(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년03월09일
(11) 등록번호 10-1836211
(24) 등록일자 2018년03월02일

(51) 국제특허분류(Int. Cl.)
G06F 21/44 (2013.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
G06F 21/44 (2013.01)
G06F 21/606 (2013.01)
(21) 출원번호 10-2016-0172743
(22) 출원일자 2016년12월16일
심사청구일자 2016년12월16일
(56) 선행기술조사문헌
KR1020040075191 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 시옷
부산광역시 해운대구 센텀중앙로 78 ,센텀그린타워3층(우동)
(72) 발명자
박현주
경기도 용인시 수지구 신봉1로 28, 402동 1703호 (신봉동, 서홍마을효성화운트빌아파트)
박한나
인천광역시 서구 청마로51번안길 11, 603동 1003 (당하동, 검단힐스테이트6차)
(74) 대리인
특허법인(유)화우

전체 청구항 수 : 총 4 항 심사관 : 문남두

(54) 발명의 명칭 **전자 기기 인증 매니저 장치**

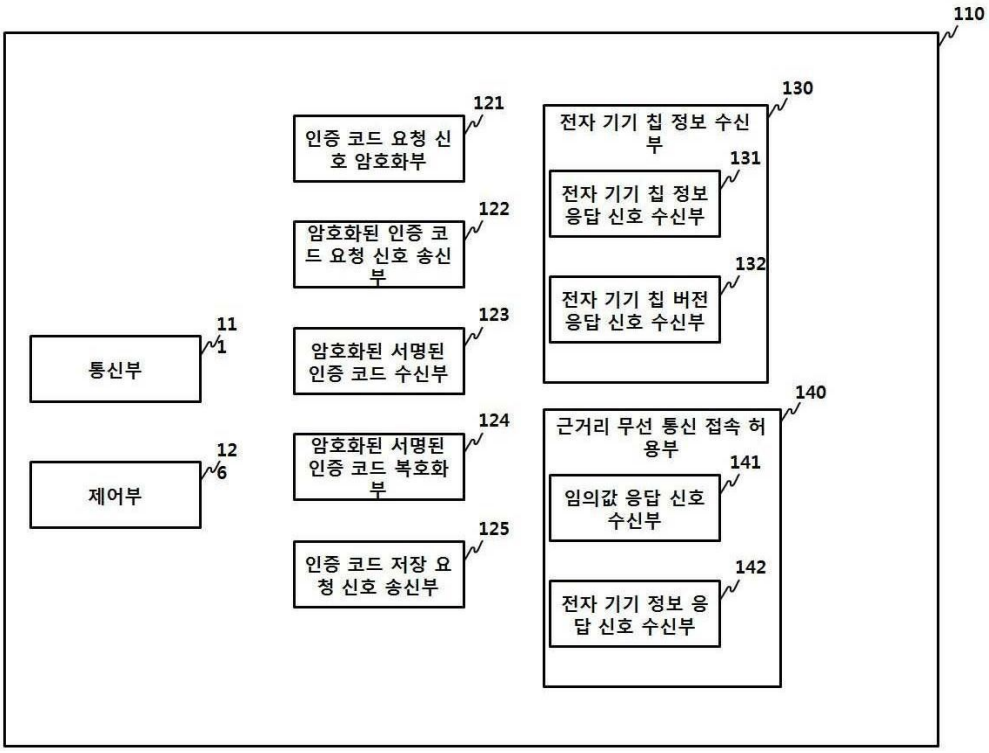
(57) 요 약

전자 기기를 인증하는 기술에 관한 것으로, 자세하게는 간소화된 인증 코드를 이용하여 전자 기기를 인증하는 방법에 관한 것이다.

제안된 발명이 해결하고자 하는 하나의 과제는 간소화된 인증 코드를 이용하여 하드웨어 성능 사항이 낮은 전자

(뒷면에 계속)

대 표 도



기기의 인증을 용이하게 하는 것이다.

일 양상에 있어서, 전자 기기 인증 매니저 장치는 전자 기기 인증 서버 장치 및 전자 기기와 통신하는 통신부, 전자 기기 인증 매니저 장치를 총괄 제어하는 제어부, 인증 코드 요청 신호를 암호화하는 인증 코드 요청 신호 암호화부, 통신부를 통해 암호화된 인증 코드 요청 신호를 송신하는 암호화된 인증 코드 요청 신호 송신부, 전자 기기 인증 서버 장치로부터 통신부를 통해 암호화된 서명된 인증 코드를 수신하는 암호화된 서명된 인증 코드 수신부, 암호화된 서명된 인증 코드를 복호화하는 암호화된 서명된 인증 코드 복호화부 및 통신부를 통해 전자 기기로 인증 코드 저장 요청 신호를 송신하는 인증 코드 저장 요청 신호 송신부를 포함하되, 상기 전자 기기와 GPIO 인터페이스를 통해 연결되는 것을 특징으로 할 수 있다.

(52) CPC특허분류
H04L 9/3226 (2013.01)
H04L 2209/122 (2013.01)

명 세 서

청구범위

청구항 1

전자 기기 인증 매니저 장치를 총괄 제어하는 제어부;

인증 코드 요청 신호를 암호화하는 인증 코드 요청 신호 암호화부;

전자 기기로 암호화된 인증 코드 요청 신호를 송신하는 암호화된 인증 코드 요청 신호 송신부;

전자 기기로부터 암호화된 서명된 인증 코드를 수신하는 암호화된 서명된 인증 코드 수신부;

암호화된 서명된 인증 코드를 복호화하는 암호화된 서명된 인증 코드 복호화부;

전자 기기로 인증 코드 저장 요청 신호를 송신하는 인증 코드 저장 요청 신호 송신부;

전자 기기로부터 전자 기기 내부에 실장된 칩 정보를 수신하는 전자 기기 칩 정보 수신부; 및

전자 기기의 근거리 무선 통신 접속을 허용하는 근거리 무선 통신 접속 허용부; 를 포함하되,

상기 전자 기기와 GPIO 인터페이스를 통해 연결되는 것을 특징으로 하는 전자 기기 인증 매니저 장치.

청구항 2

제 1 항에 있어서,

상기 인증 코드는,

시리얼 번호, 유니크 아이디, 난수, 트랜잭션 아이디, 유효 시간, 유효 횟수, 접근 제어 정책, 암호화 알고리즘 중 적어도 하나를 포함하는 것을 특징으로 하는 전자 기기 인증 매니저 장치.

청구항 3

삭제

청구항 4

제 1 항에 있어서,

상기 전자 기기 칩 정보 수신부는,

전자 기기로부터 전자 기기 칩 정보 응답 신호를 수신하는 전자 기기 칩 정보 응답 신호 수신부; 및

전자 기기로부터 전자 기기 칩 버전 응답 신호를 수신하는 전자 기기 칩 버전 응답 신호 수신부;

를 포함하는 전자 기기 인증 매니저 장치.

청구항 5

제 1 항에 있어서,

상기 근거리 무선 통신 접속 허용부는,

전자 기기로부터 임의 값 응답 신호를 수신하는 임의값 응답 신호 수신부; 및

전자 기기로부터 전자 기기 정보 응답 신호를 수신하는 전자 기기 정보 응답 신호를 수신하는 전자 기기 정보 응답 신호 수신부;

를 포함하는 전자 기기 인증 매니저 장치.

발명의 설명

기 술 분 야

[0001] 전자 기기를 인증하는 기술에 관한 것으로, 자세하게는 간소화된 인증 코드를 이용하여 전자 기기를 인증하는 방법에 관한 것이다.

배 경 기 술

[0002] 보안에 대한 수많은 발전에도 불구하고, 해킹은 정보통신기술 분야에서 빈번하게 발생한다. 그러므로, 여러 장치를 식별하는 사물 인터넷(IOT, INTERNET OF THINGS)의 보안을 위한 프레임 워크가 제안될 필요가 있다.

[0003] 사물 인터넷 분야에서는 사람, 장치, 서비스, 컨텐츠가 서로 네트워크로 연결 된다. 이 과정에서 모든 사물 인터넷의 신원 확인, 인증 및 통합 관리를 통한 사물 인터넷 장치로의 접근 제어가 필요하다. 공개키 기반 구조(PKI, Public Key Infrastructure)에 기초한 장치 인증은 광범위하게 사용된다. 공개키 기반 구조에 기초한 장치 인증은 네트워크 그리고 장치와 같은 환경으로부터 자유로워 지도록 어플리케이션 층에 의해 보안된다. 그러므로, 공개키 기반 구조에 기초한 장치 인증은 사물 인터넷 환경에서 장치 확인의 가장 적절한 시스템으로 선택된다.

[0004] 그러나, 공개키 기반 구조에 기초한 장치 인증을 적용하기 위해, 장치는 전자 서명을 만들고 확인할 수 있는 산술 연산 장치(arithmetic unit)를 포함해야 하는데, 그것을 제한된 리소스 및 용량을 가지는 사물 인터넷 장치에 적용하는 것은 어렵다. 장치의 인증에 사용되는 인증 코드에 포함된 정보를 최소화하여 장치의 크기 및 하드웨어의 성능에 관계없이 장치에 저장된 인증 코드를 통해 장치를 인증할 수 있는 방법이 제안될 필요가 있다.그러나 종래 사주정보 서비스는 사주명식을 해석한 추상적이고 애매한 문구들의 집합을 여과없이 단순 제공하는 것에 머물러 있어, 사용자마다 동일한 문구들을 자기에 맞게 서로 다르게 받아들이는 문제점을 내포하고 있다. 경우에 따라 전문가의 첨언이 첨부되기도 하지만 추상적이고 애매한 문구들은 사용자의 정신적 스트레스를 해소하고 자가 심리치료를 제공한다는 사주정보 서비스의 순기능을 방해하는 요소로 작용하고 있다.

발명의 내용

해결하려는 과제

[0005] 제안된 발명이 해결하고자 하는 하나의 과제는 간소화된 인증 코드를 이용하여 하드웨어 성능 사항이 낮은 전자 기기의 인증을 용이하게 하는 것이다.

[0006] 제안된 발명이 해결하고자 하는 다른 과제는 전자 기기가 통신하는 대상에 대한 정보인 클라이언트 타입 정보와 전자 기기가 임의로 생성한 값을 해쉬함수를 통해 산출한 값을 통해 전자 기기와 전자 기기로 인증 코드 발급을 중계하는 장치간에 인증이 이루어지도록 하는 것이다.

[0007] 제안된 발명이 해결하고자 하는 또 다른 과제는 전자 기기와 전자 기기로의 인증 코드 발급을 중계하는 장치간에 송수신하는 신호를 디폴트 값 또는 난수 값인 에드 값과 키 값을 통해 암호화 및 복호화 하는 것이다.

과제의 해결 수단

[0008] 일 양상에 있어서, 전자 기기 인증 매니저 장치는 전자 기기 인증 매니저 장치를 총괄 제어하는 제어부; 인증 코드 요청 신호를 암호화하는 인증 코드 요청 신호 암호화부; 전자 기기로 암호화된 인증 코드 요청 신호를 송신하는 암호화된 인증 코드 요청 신호 송신부; 전자 기기로부터 암호화된 서명된 인증 코드를 수신하는 암호화된 서명된 인증 코드 수신부; 암호화된 서명된 인증 코드를 복호화하는 암호화된 서명된 인증 코드 복호화부; 및 전자 기기로 인증 코드 저장 요청 신호를 송신하는 인증 코드 저장 요청 신호 송신부;를 포함하되, 상기 전자 기기와 GPIO 인터페이스를 통해 연결되는 것을 특징으로 하는 할 수 있다.

[0009] 또 다른 양상에 있어서, 전자 기기 인증 매니저 장치는 전자 기기로부터 전자 기기 내부에 실장된 칩 정보를 수신하는 전자 기기 칩 정보 수신부 및 전자 기기의 근거리 무선 통신 접속을 허용하는 근거리 무선 통신 접속 허용부를 더 포함한다.

[0010] 또 다른 양상에 있어서, 상기 전자 기기 칩 정보 수신부는 전자 기기로부터 전자 기기 칩 정보 응답 신호를 수

신하는 전자 기기 칩 정보 응답 신호 수신부 및 전자 기기로부터 전자 기기 칩 버전 응답 신호를 수신하는 전자 기기 칩 버전 응답 신호 수신부를 포함할 수 있다.

[0011] 또 다른 양상에 있어서, 상기 근거리 무선 통신 접속 허용부는 전자 기기로부터 임의 값 응답 신호를 수신하는 임의값 응답 신호 수신부 및 전자 기기로부터 전자 기기 정보 응답 신호를 수신하는 전자 기기 정보 응답 신호를 수신하는 전자 기기 정보 응답 신호 수신부를 포함한다.

발명의 효과

[0012] 제안된 발명은 간소화된 인증 코드를 이용하여 하드웨어 적인 사항이 낮은 전자 기기의 인증을 용이하게 한다.

[0013] 제안된 발명은 전자 기기가 통신하는 대상에 대한 정보인 클라이언트 타입 정보와 전자 기기가 임의로 생성한 값을 해쉬함수를 통해 산출한 값을 통해 전자 기기와 전자 기기로의 인증 코드 발급을 중계하는 장치간에 인증이 이루어지도록 한다.

[0014] 제안된 발명은 전자 기기와 전자 기기로의 인증 코드 발급을 중계하는 장치간에 송수신하는 신호를 디폴트 값 또는 난수 값인 에드 값과 키 값을 통해 암호화 및 복호화 한다.

도면의 간단한 설명

[0015] 도 1은 일 실시예에 따른 전자 기기 인증 방법의 흐름을 도시한다.

도 2는 전자 기기와 전자 기기 인증 매니저 장치 및 전자 기기 인증 서버 장치간의 전자 기기 인증 방법의 동작 과정을 설명하기 위한 흐름도이다.

도 3은 일 실시예에 따란 인증 코드가 포함하는 정보를 도시한다.

도 4는 일 실시예에 따른 전자 기기 인증 방법의 흐름을 도시한다.

도 5는 일 실시예에 따른 전자 기기 칩 정보 수신 단계의 구체적인 흐름을 도시한다.

도 6은 전자 기기와 전자 기기 인증 매니저 장치간의 전자 기기 칩 정보 수신 단계의 동작 과정을 설명하기 위한 흐름도이다.

도 7은 일 실시예에 따른 근거리 무선 통신 접속 단계의 구체적인 흐름을 도시한다.

도 8은 전자 기기와 전자 기기 인증 매니저 장치간의 근거리 무선 통신 접속 단계의 동작 과정을 설명하기 위한 흐름도이다.

도 9는 전자 기기 인증 시스템의 구성을 도시한다.

도 10은 전자 기기 인증 매니저 장치의 구성을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0016] 전술한, 그리고 추가적인 양상들은 첨부된 도면을 참조하여 설명하는 실시예들을 통해 구체화된다. 각 실시예들의 구성 요소들은 다른 언급이나 상호간에 모순이 없는 한 실시예 내에서 다양한 조합이 가능한 것으로 이해된다. 나아가 제안된 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다.

[0017] 도면에서 제안된 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다. 그리고, 어떤 부분이 어떤 구성 요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성 요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것을 의미한다.

[0018] 또한, 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 나아가, 명세서 전체에서 신호는 전압이나 전류 등의 전기량을 의미한다.

[0019] 명세서에서 기술한 부란, "하드웨어 또는 소프트웨어의 시스템을 변경이나 플러그인 가능하도록 구성한 블록"을 의미하는 것으로서, 즉 하드웨어나 소프트웨어에 있어 특정 기능을 수행하는 하나의 단위 또는 블록을 의미한다.

[0020] 도 1은 일 실시예에 따른 전자 기기(100) 인증 방법의 흐름을 도시한다.

[0021] 일 양상에 있어서, 전자 기기(100) 인증 방법은 인증 코드 요청 신호 암호화 단계(S110), 암호화된 인증 코드 요청 신호 송신 단계(S120), 암호화된 인증 코드 요청 신호 복호화 단계(S130), 인증 코드 생성 단계(S140), 서명된 인증 코드 생성 단계(S150), 서명된 인증 코드 암호화 단계(S160), 암호화된 서명된 인증 코드 수신 단계(S170), 암호화된 서명된 인증 코드 복호화 단계(S180), 서명된 인증 코드 송신 단계, 인증 코드 저장 응답 신호 송신 단계를 포함한다.

[0022] 일 실시예에 있어서, 인증 코드 요청 신호 암호화 단계(S110)는 전자 기기 인증 매니저 장치(110)가 인증 코드 요청 신호를 암호화한다. 인증 코드 요청 신호 암호화 단계(S110)는 인증 코드 요청 신호 자체를 암호화 하는 단계이다. 인증 코드 요청 신호에는 후술할 전자 기기(100)에 대한 정보가 포함되어 있기에 보안상의 이유로 인증코드 요청 신호 자체를 암호화한다. 전자 기기 인증 매니저 장치(110)는 전자 기기(100)를 인증하는 인증 코드를 전자 기기 인증 서버(120) 장치로부터 발급받는 절차를 중계한다. 즉, 전자 기기 인증 매니저 장치(110)는 전자 기기 인증 서버(120) 장치로부터 인증 코드를 수신하여 전자 기기(100)로 송신한다. 전자 기기 인증 매니저 장치(110)는 예를 들어, 핸드폰, 노트북 등의 단말이다. 단말에 설치된 어플리케이션을 통해 전자 기기(100)와 전자 기기 인증 서버(120) 장치를 중계하여 전자 기기(100)가 서명된 인증 코드를 수신하여 저장할 수 있도록 한다.

