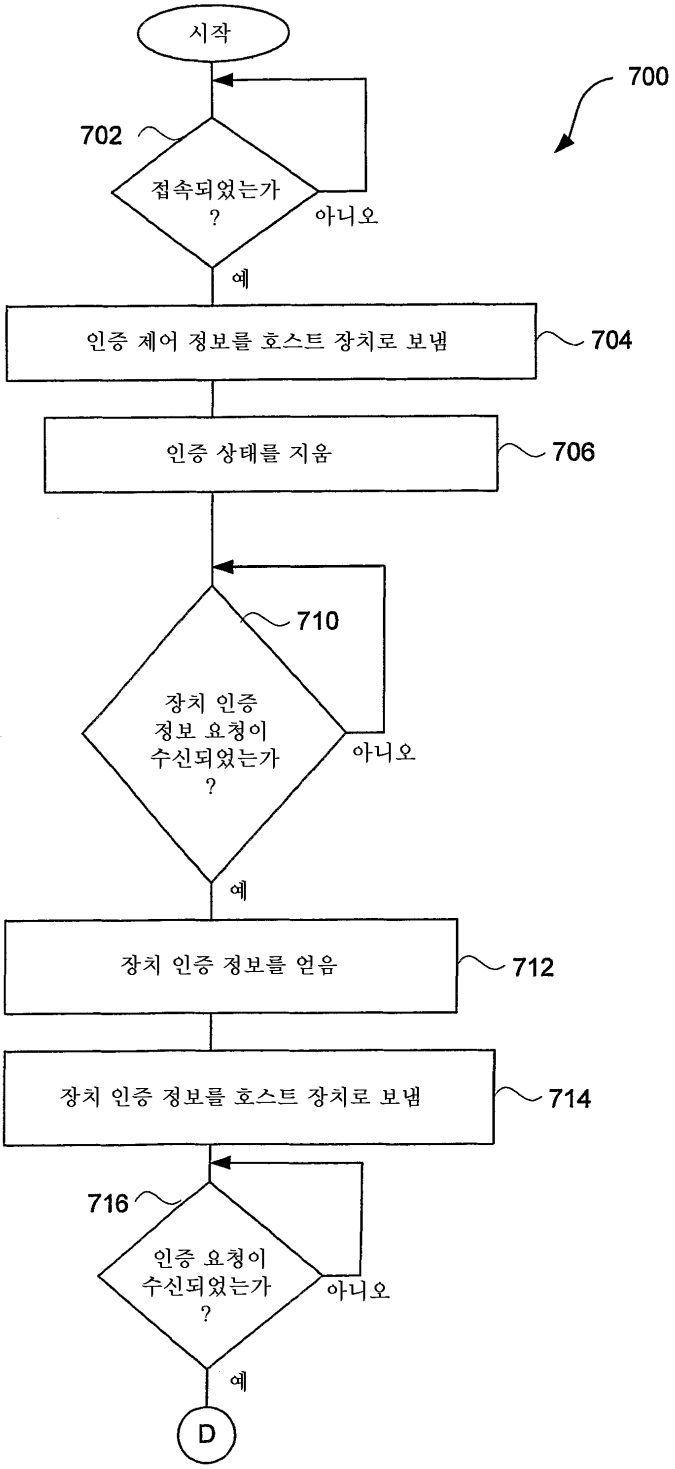
도면6b


A
인코딩된 숫자 및 장치 식별자를 포함하는 인증 응답을 호스트 장치로 보냄
614
616
액세스가 인증되었는가 ?
아니오
예
618
인증된 특징들에 따라 액세서리 장치를 동작시킴
620
액세서리 장치의 동작이 있는 경우 이 동작은 특징들을 이용하는 것이 금지됨
622
액세서리 장치가 제거되었는가 ?
아니오
예
끝

