



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0084934
(43) 공개일자 2017년07월21일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) G06F 21/57 (2013.01)
H04L 9/08 (2006.01)

(52) CPC특허분류
H04L 9/3247 (2013.01)
G06F 21/575 (2013.01)

(21) 출원번호 10-2016-0004376
(22) 출원일자 2016년01월13일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)

(72) 발명자
김경문
경기도 용인시 기흥구 흥덕1로79번길 37, 504동 1102호(영덕동, 흥덕마을5단지호반베르디움아파트)

이재영
서울특별시 종로구 창경궁로 265, 101동 908호(명륜2가, 아남아파트)

오명진
경기도 성남시 분당구 미금로 66, 401동 405호(구미동, 무지개마을주공4단지아파트)

(74) 대리인
윤동열

전체 청구항 수 : 총 15 항

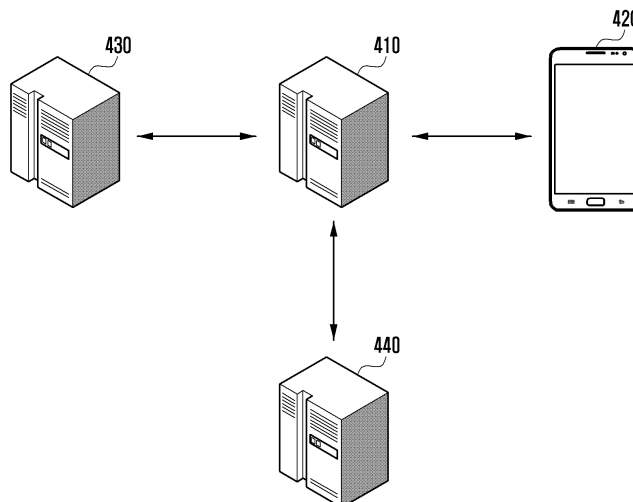
(54) 발명의 명칭 전자 장치 및 전자 장치의 식별 정보 인증 방법

(57) 요약

본 발명의 다양한 실시예에 따른 전자 장치는, 통신 프로세서를 포함하는 통신 인터페이스; 상기 전자 장치에 대응하는 제1식별 정보, 상기 통신 프로세서에 대응하는 제2식별 정보, 및 외부 전자 장치로부터 수신된 전자 서명을 저장하기 위한 메모리; 및 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는, 상기 전자 서명을 복호화 하여, 상기 전자 장치에 대응하는 제1인증 정보와 관련된 데이터를 생성하고, 상기 제1식별 정보 및 상기 제2식별 정보에 적어도 기반하여 제2인증 정보와 관련된 데이터를 생성하고, 상기 제1인증 정보와 관련된 데이터와 상기 제2인증 정보와 관련된 데이터를 비교하고, 및 상기 비교의 결과에 적어도 기반하여 상기 전자 장치에 대한 인증을 수행하도록 설정될 수 있다.

그 외에 다양한 실시예가 가능하다.

대표도 - 도4



(52) CPC특허분류

H04L 9/083 (2013.01)

H04L 9/0861 (2013.01)

H04L 9/3236 (2013.01)

명세서

청구범위

청구항 1

전자 장치에 있어서,
통신 인터페이스;
외부 전자 장치에 대응하는 제1식별 정보와 상기 외부 전자 장치의 통신 프로세서에 대응하는 제2식별 정보를 저장하기 위한 메모리; 및
프로세서를 포함하며,
상기 프로세서는,
상기 제1식별 정보 및 상기 제2식별 정보에 적어도 기반하여 인증 정보를 생성하고,
상기 인증 정보와 관련된 데이터의 적어도 일부를 암호화 하여 상기 인증 정보에 대응하는 전자 서명을 생성하고, 및
상기 통신 인터페이스를 이용하여 상기 전자 서명을 상기 외부 전자 장치로 전송하도록 설정된 전자 장치.

청구항 2

제 1항에 있어서,
상기 프로세서는,
상기 전자 서명을 상기 제1식별 정보와 결합한 상태로 상기 외부 전자 장치로 전송하도록 설정된 전자 장치.

청구항 3

제 1항에 있어서,
상기 프로세서는,
상기 통신 인터페이스를 이용하여, 다른 외부 전자 장치로부터 키 값을 수신하고,
상기 키 값을 이용하여 상기 암호화하는 동작을 수행하도록 설정된 전자 장치.

청구항 4

제 1항에 있어서,
상기 프로세서는,
상기 인증 정보의 해시값(hash value)을 생성하고,
상기 인증 정보의 해시값의 적어도 일부를 암호화 하여 상기 전자 서명을 생성하도록 설정된 전자 장치.

청구항 5

전자 장치가 외부 전자 장치의 인증 정보에 대응하는 전자 서명을 생성하는 방법에 있어서,
상기 외부 전자 장치에 대응하는 제1식별 정보를 수신하는 동작;

상기 외부 전자 장치의 통신 프로세서에 대응하는 제2식별 정보를 수신하는 동작;
상기 제1식별 정보 및 상기 제2식별 정보에 적어도 기반하여 인증 정보를 생성하는 동작;
상기 인증 정보와 관련된 데이터의 적어도 일부를 암호화 하여 상기 인증 정보에 대응하는 전자 서명을 생성하는 동작; 및
상기 전자 서명을 상기 외부 전자 장치로 전송하는 동작을 포함하는 방법.

청구항 6

제 5항에 있어서,
상기 전자 서명을 전송하는 동작은,
상기 전자 서명을 상기 제1식별 정보와 결합한 상태로 상기 외부 전자 장치로 전송하는 동작을 포함하는 방법.

청구항 7

제 5항에 있어서,
다른 외부 전자 장치로부터 키 값을 수신하는 동작을 더 포함하며,
상기 전자 서명을 생성하는 동작은, 상기 키 값을 이용하여 상기 암호화하는 동작을 포함하는 전자 장치.

청구항 8

제 5항에 있어서,
상기 인증 정보의 해시값(hash value)을 생성하는 동작을 더 포함하며,
상기 전자 서명을 생성하는 동작은,
상기 인증 정보의 해시값의 적어도 일부를 암호화 하여 상기 전자 서명을 생성하는 동작을 포함하는 방법.

청구항 9

전자 장치에 있어서,
통신 프로세서를 포함하는 통신 인터페이스;
상기 전자 장치에 대응하는 제1식별 정보, 상기 통신 프로세서에 대응하는 제2식별 정보, 및 외부 전자 장치로부터 수신된 전자 서명을 저장하기 위한 메모리; 및
적어도 하나의 프로세서를 포함하고,
상기 적어도 하나의 프로세서는,
상기 전자 서명을 복호화 하여, 상기 전자 장치에 대응하는 제1인증 정보와 관련된 데이터를 생성하고,
상기 제1식별 정보 및 상기 제2식별 정보에 적어도 기반하여 제2인증 정보와 관련된 데이터를 생성하고,
상기 제1인증 정보와 관련된 데이터와 상기 제2인증 정보와 관련된 데이터를 비교하고, 및
상기 비교의 결과에 적어도 기반하여 상기 전자 장치에 대한 인증을 수행하도록 설정된 전자 장치.

청구항 10

제 9항에 있어서,
출력 장치를 더 포함하고,
상기 프로세서는,
상기 출력 장치를 통하여 상기 인증의 결과에 대응하는 알림(notification)을 제공하도록 설정된 전자 장치.

청구항 11

제 9항에 있어서,
상기 제1인증 정보와 관련된 데이터는,
상기 제1인증 정보의 해시값(hash value)을 포함하며,
상기 프로세서는,
상기 제2인증 정보의 해시값을 생성하고, 상기 제1인증 정보의 해시값과 상기 제2인증 정보의 해시값이 동일한 경우, 상기 제1식별 정보가 유효한 것으로 판단하도록 설정된 전자 장치.

청구항 12

제 9항에 있어서,
상기 프로세서는,
상기 전자 장치의 부팅(booting) 과정에 상기 전자 장치에 대한 인증을 수행하도록 설정된 전자 장치.

청구항 13

전자 장치가 식별 정보를 인증하는 방법에 있어서,
외부 전자 장치로부터 수신된 전자 서명을 복호화 하여, 상기 전자 장치에 대응하는 제1인증 정보와 관련된 데이터를 생성하는 동작;
상기 전자 장치에 대응하는 제1식별 정보 및 상기 전자 장치의 통신 프로세서에 대응하는 제2식별 정보에 적어도 기반하여 제2인증 정보와 관련된 데이터를 생성하는 동작;
상기 제1인증 정보와 관련된 데이터와 상기 제2인증 정보와 관련된 데이터를 비교하는 동작; 및
상기 비교의 결과에 적어도 기반하여 상기 전자 장치에 대한 인증을 수행하는 동작을 포함하는 방법.

청구항 14

제 13항에 있어서,
상기 인증의 결과에 대응하는 알림(notification)을 제공하는 동작을 더 포함하는 방법.

청구항 15

제 13항에 있어서,
상기 제1인증 정보와 관련된 데이터는,
상기 제1인증 정보의 해시값(hash value)을 포함하며,

상기 제2인증 정보의 해시값(hash value)을 생성하는 동작을 더 포함하고,

상기 인증을 수행하는 동작은,

상기 제1인증 정보의 해시값 및 상기 제2인증 정보의 해시값이 동일한 경우, 상기 제1식별 정보가 유효한 것으로 판단하는 동작을 포함하는 방법.

발명의 설명

기술 분야

[0001] 본 실시 예는 전자 장치에 관한 것이며, 보다 상세하게는 고유한 식별 정보를 갖는 전자 장치에 관한 것이다.

배경 기술

[0003] 이동통신 기술 및 프로세서 기술의 발달에 따라 휴대용 단말 장치(이하, 전자 장치)는 종래의 통화 기능에서 나아가 다양한 기능을 구비하게 되었다. 전자 장치의 다양한 기능들은 예를 들어, 카메라 기능, 멀티 미디어 재생 기능, 다양한 어플리케이션 실행 등을 들 수 있으며, 이러한 다양한 기능들을 실행하기 위해 전자 장치는 고사양의 하드웨어 및 소프트웨어 들을 구비하게 되고, 이에 따라 전자 장치의 가격이 높아지고 있다.

[0004] 전자 장치의 제조사 및 통신사 등은 전자 장치의 식별 정보를 이용해 다양한 서비스를 제공할 수 있다. 예를 들어, OTA(over the air) 등의 무선 방식으로 전자 장치의 펌웨어(firmware) 또는 운영체제를 업데이트 할 수 있다.

발명의 내용

해결하려는 과제

[0006] 전자 장치의 가격이 높아짐에 따라 전자 장치의 업데이트 또는 프로모션을 얻기 위해, 불법적으로 다른 전자 장치의 식별 정보를 복제하여 전자 장치의 식별 정보를 위조 및 변조 하는 경우가 발생할 수 있다. 전자 장치의 식별 정보는 전자 장치 별로 고유하게 결정되는 것이나, 메모리 상에 다시 쓰기(re-write)가 가능하기 때문에 수많은 해킹 업체의 해킹 tool에 의해 도용되어 전자장치의 식별 정보를 복제한 복제폰 생성 등 치명적인 문제를 야기할 수 있다.

[0007] 종래의 전자 장치는 식별 정보의 도용을 방지하기 위해, 식별 정보를 암호화 하여 저장해 두고 있다. 실제 생산 및 유통되고 있는 전자 장치의 수는 거의 무한하다고 볼 수 있으므로, 각 전자 장치마다 상이한 암호화 키를 사용하여 식별 정보를 암호화 하는 것은 불가능 하며, 동일한 암호화 키를 사용하는 경우 보안에 취약할 수 밖에 없다.

[0008] 본 발명의 다양한 실시 예들은, 전자 장치의 고유 값인 식별 정보를 제조사 이외의 주체에 의해 악의적으로 복제되거나, 위조 및 변조 되는 것을 방지할 수 있는 방안을 제공하고자 함에 그 목적이 있다.

과제의 해결 수단

[0010] 본 발명의 다양한 실시 예에 따른 전자 장치는, 통신 인터페이스; 외부 전자 장치에 대응하는 제1식별 정보와 상기 외부 전자 장치의 통신 프로세서에 대응하는 제2식별 정보를 저장하기 위한 메모리; 및 프로세서를 포함하며, 상기 프로세서는, 상기 제1식별 정보 및 상기 제2식별 정보에 적어도 기반하여 인증 정보를 생성하고, 상기 인증 정보와 관련된 데이터의 적어도 일부를 암호화 하여 상기 인증 정보에 대응하는 전자 서명을 생성하고, 및 상기 통신 인터페이스를 이용하여 상기 전자 서명을 상기 외부 전자 장치로 전송하도록 설정될 수 있다.

[0011] 본 발명의 다양한 실시예에 따른 전자 장치가 외부 전자 장치의 인증 정보에 대응하는 전자 서명을 생성하는 방법은, 상기 외부 전자 장치에 대응하는 제1식별 정보를 수신하는 동작; 상기 외부 전자 장치의 통신 프로세서에

대응하는 제2식별 정보를 수신하는 동작; 상기 제1식별 정보 및 상기 제2식별 정보에 적어도 기반하여 인증 정보를 생성하는 동작; 상기 인증 정보와 관련된 데이터의 적어도 일부를 암호화 하여 상기 인증 정보에 대응하는 전자 서명을 생성하는 동작; 및 상기 전자 서명을 상기 외부 전자 장치로 전송하는 동작을 포함할 수 있다.

[0012] 본 발명의 다양한 실시예에 따른 전자 장치는, 통신 프로세서를 포함하는 통신 인터페이스; 상기 전자 장치에 대응하는 제1식별 정보, 상기 통신 프로세서에 대응하는 제2식별 정보, 및 외부 전자 장치로부터 수신된 전자 서명을 저장하기 위한 메모리; 및 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는, 상기 전자 서명을 복호화 하여, 상기 전자 장치에 대응하는 제1인증 정보와 관련된 데이터를 생성하고, 상기 제1식별 정보 및 상기 제2식별 정보에 적어도 기반하여 제2인증 정보와 관련된 데이터를 생성하고, 상기 제1인증 정보와 관련된 데이터와 상기 제2인증 정보와 관련된 데이터를 비교하고, 및 상기 비교의 결과에 적어도 기반하여 상기 전자 장치에 대한 인증을 수행하도록 설정될 수 있다.

[0013] 본 발명의 다양한 실시예에 따른 전자 장치가 식별 정보를 인증하는 방법은, 외부 전자 장치로부터 수신된 전자 서명을 복호화 하여, 상기 전자 장치에 대응하는 제1인증 정보와 관련된 데이터를 생성하는 동작; 상기 전자 장치에 대응하는 제1식별 정보 및 상기 전자 장치의 통신 프로세서에 대응하는 제2식별 정보에 적어도 기반하여 제2인증 정보와 관련된 데이터를 생성하는 동작; 상기 제1인증 정보와 관련된 데이터와 상기 제2인증 정보와 관련된 데이터를 비교하는 동작; 및 상기 비교의 결과에 적어도 기반하여 상기 전자 장치에 대한 인증을 수행하는 동작을 포함할 수 있다.

발명의 효과

[0015] 상술한 본 발명의 다양한 실시 예에 따르면, 전자 장치의 고유 값인 식별 정보를 제조사 이외의 주체에 의해 악의적으로 복제하거나, 위조 및 변조 하는 것을 방지할 수 있다.