[0023] 인증 코드 요청 신호는 메시지 타입, 메시지 길이, 시리얼 번호, 게이트웨이 아이디, 유니크 아이디, 전자 기기(100) 비밀번호 중 적어도 하나를 포함한다. 메시지 타입, 메시지 길이, 시리얼 번호, 게이트웨이 아이디, 유니크 아이디, 전자 기기(100) 비밀번호는 인증 코드 요청 신호가 포함하는 정보들이다.

[0024] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫번째 바이트에 설정되는 값으로 인증 코드 요청 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 인증 코드 요청 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 인증 코드 요청 신호의 메시지 타입은 qw06이다. qw06값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기 인증 매니저 장치(110)는, 상기 신호를 인증 코드 요청 신호라고 인식할 수 있다.

[0025] 메시지 길이는 전체 메시지 사이즈에서 메시지 타입과 메시지 길이를 뺀 메시지 사이즈이다. 인증 코드 요청 신호는 메시지 타입 및 메시지 길이를 포함하여 다른 여러 정보를 포함한다고 전술하였다. 여기서, 메시지 길이는 인증 코드 요청 신호가 포함하는 모든 정보의 사이즈, 즉 크기에서 메시지 타입에 해당하는 사이즈 및 메시지 길이에 해당하는 사이즈를 뺀 사이즈이다. 메시지 타입의 크기가 1바이트이고, 메시지 길이 자체의 크기가 4바이트 이고, 전체 메시지의 크기가 85바이트라면, 메시지 길이는 80바이트가 된다. 여기서, 전체 메시지의 크기는 인증 코드 요청 신호의 크기이다.

[0026] 시리얼 번호는 전자 기기(100)의 고유 번호이다. 전자 기기 인증 매니저 장치(110)와 근거리 무선 통신 또는 유선 통신을 할 수 있는 전자 기기(100)마다 하나의 고유 번호를 포함한다. 전자 기기 인증 매니저 장치(110)는 후술할 인증 코드 요청 신호 암호화 단계(S110) 이전 단계에서 전자 기기(100)의 고유 번호인 시리얼 번호를 수신하여 저장한다. 전자 기기 인증 매니저 장치(110)는 저장하고 있는 시리얼 번호가 포함된 인증 코드 요청 신호를 생성한다.

[0027] 게이트 웨이 아이디는 전자 기기(100)와 근거리 무선 통신 또는 유선 통신하는 게이트웨이의 아이디이다. 전자 기기(100)가 전자 기기 인증 서버(120) 장치가 생성한 서명된 인증 코드를 저장한 후, 전자 기기(100)는 서명된 인증 코드를 통해 게이트웨이로부터 인증 받는다. 게이트웨이는 지역별로 설치된다. 예를 들어 게이트 웨이는 특정 건물에 설치되고, 전자 기기(100)가 상기 특정 건물에서 게이트웨이와 통신하기 위해서는 게이트웨이로부터 인증을 받아야 한다. 게이트웨이 아이디는 전자 기기(100)가 사용될 공간에서 전자 기기(100)와 통신하는 게이트웨이의 아이디다.

[0028] 유니크 아이디는 전자 기기(100) 내부에 실장된 칩의 아이디이다. 유니크 아이디는 전자 기기(100)가 생성하는 정보이다. 유니크 아이디는 칩이 실장된 전자 기기(100)의 시리얼 번호에 솔트를 적용한 결과에 해쉬를 취한 결과이다. 전자 기기(100) 마다 고유 번호인 시리얼 번호가 있음은 전술하였다. 솔트는 사용자가 설정한 값으로 시리얼 번호와 유니크 아이디의 관련성이 노출되지 않도록 하기 위한 값이다. 솔트를 적용한 다는 것은 시리얼 번호에 사용자가 지정한 값, 예를 들면, 솔트값인 '1234'를 시리얼 번호와 논리 연산을 한다는 것이다. 솔트값과 시리얼 번호를 논리 연산 한 결과에 해쉬 함수를 취한 결과가 유니크 아이디이다. 논리 연산은 and, or, xor, nand 중 적어도 하나이다.

[0029] 전자 기기(100) 비밀번호는 후술할 인증 코드 저장 응답 신호 송신 단계에서, 전자 기기(100)가 수신한 서명된 인증 코드를 저장할 때 입력해야 하는 값이다. 전자 기기(100)는 서명된 인증 코드의 저장시 인증 코드 요청 신호에 포함된 전자 기기(100) 비밀번호와 동일한 비밀번호를 입력해야, 서명된 인증 코드를 저장할 수 있다.

[0030] 일 실시예에 있어서, 암호화된 인증 코드 요청 신호 송신 단계(S120)는 전자 기기 인증 매니저 장치(110)가 암호화된 인증 코드 요청 신호를 전자 기기 인증 서버(120) 장치로 송신한다. 인증 코드 요청 신호에 대한 자세한 설명은 전술하였다.

[0031] 일 실시예에 있어서, 암호화된 인증 코드 요청 신호 복호화 단계(S130)는 전자 기기 인증 서버(120) 장치가 수신한 암호화된 인증 코드 요청 신호를 복호화 한다. 전자 기기 인증 서버(120) 장치는 복호화 한 암호화된 인증 코드 요청 신호에 포함된 메시지 타입을 통해 전자 기기 인증 매니저 장치(110)가 송신한 신호는 인증 코드를 요청하는 신호임을 인식한다.

[0032] 일 실시예에 있어서, 인증 코드 생성 단계(S140)는 전자 기기 인증 서버(120) 장치는 인증 코드 요청 신호에 따라 인증 코드를 생성한다. 전자 기기 인증 서버(120) 장치는 전자 기기 인증 매니저 장치(110)가 송신한 인증 코드 요청 신호에 포함된 일부 정보가 포함된 인증 코드를 생성한다. 전자 기기 인증 서버(120) 장치는 인증 코드를 생성하는 장치다. 전자 기기 인증 서버(120) 장치는 인증 코드를 생성할 자격을 갖춘 기관의 서버 장치이다. 인증 코드가 포함하는 구체적인 정보에 대한 자세한 설명은 후술한다.

[0033] 일 실시예에 있어서, 서명된 인증 코드 생성 단계(S150)는 전자 기기 인증 서버(120) 장치가 생성한 인증 코드에 서명하여 서명된 인증 코드를 생성한다. 전자 기기 인증 서버(120) 장치가 생성한 인증 코드 자체가 복제될 수 있기 때문에 전자 기기 인증 서버(120) 장치는 인증 코드에 서명한다. 서명된 인증 코드는 전자 기기 인증 서버(120) 장치가 직접 생성한 인증 코드라는 것을 의미한다. 전자 기기 인증 서버(120) 장치가 인증 코드에 서명한다는 것은 인증 코드가 서명 관련 데이터를 포함한다는 것을 의미한다.

[0034] 일 실시예에 있어서, 서명된 인증 코드 암호화 단계(S160)는 전자 기기 인증 서버(120) 장치가 서명된 인증 코드를 암호화한다. 전자 기기 인증 서버(120) 장치는 인증 코드에 포함된 암호화 알고리즘으로 서명된 인증 코드를 암호화 한다. 보안을 위해 서명된 인증 코드는 암호화 되어 관리된다.

[0035] 일 실시예에 있어서, 암호화된 서명된 인증 코드 수신 단계(S170)는 전자 기기 인증 매니저 장치(110)가 암호화된 서명된 인증 코드를 전자 기기 인증 서버(120) 장치로부터 수신한다. 암호화된 서명된 인증 코드 수신 단계(S170)에서 전자 기기 인증 매니저 장치(110)는 서명된 인증코드에 나아가, 결과 코드, 인증 코드 크기, 해쉬를 취한 전자 기기(100) 비밀번호도 수신한다. 결과 코드는 전자 기기 인증 서버(120) 장치가 전자 기기 인증 매니저 장치(110)로부터 암호화된 인증 코드 요청 신호를 오류 없이 수신했는지를 나타내는 값이다. 인증 코드 크기는 인증 코드 자체의 사이즈를 의미한다. 인증 코드의 크기는 예를 들면 1000 바이트다. 해쉬를 취한 전자 기기(100) 비밀번호는 전술한 전자 기기(100) 비밀번호에 해쉬함수를 취한 결과이다. 전자 기기(100) 비밀번호 자체의 도난을 방지하기 위해 해쉬를 취해서 전자 기기 인증 서버(120) 장치가 송신한다.

[0036] 일 실시예에 있어서, 암호화된 서명된 인증 코드 복호화 단계(S180)는 전자 기기 인증 매니저 장치(110)가 암호화된 서명된 인증 코드를 복호화 한다. 인증 코드 자체에는 인증 코드가 어떻게 암호화 되어 있는 지의 정보인 암호화 알고리즘을 포함하기 때문에, 상기 암호화 알고리즘을 이용하여 암호화된 서명된 인증 코드를 복호화 한다.

[0037] 일 실시예에 있어서, 인증 코드 저장 요청 신호 송신 단계(S191)는 전자 기기 인증 매니저 장치(110)가 서명된 인증 코드를 확인하여 전자 기기(100)로 인증 코드 저장 요청 신호를 송신한다. 서명된 인증 코드를 확인하는 것은 전자 기기 인증 매니저 장치(110)가 인증 코드에 포함된 정보와 인증 코드 요청 신호에 포함된 정보를 비교하는 것이다. 예를 들어 인증 코드 요청 신호와 인증 코드는 모두 유니크 아이디를 포함하는데, 유니크 아이디가 동일한지를 확인하는 것이다.

[0038] 인증 코드 저장 요청 신호는 메시지 타입, 메시지 길이, 인증 코드 크기, 인증 코드, 전자 기기(100) 정보 요청 명령 정보, 전자 기기(100) 비밀번호, 해쉬를 취한 전자 기기(100) 비밀번호, 및 세션 아이디를 포함한다.

[0039] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫번째 바이트에 설정되는 값으로 인증 코드 요청 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 인증 코드 저장 요청 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 인증 코드 저장 요청 신호의 메시지 타입은 qw07이다. qw07값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기(100)는,

상기 신호를 인증 코드 저장 요청 신호라고 인식할 수 있다.

[0040] 메시지 길이는 전체 메시지 사이즈에서 메시지 타입과 메시지 길이를 뺀 메시지 사이즈이다. 여기서 사이즈는 크기이다. 인증 코드 저장 요청 신호는 메시지 타입 및 메시지 길이를 포함하여 다른 여러 정보를 포함한다고 전술하였다. 여기서, 메시지 길이는 인증 코드 저장 요청 신호가 포함하는 모든 정보의 사이즈, 즉 크기에서 메시지 타입에 해당하는 사이즈 및 메시지 길이에 해당하는 사이즈를 뺀 사이즈이다. 메시지 타입의 크기가 1 바이트이고, 메시지 길이 자체의 크기가 4바이트 이고, 전체 메시지의 크기가 85바이트라면, 메시지 길이는 80 바이트가 된다. 여기서, 전체 메시지의 크기는 인증 코드 저장 요청 신호의 크기이다.

[0041] 인증 코드 크기는 인증서 자체의 용량으로 예를 들면 인증 코드 크기는 1000 바이트다.

[0042] 인증 코드는 전술한 전자 기기 인증 서버(120) 장치가 생성한 인증 코드이다.

[0043] 전자 기기(100) 정보 요청 명령 정보는 전자 기기 인증 매니저 장치(110)가 전자 기기 인증 매니저 장치(110)에기 저장된 클라이언트 타입과 임의값을 논리 연산 하여 해쉬를 취한 것이다. 즉, 전자 기기(100) 정보 요청 명령 정보는 Hash(클라이언트 타입 | 임의값)인 것이다. 여기서 임의값은 현재 시간 또는 전자 기기 인증 매니저 장치(110)가 임의로 생성한 난수이다. 어떤 값을 해쉬를 취한다 또는 해쉬 함수를 취한다는 것은 Hash(어떤 값)을 한다는 것이다. 제1의 값과 제 2의 값을 논리 연산해서 해쉬를 취한다 또는 해쉬 함수를 취한다는 것은 Hash(제1의 값 | 제2의 값)을 한다는 것이다.

[0044] 전자 기기(100) 비밀번호는 전자 기기(100) 비밀번호는 후술할 인증 코드 저장 응답 신호 송신 단계에서, 전자 기기(100)가 수신한 서명된 인증 코드를 저장할 때 입력해야 하는 값이다. 전자 기기(100)는 서명된 인증 코드의 저장시 인증 코드 요청 신호에 포함된 전자 기기(100) 비밀번호와 동일한 비밀번호를 입력해야, 서명된 인증 코드를 저장할 수 있다.

[0045] 해쉬를 취한 전자 기기(100) 비밀번호는 전자 기기(100) 비밀 번호에 해쉬함수를 취한 결과이다.

[0046] 세션 아이디는 전자 기기 인증 매니저 장치(110)가 트랜잭션 아이디, 시리얼 번호, 클라이언트 타입 및 임의값을 논리 연산한 결과에 Hash함수를 취해서 산출된 아이디이다. 여기서 임의값은 세션 아이디를 생성하는 시점의 시간 또는 전자 기기 인증 매니저 장치(110)가 임의로 생성한 난수이다.

[0047] 일 실시예에 있어서, 인증 코드 저장 응답 신호 송신 단계는 전자 기기(100)가 수신한 서명된 인증 코드를 저장하고 인증 코드 저장 응답 신호를 전자 기기 인증 매니저 장치(110)로 송신한다. 인증 코드 저장 응답 신호는 메시지 타입, 메시지 길이 및 결과 코드를 포함한다.

[0048] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫번째 바이트에 설정되는 값으로 인증 코드 요청 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 인증 코드 저장 응답 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 인증 코드 저장 응답 신호의 메시지 타입은 qw87이다. qw87값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기(100)는, 상기 신호를 인증 코드 저장 응답 신호라고 인식할 수 있다.

[0049] 메시지 길이는 전체 메시지 사이즈에서 메시지 타입과 메시지 길이를 뺀 메시지 사이즈이다. 여기서 사이즈는 크기이다. 인증 코드 저장 응답 신호는 메시지 타입 및 메시지 길이를 포함하여 다른 여러 정보를 포함한다고 전술하였다. 여기서, 메시지 길이는 인증 코드 저장 응답 신호가 포함하는 모든 정보의 사이즈, 즉 크기에서 메시지 타입에 해당하는 사이즈 및 메시지 길이에 해당하는 사이즈를 뺀 사이즈이다. 메시지 타입의 크기가 1 바이트이고, 메시지 길이 자체의 크기가 4바이트 이고, 전체 메시지의 크기가 85바이트라면, 메시지 길이는 80 바이트가 된다. 여기서, 전체 메시지의 크기는 인증 코드 저장 응답 신호의 크기이다.

[0050] 결과 코드는 인증 코드가 오류 없이 저장했는지 여부를 표시하는 코드이다. 예를 들어 결과 코드가 0이면 인증 코드가 오류 없이 전자 기기(100)에 저장됨을 의미한다.

[0051] 도 2는 전자 기기(100)와 전자 기기 인증 매니저 장치(110) 및 전자 기기 인증 서버(120) 장치의 전자 기기(100) 인증 방법의 동작 과정을 설명하기 위한 흐름도이다.

[0052] **후술할 암호화된 인증 코드 요청 신호 송신 단계 및 암호화된 서명된 은증 코드 수신 단계는 전자 기기와 전자 기기 인증 서버간에 이루어 질 수 있다.**

[0053] **즉, 전자 기기 인증 매니저 장치는 GPIO 인터페이스를 통해 전자기기와 연결된 후 인증 코드 요청 신호를 암호화하고 암호화된 서명된 인증 코드를 복호화 하는 역할만 수행 할 수 있다.**

[0054] **전자 기기 인증 매니저 장치가 암호화한 인증 코드 요청 신호를 전자 기기가 전자 기기 인증 서버로 송신할 수 있다.**

[0055] **또한, 전자 기기 인증 매니저 장치가 복호화한 암호화된 서명된 인증 코드를 전자기기가 전자 기기 인증 서버로 송신할 수 있다.**

[0056] 일 실시예에 있어서, 인증 코드 요청 신호 암호화 단계(S110)는 전자 기기 인증 매니저 장치(110)가 인증 코드 요청 신호를 암호화한다. 인증 코드 요청 신호 암호화 단계(S110)는 인증 코드 요청 신호 자체를 암호화 하는 단계이다. 인증 코드 요청 신호에는 후술할 전자 기기(100)에 대한 정보가 포함되어 있기에 보안상의 이유로 인증코드 요청 신호 자체를 암호화한다. 전자 기기 인증 매니저 장치(110)는 전자 기기(100)를 인증하는 인증 코드를 전자 기기 인증 서버(120) 장치로부터 발급받는 절차를 중계한다. 즉, 전자 기기 인증 매니저 장치(110)는 전자 기기 인증 서버(120) 장치로부터 인증 코드를 수신하여 전자 기기(100)로 송신한다. 전자 기기 인증 매니저 장치(110)는 예를 들어, 핸드폰, 노트북 등의 단말이다. 단말에 설치된 어플리케이션을 통해 전자 기기(100)와 전자 기기 인증 서버(120) 장치를 중계하여 전자 기기(100)가 서명된 인증 코드를 수신하여 저장할 수 있도록 한다.