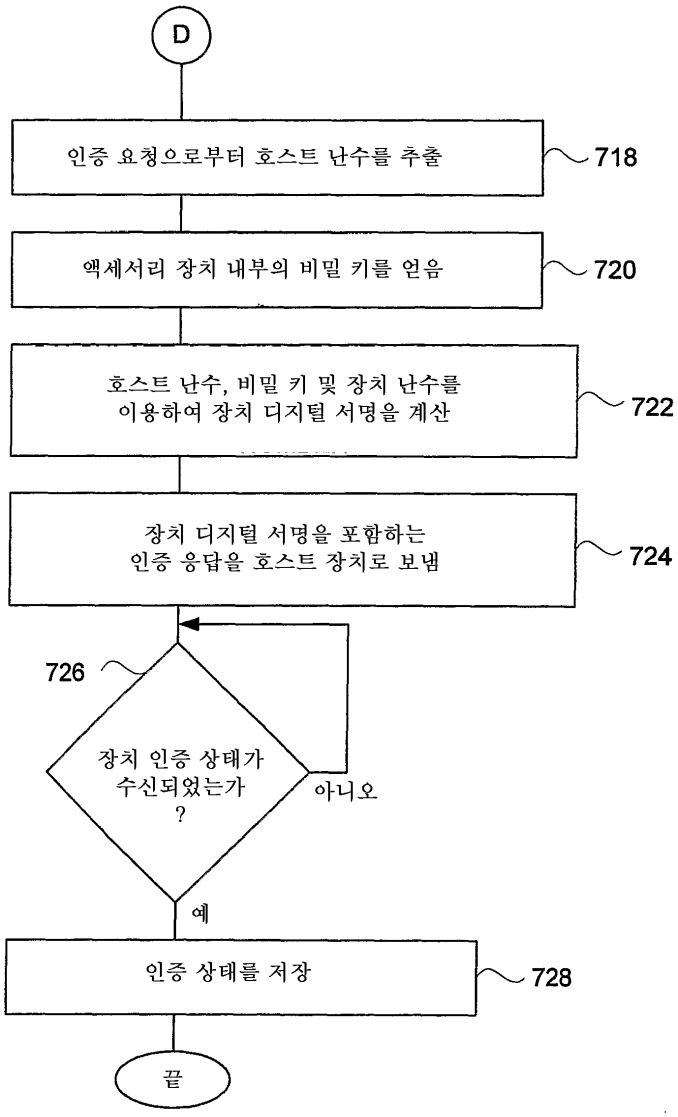
도면6c



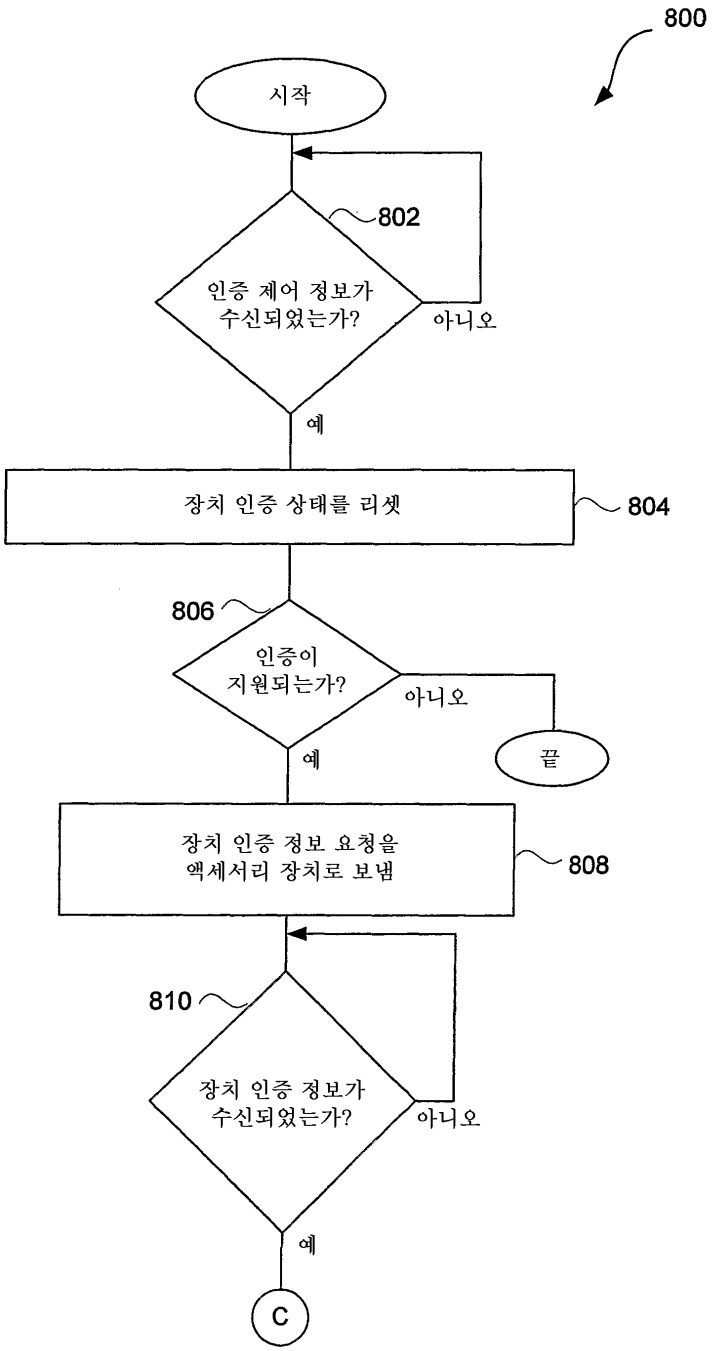
도면7a


시작
700
702
접속되었는가 ?
아니오
예
인증 제어 정보를 호스트 장치로 보냄
704
인증 상태를 지움
706
710
장치 인증 정보 요청이 수신되었는가 ?
아니오
예
장치 인증 정보를 얻음
712
장치 인증 정보를 호스트 장치로 보냄
714
716
인증 요청이 수신되었는가 ?
아니오
예
D