도면의 간단한 설명

- [0017] 도 1은 다양한 실시예에서의 네트워크 환경 내의 전자 장치를 도시한 것이다.
- 도 2는 다양한 실시예에 따른 전자 장치의 블록도이다.
- 도 3은 다양한 실시예에 따른 프로그램 모듈의 블록도이다.
- 도 4는 본 발명의 다양한 실시예에 따른 전자 장치, 전자 서명 장치, 식별 정보 생성 장치 및 키 서버 장치를 간략히 도시한 것이다.
- 도 5는 본 발명의 다양한 실시예에 따른 전자 서명 장치의 블록도이다.
- 도 6은 본 발명의 다양한 실시예에 따른 전자 서명 장치가 전자 장치의 인증 정보에 대응하는 전자 서명을 생성하는 방법의 흐름도이다.
- 도 7은 본 발명의 다양한 실시예에 따른 전자 장치의 블록도이다.
- 도 8은 본 발명의 다양한 실시예에 따른 전자 장치가 식별 정보를 인증하는 방법의 흐름도이다.
- 도 9는 본 발명의 다양한 실시예에 따른 전자 장치의 식별 정보 인증 후 수행되는 동작들의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 이하, 본 문서의 다양한 실시예가 첨부된 도면을 참조하여 기재된다. 그러나, 이는 본 문서에 기재된 기술을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 문서의 실시예의 다양한 변경(modifications), 균등물(equivalents), 및/또는 대체물(alternatives)을 포함하는 것으로 이해되어야 한다. 도면의 설명과 관련하여, 유사한 구성요소에 대해서는 유사한 참조 부호가 사용될 수 있다.

[0019] 본 문서에서, "가진다," "가질 수 있다," "포함한다," 또는 "포함할 수 있다" 등의 표현은 해당 특징(예: 수치, 기능, 동작, 또는 부품 등의 구성요소)의 존재를 가리키며, 추가적인 특징의 존재를 배제하지 않는다.

[0020] 본 문서에서, "A 또는 B," "A 또는/및 B 중 적어도 하나," 또는 "A 또는/및 B 중 하나 또는 그 이상" 등의 표현

은 함께 나열된 항목들의 모든 가능한 조합을 포함할 수 있다. 예를 들면, "A 또는 B," "A 및 B 중 적어도 하나," 또는 "A 또는 B 중 적어도 하나"는, (1) 적어도 하나의 A를 포함, (2) 적어도 하나의 B를 포함, 또는 (3) 적어도 하나의 A 및 적어도 하나의 B 모두를 포함하는 경우를 모두 지칭할 수 있다.

[0021] 본 문서에서 사용된 "제 1," "제 2," "첫째," 또는 "둘째," 등의 표현들은 다양한 구성요소들을, 순서 및/또는 중요도에 상관없이 수식할 수 있고, 한 구성요소를 다른 구성요소와 구분하기 위해 사용될 뿐 해당 구성요소들을 한정하지 않는다. 예를 들면, 제 1 사용자 기기와 제 2 사용자 기기는, 순서 또는 중요도와 무관하게, 서로 다른 사용자 기기를 나타낼 수 있다. 예를 들면, 본 문서에 기재된 권리 범위를 벗어나지 않으면서 제 1 구성요소는 제 2 구성요소로 명명될 수 있고, 유사하게 제 2 구성요소도 제 1 구성요소로 바꾸어 명명될 수 있다.

[0022] 어떤 구성요소(예: 제 1 구성요소)가 다른 구성요소(예: 제 2 구성요소)에 "(기능적으로 또는 통신적으로) 연결되어((operatively or communicatively) coupled with/to)" 있다거나 "접속되어(connected to)" 있다고 언급된 때에는, 상기 어떤 구성요소가 상기 다른 구성요소에 직접적으로 연결되거나, 다른 구성요소(예: 제 3 구성요소)를 통하여 연결될 수 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소(예: 제 1 구성요소)가 다른 구성요소(예: 제 2 구성요소)에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 상기 어떤 구성요소와 상기 다른 구성요소 사이에 다른 구성요소(예: 제 3 구성요소)가 존재하지 않는 것으로 이해될 수 있다.

[0023] 본 문서에서 사용된 표현 "~하도록 구성된(또는 설정된)(configured to)"은 상황에 따라, 예를 들면, "~에 적합한(suitable for)," "~하는 능력을 가지는(having the capacity to)," "~하도록 설계된(designed to)," "~하도록 변경된(adapted to)," "~하도록 만들어진(made to)," 또는 "~를 할 수 있는(capable of)"과 바꾸어 사용될 수 있다. 용어 "~하도록 구성된(또는 설정된)"은 하드웨어적으로 "특별히 설계된(specifically designed to)" 것만을 반드시 의미하지 않을 수 있다. 대신, 어떤 상황에서는, "~하도록 구성된 장치"라는 표현은, 그 장치가 다른 장치 또는 부품들과 함께 "~할 수 있는" 것을 의미할 수 있다. 예를 들면, 문구 "A, B, 및 C를 수행하도록 구성된(또는 설정된) 프로세서"는 해당 동작을 수행하기 위한 전용 프로세서(예: 임베디드 프로세서), 또는 메모리 장치에 저장된 하나 이상의 소프트웨어 프로그램들을 실행함으로써, 해당 동작들을 수행할 수 있는 범용 프로세서(generic-purpose processor)(예: CPU 또는 application processor)를 의미할 수 있다.

[0024] 본 문서에서 사용된 용어들은 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 다른 실시예의 범위를 한정하려는 의도가 아닐 수 있다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함할 수 있다. 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 용어들은 본 문서에 기재된 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가질 수 있다. 본 문서에 사용된 용어들 중 일반적인 사전에 정의된 용어들은, 관련 기술의 문맥상 가지는 의미와 동일 또는 유사한 의미로 해석될 수 있으며, 본 문서에서 명백하게 정의되지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다. 경우에 따라서, 본 문서에서 정의된 용어일지라도 본 문서의 실시예들을 배제하도록 해석될 수 없다.

[0025] 본 문서의 다양한 실시예들에 따른 전자 장치는, 예를 들면, 스마트폰(smartphone), 태블릿 PC(tablet personal computer), 이동 전화기(mobile phone), 영상 전화기, 전자책 리더기(e-book reader), 데스크탑 PC(desktop personal computer), 랩탑 PC(laptop personal computer), 넷북 컴퓨터(netbook computer), 워크스테이션(workstation), 서버, PDA(personal digital assistant), PMP(portable multimedia player), MP3 플레이어, 모바일 의료기기, 카메라(camera), 또는 웨어러블 장치(wearable device) 중 적어도 하나를 포함할 수 있다. 다양한 실시예에 따르면, 웨어러블 장치는 액세서리형(예: 시계, 반지, 팔찌, 발찌, 목걸이, 안경, 콘택트 렌즈, 또는 머리 착용형 장치(head-mounted-device(HMD)), 직물 또는 의류 일체형(예: 전자 의복), 신체 부착형(예: 스킨 패드(skin pad) 또는 문신), 또는 생체 이식형(예: implantable circuit) 중 적어도 하나를 포함할 수 있다.

[0026] 어떤 실시예들에서, 전자 장치는 가전 제품(home appliance)일 수 있다. 가전 제품은, 예를 들면, 텔레비전, DVD(digital video disk) 플레이어, 오디오, 냉장고, 에어컨, 청소기, 오븐, 전자레인지, 세탁기, 공기 청정기, 셋톱 박스(set-top box), 홈 오토메이션 컨트롤 패널(home automation control panel), 보안 컨트롤 패널(security control panel), TV 박스(예: 삼성 HomeSync™, 애플TV™, 또는 구글 TV™), 게임 콘솔(예: Xbox™, PlayStation™), 전자 사전, 전자 키, 캠코더(camcorder), 또는 전자 액자 중 적어도 하나를 포함할 수 있다.

[0027] 다른 실시예에서, 전자 장치는, 각종 의료기기(예: 각종 휴대용 의료측정기기(혈당 측정기, 심박 측정기, 혈압 측정기, 또는 체온 측정기 등), MRA(magnetic resonance angiography), MRI(magnetic resonance imaging), CT(computed tomography), 촬영기, 또는 초음파기 등), 네비게이션(navigation) 장치, 위성 항법 시스템

(GNSS(global navigation satellite system)), EDR(event data recorder), FDR(flight data recorder), 자동차 인포테인먼트(infotainment) 장치, 선박용 전자 장비(예: 선박용 항법 장치, 자이로 콤팩스 등), 항공 전자 기기(avionics), 보안 기기, 차량용 헤드 유닛(head unit), 산업용 또는 가정용 로봇, 금융 기관의 ATM(automatic teller's machine), 상점의 POS(point of sales), 또는 사물 인터넷 장치(internet of things)(예: 전구, 각종 센서, 전기 또는 가스 미터기, 스프링클러 장치, 화재경보기, 온도조절기(thermostat), 가로등, 토스터(toaster), 운동기구, 온수탱크, 히터, 보일러 등) 중 적어도 하나를 포함할 수 있다.

- [0028] 어떤 실시예에 따르면, 전자 장치는 가구(furniture) 또는 건물/구조물의 일부, 전자 보드(electronic board), 전자 사인 수신 장치(electronic signature receiving device), 프로젝터(projector), 또는 각종 계측 기기(예: 수도, 전기, 가스, 또는 전파 계측 기기 등) 중 적어도 하나를 포함할 수 있다. 다양한 실시예에서, 전자 장치는 전술한 다양한 장치들 중 하나 또는 그 이상의 조합일 수 있다. 어떤 실시예에 따른 전자 장치는 플렉서블 전자 장치일 수 있다. 또한, 본 문서의 실시예에 따른 전자 장치는 전술한 기기들에 한정되지 않으며, 기술 발전에 따른 새로운 전자 장치를 포함할 수 있다.
- [0029] 이하, 첨부 도면을 참조하여, 다양한 실시예에 따른 전자 장치가 설명된다. 본 문서에서, 사용자라는 용어는 전자 장치를 사용하는 사람 또는 전자 장치를 사용하는 장치(예: 인공지능 전자 장치)를 지칭할 수 있다.
- [0030] 도 1을 참조하여, 다양한 실시예에서의, 네트워크 환경(100) 내의 전자 장치(101)가 기재된다. 전자 장치(101)는 버스(110), 프로세서(120), 메모리(130), 입출력 인터페이스(150), 디스플레이(160), 및 통신 인터페이스(170)를 포함할 수 있다. 어떤 실시예에서는, 전자 장치(101)는, 구성요소들 중 적어도 하나를 생략하거나 다른 구성요소를 추가적으로 구비할 수 있다.
- [0031] 버스(110)는, 예를 들면, 구성요소들(110-170)을 서로 연결하고, 구성요소들 간의 통신(예: 제어 메시지 및/또는 데이터)을 전달하는 회로를 포함할 수 있다.
- [0032] 프로세서(120)는, 중앙처리장치(central processing unit(CPU)), 어플리케이션 프로세서(application processor(AP)), 또는 커뮤니케이션 프로세서(communication processor(CP)) 중 하나 또는 그 이상을 포함할 수 있다. 프로세서(120)는, 예를 들면, 전자 장치(101)의 적어도 하나의 다른 구성요소들의 제어 및/또는 통신에 관한 연산이나 데이터 처리를 실행할 수 있다.
- [0033] 메모리(130)는, 휘발성 및/또는 비휘발성 메모리를 포함할 수 있다. 메모리(130)는, 예를 들면, 전자 장치(101)의 적어도 하나의 다른 구성요소에 관계된 명령 또는 데이터를 저장할 수 있다. 한 실시예에 따르면, 메모리(130)는 소프트웨어 및/또는 프로그램(140)을 저장할 수 있다. 프로그램(140)은, 예를 들면, 커널(kernel)(141), 미들웨어(middleware)(143), 어플리케이션 프로그래밍 인터페이스(application programming interface(API))(145), 및/또는 어플리케이션 프로그램(또는 "어플리케이션")(147) 등을 포함할 수 있다. 커널(kernel)(141), 미들웨어(middleware)(143), 또는 API(API)(145)의 적어도 일부는, 운영 시스템(operating system(OS))으로 지칭될 수 있다.
- [0034] 커널(kernel)(141)은, 예를 들면, 다른 프로그램들(예: 미들웨어(middleware)(143), API(API)(145), 또는 어플리케이션 프로그램(application program)(147))에 구현된 동작 또는 기능을 실행하는 데 사용되는 시스템 리소스들(예: 버스(bus)(110), 프로세서(processor)(120), 또는 메모리(memory)(130) 등)을 제어 또는 관리할 수 있다. 또한, 커널(kernel)(141)은 미들웨어(middleware)(143), API(API)(145), 또는 어플리케이션 프로그램(application program)(147)에서 전자 장치(101)의 개별 구성요소에 접근함으로써, 시스템 리소스들을 제어 또는 관리할 수 있는 인터페이스를 제공할 수 있다.
- [0035] 미들웨어(middleware)(143)는, 예를 들면, API(API)(145) 또는 어플리케이션 프로그램(application program)(147)이 커널(kernel)(141)과 통신하여 데이터를 주고받을 수 있도록 중개 역할을 수행할 수 있다.
- [0036] 또한, 미들웨어(middleware)(143)는 어플리케이션 프로그램(application program)(147)으로부터 수신된 하나 이상의 작업 요청들을 우선 순위에 따라 처리할 수 있다. 예를 들면, 미들웨어(middleware)(143)는 어플리케이션 프로그램(application program)(147) 중 적어도 하나에 전자 장치(101)의 시스템 리소스(예: 버스(bus)(110), 프로세서(processor)(120), 또는 메모리(memory)(130) 등)를 사용할 수 있는 우선 순위를 부여할 수 있다. 예컨대, 미들웨어(middleware)(143)는 상기 적어도 하나에 부여된 우선 순위에 따라 상기 하나 이상의 작업 요청들을 처리함으로써, 상기 하나 이상의 작업 요청들에 대한 스케줄링 또는 로드 밸런싱 등을 수행할 수 있다.
- [0037] API(API)(145)는, 예를 들면, 어플리케이션(application)(147)이 커널(kernel)(141) 또는 미들웨어(middleware)(143)에서 제공되는 기능을 제어하기 위한 인터페이스로, 예를 들면, 파일 제어, 창 제어, 영상 처리, 또는 문자 제어 등을 위한 적어도 하나의 인터페이스 또는 함수(예: 명령어)를 포함할 수 있다.
- [0038] 입출력 인터페이스(input/output interface)(150)는, 예를 들면, 사용자 또는 다른 외부 기기로부터 입력된 명령 또는 데이터를 전자 장

치(101)의 다른 구성요소(들)에 전달할 수 있는 인터페이스의 역할을 할 수 있다. 또한, 입출력 인터페이스(150)는 전자 장치(101)의 다른 구성요소(들)로부터 수신된 명령 또는 데이터를 사용자 또는 다른 외부 기기로 출력할 수 있다.

[0039] 디스플레이(160)는, 예를 들면, 액정 디스플레이(liquid crystal display(LCD)), 발광 다이오드(light-emitting diode(LED)) 디스플레이, 유기 발광 다이오드(organic light-emitting diode(OLED)) 디스플레이, 또는 마이크로 전자기계 시스템(microelectromechanical systems(MEMS)) 디스플레이, 또는 전자종이(electronic paper) 디스플레이를 포함할 수 있다. 디스플레이(160)는, 예를 들면, 사용자에게 각종 콘텐츠(예: 텍스트, 이미지, 비디오, 아이콘, 또는 심볼 등)를 표시할 수 있다. 디스플레이(160)는, 터치 스크린을 포함할 수 있으며, 예를 들면, 전자 펜 또는 사용자의 신체의 일부를 이용한 터치, 제스처, 근접, 또는 호버링 입력을 수신할 수 있다.