[0057] 인증 코드 요청 신호는 메시지 타입, 메시지 길이, 시리얼 번호, 게이트웨이 아이디, 유니크 아이디, 전자 기기(100) 비밀번호를 포함한다. 메시지 타입, 메시지 길이, 시리얼 번호, 게이트웨이 아이디, 유니크 아이디, 전자 기기(100) 비밀번호는 인증 코드 요청 신호가 포함하는 정보들이다.

[0058] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫번째 바이트에 설정되는 값으로 인증 코드 요청 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 인증 코드 요청 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 인증 코드 요청 신호의 메시지 타입은 qw06이다. qw06값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기 인증 매니저 장치(110)는, 상기 신호를 인증 코드 요청 신호라고 인식할 수 있다.

[0059] 메시지 길이는 전체 메시지 사이즈에서 메시지 타입과 메시지 길이를 뺀 메시지 사이즈이다. 인증 코드 요청 신호는 메시지 타입 및 메시지 길이를 포함하여 다른 여러 정보를 포함한다고 전술하였다. 여기서, 메시지 길이는 인증 코드 요청 신호가 포함하는 모든 정보의 사이즈, 즉 크기에서 메시지 타입에 해당하는 사이즈 및 메시지 길이에 해당하는 사이즈를 뺀 사이즈이다. 메시지 타입의 크기가 1바이트이고, 메시지 길이 자체의 크기가 4바이트 이고, 전체 메시지의 크기가 85바이트라면, 메시지 길이는 80바이트가 된다. 여기서, 전체 메시지의 크기는 인증 코드 요청 신호의 크기이다.

[0060] 시리얼 번호는 전자 기기(100)의 고유 번호이다. 전자 기기 인증 매니저 장치(110)와 근거리 무선 통신 또는 유선 통신을 할 수 있는 전자 기기(100)마다 하나의 고유 번호를 포함한다. 전자 기기 인증 매니저 장치(110)는 후술할 인증 코드 요청 신호 암호화 단계(S110) 이전 단계에서 전자 기기(100)의 고유 번호인 시리얼 번호를 수신하여 저장한다. 전자 기기 인증 매니저 장치(110)는 저장하고 있는 시리얼 번호가 포함된 인증 코드 요청 신호를 생성한다.

[0061] 게이트 웨이 아이디는 전자 기기(100)와 근거리 무선 통신 또는 유선 통신하는 게이트웨이의 아이디이다. 전자 기기(100)가 전자 기기 인증 서버(120) 장치가 생성한 서명된 인증 코드를 저장한 후, 전자 기기(100)는 서명된 인증 코드를 통해 게이트웨이로부터 인증 받는다. 게이트웨이는 지역별로 설치된다. 예를 들어 게이트 웨이는 특정 건물에 설치되고, 전자 기기(100)가 상기 특정 건물에서 게이트웨이와 통신하기 위해서는 게이트웨이로부터 인증을 받아야 한다. 게이트웨이 아이디는 전자 기기(100)가 사용될 공간에서 전자 기기(100)와 통신하는 게이트웨이의 아이디다.

[0062] 유니크 아이디는 전자 기기(100) 내부에 실장된 칩의 아이디이다. 유니크 아이디는 전자 기기(100)가 생성하는 정보이다. 유니크 아이디는 칩이 실장된 전자 기기(100)의 시리얼 번호에 솔트를 적용한 결과에 해쉬를 취한 결과이다. 전자 기기(100) 마다 고유 번호인 시리얼 번호가 있음은 전술하였다. 솔트는 사용자가 설정한 값으로 시리얼 번호와 유니크 아이디의 관련성이 노출되지 않도록 하기 위한 값이다. 솔트를 적용한 다는 것은 시리얼 번호에 사용자가 지정한 값, 예를 들면, 솔트값인 '1234'를 시리얼 번호와 논리 연산을 한다는 것이다. 솔트값과 시리얼 번호를 논리 연산 한 결과에 해쉬를 취한 결과가 유니크 아이디이다.

[0063] 전자 기기(100) 비밀번호는 후술할 인증 코드 저장 응답 신호 송신 단계에서, 전자 기기(100)가 수신한 서명된 인증 코드를 저장할 때 입력해야 하는 값이다. 전자 기기(100)는 서명된 인증 코드의 저장시 인증 코드 요청 신호에 포함된 전자 기기(100) 비밀번호와 동일한 비밀번호를 입력해야, 서명된 인증 코드를 저장할 수 있다.

[0064] 일 실시예에 있어서, 암호화된 인증 코드 요청 신호 송신 단계(S120)는 전자 기기 인증 매니저 장치(110)가 암호화된 인증 코드 요청 신호를 전자 기기 인증 서버(120) 장치로 송신한다. 인증 코드 요청 신호에 대한 자세한 설명은 전술하였다.

[0065] 일 실시예에 있어서, 암호화된 인증 코드 요청 신호 복호화 단계(S130)는 전자 기기 인증 서버(120) 장치가 수신한 암호화된 인증 코드 요청 신호를 복호화 한다. 전자 기기 인증 서버(120) 장치는 복호화 한 암호화된 인증 코드 요청 신호에 포함된 메시지 타입을 통해 전자 기기 인증 매니저 장치(110)가 송신한 신호는 인증 코드를 요청하는 신호임을 인식한다.

[0066] 일 실시예에 있어서, 인증 코드 생성 단계(S140)는 전자 기기 인증 서버(120) 장치는 인증 코드 요청 신호에 따라 인증 코드를 생성한다. 전자 기기 인증 서버(120) 장치는 전자 기기 인증 매니저 장치(110)가 송신한 인증 코드 요청 신호에 포함된 일부 정보가 포함된 인증 코드를 생성한다. 전자 기기 인증 서버(120) 장치는 인증 코드를 생성하는 장치다. 전자 기기 인증 서버(120) 장치는 인증 코드를 생성할 자격을 갖춘 기관의 서버 장치이다. 인증 코드가 포함하는 구체적인 정보에 대한 자세한 설명은 후술한다.

[0067] 일 실시예에 있어서, 서명된 인증 코드 생성 단계(S150)는 전자 기기 인증 서버(120) 장치가 생성한 인증 코드에 서명하여 서명된 인증 코드를 생성한다. 전자 기기 인증 서버(120) 장치가 생성한 인증 코드 자체가 복제될 수 있기 때문에 전자 기기 인증 서버(120) 장치는 인증 코드에 서명한다. 서명된 인증 코드는 전자 기기 인증 서버(120) 장치가 직접 생성한 인증 코드라는 것을 의미한다. 전자 기기 인증 서버(120) 장치가 인증 코드에 서명한다는 것은 인증 코드가 서명 관련 데이터를 포함한다는 것을 의미한다.

[0068] 일 실시예에 있어서, 서명된 인증 코드 암호화 단계(S160)는 전자 기기 인증 서버(120) 장치가 서명된 인증 코드를 암호화한다. 전자 기기 인증 서버(120) 장치는 인증 코드에 포함된 암호화 알고리즘으로 서명된 인증 코드를 암호화 한다. 보안을 위해 서명된 인증 코드는 암호화 되어 관리된다.

[0069] 일 실시예에 있어서, 암호화된 서명된 인증 코드 수신 단계(S170)는 전자 기기 인증 매니저 장치(110)가 암호화된 서명된 인증 코드를 전자 기기 인증 서버(120) 장치로부터 수신한다. 암호화된 서명된 인증 코드 수신 단계(S170)에서 전자 기기 인증 매니저 장치(110)는 서명된 인증코드에 나아가, 결과 코드, 인증 코드 크기, 해쉬를 취한 전자 기기(100) 비밀번호도 수신한다. 결과 코드는 전자 기기 인증 서버(120) 장치가 전자 기기 인증 매니저 장치(110)로부터 암호화된 인증 코드 요청 신호를 오류 없이 수신했는지를 나타내는 값이다. 인증 코드 크기는 인증 코드 자체의 사이즈를 의미한다. 인증 코드의 크기는 예를 들면 1000 바이트다. 해쉬를 취한 전자 기기(100) 비밀번호는 전술한 전자 기기(100) 비밀번호에 해쉬함수를 취한 결과이다. 전자 기기(100) 비밀번호 자체의 도난을 방지하기 위해 해쉬를 취해서 전자 기기 인증 서버(120) 장치가 송신한다.

[0070] 일 실시예에 있어서, 암호화된 서명된 인증 코드 복호화 단계(S180)는 전자 기기 인증 매니저 장치(110)가 암호화된 서명된 인증 코드를 복호화 한다. 인증 코드 자체에는 인증 코드가 어떻게 암호화 되어 있는 지의 정보인 암호화 알고리즘을 포함하기 때문에, 상기 암호화 알고리즘을 이용하여 암호화된 서명된 인증 코드를 복호화 한다.

[0071] 일 실시예에 있어서, 인증 코드 저장 요청 신호 송신 단계(S191)는 전자 기기 인증 매니저 장치(110)가 서명된 인증 코드를 확인하여 전자 기기(100)로 인증 코드 저장 요청 신호를 송신한다. 서명된 인증 코드를 확인하는 것은 전자 기기 인증 매니저 장치(110)가 인증 코드에 포함된 정보와 인증 코드 요청 신호에 포함된 정보를 비교하는 것이다. 예를 들어 인증 코드 요청 신호와 인증 코드는 모두 유니크 아이디를 포함하는데, 유니크 아이디가 동일한지를 확인하는 것이다.

[0072] 인증 코드 저장 요청 신호는 메시지 타입, 메시지 길이, 인증 코드 크기, 인증 코드, 전자 기기(100) 정보 요청 명령 정보, 전자 기기(100) 비밀번호, 해쉬를 취한 전자 기기(100) 비밀번호, 및 세션 아이디를 포함한다.

[0073] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫번째 바이트에 설정되는 값으로 인증 코드 요청 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 인증 코드 저장 요청 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 인증 코드 저장 요청 신호의 메시지 타입은 qw07이다. qw07값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기(100)는, 상기 신호를 인증 코드 저장 요청 신호라고 인식할 수 있다.

[0074] 메시지 길이는 전체 메시지 사이즈에서 메시지 타입과 메시지 길이를 뺀 메시지 사이즈이다. 여기서 사이즈는 크기이다. 인증 코드 저장 요청 신호는 메시지 타입 및 메시지 길이를 포함하여 다른 여러 정보를 포함한다고

전술하였다. 여기서, 메시지 길이는 인증 코드 저장 요청 신호가 포함하는 모든 정보의 사이즈, 즉 크기에서 메시지 타입에 해당하는 사이즈 및 메시지 길이에 해당하는 사이즈를 뺀 사이즈이다. 메시지 타입의 크기가 1 바이트이고, 메시지 길이 자체의 크기가 4바이트 이고, 전체 메시지의 크기가 85바이트라면, 메시지 길이는 80 바이트가 된다. 여기서, 전체 메시지의 크기는 인증 코드 저장 요청 신호의 크기이다.

[0075] 인증 코드 크기는 인증서 자체의 용량으로 예를 들면 인증 코드 크기는 1000 바이트다.

[0076] 인증 코드는 전술한 전자 기기 인증 서버(120) 장치가 생성한 인증 코드이다.

[0077] 전자 기기(100) 정보 요청 명령 정보는 전자 기기 인증 매니저 장치(110)가 전자 기기 인증 매니저 장치(110)에기 저장된 클라이언트 타입과 임의값을 논리 연산 하여 해쉬를 취한 것이다. 즉, 전자 기기(100) 정보 요청 명령 정보는 Hash(클라이언트 타입 | 임의값)인 것이다. 여기서 임의값은 현재 시간 또는 전자 기기 인증 매니저 장치(110)가 임의로 생성한 난수이다. 어떤 값을 해쉬를 취한다 또는 해쉬 함수를 취한다는 것은 Hash(어떤 값)을 한다는 것이다. 제1의 값과 제 2의 값을 논리 연산해서 해쉬를 취한다 또는 해쉬 함수를 취한다는 것은 Hash(제1의 값 | 제2의 값)을 한다는 것이다.

[0078] 전자 기기(100) 비밀번호는 전자 기기(100) 비밀번호는 후술할 인증 코드 저장 응답 신호 송신 단계에서, 전자 기기(100)가 수신한 서명된 인증 코드를 저장할 때 입력해야 하는 값이다. 전자 기기(100)는 서명된 인증 코드의 저장시 인증 코드 요청 신호에 포함된 전자 기기(100) 비밀번호와 동일한 비밀번호를 입력해야, 서명된 인증 코드를 저장할 수 있다.

[0079] 해쉬를 취한 전자 기기(100) 비밀번호는 전자 기기(100) 비밀 번호에 해쉬함수를 취한 결과이다.

[0080] 세션 아이디는 전자 기기 인증 매니저 장치(110)가 트랜잭션 아이디, 시리얼 번호, 클라이언트 타입 및 임의값을 논리 연산한 결과에 Hash함수를 취해서 산출된 아이디이다. 여기서 임의값은 세션 아이디를 생성하는 시점의 시간 또는 전자 기기 인증 매니저 장치(110)가 임의로 생성한 난수이다.

[0081] 일 실시예에 있어서, 인증 코드 저장 응답 신호 송신 단계는 전자 기기(100)가 수신한 서명된 인증 코드를 저장하고 인증 코드 저장 응답 신호를 전자 기기 인증 매니저 장치(110)로 송신한다. 인증 코드 저장 응답 신호는 메시지 타입, 메시지 길이 및 결과 코드를 포함한다.

[0082] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫번째 바이트에 설정되는 값으로 인증 코드 요청 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 인증 코드 저장 응답 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 인증 코드 저장 응답 신호의 메시지 타입은 qw87이다. qw87값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기(100)는, 상기 신호를 인증 코드 저장 응답 신호라고 인식할 수 있다.

[0083] 메시지 길이는 전체 메시지 사이즈에서 메시지 타입과 메시지 길이를 뺀 메시지 사이즈이다. 여기서 사이즈는 크기이다. 인증 코드 저장 응답 신호는 메시지 타입 및 메시지 길이를 포함하여 다른 여러 정보를 포함한다고 전술하였다. 여기서, 메시지 길이는 인증 코드 저장 응답 신호가 포함하는 모든 정보의 사이즈, 즉 크기에서 메시지 타입에 해당하는 사이즈 및 메시지 길이에 해당하는 사이즈를 뺀 사이즈이다. 메시지 타입의 크기가 1 바이트이고, 메시지 길이 자체의 크기가 4바이트 이고, 전체 메시지의 크기가 85바이트라면, 메시지 길이는 80 바이트가 된다. 여기서, 전체 메시지의 크기는 인증 코드 저장 응답 신호의 크기이다.

[0084] 결과 코드는 인증 코드가 오류 없이 저장했는지 여부를 표시하는 코드이다. 예를 들어 결과 코드가 0이면 인증 코드가 오류 없이 전자 기기(100)에 저장됨을 의미한다.

[0085] 도 3은 일 실시예에 따란 인증 코드가 포함하는 정보를 도시한다.

[0086] 일 실시예에 있어서, 인증 코드는 시리얼 번호, 유니크 아이디, 난수, 트랜잭션 아이디, 유효 시간, 유효 횟수, 접근 제어 정책, 암호화 알고리즘을 포함하는 것을 특징으로 한다. 즉, 인증 코드는 복수의 정보를 포함하되, 복수의 정보는 시리얼 번호, 유니크 아이디, 난수, 트랜잭션 아이디, 유효 시간, 유효 횟수, 접근 제어 정책, 암호화 알고리즘이다.

[0087] 시리얼 번호는 전자 기기(100)의 고유 번호이다. 전자 기기 인증 매니저 장치(110)와 근거리 무선 통신 또는 유선 통신을 할 수 있는 전자 기기(100)마다 하나의 고유 번호를 포함한다. 전자 기기 인증 매니저 장치(110)는 후술할 인증 코드 요청 신호 암호화 단계(S110) 이전 단계에서 전자 기기(100)의 고유 번호인 시리얼 번호를 수신하여 저장한다. 전자 기기 인증 매니저 장치(110)는 저장하고 있는 시리얼 번호가 포함된 인증 코드 요청

신호를 생성한다.