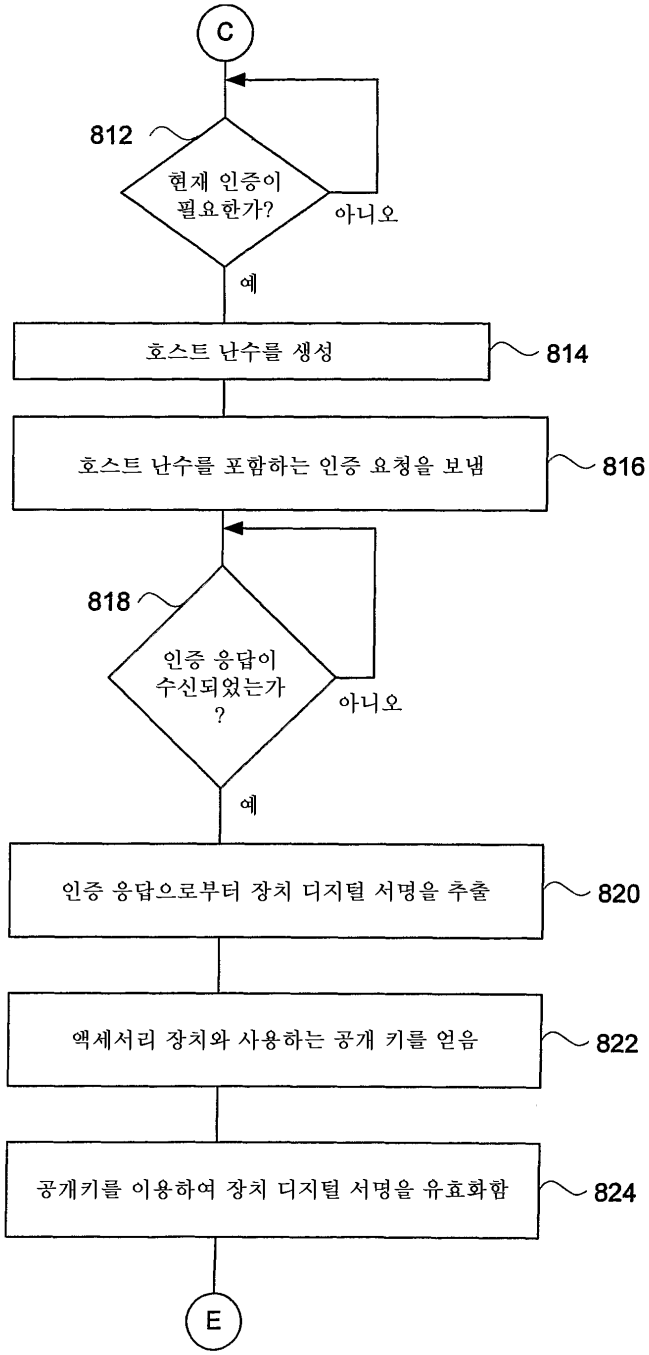
도면7b


D
인증 요청으로부터 호스트 난수를 추출
718
액세서리 장치 내부의 비밀 키를 얻음
720
호스트 난수, 비밀 키 및 장치 난수를
이용하여 장치 디지털 서명을 계산
722
장치 디지털 서명을 포함하는
인증 응답을 호스트 장치로 보냄
724
726
장치 인증 상태가
수신되었는가
?
아니오
예
인증 상태를 저장
728
끝