[0040] 통신 인터페이스(170)는, 예를 들면, 전자 장치(101)와 외부 장치(예: 제 1 외부 전자 장치(102), 제 2 외부 전자 장치(104), 또는 서버(106)) 간의 통신을 설정할 수 있다. 예를 들면, 통신 인터페이스(170)는 무선 통신 또는 유선 통신을 통해서 네트워크(162)에 연결되어 외부 장치(예: 제 2 외부 전자 장치(104) 또는 서버(106))와 통신할 수 있다.

[0041] 무선 통신은, 예를 들면, 셀룰러 통신 프로토콜로서, 예를 들면, LTE(long-term evolution), LTE-A(LTE Advance), CDMA(code division multiple access), WCDMA(wideband CDMA), UMTS(universal mobile telecommunications system), WiBro(Wireless Broadband), 또는 GSM(Global System for Mobile Communications) 등 중 적어도 하나를 사용할 수 있다. 또한, 무선 통신은, 예를 들면, 근거리 통신(164)을 포함할 수 있다. 근거리 통신(164)은, 예를 들면, WiFi(wireless fidelity), 블루투스(Bluetooth), NFC(near field communication), 또는 GNSS(global navigation satellite system) 등 중 적어도 하나를 포함할 수 있다. GNSS는 사용 지역 또는 대역폭 등에 따라, 예를 들면, GPS(Global Positioning System), Glonass(Global Navigation Satellite System), Beidou Navigation Satellite System(이하 “Beidou”) 또는 Galileo, the European global satellite-based navigation system 중 적어도 하나를 포함할 수 있다. 이하, 본 문서에서는, “GPS”는 “GNSS”와 혼용되어 사용(interchangeably used)될 수 있다. 유선 통신은, 예를 들면, USB(universal serial bus), HDMI(high definition multimedia interface), RS-232(recommended standard232), 또는 POTS(plain old telephone service) 등 중 적어도 하나를 포함할 수 있다. 네트워크(162)는 통신 네트워크(telecommunications network), 예를 들면, 컴퓨터 네트워크(computer network)(예: LAN 또는 WAN), 인터넷, 또는 전화 망(telephone network) 중 적어도 하나를 포함할 수 있다.

[0042] 제 1 및 제 2 외부 전자 장치(102, 104) 각각은 전자 장치(101)와 동일한 또는 다른 종류의 장치일 수 있다. 한 실시예에 따르면, 서버(106)는 하나 또는 그 이상의 서버들의 그룹을 포함할 수 있다. 다양한 실시예에 따르면, 전자 장치(101)에서 실행되는 동작들의 전부 또는 일부는 다른 하나 또는 복수의 전자 장치(예: 전자 장치(102, 104), 또는 서버(106))에서 실행될 수 있다. 한 실시예에 따르면, 전자 장치(101)가 어떤 기능이나 서비스를 자동으로 또는 요청에 의하여 수행해야 할 경우에, 전자 장치(101)는 기능 또는 서비스를 자체적으로 실행시키는 대신에 또는 추가적으로, 그와 연관된 적어도 일부 기능을 다른 장치(예: 전자 장치(102, 104), 또는 서버(106))에게 요청할 수 있다. 다른 전자 장치(예: 전자 장치(102, 104), 또는 서버(106))는 요청된 기능 또는 추가 기능을 실행하고, 그 결과를 전자 장치(101)로 전달할 수 있다. 전자 장치(101)는 수신된 결과를 그대로 또는 추가적으로 처리하여 요청된 기능이나 서비스를 제공할 수 있다. 이를 위하여, 예를 들면, 클라우드 컴퓨팅, 분산 컴퓨팅, 또는 클라이언트-서버 컴퓨팅 기술이 이용될 수 있다.

[0043] 도 2는 다양한 실시예에 따른 전자 장치(201)의 블록도이다. 전자 장치(201)는, 예를 들면, 도 1에 도시된 전자 장치(101)의 전체 또는 일부를 포함할 수 있다. 전자 장치(201)는 하나 이상의 프로세서(예: AP(application processor))(210), 통신 모듈(220), 가입자 식별 모듈(224), 메모리(230), 센서 모듈(240), 입력 장치(250), 디스플레이(260), 인터페이스(270), 오디오 모듈(280), 카메라 모듈(291), 전력 관리 모듈(295), 배터리(296), 인디케이터(297), 및 모터(298)를 포함할 수 있다.

[0044] 프로세서(210)는, 예를 들면, 운영 체제 또는 응용 프로그램을 구동하여 프로세서(210)에 연결된 다수의 하드웨어 또는 소프트웨어 구성요소들을 제어할 수 있고, 각종 데이터 처리 및 연산을 수행할 수 있다. 프로세서(210)는, 예를 들면, SoC(system on chip)로 구현될 수 있다. 한 실시예에 따르면, 프로세서(210)는 GPU(graphic processing unit) 및/또는 이미지 신호 프로세서(image signal processor)를 더 포함할 수 있다. 프로세서(210)는 도 2에 도시된 구성요소들 중 적어도 일부(예: 셀룰러 모듈(221))를 포함할 수도 있다. 프로세서(210)

는 다른 구성요소들(예: 비휘발성 메모리) 중 적어도 하나로부터 수신된 명령 또는 데이터를 휘발성 메모리에 로드(load)하여 처리하고, 다양한 데이터를 비휘발성 메모리에 저장(store)할 수 있다.

- [0045] 통신 모듈(220)은, 도 1의 통신 인터페이스(170)와 동일 또는 유사한 구성을 가질 수 있다. 통신 모듈(220)은, 예를 들면, 셀룰러 모듈(221), WiFi 모듈(223), 블루투스 모듈(225), GNSS 모듈(227)(예: GPS 모듈, Glonass 모듈, Beidou 모듈, 또는 Galileo 모듈), NFC 모듈(228) 및 RF(radio frequency) 모듈(229)를 포함할 수 있다.
- [0046] 셀룰러 모듈(221)은, 예를 들면, 통신망을 통해서 음성 통화, 영상 통화, 문자 서비스, 또는 인터넷 서비스 등을 제공할 수 있다. 한 실시예에 따르면, 셀룰러 모듈(221)은 가입자 식별 모듈(예: SIM 카드)(224)을 이용하여 통신 네트워크 내에서 전자 장치(201)의 구별 및 인증을 수행할 수 있다. 한 실시예에 따르면, 셀룰러 모듈(221)은 프로세서(210)가 제공할 수 있는 기능 중 적어도 일부 기능을 수행할 수 있다. 한 실시예에 따르면, 셀룰러 모듈(221)은 커뮤니케이션 프로세서(CP: communication processor)를 포함할 수 있다.
- [0047] WiFi 모듈(223), 블루투스 모듈(225), GNSS 모듈(227) 또는 NFC 모듈(228) 각각은, 예를 들면, 해당하는 모듈을 통해서 송수신되는 데이터를 처리하기 위한 프로세서를 포함할 수 있다. 어떤 실시예에 따르면, 셀룰러 모듈(221), WiFi 모듈(223), 블루투스 모듈(225), GNSS 모듈(227) 또는 NFC 모듈(228) 중 적어도 일부(예: 두 개 이상)는 하나의 integrated chip(IC) 또는 IC 패키지 내에 포함될 수 있다.
- [0048] RF 모듈(229)은, 예를 들면, 통신 신호(예: RF 신호)를 송수신할 수 있다. RF 모듈(229)은, 예를 들면, 트랜시버(transceiver), PAM(power amp module), 주파수 필터(frequency filter), LNA(low noise amplifier), 또는 안테나 등을 포함할 수 있다. 다른 실시예에 따르면, 셀룰러 모듈(221), WiFi 모듈(223), 블루투스 모듈(225), GNSS 모듈(227) 또는 NFC 모듈(228) 중 적어도 하나는 별개의 RF 모듈을 통하여 RF 신호를 송수신할 수 있다.
- [0049] 가입자 식별 모듈(224)은, 예를 들면, 가입자 식별 모듈을 포함하는 카드 및/또는 내장 SIM(embedded SIM)을 포함할 수 있으며, 고유한 식별 정보(예: ICCID(integrated circuit card identifier)) 또는 가입자 정보(예: IMSI(international mobile subscriber identity))를 포함할 수 있다.
- [0050] 메모리(230)(예: 메모리(130))는, 예를 들면, 내장 메모리(232) 또는 외장 메모리(234)를 포함할 수 있다. 내장 메모리(232)는, 예를 들면, 휘발성 메모리(예: DRAM(dynamic RAM), SRAM(static RAM), 또는 SDRAM(synchronous dynamic RAM) 등), 비휘발성 메모리(non-volatile Memory)(예: OTPROM(one time programmable ROM), PROM(programmable ROM), EPROM(erasable and programmable ROM), EEPROM(electrically erasable and programmable ROM), mask ROM, flash ROM, 플래시 메모리(예: NAND flash 또는 NOR flash 등), 하드 드라이브, 또는 솔리드 스테이트 드라이브(solid state drive(SSD)) 중 적어도 하나를 포함할 수 있다.
- [0051] 외장 메모리(234)는 플래시 드라이브(flash drive), 예를 들면, CF(compact flash), SD(secure digital), Micro-SD(micro secure digital), Mini-SD(mini secure digital), xD(extreme digital), MMC(multi-media card) 또는 메모리 스틱(memory stick) 등을 더 포함할 수 있다. 외장 메모리(234)는 다양한 인터페이스를 통하여 전자 장치(201)와 기능적으로 및/또는 물리적으로 연결될 수 있다.
- [0052] 센서 모듈(240)은, 예를 들면, 물리량을 측정하거나 전자 장치(201)의 작동 상태를 감지하여, 측정 또는 감지된 정보를 전기 신호로 변환할 수 있다. 센서 모듈(240)은, 예를 들면, 제스처 센서(240A), 자이로 센서(240B), 기압 센서(240C), 마그네틱 센서(240D), 가속도 센서(240E), 그림 센서(240F), 근접 센서(240G), 컬러(color) 센서(240H)(예: RGB(red, green, blue) 센서), 생체 센서(240I), 온/습도 센서(240J), 조도 센서(240K), 또는 UV(ultra violet) 센서(240M) 중의 적어도 하나를 포함할 수 있다. 추가적으로 또는 대체적으로(additionally or alternatively), 센서 모듈(240)은, 예를 들면, 후각 센서(E-nose sensor), EMG 센서(electromyography sensor), EEG 센서(electroencephalogram sensor), ECG 센서(electrocardiogram sensor), IR(infrared) 센서, 홍채 센서 및/또는 지문 센서를 포함할 수 있다. 센서 모듈(240)은 그 안에 속한 적어도 하나 이상의 센서들을 제어하기 위한 제어 회로를 더 포함할 수 있다. 어떤 실시예에서는, 전자 장치(201)는 프로세서(210)의 일부로서 또는 별도로, 센서 모듈(240)을 제어하도록 구성된 프로세서를 더 포함하여, 프로세서(210)가 슬립(sleep) 상태에 있는 동안, 센서 모듈(240)을 제어할 수 있다.
- [0053] 입력 장치(250)는, 예를 들면, 터치 패널(touch panel)(252),(디지털) 펜 센서(pen sensor)(254), 키(key)(256), 또는 초음파(ultrasonic) 입력 장치(258)를 포함할 수 있다. 터치 패널(252)은, 예를 들면, 정전식, 감압식, 적외선 방식, 또는 초음파 방식 중 적어도 하나의 방식을 사용할 수 있다. 또한, 터치 패널(252)은 제어 회로를 더 포함할 수도 있다. 터치 패널(252)은 텍타일 레이어(tactile layer)를 더 포함하여, 사용자에게 촉각 반응을 제공할 수 있다.

- [0054] (디지털) 펜 센서(254)는, 예를 들면, 터치 패널의 일부이거나, 별도의 인식용 쉬트(sheet)를 포함할 수 있다. 키(256)는, 예를 들면, 물리적인 버튼, 광학식 키, 또는 키패드를 포함할 수 있다. 초음파 입력 장치(258)는 마이크(예: 마이크(288))를 통해, 입력 도구에서 발생된 초음파를 감지하여, 상기 감지된 초음파에 대응하는 데이터를 확인할 수 있다.
- [0055] 디스플레이(260)(예: 디스플레이(160))는 패널(262), 홀로그램 장치(264), 또는 프로젝터(266)를 포함할 수 있다. 패널(262)은, 도 1의 디스플레이(160)와 동일 또는 유사한 구성을 포함할 수 있다. 패널(262)은, 예를 들면, 유연하게(flexible), 투명하게(transparent), 또는 착용할 수 있게(wearable) 구현될 수 있다. 패널(262)은 터치 패널(252)과 하나의 모듈로 구성될 수도 있다. 홀로그램 장치(264)는 빛의 간섭을 이용하여 입체 영상을 허공에 보여줄 수 있다. 프로젝터(266)는 스크린에 빛을 투사하여 영상을 표시할 수 있다. 스크린은, 예를 들면, 전자 장치(201)의 내부 또는 외부에 위치할 수 있다. 한 실시예에 따르면, 디스플레이(260)는 패널(262), 홀로그램 장치(264), 또는 프로젝터(266)를 제어하기 위한 제어 회로를 더 포함할 수 있다.
- [0056] 인터페이스(270)는, 예를 들면, HDMI(high-definition multimedia interface)(272), USB(universal serial bus)(274), 광 인터페이스(optical interface)(276), 또는 D-sub(D-subminiature)(278)를 포함할 수 있다. 인터페이스(270)는, 예를 들면, 도 1에 도시된 통신 인터페이스(170)에 포함될 수 있다. 추가적으로 또는 대체적으로(additionally and alternatively), 인터페이스(270)는, 예를 들면, MHL(mobile high-definition link) 인터페이스, SD(secure digital) 카드/MMC(multi-media card) 인터페이스, 또는 IrDA(infrared data association) 규격 인터페이스를 포함할 수 있다.
- [0057] 오디오 모듈(280)은, 예를 들면, 소리(sound)와 전기 신호를 쌍방향으로 변환시킬 수 있다. 오디오 모듈(280)의 적어도 일부 구성요소는, 예를 들면, 도 1에 도시된 입력력 인터페이스(145)에 포함될 수 있다. 오디오 모듈(280)은, 예를 들면, 스피커(282), 리시버(284), 이어폰(286), 또는 마이크(288) 등을 통해 입력 또는 출력되는 소리 정보를 처리할 수 있다.
- [0058] 카메라 모듈(291)은, 예를 들면, 정지 영상 및 동영상을 촬영할 수 있는 장치로서, 한 실시예에 따르면, 하나 이상의 이미지 센서(예: 전면 센서 또는 후면 센서), 렌즈, ISP(image signal processor), 또는 플래시(flash)(예: LED 또는 xenon lamp 등)를 포함할 수 있다.
- [0059] 전력 관리 모듈(295)은, 예를 들면, 전자 장치(201)의 전력을 관리할 수 있다. 한 실시예에 따르면, 전력 관리 모듈(295)은 PMIC(power management integrated circuit), 충전 IC(charger integrated circuit), 또는 배터리 또는 연료 게이지(battery or fuel gauge)를 포함할 수 있다. PMIC는, 유선 및/또는 무선 충전 방식을 가질 수 있다. 무선 충전 방식은, 예를 들면, 자기공명 방식, 자기유도 방식 또는 전자기파 방식 등을 포함하며, 무선 충전을 위한 부가적인 회로, 예를 들면, 코일 루프, 공진 회로, 또는 정류기 등을 더 포함할 수 있다. 배터리 게이지는, 예를 들면, 배터리(296)의 잔량, 충전 중 전압, 전류, 또는 온도를 측정할 수 있다. 배터리(296)는, 예를 들면, 충전식 전지(rechargeable battery) 및/또는 태양 전지(solar battery)를 포함할 수 있다.
- [0060] 인디케이터(297)는 전자 장치(201) 또는 그 일부(예: 프로세서(210))의 특정 상태, 예를 들면, 부팅 상태, 메시지 상태 또는 충전 상태 등을 표시할 수 있다. 모터(298)는 전기적 신호를 기계적 진동으로 변환할 수 있고, 진동(vibration), 또는 햅틱(haptic) 효과 등을 발생시킬 수 있다. 도시되지는 않았으나, 전자 장치(201)는 모바일 TV 지원을 위한 처리 장치(예: GPU)를 포함할 수 있다. 모바일 TV 지원을 위한 처리 장치는, 예를 들면, DMB(digital multimedia broadcasting), DVB(digital video broadcasting), 또는 미디어플로(mediaFlo™) 등의 규격에 따른 미디어 데이터를 처리할 수 있다.
- [0061] 본 문서에서 기술된 구성요소들 각각은 하나 또는 그 이상의 부품(component)으로 구성될 수 있으며, 해당 구성요소의 명칭은 전자 장치의 종류에 따라서 달라질 수 있다. 다양한 실시예에서, 전자 장치는 본 문서에서 기술된 구성요소 중 적어도 하나를 포함하여 구성될 수 있으며, 일부 구성요소가 생략되거나 또는 추가적인 다른 구성요소를 더 포함할 수 있다. 또한, 다양한 실시예에 따른 전자 장치의 구성요소들 중 일부가 결합되어 하나의 개체(entity)로 구성됨으로써, 결합되기 이전의 해당 구성요소들의 기능을 동일하게 수행할 수 있다.
- [0062] 도 3은 다양한 실시예에 따른 프로그램 모듈의 블록도이다. 한 실시예에 따르면, 프로그램 모듈(310)(예: 프로그램(140))은 전자 장치(예: 전자 장치(101))에 관련된 자원을 제어하는 운영 체제(operating system(OS)) 및/또는 운영 체제 상에서 구동되는 다양한 어플리케이션(예: 어플리케이션 프로그램(147))을 포함할 수 있다. 운영 체제는, 예를 들면, 안드로이드(android), iOS, 윈도우즈(windows), 심비안(symbian), 타이젠(tizen), 또는 바다(bada) 등이 될 수 있다.