[0088] 유니크 아이디는 전자 기기(100) 내부에 실장된 칩의 아이디이다. 유니크 아이디는 전자 기기(100)가 생성하는 정보이다. 유니크 아이디는 칩이 실장된 전자 기기(100)의 시리얼 번호에 솔트를 적용한 결과에 해쉬를 취한 결과이다. 전자 기기(100) 마다 고유 번호인 시리얼 번호가 있음은 전술하였다. 솔트는 사용자가 설정한 값으로 시리얼 번호와 유니크 아이디의 관련성이 노출되지 않도록 하기 위한 값이다. 솔트를 적용한 다는 것은 시리얼 번호에 사용자가 지정한 값, 예를 들면, "1234"를 시리얼 번호와 논리 연산을 한다는 것이다. 솔트값과 시리얼 번호를 논리 연산 한 결과에 해쉬를 취한 결과가 유니크 아이디이다.

[0089] 난수는 랜덤 값으로, 전자 기기 인증 매니저 장치(110)가 생성한 값이다.

[0090] 트랜잭션 아이디는 상기 트랜잭션 아이디를 포함하는 신호를 전자 기기 인증 서버(120) 장치가 몇번째로 수신한 신호인지를 의미하는 아이디이다. 전자 기기 인증 서버(120) 장치는 하나 이상의 전자 기기 인증 매니저 장치(110)와 통신하여 인증 코드를 생성한다. 전자 기기 인증 서버(120) 장치는 복수의 전자 기기 인증 매니저 장치(110)로부터 암호화된 인증 코드 요청 신호를 한번 이상 수신할 수 있다. 전자 기기 인증 서버(120) 장치가 암호화된 인증 코드 요청 신호를 통해 인증 코드 요청을 받는 횟수는 적어도 한번 이상이다. 전자 기기 인증 서버(120) 장치는 암호화된 인증 코드 요청 신호가 수신된 순서에 따라 트랜잭션 아이디를 생성하여, 트랜잭션 아이디가 포함된 인증 코드를 생성한다.

[0091] 유효 시간은 인증 코드의 유효 기간이다. 전자 기기 인증 서버(120) 장치는 전자 기기(100)의 종류 및 사용될 위치에 따라 유효 시간을 다양하게 설정할 수 있다. 서명된 인증 코드가 전자 기기(100)에 저장된 시점을 기산점으로 하여 유효 시간만큼 전자 기기(100)를 사용할 수 있는 것이다. 유효 시간은 예를 들어 1년이다.

[0092] 유효 횟수는 서명된 인증 코드가 저장된 전자 기기(100)가 특정 위치에서 사용되기 위해 특정 위치에 설치된 게이트웨이와 통신할 때 최대 통신 횟수이다. 유효 횟수가 5라면 전자 기기(100)는 게이트웨이와 5번 통신할 수 있다.

[0093] 접근 제어 정책은 전자 기기(100)를 어떤 게이트웨이와 연결할 수 있는지에 대한 정보이다. 전자 기기(100) 별로 모든 게이트웨이와 통신할 수 있는 전자 기기(100), 특정 게이트웨이와만 연결할 수 있는 전자 기기(100)로 구별될 수 있다. 접근 제어 정책 정보에는 예를 들어, 전자 기기(100)가 접속 가능한 또는 접속 불가능한 게이트우에이의 아이디가 포함될 수 있다.

[0094] 암호화 알고리즘은 전자 기기 인증 서버(120) 장치가 서명된 인증 코드를 암호활 할 때 어떤 암호화 알고리즘을 통해 암호화 했는지를 나타내는 정보이다. 전자 기기 인증 매니저 장치(110)는 인증 코드에 포함된 암호화 알고리즘을 통해 암호화된 서명된 인증 코드를 복호화한다.

[0095] 본 발명에 따른 인증 코드는 종래의 인증 코드와 달리 전자 기기(100)를 인증하기 위해 필요한 최소한의 정보만을 포함하되, 종래의 인증 코드와 구별되는 정보인 유효 시간 및 유효 횟수를 포함한다.

[0096] 도 4는 일 실시예에 따른 전자 기기(100) 인증 방법의 흐름을 도시한다.

[0097] 일 양상에 있어서, 전자 기기(100) 인증 방법은 인증 코드 요청 신호 암호화 단계(S110) 이전에 전자 기기(100) 칩 정보 수신 단계(S410) 및 근거리 무선 통신 접속 단계(S420)를 더 포함할 수 있다. 도 1 에 도시된 전자 기기(100) 인증 방법은 전자 기기(100)가 전자 기기 인증 서버(120)로부터 인증 코드를 발급받는 과정의 흐름을 도시한 것이다. 전자 기기(100)가 전자 기기 인증 서버(120)로부터 인증 코드를 발급 받기 전에 전자 기기(100)는 전자 기기 인증 매니저 장치(110)와 무선 통신을 해야한다. 즉, 도 4에 도시된 흐름도는 도 1에 따라 전자 기기(100)가 인증 코드를 부여 받기 전에 전자 기기(100)가 전자 기기 인증 매니저 장치(110)에 접속하는 과정을 도시하는 것이다.

[0098] 일 실시예에 있어서, 전자 기기(100) 칩 정보 수신 단계(S410)는 전자 기기(100) 매니저 장치가 전자 기기(100) 내부에 실장된 칩 정보를 수신한다. 이에 대한 상세한 과정은 후술한다.

[0099] 일 실시예에 있어서, 근거리 무선 통신 접속 단계(S420)는 전자 기기(100) 매니저 장치가 전자 기기(100)의 근거리 무선 통신 접속을 허용한다. 후술할 전자 기기(100) 정보 요청 신호에 포함된 전자 기기(100) 정보 요청 명령 정보와 전자 기기(100)가 생성한 전자 기기(100) 정보 요청 명령 정보가 일치하는 경우, 전자 기기 인증 매니저 장치(110)는 전자 기기(100)의 근거리 무선 통신 접속을 허용한다. 이에 대한 상세한 과정은 후술한다.

[0100] 도 5는 일 실시예에 따른 전자 기기(100) 칩 정보 수신 단계(S410)의 구체적인 흐름을 도시한다.

[0101] 일 양상에 있어서, 전자 기기(100) 정보 수신 단계는 전자 기기(100) 칩 정보 요청 신호 송신 단계(S510), 전자 기기(100) 칩 정보 응답 신호 송신 단계(S520), 전자 기기(100) 칩 버전 요청 신호 송신 단계(S530), 전자 기기(100) 칩 버전 요청 신호 송신 단계(S530), 전자 기기(100) 칩 버전 응답 신호 송신 단계(S540)를 포함한다.

[0102] 일 실시예에 있어서, 전자 기기(100) 칩 정보 요청 신호 송신 단계(S510)는 전자 기기 인증 매니저 장치(110)가 전자 기기(100)로 전자 기기(100) 칩 정보 요청 신호를 송신한다. 전자 기기(100) 칩 정보 요청 신호는 메시지 타입, 체크 아이디 및 기타 정보를 포함한다.

[0103] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫 번째 바이트에 설정되는 값으로 전자 기기(100) 칩 정보 요청 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 전자 기기(100) 칩 정보 요청 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 전자 기기(100) 칩 정보 요청 신호의 메시지 타입은 qwE0이다. qwE0값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기(100)는, 상기 신호를 전자 기기(100) 칩 정보 요청 신호라고 인식할 수 있다.

[0104] 체크 아이디는 전자 기기 인증 매니저 장치(110)의 명칭에 현재 시간을 더한 값과 솔트 값을 논리 연산한 결과에 해쉬함수를 취해서 산출된 아이디이다. 즉, 전자 기기 인증 매니저 장치(110)는 Hash(솔트 | 전자 기기 인증 매니저 장치(110) 명칭, 현재 시간)을 통해 체크 아이디를 산출한다.

[0105] 기타 정보에는 전자 기기 인증 매니저 장치(110)의 명칭 및 현재 시간을 포함한다.

[0106] 일 실시예에 있어서, 전자 기기(100) 칩 정보 응답 신호 송신 단계(S520)는 전자 기기(100)가 전자 기기 인증 매니저 장치(110)로 전자 기기(100) 칩 정보 응답 신호를 송신한다. 전자 기기(100) 칩 정보 응답 신호는 메시지 타입, 체크 아이디 및 기타 정보를 포함한다.

[0107] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫 번째 바이트에 설정되는 값으로 전자 기기(100) 칩 정보 응답 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 전자 기기(100) 칩 정보 응답 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 전자 기기(100) 칩 정보 응답 신호의 메시지 타입은 qwE0이다. qwE0값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기 인증 매니저 장치(110)는, 상기 신호를 전자 기기(100) 칩 정보 응답 신호라고 인식할 수 있다.

[0108] 체크 아이디는 솔트 값, 시리얼 번호, 에드 값 및 키 값을 논리 연산한 결과에 해쉬함수를 취해서 산출된 아이디이다. 즉, 전자 기기(100)는 Hash(솔트 값 |시리얼 번호 |에드 값 |키 값)을 통해 체크 아이디를 산출한다. 여기서 에드 값 및 키 값은 전자 기기(100)가 생성한 난수 값이다.

[0109] 기타 정보에는 시리얼 번호, 에드 값 및 키 값을 포함 한다.

[0110] 일 실시예에 있어서, 전자 기기(100) 칩 버전 요청 신호 송신 단계(S530)는 전자 기기 인증 매니저 장치(110)가 전자 기기(100)로 전자 기기(100) 칩 버전 요청 신호를 송신한다.

[0111] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫 번째 바이트에 설정되는 값으로 전자 기기(100) 칩 정보 요청 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 전자 기기(100) 칩 버전 요청 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 전자 기기(100) 칩 버전 요청 신호의 메시지 타입은 qwE1이다. qwE1값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기(100)는, 상기 신호를 전자 기기(100) 칩 버전 요청 신호라고 인식할 수 있다.

[0112] 체크 아이디는 솔트 값, 전자 기기 인증 매니저 장치(110)의 명칭, 버전, 현재 시간을 논리 연산 한 결과에 해쉬함수를 취해서 산출된 아이디이다. 즉, 전자 기기 인증 매니저 장치(110)는 Hash(솔트 값 | 전자 기기 인증 매니저 장치(110) 명칭 | 버전 |현재 시간)을 통해 체크 아이디를 산출한다. 버전은 전자 기기(100) 인증 방법의 버전에 대한 버전값이다. 예를 들어, 현재 버전이 0.1이면 버전값은 qw01이다.

[0113] 기타 정보에는 전자 기기 인증 매니저 장치(110)의 명칭, 버전 및 현재 시간을 포함한다.

[0114] 일 실시예에 있어서, 전자 기기(100) 칩 버전 응답 신호 송신 단계(S540)는 전자 기기(100)가 전자 기기 인증 매니저 장치(110)로 전자 기기(100) 칩 버전 응답 신호를 송신한다. 전자 기기(100) 칩 버전 응답 신호는 메시지 타입, 체크 아이디 및 기타 정보를 포함한다.

[0115] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫 번째 바이트에 설정되는 값으로 전자 기기(100) 칩 버전 응답 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 전자 기기(100)

칩 버전 응답 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 전자 기기(100) 칩 정보 응답 신호의 메시지 타입은 qwE1이다. qwE1값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기 인증 매니저 장치(110)는, 상기 신호를 전자 기기(100) 칩 버전 응답 신호라고 인식할 수 있다.

[0116] 체크 아이디는 솔트 값, 시리얼 번호, 버전을 논리 연산한 결과에 해쉬함수를 취해서 산출된 아이디이다. 즉, 전자 기기(100)는 Hash(솔트 값 |시리얼 번호 |버전)을 통해 체크 아이디를 산출한다. 여기서 버전은 전자 기기(100) 칩 버전요청 신호 송신 단계에서 전자 기기(100) 칩 버전 요청 신호가 포함하는 버전과 동일하다. 솔트 값은 전자 기기(100) 또는 잔자 기기 인증 매니저 장치가 설정하는 값으로 자유롭게 설정될 수 있다.

[0117] 기타 정보에는 시리얼 번호, 버전을 포함 한다.

[0118] 일 실시예에 있어서, 전자 기기(100) 칩 정보 요청 신호 송신 단계(S510)는 전자 기기 인증 매니저 장치(110)가 전자 기기(100) 칩 정보 요청 신호 송신 신호에 포함된 데이터와 디폴트 값인 에드값을 더한 결과에 디폴트 값인 키 값과 논리 연산을 취하여 암호화하고, 암호화된 전자 기기(100) 칩 정보 요청 신호를 송신한다.

[0119] 전자 기기 인증 매니저 장치(110)는 전자 기기(100) 칩 정보 요청 신호를 암호화하는데 전술한 방법으로 암호화하여 전자 기기(100)로 송신한다. 즉, 전자 기기 인증 매니저 장치(110)는 (전자 기기(100) 칩 정보 요청 신호에 포함된 데이터 + 에드 값) 논리 연산 키 값이라는 연산을 통해 전자 기기(100) 칩 정보 요청 신호에 포함된 데이터를 암호화 한다. 논리 연산은 and, or, xor, nand 중 적어도 하나이다. 전자 기기(100) 칩 정보 요청 신호에 포함된 데이터를 암호화 한 것은 전자 기기(100) 칩 정보 요청 신호를 암호화 한 것과 같은 의미이다. 여기서 에드 값 및 키 값은 디폴트 값이다. 예를 들어, 에드 값의 디폴트 값은 qw1234이고 키 값의 디폴트 값은 qw7445이다.

[0120] 암호화된 전자 기기(100) 칩 정보 요청 신호를 수신한 전자 기기(100)는 암호화된 전자 기기(100) 칩 정보 요청 신호를 복호화 한다. 암호화된 전자 기기(100) 칩 정보 요청 신호에 포함된 데이터와 키 값을 논리 연산하고 에드 값을 빼서 전자 기기(100) 칩 정보 요청 신호가 포함하는 데이터를 산출한다. 즉, (암호화된 전자 기기(100) 칩 정보 요청 신호에 포함된 데이터 논리 연산 키 값) - 에드 값 이란 연산을 통해 전자 기기(100)는 전자 기기(100) 칩 정보 요청 신호에 포함된 데이터를 얻는다.

[0121] 일 실시예에 있어서, 전자 기기(100) 칩 정보 응답 신호 송신 단계(S520)는 전자 기기(100)가 전자 기기(100) 칩 정보 응답 신호에 포함된 데이터와 디폴트 값인 에드값을 더한 결과에 디폴트 값인 키 값과 논리 연산을 취하여 암호화하고, 암호화된 전자 기기(100) 칩 정보 응답 신호를 송신한다.

[0122] 전자 기기(100)는 전자 기기(100) 칩 정보 응답 신호를 암호화하는데 전술한 방법으로 암호화하여 전자 기기 인증 매니저 장치(110)로 송신한다. 즉, 전자 기기 인증 매니저 장치(110)는 (전자 기기(100) 칩 정보 응답 신호에 포함된 데이터 + 에드 값) 논리 연산 키 값이라는 연산을 통해 전자 기기(100) 칩 정보 요청 신호에 포함된 데이터를 암호화 한다. 전자 기기(100) 칩 정보 응답 신호에 포함된 데이터를 암호화 한 것은 전자 기기(100) 칩 정보 응답 신호를 암호화 한 것과 같은 의미이다. 여기서 에드 값 및 키 값은 전자 기기(100)가 생성한 난수 값이다.

[0123] 암호화된 전자 기기(100) 칩 정보 응답 신호를 수신한 전자 기기 인증 매니저 장치(110)는 암호화된 전자 기기(100) 칩 정보 응답 신호를 복호화 한다. 암호화된 전자 기기(100) 칩 정보 응답 신호에 포함된 데이터와 키 값을 논리 연산하고 에드 값을 빼서 전자 기기(100) 칩 정보 응답 신호가 포함하는 데이터를 산출한다. 즉, (암호화된 전자 기기(100) 칩 정보 응답 신호에 포함된 데이터 논리 연산 키 값) - 에드 값 이란 연산을 통해 전자 기기 인증 매니저 장치(110)는 전자 기기(100) 칩 정보 응답 신호에 포함된 데이터를 얻는다. 전자 기기 인증 매니저 장치(110)는 전자 기기(100)가 송신한 전자 기기(100) 칩 정보 응답 신호에 포함된 에드 값 및 키 값을 수신하기에 에드 값 및 키 값을 통해 복호화할 수 있다.

[0124] 일 실시예에 있어서, 전자 기기(100) 칩 버전 요청 신호 송신 단계(S530)는 전자 기기 인증 매니저 장치(110)가 전자 기기(100) 칩 버전 요청 신호 송신 신호에 포함된 데이터와 전자 기기(100) 칩 정보 응답 신호에 포함된 에드값을 더한 결과에 전자 기기(100) 칩 정보 응답 신호에 포함된 키 값과 논리 연산을 취하여 암호화하고, 암호화된 전자 기기(100) 칩 버전 요청 신호를 송신한다.