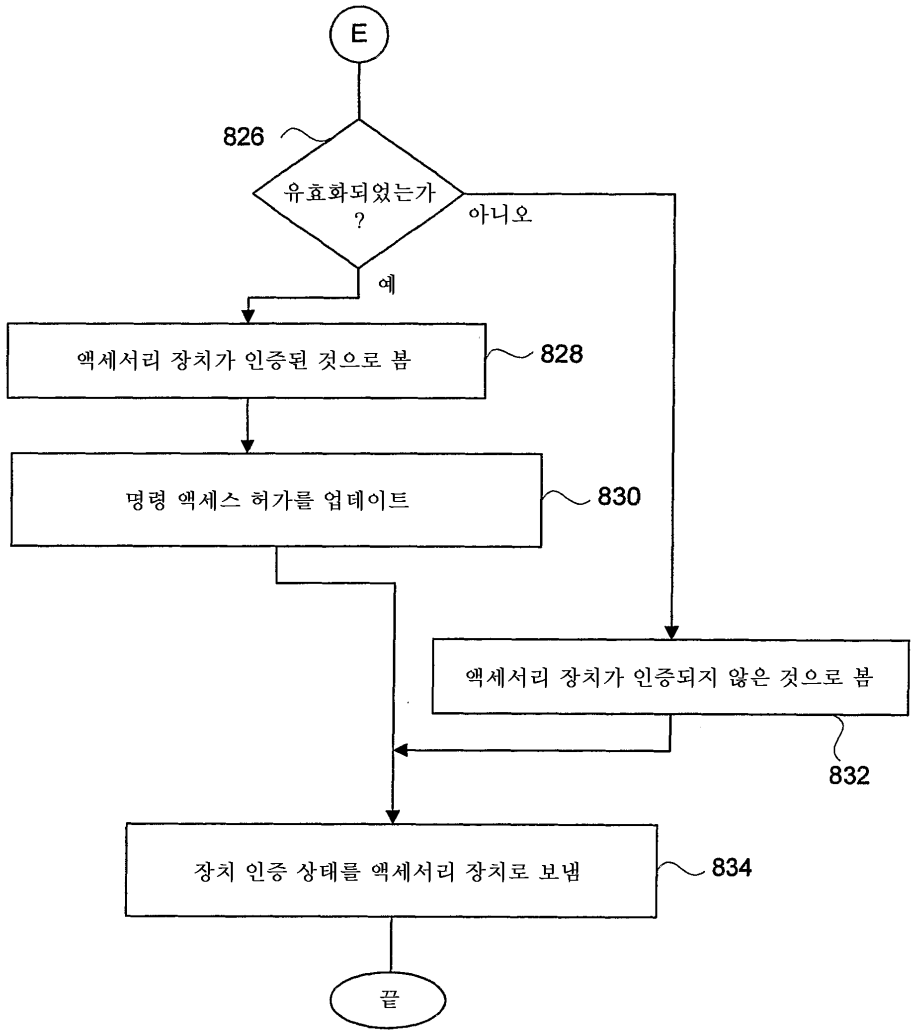
도면8a


800
시작
802
인증 제어 정보가
수신되었는가?
아니오
예
장치 인증 상태를 리셋
804
806
인증이
지원되는가?
아니오
끝
예
장치 인증 정보 요청을
액세서리 장치로 보냄
808
810
장치 인증 정보가
수신되었는가?
아니오
예
C

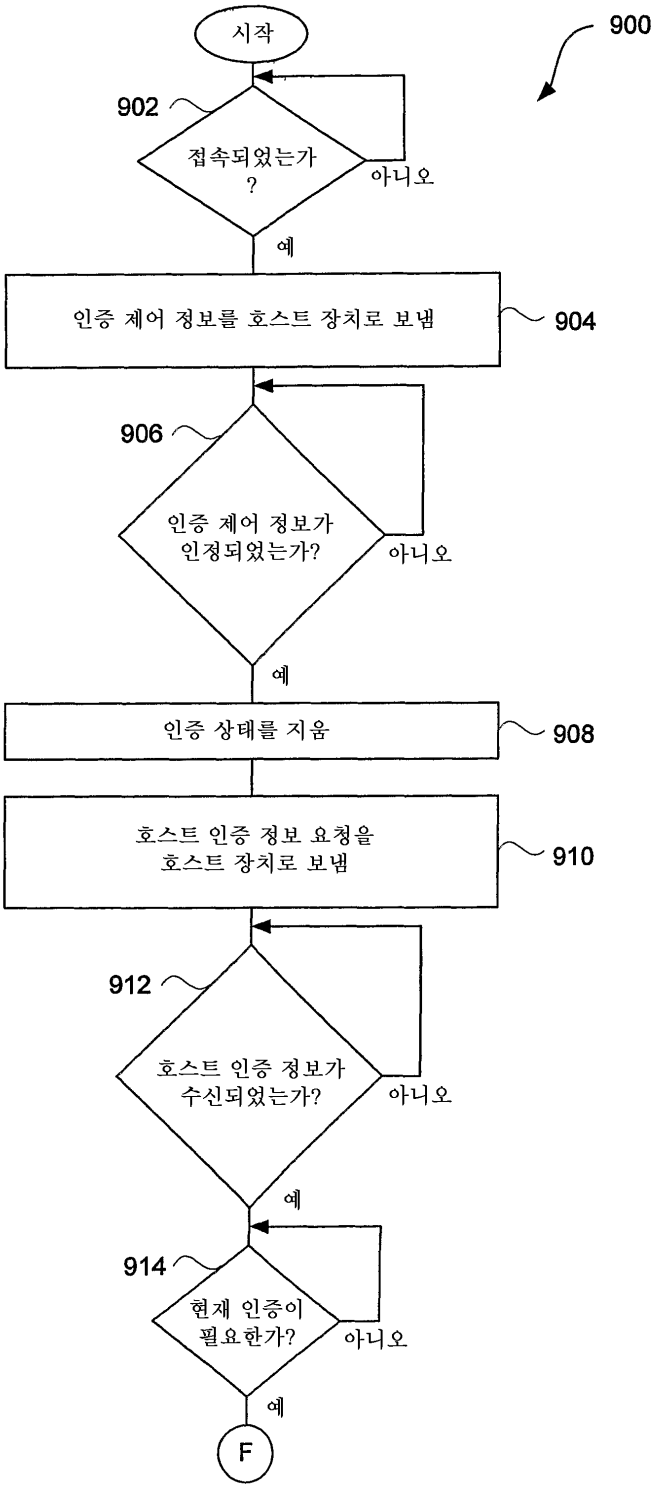
도면8b


C
812
현재 인증이 필요한가?
아니오
예
호스트 난수를 생성
814
호스트 난수를 포함하는 인증 요청을 보냄
816
818
인증 응답이 수신되었는가 ?
아니오
예
인증 응답으로부터 장치 디지털 서명을 추출
820
액세서리 장치와 사용하는 공개 키를 얻음
822
공개키를 이용하여 장치 디지털 서명을 유효화함
824
E