- [0063] 프로그램 모듈(310)은 커널(320), 미들웨어(330), 어플리케이션 프로그래밍 인터페이스(application programming interface (API))(360), 및/또는 어플리케이션(370)을 포함할 수 있다. 프로그램 모듈(310)의 적어도 일부는 전자 장치 상에 프리로드(preload) 되거나, 외부 전자 장치(예: 전자 장치(102, 104), 서버(106) 등)로부터 다운로드(download) 가능하다.
- [0064] 커널(320)(예: 커널(141))은, 예를 들면, 시스템 리소스 매니저(321) 및/또는 디바이스 드라이버(323)를 포함할 수 있다. 시스템 리소스 매니저(321)는 시스템 리소스의 제어, 할당, 또는 회수 등을 수행할 수 있다. 한 실시예에 따르면, 시스템 리소스 매니저(321)는 프로세스 관리부, 메모리 관리부, 또는 파일 시스템 관리부 등을 포함할 수 있다. 디바이스 드라이버(323)는, 예를 들면, 디스플레이 드라이버, 카메라 드라이버, 블루투스 드라이버, 공유 메모리 드라이버, USB 드라이버, 키패드 드라이버, WiFi 드라이버, 오디오 드라이버, 또는 IPC(inter-process communication) 드라이버를 포함할 수 있다.
- [0065] 미들웨어(330)는, 예를 들면, 어플리케이션(370)이 공통적으로 필요로 하는 기능을 제공하거나, 어플리케이션(370)이 전자 장치 내부의 제한된 시스템 자원을 효율적으로 사용할 수 있도록 API(360)를 통해 다양한 기능들을 어플리케이션(370)으로 제공할 수 있다. 한 실시예에 따르면, 미들웨어(330)(예: 미들웨어(143))는 런타임 라이브러리(335), 어플리케이션 매니저(application manager)(341), 윈도우 매니저(window manager)(342), 멀티미디어 매니저(multimedia manager)(343), 리소스 매니저(resource manager)(344), 파워 매니저(power manager)(345), 데이터베이스 매니저(database manager)(346), 패키지 매니저(package manager)(347), 연결 매니저(connectivity manager)(348), 통지 매니저(notification manager)(349), 위치 매니저(location manager)(350), 그래픽 매니저(graphic manager)(351), 또는 보안 매니저(security manager)(352) 중 적어도 하나를 포함할 수 있다.
- [0066] 런타임 라이브러리(335)는, 예를 들면, 어플리케이션(370)이 실행되는 동안에 프로그래밍 언어를 통해 새로운 기능을 추가하기 위해 컴파일러가 사용하는 라이브러리 모듈을 포함할 수 있다. 런타임 라이브러리(335)는 입출력 관리, 메모리 관리, 또는 산술 함수에 대한 기능 등을 수행할 수 있다.
- [0067] 어플리케이션 매니저(341)는, 예를 들면, 어플리케이션(370) 중 적어도 하나의 어플리케이션의 생명 주기(life cycle)를 관리할 수 있다. 윈도우 매니저(342)는 화면에서 사용하는 GUI 자원을 관리할 수 있다. 멀티미디어 매니저(343)는 다양한 미디어 파일들의 재생에 필요한 포맷을 파악하고, 해당 포맷에 맞는 코덱(codec)을 이용하여 미디어 파일의 인코딩(encoding) 또는 디코딩(decoding)을 수행할 수 있다. 리소스 매니저(344)는 어플리케이션(370) 중 적어도 어느 하나의 어플리케이션의 소스 코드, 메모리 또는 저장 공간 등의 자원을 관리할 수 있다.
- [0068] 파워 매니저(345)는, 예를 들면, 바이오스(BIOS: basic input/output system) 등과 함께 동작하여 배터리(battery) 또는 전원을 관리하고, 전자 장치의 동작에 필요한 전력 정보 등을 제공할 수 있다. 데이터베이스 매니저(346)는 어플리케이션(370) 중 적어도 하나의 어플리케이션에서 사용할 데이터베이스를 생성, 검색, 또는 변경할 수 있다. 패키지 매니저(347)는 패키지 파일의 형태로 배포되는 어플리케이션의 설치 또는 업데이트를 관리할 수 있다.
- [0069] 연결 매니저(348)는, 예를 들면, WiFi 또는 블루투스 등의 무선 연결을 관리할 수 있다. 통지 매니저(349)는 도착 메시지, 약속, 근접성 알람 등의 사건(event)을 사용자에게 방해되지 않는 방식으로 표시 또는 통지할 수 있다. 위치 매니저(350)는 전자 장치의 위치 정보를 관리할 수 있다. 그래픽 매니저(351)는 사용자에게 제공될 그래픽 효과 또는 이와 관련된 사용자 인터페이스를 관리할 수 있다. 보안 매니저(352)는 시스템 보안 또는 사용자 인증 등에 필요한 제반 보안 기능을 제공할 수 있다. 한 실시예에 따르면, 전자 장치(예: 전자 장치(101))가 전화 기능을 포함한 경우, 미들웨어(330)는 전자 장치의 음성 또는 영상 통화 기능을 관리하기 위한 통화 매니저(telephony manager)를 더 포함할 수 있다.
- [0070] 미들웨어(330)는 전문화된 구성요소들의 다양한 기능의 조합을 형성하는 미들웨어 모듈을 포함할 수 있다. 미들웨어(330)는 차별화된 기능을 제공하기 위해 운영 체제의 종류 별로 특화된 모듈을 제공할 수 있다. 또한, 미들웨어(330)는 동적으로 기존의 구성요소를 일부 삭제하거나 새로운 구성요소들을 추가할 수 있다.
- [0071] API(360)(예: API(145))는, 예를 들면, API 프로그래밍 함수들의 집합으로, 운영 체제에 따라 다른 구성으로 제공될 수 있다. 예를 들면, 안드로이드 또는 iOS의 경우, 플랫폼 별로 하나의 API 셋을 제공할 수 있으며, 타이젠(tizen)의 경우, 플랫폼 별로 두 개 이상의 API 셋을 제공할 수 있다.
- [0072] 어플리케이션(370)(예: 어플리케이션 프로그램(147))은, 예를 들면, 홈(371), 다이얼러(372), SMS/MMS(373),

IM(instant message)(374), 브라우저(375), 카메라(376), 알람(377), 컨택트(378), 음성 다이얼(379), 이메일(380), 달력(381), 미디어 플레이어(382), 앨범(383), 또는 시계(384), 건강 관리(health care)(예: 운동량 또는 혈당 등을 측정), 또는 환경 정보 제공(예: 기압, 습도, 또는 온도 정보 등을 제공) 등의 기능을 수행할 수 있는 하나 이상의 어플리케이션을 포함할 수 있다.

[0073] 한 실시예에 따르면, 어플리케이션(370)은 전자 장치(예: 전자 장치(101))와 외부 전자 장치(예: 전자 장치(102, 104)) 사이의 정보 교환을 지원하는 어플리케이션(이하, 설명의 편의 상, "정보 교환 어플리케이션")을 포함할 수 있다. 정보 교환 어플리케이션은, 예를 들면, 외부 전자 장치에 특정 정보를 전달하기 위한 알림 전달(notification relay) 어플리케이션, 또는 외부 전자 장치를 관리하기 위한 장치 관리(device management) 어플리케이션을 포함할 수 있다.

[0074] 예를 들면, 알림 전달 어플리케이션은 전자 장치의 다른 어플리케이션(예: SMS/MMS 어플리케이션, 이메일 어플리케이션, 건강 관리 어플리케이션, 또는 환경 정보 어플리케이션 등)에서 발생한 알림 정보를 외부 전자 장치(예: 전자 장치(102, 104))로 전달하는 기능을 포함할 수 있다. 또한, 알림 전달 어플리케이션은, 예를 들면, 외부 전자 장치로부터 알림 정보를 수신하여 사용자에게 제공할 수 있다.

[0075] 장치 관리 어플리케이션은, 예를 들면, 전자 장치와 통신하는 외부 전자 장치(예: 전자 장치(102, 104))의 적어도 하나의 기능(예: 외부 전자 장치 자체(또는, 일부 구성 부품)의 턴-온/턴-오프 또는 디스플레이의 밝기(또는, 해상도) 조절), 외부 전자 장치에서 동작하는 어플리케이션 또는 외부 전자 장치에서 제공되는 서비스(예: 통화 서비스 또는 메시지 서비스 등)를 관리(예: 설치, 삭제, 또는 업데이트)할 수 있다.

[0076] 한 실시예에 따르면, 어플리케이션(370)은 외부 전자 장치(예: 전자 장치(102, 104))의 속성(에 따라 지정된 어플리케이션(예: 모바일 의료 기기의 건강 관리 어플리케이션 등)을 포함할 수 있다. 한 실시예에 따르면, 어플리케이션(370)은 외부 전자 장치(예: 서버(106) 또는 전자 장치(102, 104))로부터 수신된 어플리케이션을 포함할 수 있다. 한 실시예에 따르면, 어플리케이션(370)은 프리로드 어플리케이션(preloaded application) 또는 서버로부터 다운로드 가능한 제3자 어플리케이션(third party application)을 포함할 수 있다. 도시된 실시예에 따른 프로그램 모듈(310)의 구성요소들의 명칭은 운영 체제의 종류에 따라서 달라질 수 있다.

[0077] 다양한 실시예에 따르면, 프로그램 모듈(310)의 적어도 일부는 소프트웨어, 펌웨어, 하드웨어, 또는 이들 중 적어도 둘 이상의 조합으로 구현될 수 있다. 프로그램 모듈(310)의 적어도 일부는, 예를 들면, 프로세서(예: 프로세서(210))에 의해 구현(implement)(예: 실행)될 수 있다. 프로그램 모듈(310)의 적어도 일부는 하나 이상의 기능을 수행하기 위한, 예를 들면, 모듈, 프로그램, 루틴, 명령어 세트(sets of instructions) 또는 프로세스 등을 포함할 수 있다.

[0078] 본 문서에서 사용된 용어 "모듈"은, 예를 들면, 하드웨어, 소프트웨어 또는 펌웨어(firmware) 중 하나 또는 둘 이상의 조합을 포함하는 단위(unit)를 의미할 수 있다. "모듈"은, 예를 들면, 유닛(unit), 로직(logic), 논리 블록(logical block), 부품(component), 또는 회로(circuit) 등의 용어와 바꾸어 사용(interchangeably use)될 수 있다. "모듈"은, 일체로 구성된 부품의 최소 단위 또는 그 일부가 될 수 있다. "모듈"은 하나 또는 그 이상의 기능을 수행하는 최소 단위 또는 그 일부가 될 수도 있다. "모듈"은 기계적으로 또는 전자적으로 구현될 수 있다. 예를 들면, "모듈"은, 알려졌거나 앞으로 개발될, 어떤 동작들을 수행하는 ASIC(application-specific integrated circuit) 칩, FPGAs(field-programmable gate arrays) 또는 프로그램 가능 논리 장치(programmable-logic device) 중 적어도 하나를 포함할 수 있다.

[0079] 다양한 실시예에 따른 장치(예: 모듈들 또는 그 기능들) 또는 방법(예: 동작들)의 적어도 일부는, 예컨대, 프로그램 모듈의 형태로 컴퓨터로 읽을 수 있는 저장매체(computer-readable storage media)에 저장된 명령어로 구현될 수 있다. 상기 명령어가 프로세서(예: 프로세서(120))에 의해 실행될 경우, 상기 하나 이상의 프로세서가 상기 명령어에 해당하는 기능을 수행할 수 있다. 컴퓨터로 읽을 수 있는 저장매체는, 예를 들면, 메모리(130)가 될 수 있다.

[0080] 컴퓨터로 판독 가능한 기록 매체는, 하드디스크, 플로피디스크, 마그네틱 매체(magnetic media)(예: 자기테이프), 광기록 매체(optical media)(예: CD-ROM(compact disc read only memory), DVD(digital versatile disc), 자기-광 매체(magneto-optical media)(예: 플롭티컬 디스크(floptical disk))), 하드웨어 장치(예: ROM(read only memory), RAM(random access memory), 또는 플래시 메모리 등) 등을 포함할 수 있다. 또한, 프로그램 명령어는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다. 상술한 하드웨어 장치는 다양한 실시예

의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지다.