[0125] 전자 기기 인증 매니저 장치(110)는 전자 기기(100) 칩 버전 요청 신호를 암호화하는데 전술한 방법으로 암호화하여 전자 기기(100)로 송신한다. 즉, 전자 기기 인증 매니저 장치(110)는 (전자 기기(100) 칩 버전 요청 신호에 포함된 데이터 + 에드 값) 논리 연산 키 값이라는 연산을 통해 전자 기기(100) 칩 버전 요청 신호에 포함된

데이터를 암호화 한다. 전자 기기(100) 칩 버전 요청 신호에 포함된 데이터를 암호화 한 것은 전자 기기(100) 칩 버전 요청 신호를 암호화 한 것과 같은 의미이다. 여기서 에드 값 및 키 값은 전자 기기(100)가 생성한 난수 값이다.

[0126] 암호화된 전자 기기(100) 칩 버전 요청 신호를 수신한 전자 기기(100)는 암호화된 전자 기기(100) 칩 버전 요청 신호를 복호화 한다. 암호화된 전자 기기(100) 칩 버전 요청 신호에 포함된 데이터와 키 값을 논리 연산하고, 그 결과에 에드 값을 빼서 전자 기기(100) 칩 버전 요청 신호가 포함하는 데이터를 산출한다. 즉, (암호화된 전자 기기(100) 칩 버전 요청 신호에 포함된 데이터 논리 연산 키 값) - 에드 값 이란 연산을 통해 전자 기기(100)는 전자 기기(100) 칩 버전 요청 신호에 포함된 데이터를 얻는다.

[0127] 일 실시예에 있어서, 전자 기기(100) 칩 버전 응답 신호 송신 단계(S540)는 전자 기기(100)가 전자 기기(100) 칩 버전 응답 신호에 포함된 데이터와 전자 기기(100) 칩 정보 응답 신호에 포함된 에드값을 더한 결과에 전자 기기(100) 칩 정보 응답 신호에 포함된 키 값과 논리 연산을 취하여 암호화하고, 암호화된 전자 기기(100) 칩 버전 응답 신호를 송신한다.

[0128] 전자 기기(100)는 전자 기기(100) 칩 버전 응답 신호를 암호화하는데 전술한 방법으로 암호화하여 전자 기기 인증 매니저 장치(110)로 송신한다. 즉, 전자 기기 인증 매니저 장치(110)는 (전자 기기(100) 칩 버전 응답 신호에 포함된 데이터 + 에드 값) 논리 연산 키 값이라는 연산을 통해 전자 기기(100) 칩 버전 요청 신호에 포함된 데이터를 암호화 한다. 전자 기기(100) 칩 버전 응답 신호에 포함된 데이터를 암호화 한 것은 전자 기기(100) 칩 버전 응답 신호를 암호화 한 것과 같은 의미이다. 여기서 에드 값 및 키 값은 전자 기기(100)가 생성한 난수 값이다.

[0129] 암호화된 전자 기기(100) 칩 버전 응답 신호를 수신한 전자 기기 인증 매니저 장치(110)는 암호화된 전자 기기(100) 칩 버전 응답 신호를 복호화 한다. 암호화된 전자 기기(100) 칩 버전 응답 신호에 포함된 데이터와 키 값을 논리 연산하고 에드 값을 빼서 전자 기기(100) 칩 버전 응답 신호가 포함하는 데이터를 산출한다. 즉, (암호화된 전자 기기(100) 칩 버전 응답 신호에 포함된 데이터 논리 연산 키 값) - 에드 값 이란 연산을 통해 전자 기기 인증 매니저 장치(110)는 전자 기기(100) 칩 버전 응답 신호에 포함된 데이터를 얻는다. 전자 기기 인증 매니저 장치(110)는 전자 기기(100)가 송신한 전자 기기(100) 칩 정보 응답 신호에 포함된 에드 값 및 키 값을 수신하기에 에드 값 및 키 값을 통해 복호화할 수 있다.

[0130] 도 6은 전자 기기(100)와 전자 기기 인증 매니저 장치(110)간의 전자 기기(100) 칩 정보 수신 단계(S410)의 동작 과정을 설명하기 위한 흐름도이다.

[0131] 일 실시예에 있어서, 전자 기기(100) 칩 정보 요청 신호 송신 단계(S510)는 전자 기기 인증 매니저 장치(110)가 전자 기기(100)로 전자 기기(100) 칩 정보 요청 신호를 송신한다. 전자 기기(100) 칩 정보 요청 신호는 메시지 타입, 체크 아이디 및 기타 정보를 포함한다.

[0132] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫 번째 바이트에 설정되는 값으로 전자 기기(100) 칩 정보 요청 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 전자 기기(100) 칩 정보 요청 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 전자 기기(100) 칩 정보 요청 신호의 메시지 타입은 qwE0이다. qwE0값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기(100)는, 상기 신호를 전자 기기(100) 칩 정보 요청 신호라고 인식할 수 있다.

[0133] 체크 아이디는 전자 기기 인증 매니저 장치(110)의 명칭에 현재 시간을 더한 값과 솔트 값을 논리연산한 결과에 해쉬함수를 취해서 산출된 아이디이다. 즉, 전자 기기 인증 매니저 장치(110)는 Hash(솔트 | 전자 기기 인증 매니저 장치(110) 명칭, 현재 시간)을 통해 체크 아이디를 산출한다.

[0134] 기타 정보에는 전자 기기 인증 매니저 장치(110)의 명칭 및 현재 시간을 포함한다.

[0135] 일 실시예에 있어서, 전자 기기(100) 칩 정보 응답 신호 송신 단계(S520)는 전자 기기(100)가 전자 기기 인증 매니저 장치(110)로 전자 기기(100) 칩 정보 응답 신호를 송신한다. 전자 기기(100) 칩 정보 응답 신호는 메시지 타입, 체크 아이디 및 기타 정보를 포함한다.

[0136] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫 번째 바이트에 설정되는 값으로 전자 기기(100) 칩 정보 응답 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 전자 기기(100) 칩 정보 응답 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 전자 기기(100) 칩 정보 응답 신호의 메시지 타입은 qwE0이다. qwE0값이 신호의 첫번째 바이트로 설정된 신호

를 수신하는 전자 기기 인증 매니저 장치(110)는, 상기 신호를 전자 기기(100) 칩 정보 응답 신호라고 인식할 수 있다.

[0137] 체크 아이디는 솔트 값, 시리얼 번호, 에드 값 및 키 값을 논리 연산한 결과에 해쉬함수를 취해서 산출된 아이디이다. 즉, 전자 기기(100)는 Hash(솔트 값 |시리얼 번호 |에드 값 |키 값)을 통해 체크 아이디를 산출한다. 여기서 에드 값 및 키 값은 전자 기기(100)가 생성한 난수 값이다.

[0138] 기타 정보에는 시리얼 번호, 에드 값 및 키 값을 포함 한다.

[0139] 일 실시예에 있어서, 전자 기기(100) 칩 버전 요청 신호 송신 단계(S530)는 전자 기기 인증 매니저 장치(110)가 전자 기기(100)로 전자 기기(100) 칩 버전 요청 신호를 송신한다.

[0140] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫 번째 바이트에 설정되는 값으로 전자 기기(100) 칩 정보 요청 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 전자 기기(100) 칩 버전 요청 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 전자 기기(100) 칩 버전 요청 신호의 메시지 타입은 qwE1이다. qwE1값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기(100)는, 상기 신호를 전자 기기(100) 칩 버전 요청 신호라고 인식할 수 있다.

[0141] 체크 아이디는 솔트 값, 전자 기기 인증 매니저 장치(110)의 명칭, 버전, 현재 시간을 논리 연산 한 결과에 해쉬함수를 취해서 산출된 아이디이다. 즉, 전자 기기 인증 매니저 장치(110)는 Hash(솔트 값 | 전자 기기 인증 매니저 장치(110) 명칭 | 버전 |현재 시간)을 통해 체크 아이디를 산출한다. 버전은 전자 기기(100) 인증 방법의 버전이다. 예를 들어, 현재 버전은 0.1이다.

[0142] 기타 정보에는 전자 기기 인증 매니저 장치(110)의 명칭, 버전 및 현재 시간을 포함한다.

[0143] 일 실시예에 있어서, 전자 기기(100) 칩 버전 응답 신호 송신 단계(S540)는 전자 기기(100)가 전자 기기 인증 매니저 장치(110)로 전자 기기(100) 칩 버전 응답 신호를 송신한다. 전자 기기(100) 칩 버전 응답 신호는 메시지 타입, 체크 아이디 및 기타 정보를 포함한다.

[0144] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫 번째 바이트에 설정되는 값으로 전자 기기(100) 칩 버전 응답 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 전자 기기(100) 칩 버전 응답 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 전자 기기(100) 칩 정보 응답 신호의 메시지 타입은 qwE1이다. qwE1값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기 인증 매니저 장치(110)는, 상기 신호를 전자 기기(100) 칩 버전 응답 신호라고 인식할 수 있다.

[0145] 체크 아이디는 솔트 값, 시리얼 번호, 버전을 논리 연산한 결과에 해쉬함수를 취해서 산출된 아이디이다. 즉, 전자 기기(100)는 Hash(솔트 값 |시리얼 번호 |버전)을 통해 체크 아이디를 산출한다. 여기서 버전은 전자 기기(100) 칩 버전요청 신호 송신 단계에서 전자 기기(100) 칩 버전 요청 신호가 포함하는 버전과 동일하다. 솔트 값은 전자 기기(100) 또는 전자 기기 인증 매니저 장치(110)가 설정하는 값으로 자유롭게 설정될 수 있다.

[0146] 기타 정보에는 시리얼 번호, 버전을 포함 한다.

[0147] 일 실시예에 있어서, 전자 기기(100) 칩 정보 요청 신호 송신 단계(S510)는 전자 기기 인증 매니저 장치(110)가 전자 기기(100) 칩 정보 요청 신호 송신 신호에 포함된 데이터와 디폴트 값인 에드값을 더한 결과에 디폴트 값인 키 값과 논리 연산을 취하여 암호화하고, 암호화된 전자 기기(100) 칩 정보 요청 신호를 송신한다.

[0148] 전자 기기 인증 매니저 장치(110)는 전자 기기(100) 칩 정보 요청 신호를 암호화하는데 전술한 방법으로 암호화하여 전자 기기(100)로 송신한다. 즉, 전자 기기 인증 매니저 장치(110)는 (전자 기기(100) 칩 정보 요청 신호에 포함된 데이터 + 에드 값) 논리 연산 키 값이라는 연산을 통해 전자 기기(100) 칩 정보 요청 신호에 포함된 데이터를 암호화 한다. 전자 기기(100) 칩 정보 요청 신호에 포함된 데이터를 암호화 한 것은 전자 기기(100) 칩 정보 요청 신호를 암호화 한 것과 같은 의미이다. 여기서 에드 값 및 키 값은 디폴트 값이다. 예를 들어, 에드 값의 디폴트 값은 qw1234이고 키 값의 디폴트 값은 qw7445이다.

[0149] 암호화된 전자 기기(100) 칩 정보 요청 신호를 수신한 전자 기기(100)는 암호화된 전자 기기(100) 칩 정보 요청 신호를 복호화 한다. 암호화된 전자 기기(100) 칩 정보 요청 신호에 포함된 데이터와 키 값을 논리 연산하고 에드 값을 빼서 전자 기기(100) 칩 정보 요청 신호가 포함하는 데이터를 산출한다. 즉, (암호화된 전자 기기(100) 칩 정보 요청 신호에 포함된 데이터 논리 연산 키 값) - 에드 값 이란 연산을 통해 전자 기기(100)는 전

자 기기(100) 칩 정보 요청 신호에 포함된 데이터를 얻는다.

[0150] 일 실시예에 있어서, 전자 기기(100) 칩 정보 응답 신호 송신 단계(S520)는 전자 기기(100)가 전자 기기(100) 칩 정보 응답 신호에 포함된 데이터와 디폴트 값인 에드값을 더한 결과에 디폴트 값인 키 값과 논리 연산을 취하여 암호화하고, 암호화된 전자 기기(100) 칩 정보 응답 신호를 송신한다.

[0151] 전자 기기(100)는 전자 기기(100) 칩 정보 응답 신호를 암호화하는데 전술한 방법으로 암호화하여 전자 기기 인증 매니저 장치(110)로 송신한다. 즉, 전자 기기 인증 매니저 장치(110)는 (전자 기기(100) 칩 정보 응답 신호에 포함된 데이터 + 에드 값) 논리 연산 키 값이라는 연산을 통해 전자 기기(100) 칩 정보 요청 신호에 포함된 데이터를 암호화 한다. 전자 기기(100) 칩 정보 응답 신호에 포함된 데이터를 암호화 한 것은 전자 기기(100) 칩 정보 응답 신호를 암호화 한 것과 같은 의미이다. 여기서 에드 값 및 키 값은 전자 기기(100)가 생성한 난수 값이다.

[0152] 암호화된 전자 기기(100) 칩 정보 응답 신호를 수신한 전자 기기 인증 매니저 장치(110)는 암호화된 전자 기기(100) 칩 정보 응답 신호를 복호화 한다. 암호화된 전자 기기(100) 칩 정보 응답 신호에 포함된 데이터와 키 값을 논리 연산하고 에드 값을 빼서 전자 기기(100) 칩 정보 응답 신호가 포함하는 데이터를 산출한다. 즉, (암호화된 전자 기기(100) 칩 정보 응답 신호에 포함된 데이터 논리 연산 키 값) - 에드 값 이란 연산을 통해 전자 기기 인증 매니저 장치(110)는 전자 기기(100) 칩 정보 응답 신호에 포함된 데이터를 얻는다. 전자 기기 인증 매니저 장치(110)는 전자 기기(100)가 송신한 전자 기기(100) 칩 정보 응답 신호에 포함된 에드 값 및 키 값을 수신하기에 에드 값 및 키 값을 통해 복호화할 수 있다.

[0153] 일 실시예에 있어서, 전자 기기(100) 칩 버전 요청 신호 송신 단계(S530)는 전자 기기 인증 매니저 장치(110)가 전자 기기(100) 칩 버전 요청 신호 송신 신호에 포함된 데이터와 전자 기기(100) 칩 정보 응답 신호에 포함된 에드값을 더한 결과에 전자 기기(100) 칩 정보 응답 신호에 포함된 키 값과 논리 연산을 취하여 암호화하고, 암호화된 전자 기기(100) 칩 버전 요청 신호를 송신한다.

[0154] 전자 기기 인증 매니저 장치(110)는 전자 기기(100) 칩 버전 요청 신호를 암호화하는데 전술한 방법으로 암호화하여 전자 기기(100)로 송신한다. 즉, 전자 기기 인증 매니저 장치(110)는 (전자 기기(100) 칩 버전 요청 신호에 포함된 데이터 + 에드 값) 논리 연산 키 값이라는 연산을 통해 전자 기기(100) 칩 버전 요청 신호에 포함된 데이터를 암호화 한다. 전자 기기(100) 칩 버전 요청 신호에 포함된 데이터를 암호화 한 것은 전자 기기(100) 칩 버전 요청 신호를 암호화 한 것과 같은 의미이다. 여기서 에드 값 및 키 값은 전자 기기(100)가 생성한 난수 값이다.

[0155] 암호화된 전자 기기(100) 칩 버전 요청 신호를 수신한 전자 기기(100)는 암호화된 전자 기기(100) 칩 버전 요청 신호를 복호화 한다. 암호화된 전자 기기(100) 칩 버전 요청 신호에 포함된 데이터와 키 값을 논리 연산하고, 그 결과에 에드 값을 빼서 전자 기기(100) 칩 버전 요청 신호가 포함하는 데이터를 산출한다. 즉, (암호화된 전자 기기(100) 칩 버전 요청 신호에 포함된 데이터 논리 연산 키 값) - 에드 값 이란 연산을 통해 전자 기기(100)는 전자 기기(100) 칩 버전 요청 신호에 포함된 데이터를 얻는다.

[0156] 일 실시예에 있어서, 전자 기기(100) 칩 버전 응답 신호 송신 단계(S540)는 전자 기기(100)가 전자 기기(100) 칩 버전 응답 신호에 포함된 데이터와 전자 기기(100) 칩 정보 응답 신호에 포함된 에드값을 더한 결과에 전자 기기(100) 칩 정보 응답 신호에 포함된 키 값과 논리 연산을 취하여 암호화하고, 암호화된 전자 기기(100) 칩 버전 응답 신호를 송신한다.

[0157] 전자 기기(100)는 전자 기기(100) 칩 버전 응답 신호를 암호화하는데 전술한 방법으로 암호화하여 전자 기기 인증 매니저 장치(110)로 송신한다. 즉, 전자 기기 인증 매니저 장치(110)는 (전자 기기(100) 칩 버전 응답 신호에 포함된 데이터 + 에드 값) 논리 연산 키 값이라는 연산을 통해 전자 기기(100) 칩 버전 요청 신호에 포함된 데이터를 암호화 한다. 전자 기기(100) 칩 버전 응답 신호에 포함된 데이터를 암호화 한 것은 전자 기기(100) 칩 버전 응답 신호를 암호화 한 것과 같은 의미이다. 여기서 에드 값 및 키 값은 전자 기기(100)가 생성한 난수 값이다.