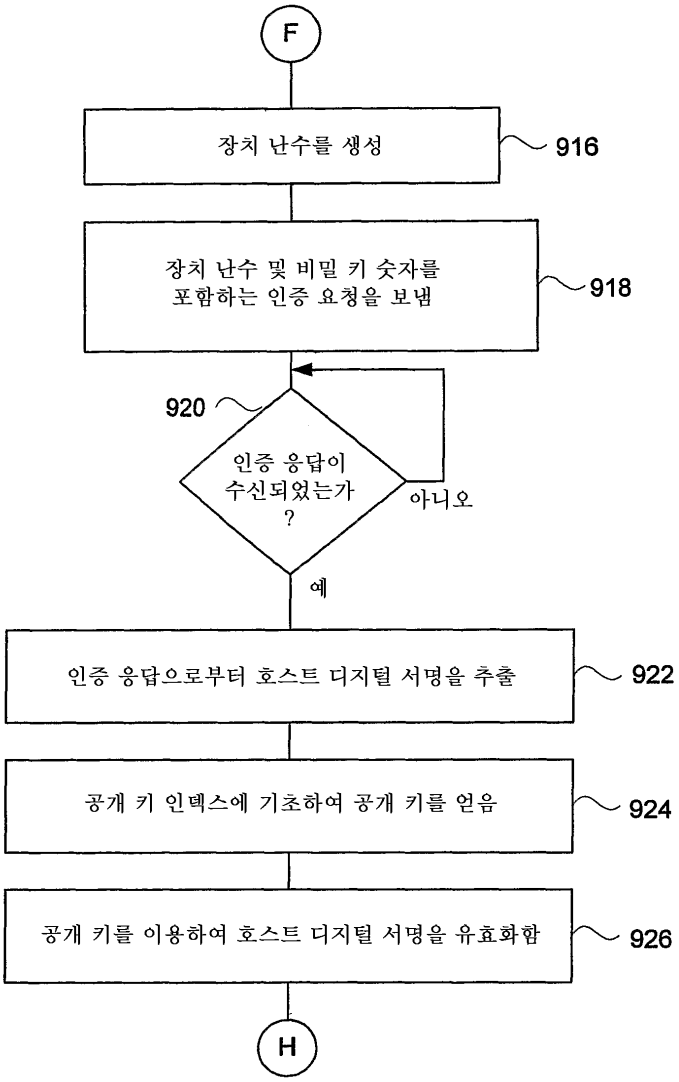
도면8c


E
826
유효화되었는가 ?
아니오
예
액세서리 장치가 인증된 것으로 봄
828
명령 액세스 허가를 업데이트
830
액세서리 장치가 인증되지 않은 것으로 봄
832
장치 인증 상태를 액세서리 장치로 보냄
834
끝