- [0081] 다양한 실시예에 따른 모듈 또는 프로그램 모듈은 전술한 구성요소들 중 적어도 하나 이상을 포함하거나, 일부가 생략되거나, 또는 추가적인 다른 구성요소를 더 포함할 수 있다. 다양한 실시예에 따른 모듈, 프로그램 모듈 또는 다른 구성요소에 의해 수행되는 동작들은 순차적, 병렬적, 반복적 또는 휴리스틱(heuristic)한 방법으로 실행될 수 있다. 또한, 일부 동작은 다른 순서로 실행되거나, 생략되거나, 또는 다른 동작이 추가될 수 있다. 그리고 본 문서에 개시된 실시예는 개시된, 기술 내용의 설명 및 이해를 위해 제시된 것이며, 본 문서에서 기재된 기술의 범위를 한정하는 것은 아니다. 따라서, 본 문서의 범위는, 본 문서의 기술적 사상에 근거한 모든 변경 또는 다양한 다른 실시예를 포함하는 것으로 해석되어야 한다.
- [0083] 이하에서는, 전자 장치의 식별 정보의 위조 및 변조를 방지하기 위한 본 발명의 다양한 실시예들에 대해 보다 구체적으로 설명하기로 한다.
- [0084] 본 발명의 다양한 실시예에 따르면, 전자 장치의 식별 정보는 국제 모바일 기기 식별코드(international mobile equipment identity, 이하 IMEI)를 예로 들 수 있다. IMEI는 GSMA(global system for mobile communications association)의 가이드라인에 따라 모든 모바일 전자 장치에 부여되는 것으로써, 식별정보 생성 장치에 의해 생성되어 전자 장치의 제조 시에 부여될 수 있다. IMEI는 10진수로써 전자 장치의 제조사 별로 구별되는 2자리, 제조사의 모델 별(또는 device type)로 구별되는 6자리, 각 전자 장치 별 시리얼 값 6자리 및 체크섬(checksum) 1자리로 총 15자리의 숫자로 구성되며, 3GPP에 DB로 등록 및 관리 될 수 있다.
- [0085] 이러한 IMEI는 전자 장치 별로 구분되는 것으로써, 이동통신 망에서 가입자를 구분하기 위한 IMSI(International mobile subscriber identifier), MIN(mobile identify number), MDN(mobile directory number) 등과 구분될 수 있다.
- [0086] 이하에서는, 전자 장치의 식별 정보의 예로 IMEI를 예시하여 설명하나, 이에 한정되지는 않으며, MEID(mobile equipment identifier) 등 전자 장치 자체를 식별할 수 있는 다양한 데이터들이 전자 장치의 식별 정보에 해당될 수 있다.
- [0088] 도 4는 본 발명의 다양한 실시예에 따른 전자 장치, 전자 서명 장치, 식별 정보 생성 장치 및 키 서버 장치를 간략히 도시한 것이다.
- [0089] 본 발명의 다양한 실시예에 따른 전자 장치(420)는 사용자가 휴대 가능한 스마트폰, 태블릿 PC 등의 휴대용 모바일 기기를 포함할 수 있다. 전자 장치(420)는 프로세서, 메모리, 통신 회로 등의 구성을 포함하며, 전자 장치(420)의 보다 상세한 구성에 대해서는 도 7을 통해 보다 상세히 후술하기로 한다.
- [0090] 본 발명의 다양한 실시예에 따른 식별 정보 생성 장치(440)는 전자 장치(420)의 제조 시에 전자 장치(420)에 할당할 식별 정보를 생성하는 장치를 의미할 수 있다. 식별 정보 생성 장치(440)는 GSMA 등에서 정해진 가이드 라인에 따라 각각의 전자 장치(420)에 식별 정보(예를 들어, IMEI)를 할당하고, 할당된 전자 서명 장치(410)를 통해 전자 장치(420)에 제공될 수 있다. 이하에서, 전자 장치(420)에 부여되는 식별 정보는 제1식별 정보로 칭할 수도 있다.
- [0091] 본 발명의 다양한 실시예에 따른 전자 서명 장치(410)는 전자 장치(420)의 식별 정보(또는 제1식별 정보)를 포함하는 인증 정보를 암호화 하여 전자 장치(420)로 전송할 수 있다. 한 실시예에 따라, 전자 서명 장치(410)는 인증 정보의 전자 서명 생성 시에, RSA 알고리즘 등 비대칭키 암호화 방식을 사용할 수 있다. 전자 서명 장치(410)의 보다 상세한 구성 및 수행하는 동작에 대해서는 도 5를 통해 보다 상세히 후술하기로 한다.
- [0092] 본 발명의 다양한 실시예에 따른 키 서버 장치(430)는 전자 서명 장치(410)에서 인증 정보의 암호화에 사용되는 암호화 키를 저장할 수 있다. 한 실시예에 따르면, 키 서버 장치(430)는 전자 서명 장치(410)를 비롯한 제조사 측에 의해서만 접근 가능하며, 그에 따라 키 서버 장치(430)의 안전한 영역에 저장된 암호화 키는 제조사 이외의 주체에 의해서는 획득이 불가능할 수 있다. 한 실시예에 따라, 암호화 키는 비밀키(또는 개인키, 비공개키)를 포함할 수 있다.
- [0093] 후술하는 바와 같이, 전자 서명 장치(410)에서 생성한 인증 정보의 전자 서명은 키 서버 장치(430)에 저장된 암호화키의 확보가 없는 한 복호화가 불가능 하며, 키 서버 장치(430)는 제조사 이외의 주체에 의한 접근이 불가

능 하므로 키 서버 장치(430)의 보안 운영을 통해 전자 장치(420)의 식별 정보의 불법적인 위조 및 변조를 방지할 수 있다.

- [0095] 도 5는 본 발명의 다양한 실시예에 따른 전자 서명 장치의 블록도이다.
- [0096] 도시된 바와 같이, 전자 서명 장치(510)는 통신 인터페이스(512), 프로세서(514) 및 메모리(516)를 포함하며, 도시된 구성 중 적어도 일부가 생략 또는 치환되더라도 본 발명의 다양한 실시예들을 구현하는 데에는 지장이 없을 것이다. 전자 서명 장치(510)는 앞서 설명한 도 4의 전자 서명 장치(410)에 해당할 수 있다.
- [0097] 한 실시예에 따르면, 통신 인터페이스(512)는 전자 장치(520), 키 서버 장치(530) 및 식별 정보 생성 장치(540) 등 외부 장치와의 데이터 송수신을 위한 유선 또는 무선 인터페이스 기능을 수행할 수 있다.
- [0098] 한 실시예에 따르면, 통신 인터페이스(512)는 전자 장치(520)와 연결 시에 전자 장치(520)로부터 통신 프로세서의 고유 값을 수신할 수 있는데, 통신 프로세서의 고유 값(unique value)은 전자 장치(520)의 통신 회로에 포함된 통신 프로세서(communication processor)의 식별 ID를 포함할 수 있다. 이하에서는, 통신 프로세서의 고유 값을 제2식별정보로 칭할 수도 있다. 통신 인터페이스(512)는 후술하는 바와 같이 생성된 전자 서명을 전자 장치(520)에 제공할 수 있다.
- [0099] 한 실시예에 따르면, 통신 인터페이스(512)는 키 서버 장치(530)와 연결 시에 키 서버 장치(530)로부터 인증 정보의 암호화에 사용될 비밀키 및/또는 비밀키에 대응하는 공개키를 수신할 수 있다. 통신 인터페이스(512)는 네트워크를 통해 키 서버 장치(530)와 연결될 수 있다.
- [0100] 한 실시예에 따르면, 통신 인터페이스(512)는 식별 정보 생성 장치(540)로부터 전자 장치(520)의 식별 정보를 수신할 수 있다. 여기서, 식별 정보는 앞서 설명한 IMEI일 수 있으며, IMEI는 전자 장치의 제조사 별로 구별되는 2자리, 제조사의 모델 별(또는 device type)로 구별되는 6자리, 각 전자 장치 별 시리얼 값 6자리 및 체크섬(checksum) 1자리로 총 15자리의 숫자로 구성될 수 있다.
- [0101] 한 실시예에 따르면, 메모리(516)는 공지의 휘발성 메모리(volatile memory) 및 비휘발성 메모리(non-volatile memory)를 포함할 수 있으며, 구체적인 구현 예에 있어서는 한정되지 않는다. 메모리(516)는 식별 정보 생성 장치(540)로부터 수신한 전자 장치(520)에 대응하는 제1식별 정보(또는 전자 장치의 식별 정보) 및/또는 전자 장치(520)로부터 수신한 전자 장치(520)의 통신 프로세서에 대응하는 제2식별 정보(또는 통신 프로세서의 고유 값)를 저장할 수 있다. 메모리(516)는 전기적으로 프로세서(514)와 연결되고, 프로세서(514)에서 수행될 수 있는 다양한 인스트럭션(instruction)들을 저장할 수 있다. 여기서, 인스트럭션들은 전자 장치(520)의 식별 정보의 생성 및 인증 정보의 암호화 등을 수행하는 공정 툴(tool) 상에 정의될 수 있다.
- [0102] 한 실시예에 따르면, 프로세서(514)는 메모리(516)에 저장된 인스트럭션들을 로딩하여, 인스트럭션 상에 정의된 기능을 수행하는 것으로 설정될 수 있다.
- [0103] 한 실시예에 따르면, 프로세서(514)는 통신 인터페이스(512)에 연결된 전자 장치(520)로부터 전자 장치(520)에 포함된 통신 프로세서의 고유 값을 수신하도록 할 수 있다. 통신 프로세서(또는 CP)의 고유 값은 CP 칩셋을 제조하는 시점에 ROM(read only memory)과 함께 쓰여지는 값으로 CP 칩셋을 구별하기 위한 목적으로 쓰여지며, 공정 과정에서 CP 칩셋마다 고유 값을 제공할 수 있다. 통신 프로세서의 고유 값은 통신 프로세서의 OTP(one time programmable) 영역에 쓰여 질 수 있다. OTP 영역은 제조 당시 하드웨어 적으로 데이터를 기록함으로써 데이터의 읽기는 가능하나, 한번 쓰여진 이상 데이터의 다시 쓰기(re-write)가 불가능한 영역에 해당한다. 따라서, 통신 프로세서의 고유 값은 변조가 실질적으로 불가능한 정보일 수 있다. 다른 실시예에 따르면, 통신 프로세서의 고유 값은 OTP 영역이 아닌 통신 프로세서 상에서 쓰여진 후 다시 쓰기가 불가능한 다른 영역에 저장될 수도 있다.
- [0104] 한 실시예에 따르면, 프로세서(514)는 메모리에 저장된 전자 장치(520)의 식별 정보(또는 제1식별 정보) 및 통신 프로세서의 고유 값(또는 제2식별 정보)에 적어도 일부 기반하여 인증 정보를 생성할 수 있다. 이 때, 10진수로 표현되는 전자 장치(520)의 식별 정보의 뒤에 통신 프로세서의 고유 값을 단순히 결합하여 인증 정보를 생성할 수 있다. 전자 장치(520)는 통신 프로세서 이외에 각각의 고유 값을 갖는 어플리케이션 프로세서(application processor, 이하 AP) 등 다양한 칩셋을 포함할 수 있으나, 예컨대 AP의 고유 값은 NAND 플래시 영역 등 다시 쓰기(re-write)가 가능한 영역에 저장되므로, 위/변조가 쉬울 수 밖에 없다. 이에, 프로세서(514)는 인증 정보의 생성 시 위/변조가 불가능한 OTP 영역에 쓰여진 통신 프로세서의 고유 값을 이용할 수

있으며, 다양한 실시예에 따르면 프로세서(514)는 통신 프로세서의 고유 값이 아닌 OTP 영역과 같이 다시 쓰기가 불가능한 영역에 고유 값을 저장하는 전자 장치(520) 내의 다른 구성들 중 적어도 하나의 고유 값을 사용할 수도 있다.

- [0105] 한 실시예에 따르면, 프로세서(514)는 인증 정보와 관련된 데이터의 적어도 일부를 암호화 하여 인증 정보에 대응하는 전자 서명을 생성할 수 있다. 전자 서명에 따라, 인증 정보와 관련된 데이터는 전자 서명 장치(510), 즉 전자 장치(520)의 제조사 측에 의해 정당하게 생성된 것임을 증명할 수 있다.
- [0106] 한 실시예에 따르면, 인증 정보와 관련된 데이터는 인증 정보의 해시값(hash value)일 수 있다. 해시 알고리즘은 임의의 길이의 입력 메시지를 고정된 길이의 출력값(해시값)으로 압축시킬 수 있어, 해시값을 구하게 되면 인증 정보보다 그 비트 수가 감소될 수 있다. 전자 서명 시에 데이터의 사이즈가 클수록 많은 시간이 소요되므로, 인증 정보 자체를 암호화 하는 것보다 인증 정보의 해시값을 암호화 하여 암호화에 소요되는 시간을 감소시킬 수 있다. 다른 한 실시예에 따르면, 프로세서(514)는 해시값을 구하는 과정을 생략하고, 인증 정보 자체를 암호화 하여 전자 서명을 생성할 수도 있다. 즉, 인증 정보와 관련된 데이터는 인증 정보 자체 또는 인증 정보의 해시 값일 수 있다.
- [0107] 한 실시예에 따르면, 프로세서(514)는 비대칭키 암호화 방식을 통해 인증 정보의 전자 서명을 생성할 수 있다. 통신 인터페이스(512)는 키 서버 장치(530)로부터 비밀키를 수신하고, 프로세서(514)는 수신한 비밀키를 이용해 인증 정보의 전자 서명을 생성할 수 있다. 앞서 설명한 바와 같이, 키 서버 장치(530)는 전자 장치(520)의 모델명 별로 각각의 암호화 키를 저장할 수 있으며, 하나의 암호화 키 만을 저장할 수도 있다.
- [0108] 한 실시예에 따르면, 프로세서(514)는 통신 인터페이스(512)를 통해 전자 장치(520)의 모델명을 포함하는 암호화 키 요청 메시지를 키 서버 장치(530)로 전송하고, 키 서버 장치(530)는 수신한 모델명에 해당되는 비밀키와 해당 비밀키에 매칭되는 공개키를 전자 서명 장치(510)에 전송할 수 있다. 다른 실시예에 따르면 키 서버 장치(530)는 하나의 비밀키만을 저장하며, 해당 비밀키 및 매칭되는 공개키를 전자 서명 장치(510)에 전송할 수 있다. 이에 따라, 키 서버 장치(530)에 저장된 암호화 키의 노출이 없는 한 인증 정보의 전자 서명에 대한 무결성은 보장될 수 있다.
- [0109] 프로세서(514)는 생성된 인증 정보의 전자 서명 및 생성된 전자 장치(520)의 식별 정보를 결합한 상태로 통신 인터페이스(512)를 통해 전자 장치(520)로 전송하도록 할 수 있다. 전송된 인증 정보의 전자 서명 및 전자 장치(520)의 식별 정보는 전자 장치(520)의 메모리(516) 상에 저장되어, 도 7 및 도 8을 통해 후술하는 바와 같이, 전자 장치(520)의 식별 정보 인증 과정에서 사용될 수 있다.
- [0110] 본 발명의 다양한 실시예에 따른 전자 장치는, 통신 인터페이스; 외부 전자 장치에 대응하는 제1식별 정보와 상기 외부 전자 장치의 통신 프로세서에 대응하는 제2식별 정보를 저장하기 위한 메모리; 및 프로세서를 포함하며, 상기 프로세서는, 상기 제1식별 정보 및 상기 제2식별 정보에 적어도 기반하여 인증 정보를 생성하고, 상기 인증 정보와 관련된 데이터의 적어도 일부를 암호화 하여 상기 인증 정보에 대응하는 전자 서명을 생성하고, 및 상기 통신 인터페이스를 이용하여 상기 전자 서명을 상기 외부 전자 장치로 전송하도록 설정될 수 있다.
- [0111] 다양한 실시예에 따르면, 상기 프로세서는, 상기 전자 서명을 상기 제1식별 정보와 결합한 상태로 상기 외부 전자 장치로 전송하도록 설정될 수 있다.
- [0112] 다양한 실시예에 따르면, 상기 프로세서는, 상기 통신 인터페이스를 이용하여, 다른 외부 전자 장치로부터 키 값을 수신하고, 상기 키 값을 이용하여 상기 암호화하는 동작을 수행하도록 설정될 수 있다.
- [0113] 다양한 실시예에 따르면, 상기 프로세서는, 상기 인증 정보의 해시값(hash value)을 생성하고, 상기 인증 정보의 해시값의 적어도 일부를 암호화 하여 상기 전자 서명을 생성하도록 설정될 수 있다.
- [0115] 도 6은 본 발명의 다양한 실시예에 따른 전자 서명 장치가 전자 장치의 인증 정보에 대응하는 전자 서명을 생성하는 방법의 흐름도이다.
- [0116] 도시된 방법은 앞서 도 4 및 도 5를 통해 설명한 전자 서명 장치(410, 510), 전자 장치(420, 520), 키 서버 장치(430, 530) 및 식별 정보 생성 장치(440, 540)에 의해 수행될 수 있으며, 이하에서는 도 5에서 이미 설명한 바 있는 기술적 특징에 대해서는 그 설명을 생략하기로 한다. 또한, 도시된 동작들은 전자 장치(620)의 제조 시

에 수행될 수 있다.