[0158] 암호화된 전자 기기(100) 칩 버전 응답 신호를 수신한 전자 기기 인증 매니저 장치(110)는 암호화된 전자 기기(100) 칩 버전 응답 신호를 복호화 한다. 암호화된 전자 기기(100) 칩 버전 응답 신호에 포함된 데이터와 키 값을 논리 연산하고 에드 값을 빼서 전자 기기(100) 칩 버전 응답 신호가 포함하는 데이터를 산출한다. 즉, (암호화된 전자 기기(100) 칩 버전 응답 신호에 포함된 데이터 논리 연산 키 값) - 에드 값 이란 연산을 통해 전자 기기 인증 매니저 장치(110)는 전자 기기(100) 칩 버전 응답 신호에 포함된 데이터를 얻는다. 전자 기기

인증 매니저 장치(110)는 전자 기기(100)가 송신한 전자 기기(100) 칩 정보 응답 신호에 포함된 에드 값 및 키 값을 수신하기에 에드 값 및 키 값을 통해 복호화할 수 있다.

[0159] 도 7은 일 실시예에 따른 근거리 무선 통신 접속 단계(S420)의 구체적인 흐름을 도시한다.

[0160] 일 양상에 있어서, 근거리 무선 통신 접속 단계(S420)는 임의값 요청 신호 송신 단계(S710), 임의값 요청 신호 송신 단계(S720), 전자 기기(100) 정보 요청 신호 송신 단계(S730), 전자 기기(100) 정보 응답 신호 송신 단계(S740)를 포함한다.

[0161] 일 실시예에 있어서, 임의값 요청 신호 송신 단계(S710)는 전자 기기 인증 매니저 장치(110)가 전자 기기(100)로 임의값(Nounce) 요청 신호를 송신한다. 임의 값 요청 신호는 메시지 타입, 메시지 길이, 클라이언트 타입, 버전을 포함한다.

[0162] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫번째 바이트에 설정되는 값으로 임의값 요청 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 임의값 요청 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 임의값 요청 신호의 메시지 타입은 qwa1이다. qwa1값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기(100)는, 상기 신호를 임의값 요청 신호라고 인식할 수 있다.

[0163] 메시지 길이는 전체 메시지 사이즈에서 메시지 타입과 메시지 길이를 뺀 메시지 사이즈이다. 여기서 사이즈는 크기이다. 임의값 요청 신호는 메시지 타입 및 메시지 길이를 포함하여 다른 여러 정보를 포함 한다고 전술하였다. 여기서, 메시지 길이는 임의 값 요청 신호가 포함하는 모든 정보의 사이즈, 즉 크기에서 메시지 타입에 해당하는 사이즈 및 메시지 길이에 해당하는 사이즈를 뺀 사이즈이다. 메시지 타입의 크기가 1바이트이고, 메시지 길이 자체의 크기가 4바이트 이고, 전체 메시지의 크기가 85바이트라면, 메시지 길이는 80바이트가 된다. 여기서, 전체 메시지의 크기는 임의 값 요청 신호의 크기이다.

[0164] 클라이언트 타입은 클라이언트 종류에 대한 정보이다. 클라이언트 종류는 예를 들어 게이트웨이 또는 전자 기기 인증 매니저 장치(110)이다. 클라이언트가 게이트웨이라면 클라이언트 타입은 qw00000001이다. 클라이언트가 전자 기기 인증 매니저 장치(110)라면 클라이언트 타입은 qw00000002이다.

[0165] 일 실시예에 있어서, 임의값 요청 신호 송신 단계(S720)는 전자 기기(100)가 임의값 응답 신호를 생성하여 임의값 응답 신호를 전자 기기 인증 매니저 장치(110)로 송신한다. 임의값 응답 신호는 메시지 타입, 메시지 길이, 결과 코드 및 임의값을 포함한다.

[0166] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫번째 바이트에 설정되는 값으로 임의값 응답 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 임의값 응답 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 임의값 응답 신호의 메시지 타입은 qwc1이다. qwc1값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기(100)는, 상기 신호를 임의값 응답 신호라고 인식할 수 있다.

[0167] 메시지 길이는 전체 메시지 사이즈에서 메시지 타입과 메시지 길이를 뺀 메시지 사이즈이다. 여기서 사이즈는 크기이다. 임의값 응답 신호는 메시지 타입 및 메시지 길이를 포함하여 다른 여러 정보를 포함 한다고 전술하였다. 여기서, 메시지 길이는 임의 값 요청 신호가 포함하는 모든 정보의 사이즈, 즉 크기에서 메시지 타입에 해당하는 사이즈 및 메시지 길이에 해당하는 사이즈를 뺀 사이즈이다. 메시지 타입의 크기가 1바이트이고, 메시지 길이 자체의 크기가 4바이트 이고, 전체 메시지의 크기가 85바이트라면, 메시지 길이는 80바이트가 된다. 여기서, 전체 메시지의 크기는 임의 값 요청 신호의 크기이다.

[0168] 결과 코드는 임의값 요청 신호가 오류 없이 전자 기기(100)로 전달됐는지 여부를 표시하는 코드이다. 예를 들어 결과 코드가 0이면 임의값 요청 신호가 오류 없이 전자 기기(100)에 수신됨을 의미한다.

[0169] 임의 값은 전자 기기(100)가 생성한 난수 또는 현재 시간이다.

[0170] 일 실시예에 있어서, 전자 기기(100) 정보 요청 신호 송신 단계(S730)는 전자 기기 인증 매니저 장치(110)가 전자 기기(100)로 전자 기기(100) 정보 요청 신호를 송신한다. 전자 기기(100) 정보 요청 신호는 메시지 타입, 메시지 길이, 전자 기기(100) 정보 요청 명령 정보, 해쉬처리된 전자 기기(100) 비밀번호 및 세션 아이디를 포함한다.

[0171] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫번째 바이트에 설정되는 값으로 전자 기기(100) 정보 요청

신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 전자 기기(100) 정보 요청 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 전자 기기(100) 정보 요청 신호의 메시지 타입은 qw05이다. qw05값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기(100)는, 상기 신호를 전자 기기(100) 정보 요청 신호라고 인식할 수 있다.

[0172] 메시지 길이는 전체 메시지 사이즈에서 메시지 타입과 메시지 길이를 뺀 메시지 사이즈이다. 여기서 사이즈는 크기이다. 전자 기기(100) 정보 요청 신호는 메시지 타입 및 메시지 길이를 포함하여 다른 여러 정보를 포함한다고 전술하였다. 여기서, 메시지 길이는 전자 기기(100) 정보 요청 신호가 포함하는 모든 정보의 사이즈, 즉 크기에서 메시지 타입에 해당하는 사이즈 및 메시지 길이에 해당하는 사이즈를 뺀 사이즈이다. 메시지 타입의 크기가 1바이트이고, 메시지 길이 자체의 크기가 4바이트 이고, 전체 메시지의 크기가 85바이트라면, 메시지 길이는 80바이트가 된다. 여기서, 전체 메시지의 크기는 전자 기기(100) 정보 요청 신호의 크기이다.

[0173] 전자 기기(100) 정보 요청 명령 정보는 전자 기기 인증 매니저 장치(110)가 클라이언트 타입 정보와 임의 값을 논리연산 한 결과에 해쉬를 취하여 산출된 정보이다. 즉, 전자 기기 인증 매니저 장치(110)는 Hash(클라이언트 타입 | 임의값)이라는 연산을 통해 전자 기기(100) 정보 요청 명령 정보를 산출한다.

[0174] 해쉬처리된 전자 기기(100) 비밀번호는 전자 기기(100) 비밀번호를 해쉬 처리한 값이다. 즉, 전자 기기 인증 매니저 장치(110)가 Hash(전자 기기(100) 비밀번호)연산을 한 결과인 것이다.

[0175] 세션 아이디는 전자 기기 인증 매니저 장치(110)가 트랜잭션 아이디, 시리얼 번호, 클라이언트 타입 및 임의값을 논리 연산한 결과에 Hash함수를 취해서 산출된 아이디이다. 여기서 임의값은 세션 아이디를 생성하는 시점의 시간 또는 전자 기기 인증 매니저 장치(110)가 임의로 생성한 난수이다.

[0176] 일 실시예에 있어서, 전자 기기(100) 정보 응답 신호 송신 단계(S740)는 전자 기기(100)가 전자 기기(100) 정보 응답 신호를 생성하여 전자 기기(100) 정보 응답 신호를 전자 기기 인증 매니저 장치(110)로 송신한다. 전자 기기(100) 정보 응답 신호는 메시지 타입, 메시지 길이, 결과 코드, 유니크 아이디, 시리얼 번호를 포함한다.

[0177] 메시지 타입은 전자 기기(100) 정보 응답 신호의 첫번째 바이트에 설정되는 값으로 전자 기기(100) 정보 응답 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 전자 기기(100) 정보 응답 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 전자 기기(100) 정보 응답 신호의 메시지 타입은 qw8이다. qw8값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기(100)는, 상기 신호를 전자 기기(100) 정보 응답 신호라고 인식할 수 있다.

[0178] 메시지 길이는 전체 메시지 사이즈에서 메시지 타입과 메시지 길이를 뺀 메시지 사이즈이다. 여기서 사이즈는 크기이다. 전자 기기(100) 정보 응답 신호는 메시지 타입 및 메시지 길이를 포함하여 다른 여러 정보를 포함한다고 전술하였다. 여기서, 메시지 길이는 전자 기기(100) 정보 응답 신호가 포함하는 모든 정보의 사이즈, 즉 크기에서 메시지 타입에 해당하는 사이즈 및 메시지 길이에 해당하는 사이즈를 뺀 사이즈이다. 메시지 타입의 크기가 1바이트이고, 메시지 길이 자체의 크기가 4바이트 이고, 전체 메시지의 크기가 85바이트라면, 메시지 길이는 80바이트가 된다. 여기서, 전체 메시지의 크기는 전자 기기(100) 정보 응답 신호의 크기이다.

[0179] 결과 코드는 전자 기기(100) 정보 요청 신호에 포함된 전자 기기(100) 정보 요청 명령 정보와 전자 기기(100)가 생성한 전자 기기(100) 정보 요청 명령 정보의 일치 여부에 따라 다른 값이 된다. 전술한 전자 기기(100) 정보 요청 명령 정보가 일치하면 결과 코드는 예를 들어 0으로 산출된다. 전술한 전자 기기(100) 정보 요청 명령 정보가 일치하지 않으면 결과 코드는 예를 들어 106으로 산출된다. 전자 기기 인증 매니저 장치(110)와 전자 기기(100) 각각이 클라이언트 타입 정보와 임의값 정보를 논리 연산 한 결과에 해쉬를 취하여 산출된 결과를 비교하여 인증 과정을 거치기에 보안이 강화된다.

[0180] 유니크 아이디

[0181] 시리얼 번호는 전자 기기(100)의 고유 번호이다. 전자 기기 인증 매니저 장치(110)와 근거리 무선 통신 또는 유선 통신을 할 수 있는 전자 기기(100)마다 하나의 고유 번호를 포함한다.

[0182] 유니크 아이디는 전자 기기(100) 내부에 실장된 칩의 아이디이다. 유니크 아이디는 전자 기기(100)가 생성하는 정보이다. 유니크 아이디는 칩이 실장된 전자 기기(100)의 시리얼 번호에 솔트를 적용한 결과에 해쉬를 취한 결과이다. 전자 기기(100) 마다 고유 번호인 시리얼 번호가 있음은 전술하였다. 솔트는 사용자가 설정한 값으로 시리얼 번호와 유니크 아이디의 관련성이 노출되지 않도록 하기 위한 값이다. 솔트를 적용한 다는 것은 시리얼 번호에 사용자가 지정한 값, 예를 들면, 솔트값인 '1234'를 시리얼 번호와 논리 연산을 한다는 것이다.

솔트값과 시리얼 번호를 논리 연산 한 결과에 해쉬 함수를 취한 결과가 유니크 아이디이다.

[0183] 일 실시예에 있어서, 임의 값 응답 신호는 임의값 정보를 포함하되, 임의값 정보는 현재 시간 또는 전자 기기(100)가 생성한 난수이다. 현재 시간은 임의 값 응답 신호가 생성되는 시점의 시간이다.

[0184] 일 실시예에 있어서, 전자 기기(100) 정보 요청 신호는 전자 기기 인증 매니저 장치(110)가 임의값을 포함하는 입력과 해쉬함수를 통해 산출된 전자 기기(100) 정보 요청 커맨드 정보를 포함한다. 임의값을 포함하는 입력은 클라이언트 타입 정보와 임의값 정보이다. 입력과 해쉬함수를 통해 산출된다는 것은 전술한 입력을 해쉬 함수의 정의역으로 한다는 것이다. 본 실시예에서는 입력이 두개이기에, 입력인 클라이언트 타입 정보와 임의값 정보를 논리 연산 한 결과에 해쉬함수 취하는 것이다.

[0185] 일 실시예에 있어서, 전자 기기(100) 정보 응답 신호 송신 단계(S740)는 전자 기기(100)가 수신한 전자 기기(100) 정보 요청 신호에 포함된 전자 기기(100) 정보 요청 커맨드 정보와 전자 기기(100)가 생성한 전자 기기(100) 정보 요청 커맨드 정보를 비교하여 일치 여부에 대한 정보를 전자 기기(100) 정보 응답 신호에 포함시키고 전자 기기(100) 정보 응답 신호를 전자 기기 인증 매니저 장치(110)로 송신한다. 일치 여부에 대한 정보가 전술한 결과 코드이다.

[0186] 도 8은 전자 기기(100)와 전자 기기 인증 매니저 장치(110)간의 근거리 무선 통신 접속 단계(S420)의 동작 과정을 설명하기 위한 흐름도이다.

[0187] 일 실시예에 있어서, 임의값 요청 신호 송신 단계(S710)는 전자 기기 인증 매니저 장치(110)가 전자 기기(100)로 임의값(Nounce) 요청 신호를 송신한다. 임의 값 요청 신호는 메시지 타입, 메시지 길이, 클라이언트 타입, 버전을 포함한다.

[0188] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫번째 바이트에 설정되는 값으로 임의값 요청 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 임의값 요청 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 임의값 요청 신호의 메시지 타입은 qwa1이다. qwa1값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기(100)는, 상기 신호를 임의값 요청 신호라고 인식할 수 있다.

[0189] 메시지 길이는 전체 메시지 사이즈에서 메시지 타입과 메시지 길이를 뺀 메시지 사이즈이다. 여기서 사이즈는 크기이다. 임의값 요청 신호는 메시지 타입 및 메시지 길이를 포함하여 다른 여러 정보를 포함 한다고 전술하였다. 여기서, 메시지 길이는 임의 값 요청 신호가 포함하는 모든 정보의 사이즈, 즉 크기에서 메시지 타입에 해당하는 사이즈 및 메시지 길이에 해당하는 사이즈를 뺀 사이즈이다. 메시지 타입의 크기가 1바이트이고, 메시지 길이 자체의 크기가 4바이트 이고, 전체 메시지의 크기가 85바이트라면, 메시지 길이는 80바이트가 된다. 여기서, 전체 메시지의 크기는 임의 값 요청 신호의 크기이다.

[0190] 클라이언트 타입은 클라이언트 종류에 대한 정보이다. 클라이언트 종류는 예를 들어 게이트웨이 또는 전자 기기 인증 매니저 장치(110)이다. 클라이언트가 게이트웨이라면 클라이언트 타입은 qw00000001이다. 클라이언트가 전자 기기 인증 매니저 장치(110)라면 클라이언트 타입은 qw00000002이다.

[0191] 일 실시예에 있어서, 임의값 요청 신호 송신 단계(S720)는 전자 기기(100)가 임의값 응답 신호를 생성하여 임의값 응답 신호를 전자 기기 인증 매니저 장치(110)로 송신한다. 임의값 응답 신호는 메시지 타입, 메시지 길이, 결과 코드 및 임의값을 포함한다.

[0192] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫번째 바이트에 설정되는 값으로 임의값 응답 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 임의값 응답 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 임의값 응답 신호의 메시지 타입은 qwc1이다. qwc1값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기(100)는, 상기 신호를 임의값 응답 신호라고 인식할 수 있다.

[0193] 메시지 길이는 전체 메시지 사이즈에서 메시지 타입과 메시지 길이를 뺀 메시지 사이즈이다. 여기서 사이즈는 크기이다. 임의값 응답 신호는 메시지 타입 및 메시지 길이를 포함하여 다른 여러 정보를 포함 한다고 전술하였다. 여기서, 메시지 길이는 임의 값 요청 신호가 포함하는 모든 정보의 사이즈, 즉 크기에서 메시지 타입에 해당하는 사이즈 및 메시지 길이에 해당하는 사이즈를 뺀 사이즈이다. 메시지 타입의 크기가 1바이트이고, 메시지 길이 자체의 크기가 4바이트 이고, 전체 메시지의 크기가 85바이트라면, 메시지 길이는 80바이트가 된다. 여기서, 전체 메시지의 크기는 임의 값 요청 신호의 크기이다.