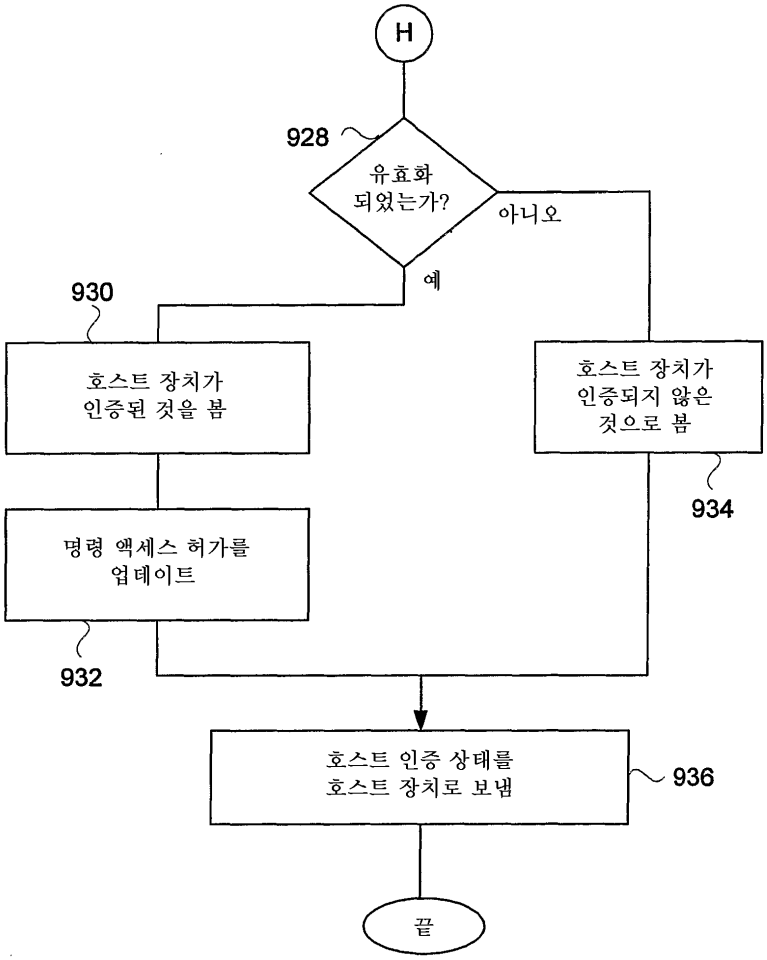
도면9a


900
시작
902
접속되었는가 ?
아니오
예
인증 제어 정보를 호스트 장치로 보냄
904
906
인증 제어 정보가 인정되었는가?
아니오
예
인증 상태를 지움
908
호스트 인증 정보 요청을 호스트 장치로 보냄
910
912
호스트 인증 정보가 수신되었는가?
아니오
예
914
현재 인증이 필요한가?
아니오
예
F

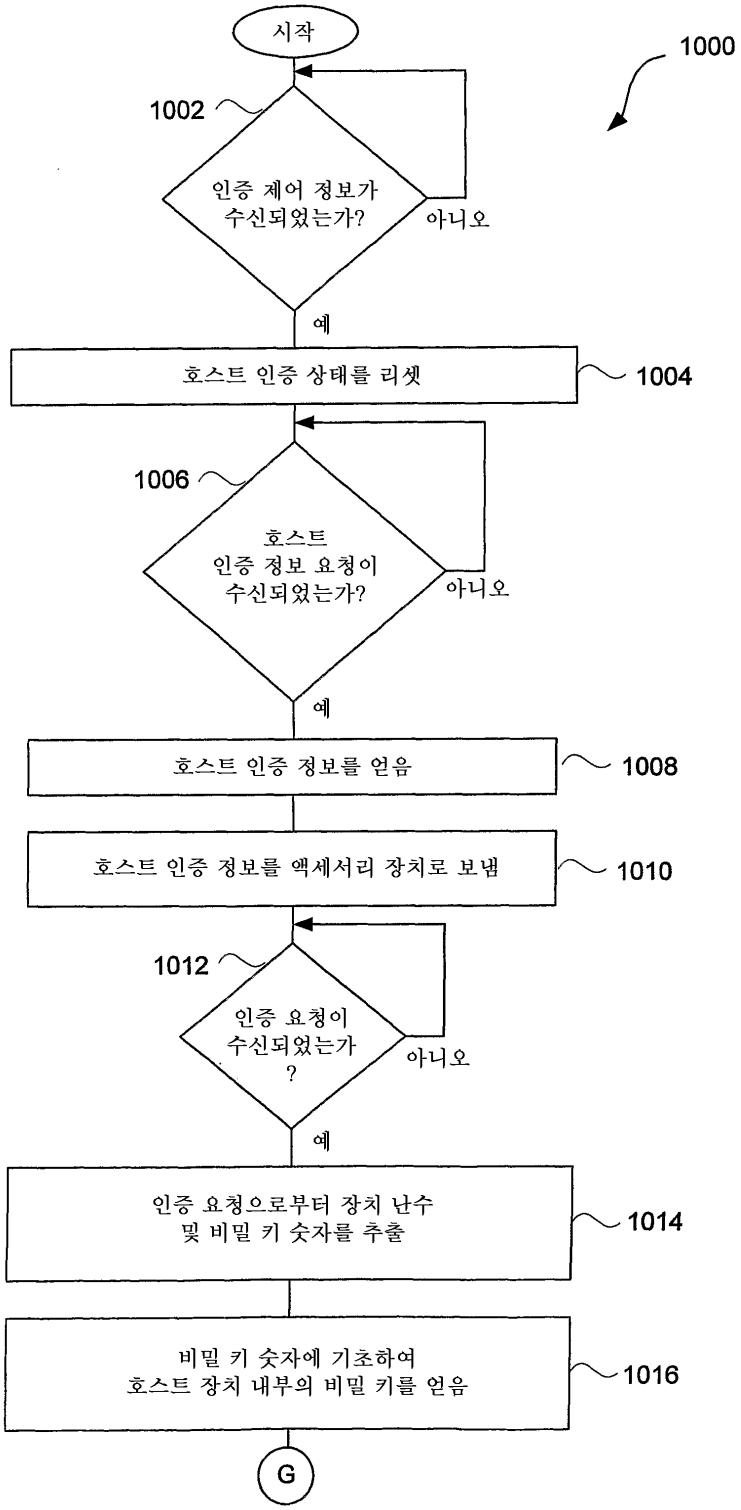
도면9b


F
장치 난수를 생성
916
장치 난수 및 비밀 키 숫자를 포함하는 인증 요청을 보냄
918
920
인증 응답이 수신되었는가 ?
아니오
예
인증 응답으로부터 호스트 디지털 서명을 추출
922
공개 키 인덱스에 기초하여 공개 키를 얻음
924
공개 키를 이용하여 호스트 디지털 서명을 유효화함
926
H