- [0117] 동작 652에서, 식별 정보 생성 장치(640)는 전자 장치(620)의 식별 정보를 할당하고, 전자 서명 장치(610)에 전송할 수 있다. 여기서, 식별 정보는 IMEI일 수 있으며, 전자 장치(620)의 제조 시에 전자 장치(620)를 식별하기 위해 제조사에서 할당할 수 있는 다양한 식별 정보 중 적어도 하나를 포함할 수 있다.
- [0118] 동작 654에서, 전자 장치(620)는 통신 프로세서의 고유 값을 식별 정보 생성 장치(610)에 전송할 수 있다. 다양한 실시예에 따르면, 통신 프로세서의 고유 값은 통신 회로에 포함된 CP(communication processor)의 고유 값(unique value)을 포함할 수 있으며, 이는 통신 프로세서의 OTP(one time programmable) 영역에 쓰여져 다시 쓰기(re-write)가 불가능한 값일 수 있다.
- [0119] 동작 656에서, 전자 서명 장치(610)는 키 서버 장치(630)에 인증 정보의 암호화에 사용할 비밀키를 요청할 수 있다. 키 서버 장치(630)는 전자 장치(620)의 모델명 별로 각각의 암호화 키를 저장할 수 있으며, 하나의 암호화 키 만을 저장할 수도 있다. 전자 장치(620)의 모델명 별로 암호화 키를 구분하는 경우, 전자 서명 장치(610)는 전자 장치(620)의 모델명을 포함하는 암호화 키 요청 메시지를 키 서버 장치(630)로 전송할 수 있다.
- [0120] 동작 658에서, 키 서버 장치(630)는 요청 받은 비밀키를 전자 서명 장치(610)에 전송할 수 있다. 키 서버 장치(630)는 수신한 모델명에 해당되는 비밀키와 해당 비밀키에 매칭되는 공개키를 전자 서명 장치(610)에 전송하거나, 하나의 비밀키만을 사용하는 경우 해당 비밀키 및 매칭되는 공개키를 전자 서명 장치(610)에 전송할 수 있다.
- [0121] 동작 660에서, 전자 서명 장치(610)는 할당된 식별 정보 및 전자 장치(620)로부터 수신한 통신 프로세서의 고유 값을 결합하여 인증 정보를 생성할 수 있다. 한 실시예에 따르면, 10진수로 표현되는 전자 장치(620)의 식별 정보의 뒤에 통신 프로세서의 고유 값을 단순히 결합하여 인증 정보를 생성할 수 있다.
- [0122] 동작 662에서, 전자 서명 장치(610)는 인증 정보의 해시값(hash value)을 생성할 수 있다. 해시값을 생성함에 따라, 후술할 암호화 시에 인증 정보 자체를 암호화 하는 것보다 연산 처리 양을 감소 시킬 수 있는 장점이 있다. 한 실시예에 따르면, 전자 서명 장치(610)는 인증 정보를 해시 하지 않고, 인증 정보 자체를 암호화 하여 전자 서명을 생성할 수 있으며, 이 경우 동작 662는 생략될 수 있다.
- [0123] 동작 664에서, 전자 서명 장치(610)는 인증 정보와 관련된 데이터(예를 들어, 인증 정보의 해시값 또는 인증 정보 자체)를 키 서버 장치(630)를 통해 수신한 비밀키를 이용하여 암호화 하고, 인증 정보의 전자 서명을 생성할 수 있다. 전자 서명에 따라, 인증 정보와 관련된 데이터는 전자 서명 장치(610), 즉 전자 장치(620)의 제조사 측에 의해 정당하게 생성된 것임을 증명할 수 있다.
- [0124] 동작 666에서, 전자 서명 장치(610)는 인증 정보의 전자 서명 및 생성된 전자 장치(620)의 식별 정보를 결합한 상태로 전자 장치(620)로 전송할 수 있다.
- [0125] 동작 688에서, 전자 장치(620)는 수신한 인증 정보의 전자 서명 및 전자 장치(620)의 식별 정보를 메모리에 저장할 수 있다.
- [0126] 본 발명의 다양한 실시예에 따른, 전자 장치가 외부 전자 장치의 인증 정보에 대응하는 전자 서명을 생성하는 방법은, 상기 외부 전자 장치에 대응하는 제1식별 정보를 수신하는 동작; 상기 외부 전자 장치의 통신 프로세서에 대응하는 제2식별 정보를 수신하는 동작; 상기 제1식별 정보 및 상기 제2식별 정보에 적어도 기반하여 인증 정보를 생성하는 동작; 상기 인증 정보와 관련된 데이터의 적어도 일부를 암호화 하여 상기 인증 정보에 대응하는 전자 서명을 생성하는 동작; 및 상기 전자 서명을 상기 외부 전자 장치로 전송하는 동작을 포함할 수 있다.
- [0127] 다양한 실시예에 따르면, 상기 전자 서명을 전송하는 동작은, 상기 전자 서명을 상기 제1식별 정보와 결합한 상태로 상기 외부 전자 장치로 전송하는 동작을 포함할 수 있다.
- [0128] 다양한 실시예에 따르면, 다른 외부 전자 장치로부터 키 값을 수신하는 동작을 더 포함하며, 상기 전자 서명을 생성하는 동작은, 상기 키 값을 이용하여 상기 암호화하는 동작을 포함할 수 있다.
- [0129] 다양한 실시예에 따르면, 상기 인증 정보의 해시값(hash value)을 생성하는 동작을 더 포함하며, 상기 전자 서명을 생성하는 동작은, 상기 인증 정보의 해시값의 적어도 일부를 암호화 하여 상기 전자 서명을 생성하는 동작을 포함할 수 있다.

- [0131] 도 7은 본 발명의 다양한 실시예에 따른 전자 장치의 블록도이다.
- [0132] 전자 장치(720)는 앞서 설명한 도 5의 전자 장치(520) 및/또는 도 6의 전자 장치(620)일 수 있다. 또한, 전자 장치(720)는 도 1의 전자 장치(101) 및/또는 도 2의 전자 장치(201)의 구성 중 적어도 일부를 포함할 수 있다.
- [0133] 전자 장치(720)는 통신 회로(722), 프로세서(724), 메모리(726) 및 출력 장치(728)를 포함하며, 도시된 구성 중 일부가 생략 또는 치환되더라도 본 발명의 다양한 실시예를 구현함에는 지장이 없을 것이다. 도시된 구성 이외에, 전자 장치(720)는 디스플레이(미도시), 입력 장치(미도시), 각종 센서(미도시) 등 다양한 구성을 추가로 포함할 수 있으며, 이하에서는 전자 장치(720)의 식별 정보를 인증하기 위한 기술적 구성에 대해서 설명하기로 한다.
- [0134] 통신 회로(722)는 외부 장치와 데이터를 송수신하기 위한 구성으로, 도 1의 통신 인터페이스(170) 및/또는 도 2의 통신 모듈(220)의 구성 중 적어도 일부를 포함할 수 있다. 통신 회로(722)는 통신 프로세서(communication processor, CP(723))를 포함할 수 있다. 통신 프로세서(723)는 안테나를 통해 송/수신 되는 데이터의 변조 및 복조 등 신호 처리를 수행하기 위한 프로세서로써, 하나의 칩셋으로 구현될 수 있다.
- [0135] 한 실시예에 따르면, 통신 프로세서(723)는 통신 프로세서(723)의 제조 시에 할당되는 고유 값(unique value)을 포함하는데, 고유 값은 CP 칩셋을 제조하는 시점에 ROM(read only memory)과 함께 쓰여지는 값으로 CP 칩셋을 구별하기 위한 목적으로 쓰여지며, 공정 과정에서 CP 칩셋마다 고유의 값을 제공할 수 있다. 통신 프로세서(723)의 고유 값은 통신 프로세서(723)의 OTP(one time programmable) 영역에 쓰여 질 수 있다. OTP 영역은 제조 당시 하드웨어 적으로 데이터를 기록함으로써 데이터의 읽기는 가능하나, 한번 쓰여진 이상 데이터의 다시 쓰기(re-write)가 불가능한 영역에 해당한다. 따라서, 통신 프로세서(723)의 고유 값은 변조가 실질적으로 불가능한 정보일 수 있다.
- [0136] 한 실시예에 따르면, 메모리(726)는 공지의 휘발성 메모리(volatile memory) 및 비휘발성 메모리(non-volatile memory)를 포함할 수 있으며, 구체적인 구현 예에 있어서는 한정되지 않는다. 메모리(726)는 전기적으로 프로세서(724)와 연결되고, 프로세서(724)에서 수행될 수 있는 다양한 인스트럭션(instruction)들을 저장할 수 있다. 이와 같은 인스트럭션들은 프로세서(724)에 의해 인식될 수 있는 산술 및 논리 연산, 데이터 이동, 입출력 등의 제어 명령을 포함할 수 있다.
- [0137] 한 실시예에 따르면, 메모리(726)는 코드 영역 및 데이터 영역을 포함할 수 있다. 데이터 영역은 전자 장치에 대응하는 제1식별 정보, 통신 프로세서에 대응하는 제2식별 정보 및 전자 서명 장치로부터 수신된 제1인증 정보의 전자 서명을 저장할 수 있다. 메모리(726)에 저장된 전자 장치(720)의 식별 정보(또는 제1식별 정보)는 앞서 도 5 및 도 6을 통해 설명한 식별 정보 생성 장치(540, 640)에 의해 생성되어 전자 서명 장치(510, 610)로부터 전자 장치(720)에 제공된 것이며, 제1인증 정보의 전자 서명은 전자 장치(720)의 제조 시에 전자 서명 장치(510, 610)에 의해 생성 및 전송된 것일 수 있다. 데이터 영역은 다시 쓰기(re-write)가 가능한 영역으로 제1인증 정보의 전자 서명 및 전자 장치(720)의 식별 정보는 다시 쓰여질 수 있다. 코드 영역은 제1인증 정보의 전자 서명을 복호화 할 때 사용하기 위한 공개키를 포함할 수 있으며, 공개키는 앞서 키 서버 장치에 저장된 비밀키와 매칭되는 것일 수 있다. 한 실시예에 따르면, 공개키는 공정 단계에서 전자 서명 장치가 키 서버 장치로부터 획득하여 전자 장치(720)에 제공되거나, 전자 장치(720)의 고객 센터에서 주입될 수 있다.
- [0138] 프로세서(724)는 전자 장치(720)의 각 구성요소들의 제어 및/또는 통신에 관한 연산이나 데이터 처리를 수행할 수 있는 구성으로써, 도 1의 프로세서(120) 및/또는 도 2의 어플리케이션 프로세서(210)의 구성 중 적어도 일부를 포함할 수 있다. 프로세서(724)는 통신 회로(722), 메모리(726) 등 전자 장치(720)의 다양한 구성들과 전기적으로 연결될 수 있다.
- [0139] 한 실시예에 따르면, 프로세서(724)는 전자 장치(720)의 식별 정보를 인증하기 위한 소정의 이벤트가 발생하면, 메모리(726)에 저장된 인스트럭션들을 실행하여 후술할 인증 과정을 거치도록 구성될 수 있다. 식별 정보를 인증하기 위한 이벤트는 예를 들어, 전자 장치(720)의 부팅(booting) 시에 발생할 수 있다.
- [0140] 한 실시예에 따르면, 프로세서(724)는 메모리(726)에 저장된 제1인증 정보의 전자 서명 및 전자 장치(720)의 식별 정보를 읽어 낼 수 있다. 여기서, 전자 장치(720)의 식별 정보는 전자 장치(720)의 제조 시에 식별 정보 생성 장치에 의해 할당되어 전자 서명 장치로부터 전자 장치(720)에 제공된 것이며, 제1인증 정보의 전자 서명은 전자 장치(720)의 제조 시에 전자 서명 장치(510, 610)에 의해 생성 및 전송된 것일 수 있다.
- [0141] 프로세서(724)는 메모리(726)로부터 읽어낸 제1인증 정보의 전자 서명을 메모리(726)에 저장된 공개키를 이용해

복호화 할 수 있다. 여기서, 공개키는 앞서 키 서버 장치에 저장된 비밀키, 즉 전자 서명 장치가 인증 정보의 암호화 시 사용한 비밀키와 매칭되는 것이므로, 메모리(726)에 제1인증 정보의 전자 서명이 쓰여진 이후 변조되지 않았다면, 복호화 결과 생성되는 원본 메시지는 식별 정보 생성 장치에 의한 암호화 이전의 제1인증 정보와 관련된 데이터 일 수 있다. 여기서, 제1인증 정보와 관련된 데이터는, 제1인증 정보의 해시값 또는 제1인증 정보 자체일 수 있다.

[0142] 한 실시예에 따르면, 프로세서(724)는 읽어낼 수 있다. 통신 프로세서(723)의 고유 값은 앞서 설명한 바와 같이, CP 칩셋의 OTP(one time programmable) 영역에 쓰여진 고유 값일 수 있다. 한 실시예에 따르면 상기 통신 프로세서의 고유값은 상기 OTP 영역 이외의 다른 영역에 쓰여진 값을 읽어올 수 도 있으며, 네트워크 또는 전자 장치 내부에 저장되어 있는 다른 메모리를 통해서 획득할 수 있다.

[0143] 한 실시예에 따르면, 프로세서(724)는 메모리(726)로부터 읽어낸 전자 장치(720)의 식별 정보 및 통신 회로(722)로부터 읽어낸 통신 프로세서(723)의 고유 값을 결합하여 제2인증 정보를 생성할 수 있다. 이 때, 10진수로 표현되는 식별 정보의 뒤에 통신 회로(722)의 고유 값을 단순히 결합하여 제2인증 정보를 생성할 수 있다. 한 실시예에 따르면, 상기 전자 장치(720)의 식별 정보(예: IMEI Value)와 상기 통신 프로세서에 대응하는 식별 정보(예: cp의 식별id)를 이용하여 해쉬 함수를 통해 제2인증 정보를 생성할 수 있다.

[0144] 한 실시예에 따르면, 전자 장치(720)는 통신 프로세서(723) 이외에 각각의 고유 값을 갖는 어플리케이션 프로세서(application processor, 이하 AP) 등 다양한 칩셋을 포함할 수 있으나, 예컨대 AP의 고유 값은 NAND 플래시 영역 등 다시 쓰기(re-write)가 가능한 영역에 저장되므로, 위/변조가 쉬울 수 밖에 없다. 이에, 전자 서명 장치 및 전자 장치(720)는 인증 정보의 생성 및 인증 과정에서 위/변조가 불가능한 OTP 영역에 쓰여진 통신 프로세서(723)의 고유 값을 이용할 수 있으며, 다른 실시예로써 전자 서명 장치 및 전자 장치(720)는 통신 프로세서(722)의 고유 값이 아닌 OTP 영역과 같이 다시 쓰기가 불가능한 영역에 고유 값을 저장하는 전자 장치(720) 내의 다른 구성들 중 적어도 하나의 고유 값을 사용할 수도 있다.