[0194] 결과 코드는 임의값 요청 신호가 오류 없이 전자 기기(100)로 전달됐는지 여부를 표시하는 코드이다. 예를 들어 결과 코드가 0이면 임의값 요청 신호가 오류 없이 전자 기기(100)에 수신됨을 의미한다.

[0195] 임의 값은 전자 기기(100)가 생성한 난수 또는 현재 시간이다.

[0196] 일 실시예에 있어서, 전자 기기(100) 정보 요청 신호 송신 단계(S730)는 전자 기기 인증 매니저 장치(110)가 전자 기기(100)로 전자 기기(100) 정보 요청 신호를 송신한다. 전자 기기(100) 정보 요청 신호는 메시지 타입, 메시지 길이, 전자 기기(100) 정보 요청 명령 정보, 해쉬처리된 전자 기기(100) 비밀번호 및 세션 아이디를 포함한다.

[0197] 메시지 타입은 모든 요청 신호 또는 응답 신호의 첫번째 바이트에 설정되는 값으로 전자 기기(100) 정보 요청 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 전자 기기(100) 정보 요청 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 전자 기기(100) 정보 요청 신호의 메시지 타입은 qw05이다. qw05값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기(100)는, 상기 신호를 전자 기기(100) 정보 요청 신호라고 인식할 수 있다.

[0198] 메시지 길이는 전체 메시지 사이즈에서 메시지 타입과 메시지 길이를 뺀 메시지 사이즈이다. 여기서 사이즈는 크기이다. 전자 기기(100) 정보 요청 신호는 메시지 타입 및 메시지 길이를 포함하여 다른 여러 정보를 포함한다고 전술하였다. 여기서, 메시지 길이는 전자 기기(100) 정보 요청 신호가 포함하는 모든 정보의 사이즈, 즉 크기에서 메시지 타입에 해당하는 사이즈 및 메시지 길이에 해당하는 사이즈를 뺀 사이즈이다. 메시지 타입의 크기가 1바이트이고, 메시지 길이 자체의 크기가 4바이트 이고, 전체 메시지의 크기가 85바이트라면, 메시지 길이는 80바이트가 된다. 여기서, 전체 메시지의 크기는 전자 기기(100) 정보 요청 신호의 크기이다.

[0199] 전자 기기(100) 정보 요청 명령 정보는 전자 기기 인증 매니저 장치(110)가 클라이언트 타입 정보와 임의 값을 논리 연산 한 결과에 해쉬를 취하여 산출된 정보이다. 즉, 전자 기기 인증 매니저 장치(110)는 Hash(클라이언트 타입 | 임의값)이라는 연산을 통해 전자 기기(100) 정보 요청 명령 정보를 산출한다.

[0200] 해쉬처리된 전자 기기(100) 비밀번호는 전자 기기(100) 비밀번호를 해쉬 처리한 값이다. 즉, 전자 기기 인증 매니저 장치(110)가 Hash(전자 기기(100) 비밀번호)연산을 한 결과인 것이다.

[0201] 세션 아이디는 전자 기기 인증 매니저 장치(110)가 트랜잭션 아이디, 시리얼 번호, 클라이언트 타입 및 임의값을 논리 연산한 결과에 Hash함수를 취해서 산출된 아이디이다. 여기서 임의값은 세션 아이디를 생성하는 시점의 시간 또는 전자 기기 인증 매니저 장치(110)가 임의로 생성한 난수이다.

[0202] 일 실시예에 있어서, 전자 기기(100) 정보 응답 신호 송신 단계(S740)는 전자 기기(100)가 전자 기기(100) 정보 응답 신호를 생성하여 전자 기기(100) 정보 응답 신호를 전자 기기 인증 매니저 장치(110)로 송신한다. 전자 기기(100) 정보 응답 신호는 메시지 타입, 메시지 길이, 결과 코드, 유니크 아이디, 시리얼 번호를 포함한다.

[0203] 메시지 타입은 전자 기기(100) 정보 응답 신호의 첫번째 바이트에 설정되는 값으로 전자 기기(100) 정보 응답 신호의 타입이 무엇인지 식별해주는 값이다. 여기서, 메시지 타입은 신호의 유형이다. 즉, 전자 기기(100) 정보 응답 신호의 첫 번째 바이트에 설정되는 값으로, 상기 값에 따라 신호의 유형이 구별된다. 예를 들어 전자 기기(100) 정보 응답 신호의 메시지 타입은 qw8이다. qw8값이 신호의 첫번째 바이트로 설정된 신호를 수신하는 전자 기기(100)는, 상기 신호를 전자 기기(100) 정보 응답 신호라고 인식할 수 있다.

[0204] 메시지 길이는 전체 메시지 사이즈에서 메시지 타입과 메시지 길이를 뺀 메시지 사이즈이다. 여기서 사이즈는 크기이다. 전자 기기(100) 정보 응답 신호는 메시지 타입 및 메시지 길이를 포함하여 다른 여러 정보를 포함한다고 전술하였다. 여기서, 메시지 길이는 전자 기기(100) 정보 응답 신호가 포함하는 모든 정보의 사이즈, 즉 크기에서 메시지 타입에 해당하는 사이즈 및 메시지 길이에 해당하는 사이즈를 뺀 사이즈이다. 메시지 타입의 크기가 1바이트이고, 메시지 길이 자체의 크기가 4바이트 이고, 전체 메시지의 크기가 85바이트라면, 메시지 길이는 80바이트가 된다. 여기서, 전체 메시지의 크기는 전자 기기(100) 정보 응답 신호의 크기이다.

[0205] 결과 코드는 전자 기기(100) 정보 요청에 포함된 전자 기기(100) 정보 요청 명령 정보와 전자 기기(100)가 생성한 전자 기기(100) 정보 요청 명령 정보의 일치 여부에 따라 다른 값이 된다. 전술한 전자 기기(100) 정보 요청 명령 정보가 일치하면 결과 코드는 예를 들어 0으로 산출된다. 전술한 전자 기기(100) 정보 요청 명령 정보가 일치하지 않으면 결과 코드는 예를 들어 106으로 산출된다. 전자 기기 인증 매니저 장치(110)와 전자 기기(100) 각각이 클라이언트 타입 정보와 임의값 정보를 논리 연산 한 결과에 해쉬를 취하여 산출된 결과를 비교하여 인증 과정을 거치기에 보안이 강화된다.

[0206] 유니크 아이디

[0207] 시리얼 번호는 전자 기기(100)의 고유 번호이다. 전자 기기 인증 매니저 장치(110)와 근거리 무선 통신 또는 유선 통신을 할 수 있는 전자 기기(100)마다 하나의 고유 번호를 포함한다.

[0208] 유니크 아이디는 전자 기기(100) 내부에 실장된 칩의 아이디이다. 유니크 아이디는 전자 기기(100)가 생성하는 정보이다. 유니크 아이디는 칩이 실장된 전자 기기(100)의 시리얼 번호에 솔트를 적용한 결과에 해쉬를 취한 결과이다. 전자 기기(100) 마다 고유 번호인 시리얼 번호가 있음은 전술하였다. 솔트는 사용자가 설정한 값으로 시리얼 번호와 유니크 아이디의 관련성이 노출되지 않도록 하기 위한 값이다. 솔트를 적용한 다는 것은 시리얼 번호에 사용자가 지정한 값, 예를 들면, 솔트값인 '1234'를 시리얼 번호와 논리 연산을 한다는 것이다. 솔트값과 시리얼 번호를 논리 연산 한 결과에 해쉬 함수를 취한 결과가 유니크 아이디이다.

[0209] 일 실시예에 있어서, 임의 값 응답 신호는 임의값 정보를 포함하되, 임의값 정보는 현재 시간 또는 전자 기기(100)가 생성한 난수이다. 현재 시간은 임의 값 응답 신호가 생성되는 시점의 시간이다.

[0210] 일 실시예에 있어서, 전자 기기(100) 정보 요청 신호는 전자 기기 인증 매니저 장치(110)가 임의값을 포함하는 입력과 해쉬함수를 통해 산출된 전자 기기(100) 정보 요청 커맨드 정보를 포함한다. 임의값을 포함하는 입력은 클라이언트 타입 정보와 임의값 정보이다. 입력과 해쉬함수를 통해 산출된다는 것은 전술한 입력을 해쉬 함수의 정의역으로 한다는 것이다. 본 실시예에서는 입력이 두개이기에, 입력인 클라이언트 타입 정보와 임의값 정보를 논리 연산 한 결과에 해쉬함수 취하는 것이다.

[0211] 일 실시예에 있어서, 전자 기기(100) 정보 응답 신호 송신 단계(S740)는 전자 기기(100)가 수신한 전자 기기(100) 정보 요청 신호에 포함된 전자 기기(100) 정보 요청 커맨드 정보와 전자 기기(100)가 생성한 전자 기기(100) 정보 요청 커맨드 정보를 비교하여 일치 여부에 대한 정보를 전자 기기(100) 정보 응답 신호에 포함시키고 전자 기기(100) 정보 응답 신호를 전자 기기 인증 매니저 장치(110)로 송신한다. 일치 여부에 대한 정보가 전술한 결과 코드이다.

[0212] 도 9는 전자 기기 인증 시스템의 구성을 도시한다.

[0213] 일 양상에 있어서, 전자 기기 인증 시스템은 전자 기기 인증 서버 장치, 전자 기기 인증 매니저 장치를 포함한다.

[0214] 일 실시예에 있어서, 전자 기기 인증 서버 장치는 암호화된 인증 코드 요청 신호를 복호화하고, 인증 코드 요청 신호에 따라 인증 코드를 생성하며, 생성한 인증 코드에 서명하여 서명된 인증 코드를 생성하고, 서명된 인증 코드를 암호화한다.

[0215] 전자 기기 인증 서버 장치는 전자 기기를 인증하는 인증 코드를 생성하는 장치다. 암호화된 인증 코드 요청 신호는 전자 기기 인증 매니저 장치가 송신하는데 암호화된 인증 코드 요청 신호에 대한 상세한 설명은 전술하였다. 전자 기기 인증 서버 장치는 인증 코드에 서명하여 서명된 인증 코드를 생성하는데, 서명된 인증 코드에 대한 상세한 설명은 전술하였다. 전자 기기 인증 서버 장치는 서명된 인증 코드를 암호화하여 전자 기기 인증 매니저 장치로 송신한다.

[0216] 일 실시예에 있어서, 전자 기기 인증 매니저 장치는 인증 코드 요청 신호를 암호화하여 전자 기기 인증 서버 장치로 전송하고, 전자 기기 인증 서버 장치로부터 암호화된 서명된 인증 코드를 수신하여, 암호화된 서명된 인증 코드를 복호화한다.

[0217] 전자 기기 인증 매니저 장치는 전자 기기를 인증하는 인증 코드를 전자 기기 인증 서버 장치로부터 발급받는 절차를 중계한다. 즉, 전자 기기 인증 매니저 장치는 전자 기기 인증 서버 장치로부터 인증 코드를 수신하여 전자 기기로 송신한다. 전자 기기 인증 매니저 장치는 GPIO 인터페이스를 통해 전자 기기와 연결되어 전자 기기가 서명된 인증 코드를 수신하여 저장할 수 있도록 한다.

[0218] 전자 기기 인증 매니저 장치는 인증 코드 요청 신호를 암호화 하여 전자 기기 인증 서버 장치로 전송하는데, 암호화한 인증 코드 요청 신호에 대한 상세한 설명은 전술하였다. 전자 기기 인증 매니저 장치는 암호화된 서명된 인증 코드를 수신하여 복호화하는데, 이에 대한 상세한 설명은 암호화된 서명된 인증 코드 복호화 단계에서 전술하였다.

[0219] 전자 기기 인증 시스템은 전자 기기를 더 포함할 수 있다.

[0220] 일 실시예에 있어서, 전자 기기는 전자 기기 인증 매니저 장치로부터 서명된 인증 코드를 수신하여 인증 코드

저장 응답 신호를 전자 기기 인증 매니저 장치로 송신한다. 전자 기기가 서명된 인증 코드를 수신하는 과정은 인증 코드 저장 요청 신호 송신 단계에서 전술하였다. 전자 기기가 인증 코드 저장 응답 신호를 전자 기기 인증 매니저 장치로 송신하는 과정은 인증 코드 저장 응답 신호 송신 단계에서 전술하였다.

[0221] 일 실시예에 있어서, 인증 코드는 시리얼 번호, 유니크 아이디, 난수, 트랜잭션 아이디, 유효 시간, 유효 횟수, 접근 제어 정책, 암호화 알고리즘 중 적어도 하나를 포함한다. 인증 코드가 포함하는 각 정보에 대한 구체적인 설명은 전술하였다.

[0222] 도 10은 전자 기기 인증 매니저 장치의 구성을 도시한다.

[0223] 일 실시예에 있어서, 전자 기기 인증 매니저 장치는 통신부(111), 제어부(126), 인증 코드 요청 신호 암호화부(121), 암호화된 인증 코드 요청 신호 송신부(122), 암호화된 서명된 인증 코드 수신부(123), 암호화된 서명된 인증 코드 복호화부(124) 및 인증 코드 저장 요청 신호 송신부(125)를 포함한다.

[0224] 통신부(111)는 지그비, 와이파이, 블루투스, NFC(near field communication) 중 적어도 하나 이상을 포함하는 통신 방법으로 통신한다.

[0225] 전자 기기 인증 매니저 장치는 전자 기기와 GPIO 인터페이스를 통해 연결된다.

[0226] 제어부(126)는 전자 기기 인증 매니저 장치(110)를 총괄 제어한다. 제어부(126)는 마이크로 컨트롤러(Microcontroller) 또는 마이크로 프로세서(Micro processer)이다. 인증 코드 요청 신호 암호화부(121), 암호화된 인증 코드 요청 신호 송신부(122), 암호화된 서명된 인증 코드 수신부(123), 암호화된 서명된 인증 코드 복호화부(124) 및 인증 코드 저장 요청 신호 송신부(125), 전자 기기 칩 정보 수신부(130) 및 근거리 무선 통신 접속 허용부(140), 전자 기기 칩 정보 응답 신호 수신부(131) 및 전자 기기 칩 버전 응답 신호 수신부(132), 임의값 응답 신호 수신부(141) 및 전자 기기 정보 응답 신호 수신부(142)는 제어부에 의해 실행되는 프로그램 명령어 세트들로 구현된다. 그러나 여기에 한정되는 것은 아니며, 전용의 하드웨어, 예를 들면 순차 및/또는 조합 논리 회로에 의해 구현될 수도 있다.

[0227] 일 실시예에 있어서, 인증 코드 요청 신호 암호화부(121)는 인증 코드 요청 신호를 암호화하는데, 이에 대한 설명은 인증 코드 요청 신호 암호화 단계에서 전술하였다.

[0228] 일 실시예에 있어서, 암호화된 인증 코드 요청 신호 송신부(122)는 통신부(111)를 통해 암호화된 인증 코드 요청 신호를 송신하는데, 이에 대한 상세한 설명은 암호화된 인증 코드 요청 신호 송신 단계에서 전술하였다.

[0229] 또한 암호화된 인증 코드 요청 신호 송신부는 전자 기기로 암호화된 인증 코드 요청 신호를 송신할 수 있다. 전자 기기가 암호화된 인증 코드 요청 신호를 전자 기기 인증 서버로 송신할 수 있다.

[0230] 일 실시예에 있어서, 암호화된 서명된 인증 코드 수신부(123)는 전자 기기 인증 서버 장치로부터 통신부(111)를 통해 암호화된 서명된 인증 코드를 수신하는데, 이에 대한 상세한 설명은 암호화된 서명된 인증 코드 수신 단계에서 전술하였다.

[0231] 암호화된 서명된 인증 코드 수신부(123)는 전자 기기로부터 암호화된 서명된 인증 코드를 수신할 수 있다. 즉, 전자 기기는 전자 기기 인증 서버로부터 암호화된 서명된 인증 코드를 수신하여, 전자 기기 인증 매니저 장치로 송신할 수 있다.

[0232] 일 실시예에 있어서, 암호화된 서명된 인증 코드 복호화부(124)는 암호화된 서명된 인증 코드를 복호화하는데, 이에 대한 상세한 설명은 암호화된 서명된 인증 코드 복호화 단계에서 전술하였다.

[0233] 일 실시예에 있어서, 인증 코드 저장 요청 신호 송신부(125)는 전자 기기로 인증 코드 저장 요청 신호를 송신하는데, 이에 대한 상세한 설명은 인증 코드 저장 요청 신호 송신 단계에서 전술하였다.

[0234] 일 실시예에 있어서, 전자 기기 인증 매니저 장치(110)는 전자 기기 칩 정보 수신부(130) 및 근거리 무선 통신 접속 허용부(140)를 포함한다.

[0235] 일 실시예에 있어서, 전자 기기 칩 정보 수신부(130)는 전자 기기로부터 전자 기기 내부에 실장된 칩 정보를 수신하는데, 이에 대한 상세한 설명은 전자 기기 칩 정보 수신 단계에서 전술하였다.