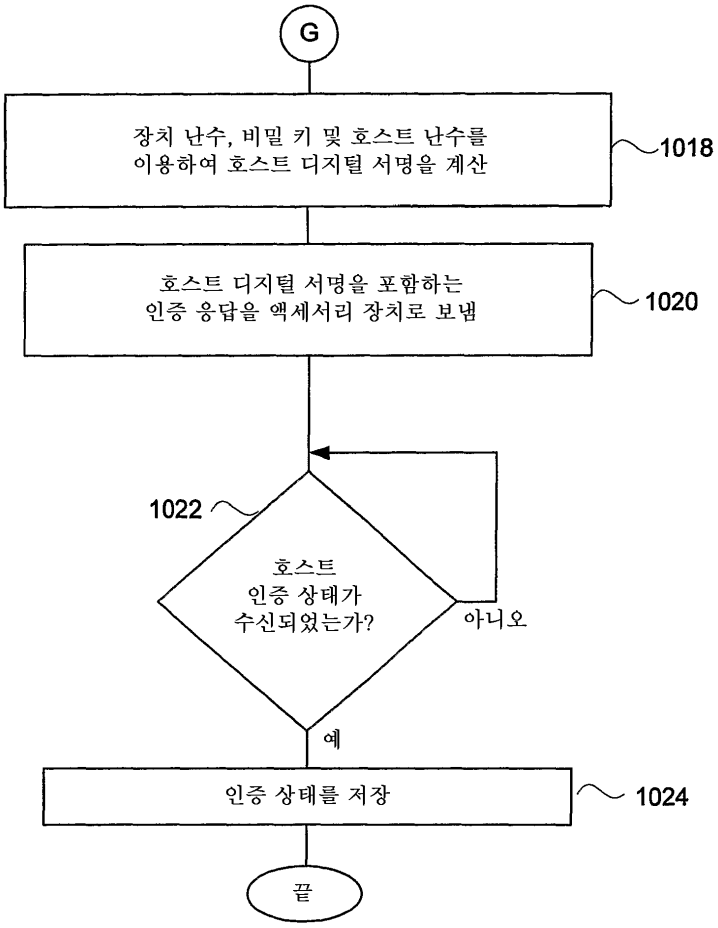
도면9c


H
928
유효화 되었는가?
아니오
예
930
호스트 장치가 인증된 것을 봄
호스트 장치가 인증되지 않은 것으로 봄
934
명령 액세스 허가를 업데이트
932
호스트 인증 상태를 호스트 장치로 보냄
936
끝