[0145] 한 실시예에 따르면, 프로세서(724)는 앞서 획득한 제1인증 정보와 관련된 데이터가 제1인증 정보의 해시값인 경우, 제2인증 정보의 해시값을 생성할 수 있다. 다른 실시예에 따라, 제1인증 정보와 관련된 데이터가 제1인증 정보 자체인 경우, 제2인증 정보의 해시값을 생성하는 과정은 생략될 수 있다.

[0146] 한 실시예에 따르면, 제1인증 정보와 관련된 데이터는 전자 서명 장치에 의해 생성되어 전자 장치(720)에 저장된 것이고, 제2인증 정보와 관련된 데이터는 전자 장치(720)에 의해 생성된 것으로 생성 주체는 다르나 동일한 알고리즘에 따라 생성된 것일 수 있다. 또한, 제1인증 정보 및 제2인증 정보에 포함된 통신 프로세서(723)의 고유 값은 통신 프로세서(723)의 OTP 영역에 쓰여진 값으로 변조가 불가능 하며, 전자 서명 장치가 제1인증 정보의 전자 서명 생성 시에 사용한 비밀키는 전자 장치(720) 상에 저장되지 않고 키 서버 장치에서 안전하게 보존된 것이므로, 제1인증 정보와 관련된 데이터 및 제2인증 정보와 관련된 데이터는 동일할 수 있다. 즉, 전자 장치(720)의 메모리(726)에 저장된 전자 장치(720)의 식별 정보가 다시 쓰여지지 않은 이상 제1인증 정보와 관련된 데이터 및 제2인증 정보와 관련된 데이터는 동일할 수 밖에 없다.

[0147] 한 실시예에 따르면, 프로세서(724)는 제1인증 정보와 관련된 데이터 및 제2인증 정보와 관련된 데이터를 비교하고, 일치 여부에 따라 전자 장치(720)의 인증을 수행할 수 있다. 즉, 제1인증 정보와 관련된 데이터 및 제2인증 정보와 관련된 데이터가 일치하는 경우, 전자 장치(720)의 메모리(726)에 저장된 전자 장치(720)의 식별 정보가 유효한 것으로 판단할 수 있다. 이와 달리, 제1인증 정보와 관련된 데이터 및 제2인증 정보와 관련된 데이터가 다른 경우 전자 장치(720)의 식별 정보가 위/변조 된 것으로 판단할 수 있다.

[0148] 한 실시예에 따르면, 전자 장치(720)의 부팅 과정에서 상기 인증 동작이 수행된 경우, 전자 장치(720)는 식별 정보가 유효한 것으로 판단되면 부팅 과정을 계속 진행하고, 식별 정보가 위/변조 된 것으로 판단되면 부팅 과정을 중단하거나 일부 제한된 동작만이 수행 가능한 제한 모드로 부팅을 수행할 수 있다.

[0149] 한 실시예에 따르면, 프로세서(724)는 출력 장치(728)를 통하여 상기 인증의 결과에 대응하는 알림(notification)을 제공하도록 설정될 수 있다. 출력 장치(728)는 예를 들어, 오디오 출력을 위한 스피커, 비디오 출력을 위한 디스플레이, 햅틱(haptic) 출력을 위한 진동 액츄에이터 중 적어도 하나를 포함할 수 있다. 프로세서(724)는 전자 장치(720)의 식별 정보의 인증 결과에 따라 출력 장치(728) 중 적어도 하나를 이용해, 음성 출력, 오디오 출력, 햅틱 출력 중 적어도 하나를 출력하도록 할 수 있다.

[0150] 본 발명의 다양한 실시예에 따른, 전자 장치는, 통신 프로세서를 포함하는 통신 인터페이스; 상기 전자 장치에 대응하는 제1식별 정보, 상기 통신 프로세서에 대응하는 제2식별 정보, 및 외부 전자 장치로부터 수신된 전자

서명을 저장하기 위한 메모리; 및 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는, 상기 전자 서명을 복호화 하여, 상기 전자 장치에 대응하는 제1인증 정보와 관련된 데이터를 생성하고, 상기 제1식별 정보 및 상기 제2식별 정보에 적어도 기반하여 제2인증 정보와 관련된 데이터를 생성하고, 상기 제1인증 정보와 관련된 데이터와 상기 제2인증 정보와 관련된 데이터를 비교하고, 및 상기 비교의 결과에 적어도 기반하여 상기 전자 장치에 대한 인증을 수행하도록 설정될 수 있다.

- [0151] 다양한 실시예에 따르면, 출력 장치를 더 포함하고, 상기 프로세서는, 상기 출력 장치를 통하여 상기 인증의 결과에 대응하는 알림(notification)을 제공하도록 설정될 수 있다.
- [0152] 다양한 실시예에 따르면, 상기 제1인증 정보와 관련된 데이터는, 상기 제1인증 정보의 해시값(hash value)을 포함하며, 상기 프로세서는, 상기 제2인증 정보의 해시값을 생성하고, 상기 제1인증 정보의 해시값과 상기 제2인증 정보의 해시값이 동일한 경우, 상기 제1식별 정보가 유효한 것으로 판단하도록 설정될 수 있다.
- [0153] 다양한 실시예에 따르면, 상기 프로세서는, 상기 전자 장치의 부팅(booting) 과정에 상기 전자 장치에 대한 인증을 수행하도록 설정될 수 있다.
- [0155] 도 8은 본 발명의 다양한 실시예에 따른 전자 장치가 식별 정보를 인증하는 방법의 흐름도이다.
- [0156] 도시된 방법은 앞서 도 7을 통해 설명한 전자 장치(720)에 의해 수행될 수 있으며, 앞서 설명한 바 있는 기술적 특징에 대해서는 그 설명을 생략하기로 한다.
- [0157] 동작 810에서, 전자 장치는 식별 정보를 인증하기 위한 이벤트 발생을 감지할 수 있다. 여기서, 식별 정보 인증 이벤트는 전자 장치의 부팅 시에 발생할 수 있다.
- [0158] 동작 820에서, 전자 장치는 메모리에 저장된 제1인증 정보의 전자 서명 및 전자 장치의 식별 정보를 읽어 낼 수 있다. 여기서, 제1인증 정보의 전자 서명은 외부의 전자 장치, 즉 전자 서명 장치로부터 수신된 것일 수 있다.
- [0159] 동작 830에서, 전자 장치는 제1인증 정보의 전자 서명을 메모리에 저장된 공개키를 이용해 복호화 할 수 있다. 복호화 결과, 제1인증 정보와 관련된 데이터가 생성되며, 제1인증 정보와 관련된 데이터는 제1인증 정보의 해시값 또는 제1인증 정보 자체일 수 있다.
- [0160] 동작 840에서, 전자 장치는 통신 프로세서의 고유 값을 읽어낼 수 있다. 통신 프로세서의 고유 값은 앞서 설명한 바와 같이, CP 칩셋의 OTP 영역에 쓰여진 고유 값일 수 있다.
- [0161] 동작 850에서, 전자 장치는 메모리로부터 읽어낸 전자 장치의 식별 정보 및 통신 회로로부터 읽어낸 통신 프로세서의 고유 값을 결합하여 제2인증 정보를 생성할 수 있다.
- [0162] 동작 860에서, 전자 장치는 제2인증 정보의 해시값을 생성할 수 있다. 한편, 다양한 실시예에 따르면 제1인증 정보와 관련된 데이터는 제1인증 정보 자체일 수 있으며, 이 경우 제2인증 정보의 해시값을 생성하는 동작 860은 생략될 수 있다.
- [0163] 동작 870에서, 전자 장치는 제1인증 정보와 관련된 데이터 및 제2인증 정보와 관련된 데이터를 비교할 수 있다.
- [0164] 동작 880에서, 전자 장치는 제1인증 정보와 관련된 데이터 및 제2인증 정보와 관련된 데이터가 동일한 경우, 전자 장치의 메모리에 저장된 식별 정보가 유효한 것으로 판단할 수 있다.
- [0165] 동작 890에서, 전자 장치는 제1인증 정보와 관련된 데이터 및 제2인증 정보와 관련된 데이터가 불일치 한 경우, 전자 장치의 식별 정보가 위/변조 된 것으로 판단할 수 있다.
- [0167] 도 9는 본 발명의 다양한 실시예에 따른 전자 장치의 식별 정보 인증 후 수행되는 동작들의 흐름도이다.
- [0168] 동작 910에서, 전자 장치는 도 8을 통해 설명한 바와 같은 식별 정보의 인증 동작을 수행할 수 있다.
- [0169] 동작 920에서, 인증 결과 식별 정보가 유효한 경우, 동작 930에서 전자 장치는 정상적으로 부팅 과정을 계속하고, 식별 정보의 유효한 인증과 관련된 알림(notification)을 오디오, 비디오 또는 햅틱 중 적어도 하나를 이용해 출력할 수 있다.
- [0170] 인증 결과, 식별 정보가 유효하지 않은 경우, 동작 940에서 전자 장치는 부팅 과정을 중단하거나, 일부 제한적

인 기능만이 사용 가능한 제한 모드로 부팅을 계속할 수 있다. 이와 적어도 일부 동시에 전자 장치는 식별 정보가 위/변조 됨을 알리기 위한 알림(notification)을 오디오, 비디오 또는 햅틱 중 적어도 하나를 이용해 출력할 수 있다.

[0171] 본 발명의 다양한 실시예에 따른, 전자 장치가 식별 정보를 인증하는 방법은, 외부 전자 장치로부터 수신된 전자 서명을 복호화 하여, 상기 전자 장치에 대응하는 제1인증 정보와 관련된 데이터를 생성하는 동작; 상기 전자 장치에 대응하는 제1식별 정보 및 상기 전자 장치의 통신 프로세서에 대응하는 제2식별 정보에 적어도 기반하여 제2인증 정보와 관련된 데이터를 생성하는 동작; 상기 제1인증 정보와 관련된 데이터와 상기 제2인증 정보와 관련된 데이터를 비교하는 동작; 및 상기 비교의 결과에 적어도 기반하여 상기 전자 장치에 대한 인증을 수행하는 동작을 포함할 수 있다.

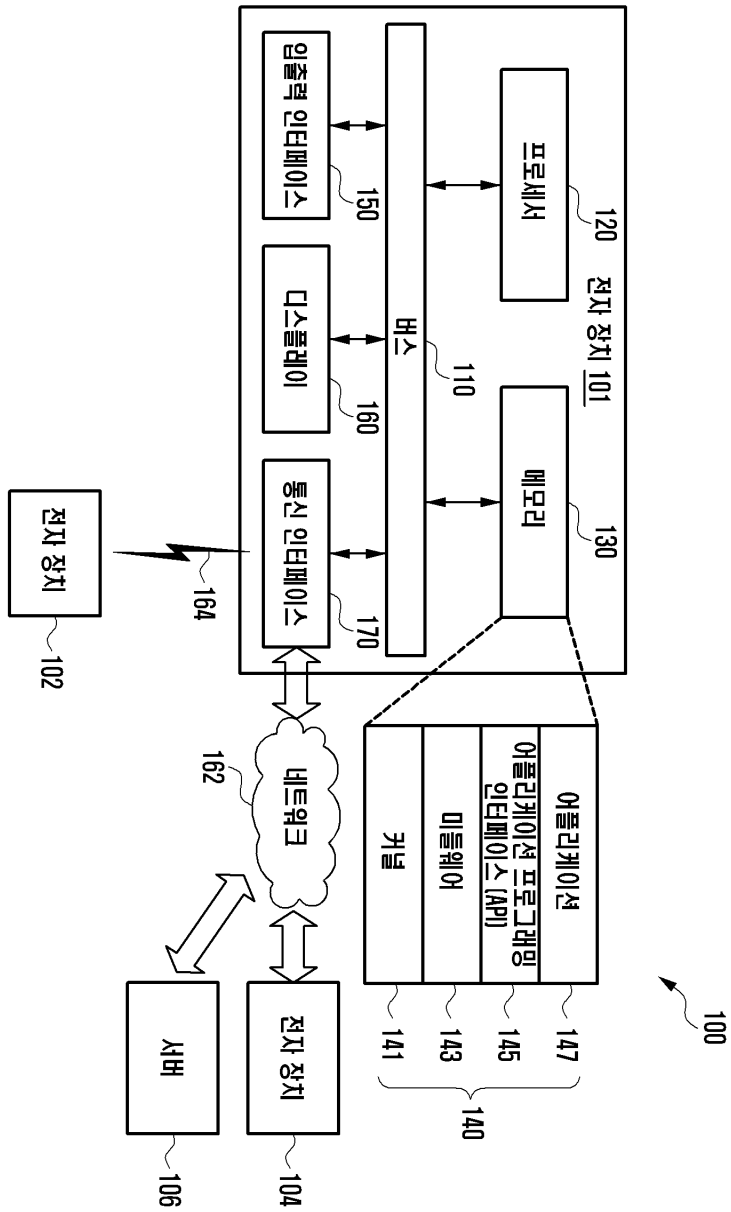
[0172] 다양한 실시예에 따르면, 상기 인증의 결과에 대응하는 알림(notification)을 제공하는 동작을 더 포함할 수 있다.

[0173] 다양한 실시예에 따르면, 상기 제1인증 정보와 관련된 데이터는, 상기 제1인증 정보의 해시값(hash value)을 포함하며, 상기 제2인증 정보의 해시값(hash value)을 생성하는 동작을 더 포함하고, 상기 인증을 수행하는 동작은, 상기 제1인증 정보의 해시값 및 상기 제2인증 정보의 해시값이 동일한 경우, 상기 제1식별 정보가 유효한 것으로 판단하는 동작을 포함할 수 있다.

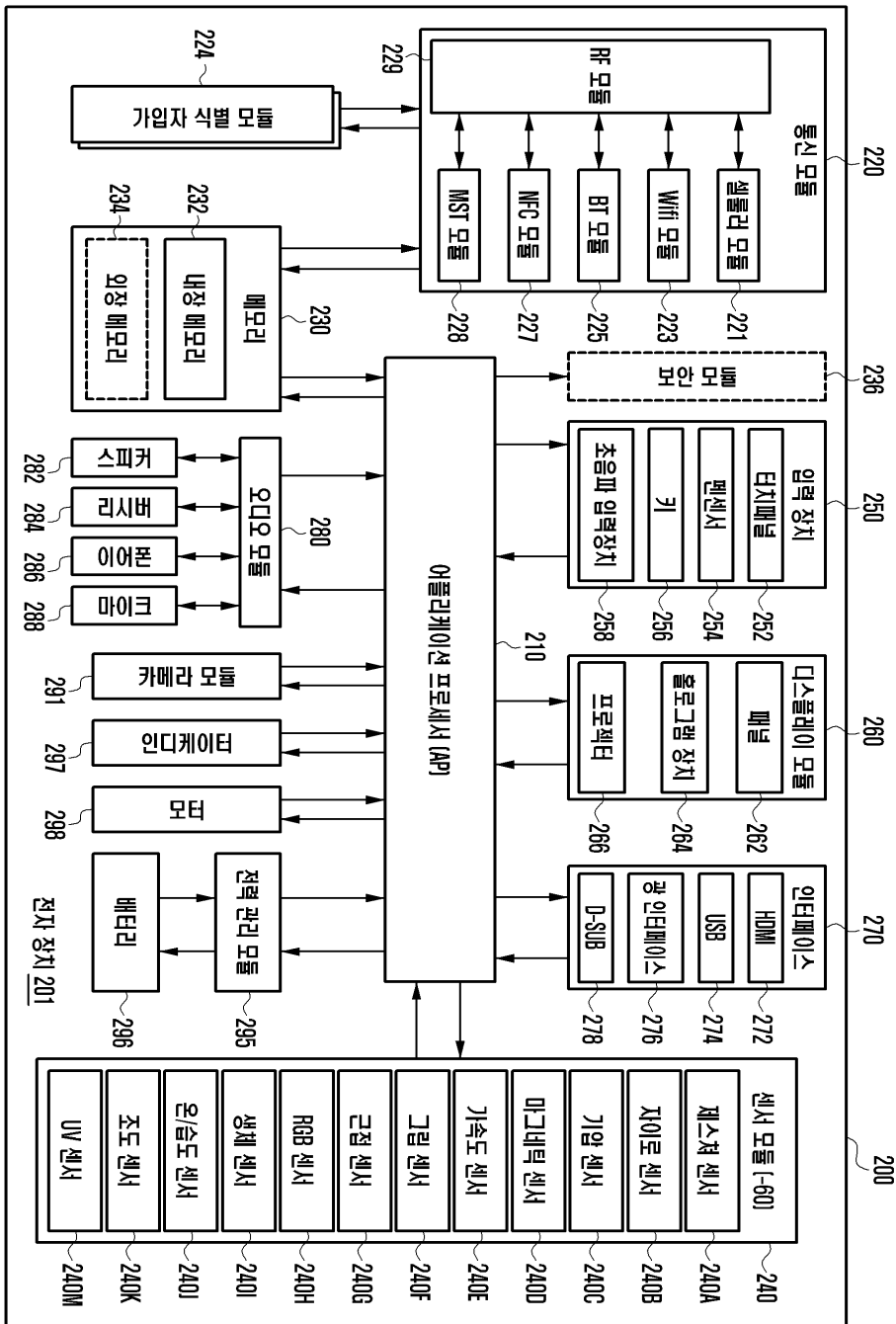
부호의 설명

- [0175] 410: 전자 서명 장치
- 420: 전자 장치
- 430: 키 서버 장치
- 440: 식별 정보 생성 장치

도면
도면1



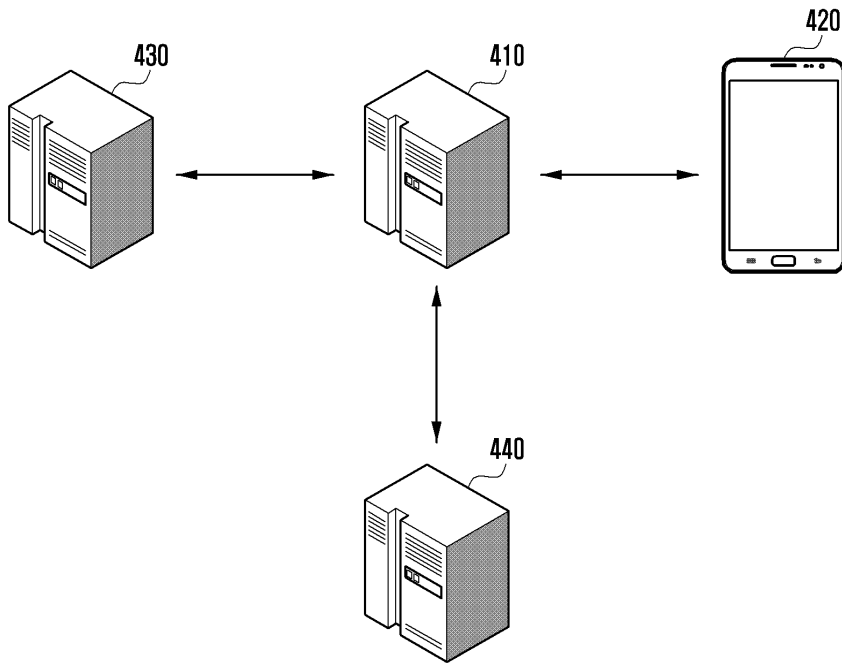
도면2



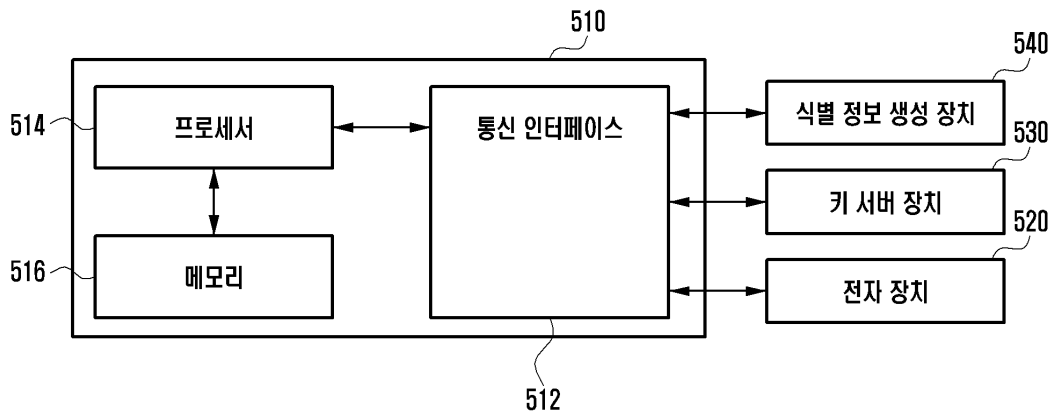
도면3

310									
아플리케이션 (370)									
홈 (371)	다이얼러 (372)	SMS/MMS (373)	IME (374)	브라우저 (375)	카메라 (376)	일람 (377)	결제 (385)		
컨택트 (378)	음성다이얼 (379)	이메일 (380)	달력 (381)	미디어 플레이어 (382)	앨범 (383)	시계 (384)			
API (360)									
미들웨어 (330)									
아플리케이션 매니저 (341)	윈도우 매니저 (342)	멀티미디어 매니저 (343)	리소스 매니저 (344)	결제 매니저 (354)					
퍼워 매니저 (345)	데이터베이스 매니저 (346)	패키지 매니저 (347)	연결 매니저 (348)	권타임 라이브리 (335)					
동지 매니저 (349)	위치 매니저 (350)	그래픽 매니저 (351)	보안 매니저 (352)						
커널 (320)									
시스템 리소스 매니저 (321)					다바이스 드라이버 (323)				

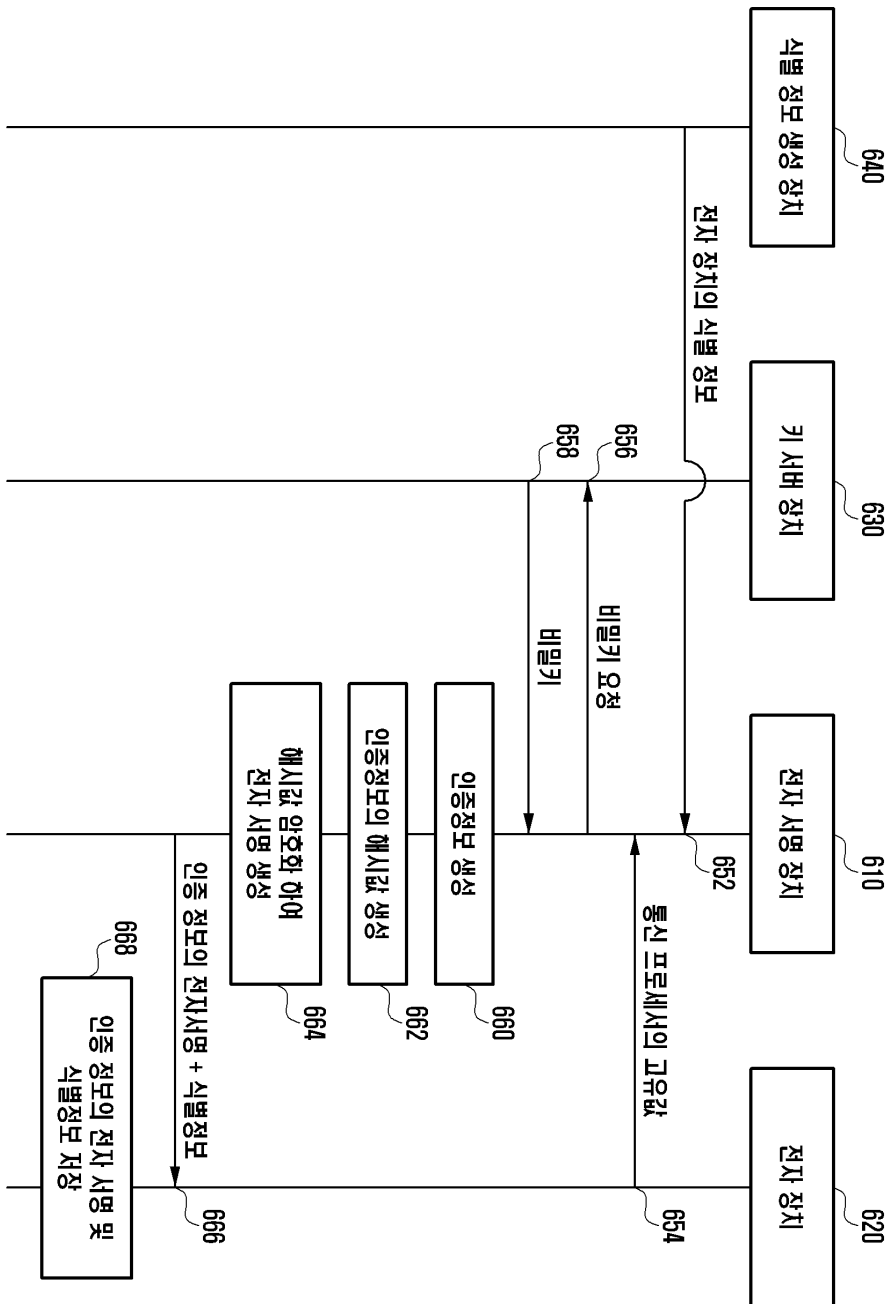
도면4



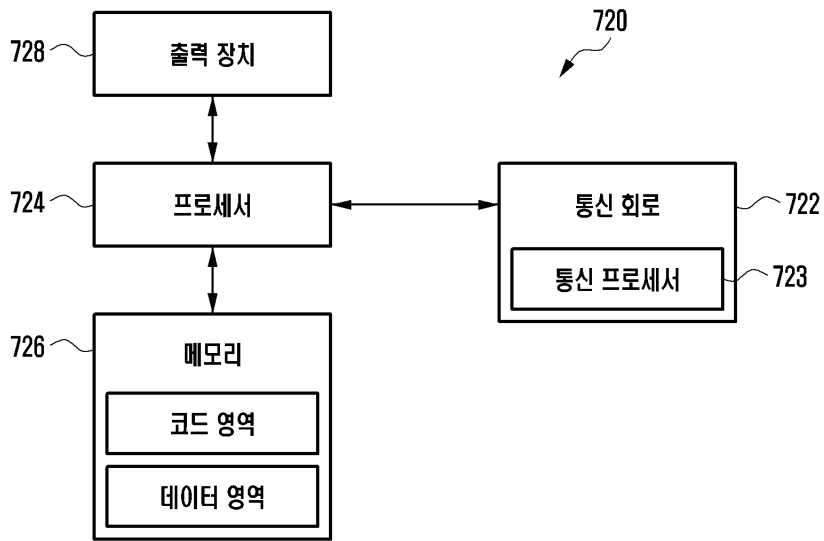
도면5



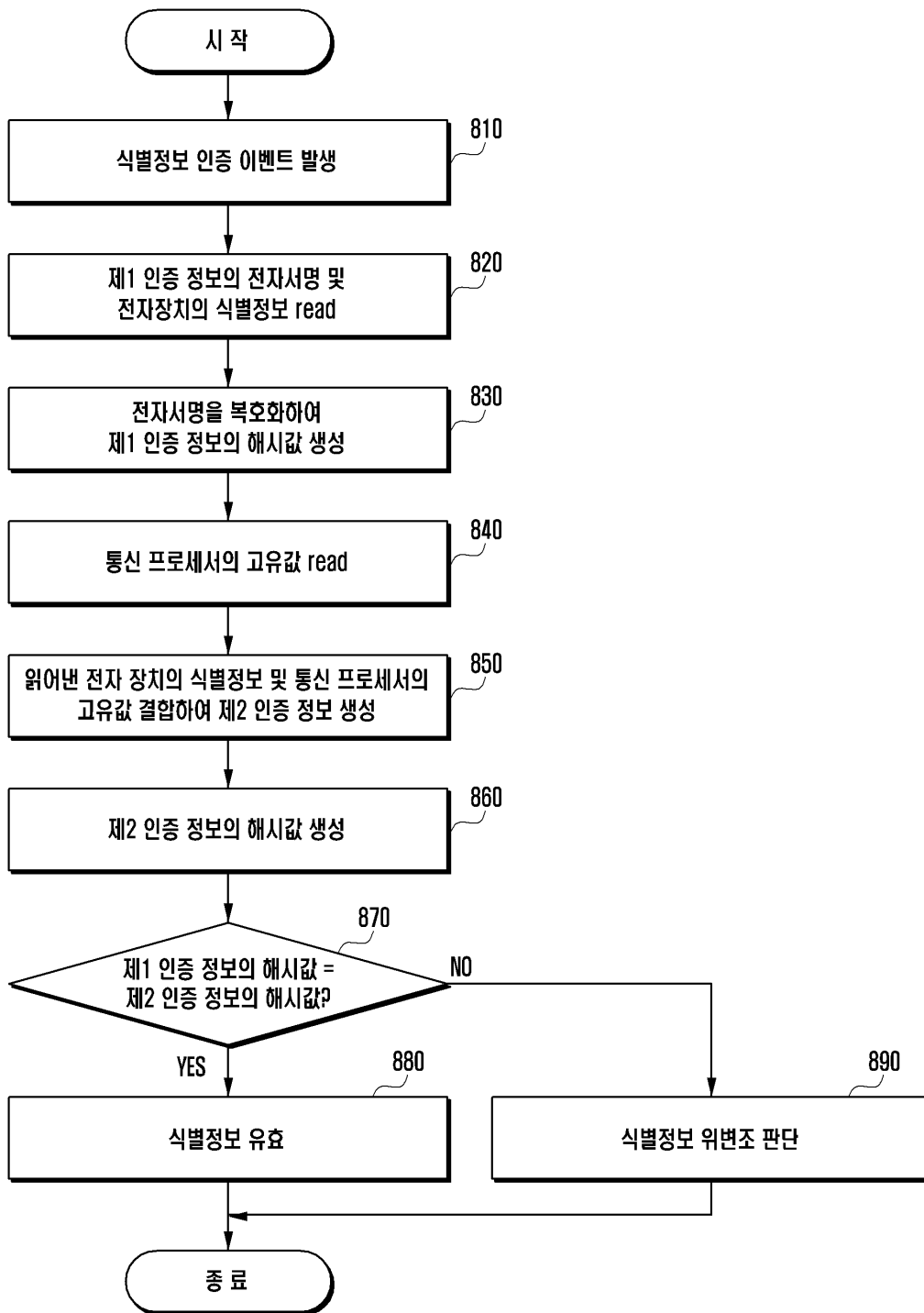
도면6



도면7



도면8



도면9