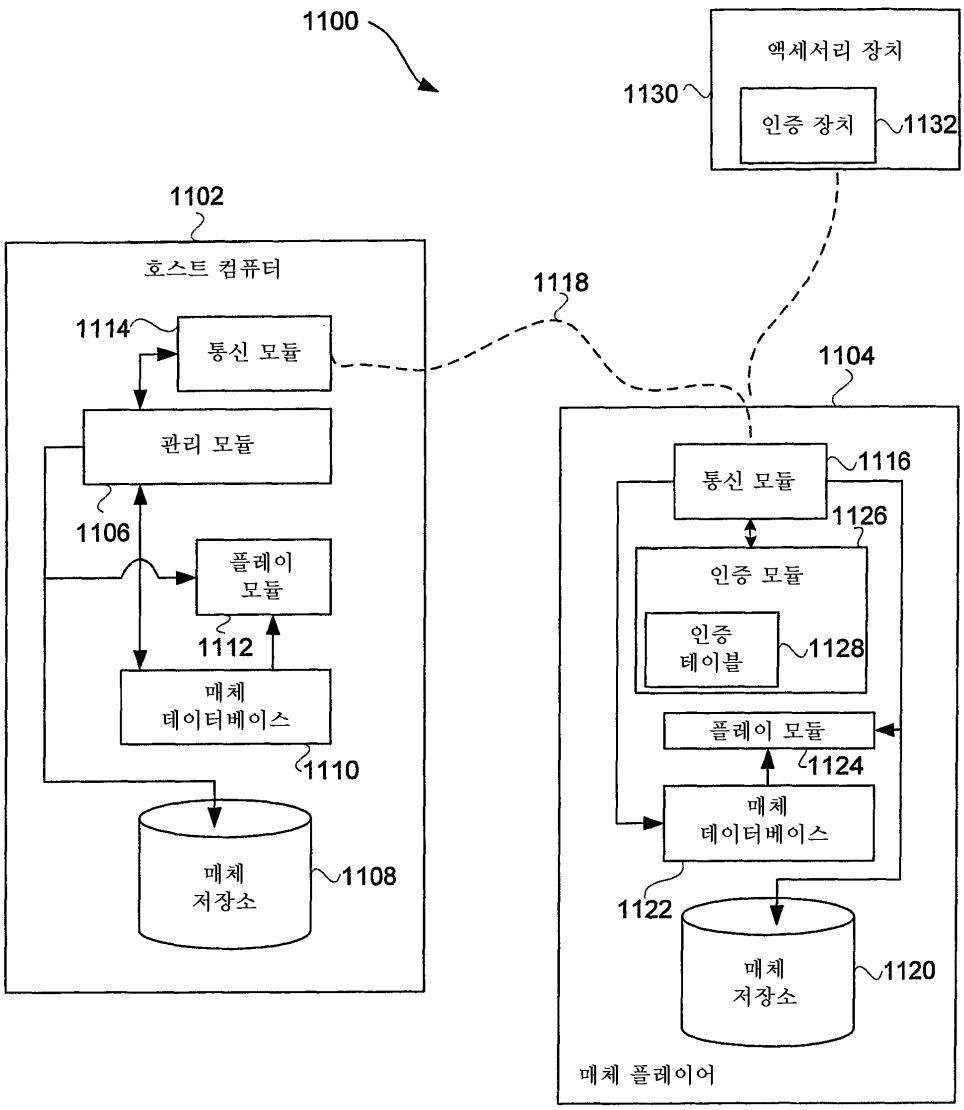
도면10a


시작
1000
1002
인증 제어 정보가 수신되었는가?
아니오
예
호스트 인증 상태를 리셋
1004
1006
호스트 인증 정보 요청이 수신되었는가?
아니오
예
호스트 인증 정보를 얻음
1008
호스트 인증 정보를 액세서리 장치로 보냄
1010
1012
인증 요청이 수신되었는가 ?
아니오
예
인증 요청으로부터 장치 난수 및 비밀 키 숫자를 추출
1014
비밀 키 숫자에 기초하여 호스트 장치 내부의 비밀 키를 얻음
1016
G

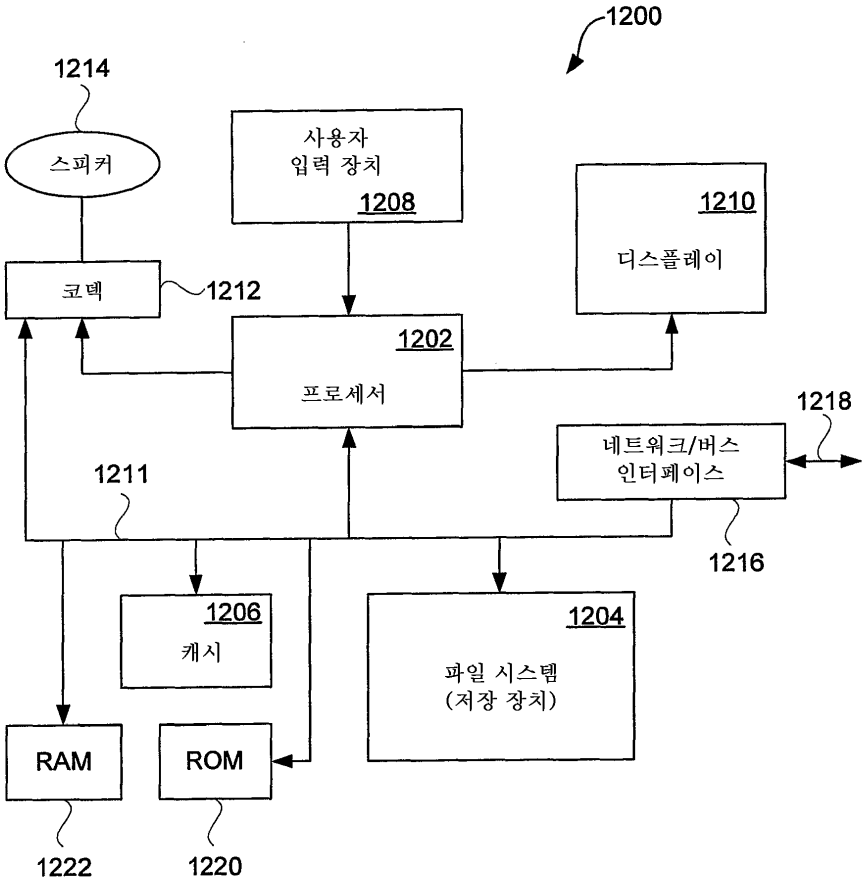
도면10b


G
장치 난수, 비밀 키 및 호스트 난수를
이용하여 호스트 디지털 서명을 계산
1018
호스트 디지털 서명을 포함하는
인증 응답을 액세서리 장치로 보냄
1020
1022
호스트
인증 상태가
수신되었는가?
아니오
예
인증 상태를 저장
1024
끝

도면11


1100
액세서리 장치
1130
인증 장치
1132
1102
호스트 컴퓨터
1118
1114
통신 모듈
1104
관리 모듈
1116
통신 모듈
1126
1106
인증 모듈
플레이
모듈
인증
테이블
1128
1112
매체
데이터베이스
플레이 모듈
1124
1110
매체
데이터베이스
매체
저장소
1108
1122
매체
저장소
1120
매체 플레이어

도면12


1200
1214
스피커
사용자
입력 장치
1208
1210
디스플레이
코덱
1212
1202
프로세서
1218
네트워크/버스
인터페이스
1211
1216
1206
캐시
1204
파일 시스템
(저장 장치)
RAM
ROM
1222
1220