[0236] 일 실시예에 있어서, 근거리 무선 통신 접속 허용부(140)는 전자 기기의 근거리 무선 통신 접속을 허용하는데, 이에 대한 상세한 설명은 근거리 무선 통신 접속 단계에서 전술하였다.

[0237] 일 실시예에 있어서, 전자 기기 칩 정보 수신부(130)는 전자 기기 칩 정보 응답 신호 수신부(131) 및 전자 기기

칩 버전 응답 신호 수신부(132)를 포함한다.

[0238] 일 실시예에 있어서, 전자 기기 칩 정보 응답 신호 수신부(131)는 전자 기기로부터 전자 기기 칩 정보 응답 신호를 수신하는데, 이에 대한 상세한 설명은 전자 기기 칩 정보 응답 신호 수신 단계에서 전술하였다.

[0239] 일 실시예에 있어서, 전자 기기 칩 버전 응답 신호 수신부(132)는 전자 기기로부터 전자 기기 칩 버전 응답 신호를 수신하는데, 이에 대한 상세한 설명은 전자 기기 칩 버전 응답 신호 수신 단계에서 전술하였다.

[0240] 일 실시예에 있어서, 근거리 무선 통신 접속 허용부(140)는 임의값 응답 신호 수신부(141) 및 전자 기기 정보 응답 신호 수신부(142)를 포함한다.

[0241] 일 실시예에 있어서, 임의값 응답 신호 수신부(141)는 전자 기기로부터 임의값 응답 신호를 수신하는데, 이에 대한 상세한 설명은 임의값 응답 신호 송신 단계에서 전술하였다.

[0242] 일 실시예에 있어서, 전자 기기 정보 응답 신호 수신부(142)는 전자 기기로부터 전자 기기 정보 응답 신호를 수신하는 전자 기기 정보 응답 신호를 수신하는데, 이에 대한 상세한 설명은 전자 기기 정보 응답 신호 송신 단계에서 전술하였다.

[0243] 이와 같이, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 실시 형태로 실시될 수 있다는 것을 인지할 수 있을 것이다. 따라서 이상에서 기술한 실시 예들은 예시적인 것일 뿐이며, 그 범위를 제한해놓은 한정적인 것이 아닌 것으로 이해해야만 한다. 또한, 도면에 도시된 순서도들은 본 발명을 실시함에 있어서 가장 바람직한 결과를 달성하기 위해 예시적으로 도시된 순차적인 순서에 불과하며, 다른 추가적인 단계들이 제공되거나, 일부 단계가 삭제될 수 있음은 물론이다.

[0244] 본 명세서에서 기술한 기술적 특징과 이를 실행하는 구현물은 디지털 전자 회로로 구현되거나, 본 명세서에서 기술하는 구조 및 그 구조적인 등가물 등을 포함하는 컴퓨터 소프트웨어, 펌웨어 또는 하드웨어로 구현되거나, 이들 중 하나 이상의 조합으로 구현 가능하다. 또한 본 명세서에서 기술한 기술적 특징을 실행하는 구현물은 컴퓨터 프로그램 제품, 다시 말해 처리 시스템의 동작을 제어하기 위하여 또는 이것에 의한 실행을 위하여 유형의 프로그램 저장매체 상에 인코딩된 컴퓨터 프로그램 명령어에 관한 모듈로서 구현될 수도 있다.

[0245] 컴퓨터로 판독 가능한 매체는 기계로 판독 가능한 저장 장치, 기계로 판독 가능한 저장 기판, 메모리 장치, 기계로 판독 가능한 전파형 신호에 영향을 미치는 물질의 조성물 또는 이들 중 하나 이상의 조합일 수 있다.

[0246] 한편, 본 명세서에서 "장치"나 "시스템"이라 함은 예를 들어, 프로세서, 컴퓨터 또는 다중 프로세서나 컴퓨터를 포함하여 정보를 처리하기 위한 모든 기구, 장치 및 기계를 모두 포함한다. 처리 시스템은, 하드웨어에 부가하여 예를 들어, 프로세서 펌웨어를 구성하는 코드, 프로토콜 스택, 정보베이스 관리 시스템, 운영 제체 또는 이들 중 하나 이상의 조합 등 요청 시 컴퓨터 프로그램에 대한 실행 환경을 형성하는 모든 코드를 포함할 수 있다.

[0247] 프로그램, 소프트웨어, 소프트웨어 애플리케이션, 스크립트 또는 코드 등으로 알려진 컴퓨터 프로그램은 컴파일되거나 해석된 언어 또는 선험적, 절차적 언어를 포함하는 프로그래밍 언어의 어떠한 형태로도 작성될 수 있으며, 독립형 프로그램이나 모듈, 컴포넌트, 서브루틴 또는 컴퓨터 환경에서 사용하기에 적합한 다른 유닛을 포함하여 어떠한 형태로도 구현될 수 있다.

[0248] 한편, 컴퓨터 프로그램은 파일 시스템의 파일에 반드시 대응되는 것은 아니며, 요청된 프로그램에 제공되는 단일 파일 내에 또는 다중의 상호 작용하는 파일(예를 들어, 하나 이상의 모듈, 하위 프로그램 또는 코드의 일부를 저장하는 파일)내에, 또는 다른 프로그램이나 정보를 보유하는 파일의 일부(예를 들어, 마크업 언어 문서 내에 저장되는 하나 이상의 스크립트)내에 저장될 수 있다.

[0249] 컴퓨터 프로그램은 하나의 사이트에 위치하거나 복수의 사이트에 걸쳐서 분산되어 유/무선 통신 네트워크에 의해 상호 접속된 다중 컴퓨터나 하나 이상의 컴퓨터 상에서 실행되도록 구현될 수 있다.

[0250] 한편, 컴퓨터 프로그램 명령어와 정보를 저장하기에 적합한 컴퓨터로 판독 가능한 매체는, 예를 들어 EPROM, EEPROM 및 플래시메모리 장치와 같은 반도체 메모리 장치, 예컨대 내부 하드디스크나 외장형 디스크와 같은 자기 디스크, 자기광학 디스크 및 CD와 DVD 디스크를 포함하여 모든 형태의 비휘발성 메모리, 매체 및 메모리 장치를 포함할 수 있다. 프로세서와 메모리는 특수 목적의 논리 회로에 의해 보충되거나, 그것에 통합될 수 있다.

[0251] 본 명세서에서 기술한 기술적 특징을 실행하는 구현물은 예를 들어, 정보 서버와 같은 백엔드 컴포넌트를 포함

하거나, 예를 들어, 애플리케이션 서버와 같은 미들웨어 컴포넌트를 포함하거나, 예컨대 사용자가 본 명세서에서 설명한 주제의 구현물과 상호 작용할 수 있는 웹 브라우저나 그래픽 유저 인터페이스를 갖는 클라이언트 컴퓨터와 같은 프론트엔드 컴포넌트 혹은 그러한 백엔드, 미들웨어 혹은 프론트엔드 컴포넌트의 하나 이상의 모든 조합을 포함하는 연산 시스템에서 구현될 수도 있다. 시스템의 컴포넌트는 예를 들어, 통신 네트워크와 같은 디지털 정보 통신의 어떠한 형태나 매체에 의해서도 상호 접속 가능하다.

[0252] 이하, 상기 기술한 내용과 더불어 본 명세서에 기술한 시스템과 방법이 포함하는 구성들을 구현할 수 있는 보다 구체적인 실시 예에 대하여 자세히 기술하도록 한다.

[0253] 본 명세서에서 방법은 클라이언트 디바이스 또는 웹 기반의 스토리지 시스템과 관련된 서버 또는 서버에 포함된 하나 이상의 프로세서(Processor) 상에서 컴퓨터 소프트웨어, 프로그램 코드 또는 명령어를 실행하는 수단을 통해 부분적 또는 전체적으로 사용될 수 있다. 여기서 프로세서는 서버, 클라이언트, 네트워크 인프라 구조, 모바일 컴퓨팅 플랫폼, 고정 컴퓨팅 플랫폼 등과 같은 컴퓨팅 플랫폼 중 일부일 수 있으며, 구체적으로 프로그램 명령어, 코드 등을 실행할 수 있는 컴퓨터 또는 프로세싱 디바이스의 한 종류일 수 있다. 또한, 프로세서는 방법, 명령어, 코드 및 프로그램을 저장하는 메모리를 더 포함할 수 있으며, 메모리를 포함하지 않는 경우 별도의 인터페이스를 통해 본 발명에 따른 방법, 명령어, 코드 및 프로그램이 저장된 CD-ROM, DVD, 메모리, 하드 디스크, 플래시 드라이브, RAM, ROM, 캐시 등과 같은 스토리지 디바이스에 접근(Access)할 수도 있다.

[0254] 또한, 본 명세서에서 기술한 시스템과 방법은 서버, 클라이언트, 게이트웨이, 허브, 라우터 또는 네트워크 하드웨어 상의 컴퓨터 소프트웨어를 실행하는 장치를 통해 부분적 또는 전체적으로 사용될 수 있다. 여기서 소프트웨어는 파일 서버, 프린트 서버, 도메인 서버, 인터넷 서버, 인트라넷 서버, 호스트 서버, 분산 서버 등과같이 다양한 종류의 서버에서 실행될 수 있으며, 상기 언급한 서버들은 메모리, 프로세서, 컴퓨터에서 판독 가능한 저장매체, 스토리지 매체, 통신 디바이스, 포트, 클라이언트 그리고 다른 서버들을 유/무선 네트워크를 통해 접근할 수 있는 인터페이스를 더 포함할 수 있다.

[0255] 또한, 본 발명에 따른 방법, 명령어, 코드 등 역시 서버에 의해 실행될 수 있으며, 방법을 실행하기 위해 필요한 다른 디바이스들은 서버와 연관된 계층구조의 일 부분으로 구현될 수 있다.

[0256] 아울러, 서버는 클라이언트, 다른 서버, 프린터, 정보베이스 서버, 프린트 서버, 파일 서버, 통신 서버, 분산 서버 등을 제한 없이 포함하는 다른 디바이스에게 인터페이스를 제공할 수 있으며, 인터페이스를 통한 연결은 유/무선 네트워크를 통해 프로그램의 원격 실행을 용이하게 할 수 있다.

[0257] 또한, 인터페이스를 통해 서버에 연결된 디바이스 중 어느 것이라도방법, 명령어, 코드 등을 저장할 수 있는 적어도 하나의 스토리지 디바이스를 더 포함할 수 있으며, 서버의 중앙 프로세서는 상이한 디바이스 상에서 실행될 명령어, 코드 등을 디바이스에 제공하여 스토리지 디바이스에 저장되게 할 수 있다.

[0258] 한편, 본 명세서에서 방법은 네트워크 인프라구조를 통해 부분적 또는 전체적으로 사용될 수 있다. 여기서 네트워크 인프라구조는 컴퓨팅 디바이스, 서버, 라우터, 허브, 방화벽, 클라이언트, 개인용 컴퓨터, 통신 디바이스, 라우팅 디바이스 등과 같은 디바이스와 각각의 기능을 실행할 수 있는 별도의 모듈 등을 모두 포함할 수 있으며, 상기 언급한 디바이스와 모듈 외에 스토리 플래시 메모리, 버퍼, 스택, RAM, ROM 등과 같은 스토리지 매체를 더 포함할 수 있다. 또한, 방법, 명령어, 코드 등 역시 네트워크 인프라구조가 포함하는 디바이스, 모듈, 스토리지 매체 중 어느 하나에 의해 실행 및 저장될 수 있으며, 방법을 실행하기 위해 필요한 다른 디바이스 역시 네트워크 인프라구조의 일 부분으로 구현될 수 있다.

[0259] 또한, 본 명세서에서 기술한 시스템과 방법은 하드웨어 또는 특정 애플리케이션(Application)에 적합한 하드웨어와 소프트웨어의 조합으로 구현될 수 있다. 여기서 하드웨어는 개인용 컴퓨터, 이동통신 단말기 등과 같은 범용 컴퓨터 디바이스와 기업형 특정 컴퓨터 디바이스를 모두 포함하며, 컴퓨터 디바이스는 메모리, 마이크로프로세서, 마이크로콘트롤러, 디지털 신호 프로세서, 애플리케이션 집적 회로, 프로그래머블 게이트 어레이, 프로그래머블 어레이 조직 등을 포함하는 디바이스 또는 이들의 조합으로 구현될 수 있다.

[0260] 이상에서 기술한 컴퓨터 소프트웨어, 명령어, 코드 등은 판독 가능한 디바이스에 의해 저장 또는 접근될 수 있으며, 여기서 판독 가능한 디바이스는 일정 시간 간격 동안 컴퓨팅하는데 사용되는 디지털 정보를 구비하는 컴퓨터 컴포넌트, RAM 또는 ROM과 같은 반도체 스토리지, 광디스크와 같은 영구적인 스토리지, 하드 디스크, 테이프, 드럼 등과 같은 대용량 스토리지, CD 또는 DVD와 같은 광 스토리지, 플래시 메모리, 플로피 디스크, 자기 테이프, 페이퍼 테이프, 독립형 RAM 디스크, 컴퓨터로부터 착탈 가능한 대용량 스토리지와 동적 메모리, 정적 메모리, 가변 스토리지, 클라우드와 같은 네트워크 접속형 스토리지 등과 같은 메모리를 포함할 수 있다. 한편,

여기서 명령어와 코드 등은 SQL, dBase 등과 같은 정보 지향 언어, C, Objective C, C++, 어셈블리 등과 같은 시스템 언어, Java, NET 등과 같은 아키텍처 언어, PHP, Ruby, Perl, Python 등과 같은 애플리케이션 언어 등과 같은 언어들을 모두 포함하지만, 이에 한정되지는 않고 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 널리 알려진 언어들을 모두 포함할 수 있다.

[0261] 또한, 본 명세서에서 기술한 "컴퓨터에서 판독 가능한 매체"는 프로그램 실행을 위해 명령어를 프로세서로 제공하는데 기여하는 모든 매체를 포함한다. 구체적으로 정보 스토리지 디바이스, 광디스크, 자기 디스크 등과 같은 비휘발성 매체, 동적 메모리 등과 같은 휘발성 매체와 정보를 전송하는 동축 케이블, 구리 와이어, 광섬유 등과 같은 전송 매체를 포함하지만 이에 한정되지는 않는다.

[0262] 한편, 본 명세서에 첨부된 도면에 도시된 블록도와 순서도에 포함된 본 발명의 기술적 특징을 실행하는 구성들은 상기 구성들 사이의 논리적인 경계를 의미한다.

[0263] 그러나 소프트웨어나 하드웨어의 실시 예에 따르면, 도시된 구성들과 그 기능들은 독립형 소프트웨어 모듈, 모놀리식 소프트웨어 구조, 코드, 서비스 및 이들을 조합한 형태로 실행되며, 저장된 프로그램 코드, 명령어 등을 실행할 수 있는 프로세서를 구비한 컴퓨터에서 실행 가능한 매체에 저장되어 그 기능들이 구현될 수 있으므로 이러한 모든 실시 예 역시 본 발명의 권리범위 내에 속하는 것으로 보아야 할 것이다.

[0264] 따라서, 첨부된 도면과 그에 대한 기술은 본 발명의 기술적 특징을 설명하기는 하나, 이러한 기술적 특징을 구현하기 위한 소프트웨어의 특정 배열이 분명하게 언급되지 않는 한, 단순히 추론되어서는 안된다. 즉, 이상에서 기술한 다양한 실시 예들이 존재할 수 있으며, 그러한 실시 예들이 본 발명과 동일한 기술적 특징을 보유하면서 일부 변형될 수 있으므로, 이 역시 본 발명의 권리범위 내에 속하는 것으로 보아야 할 것이다.

[0265] 또한, 순서도의 경우 특정한 순서로 도면에서 동작들을 묘사하고 있지만, 이는 가장 바람직한 결과를 얻기 위하여 도시된 것으로서, 도시된 특정한 순서나 순차적인 순서대로 그러한 동작들을 반드시 실행되어야 한다거나 모든 도시된 동작들이 반드시 실행되어야 하는 것으로 이해되어서는 안 된다. 특정한 경우, 멀티 태스킹과 병렬 프로세싱이 유리할 수 있다. 아울러, 이상에서 기술한 실시형태의 다양한 시스템 컴포넌트의 분리는 그러한 분리를 모든 실시형태에서 요구하는 것으로 이해되어서는 안되며, 설명한 프로그램 컴포넌트와 시스템들은 일반적으로 단일의 소프트웨어 제품으로 함께 통합되거나 다중 소프트웨어 제품에 패키징될 수 있다는 점을 이해하여야 한다.

[0266] 이와 같이, 본 명세서는 그 제시된 구체적인 용어에 의해 본 발명을 제한하려는 의도가 아니다. 따라서, 이상에서 기술한 실시 예를 참조하여 본 발명을 상세하게 설명하였지만, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면 본 발명의 범위를 벗어나지 않으면서도 본 실시 예들에 대한 개조, 변경 및 변형을 가할 수 있다.

[0267] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 등가개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 권리범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

[0268] 100: 전자 기기

110: 전자 기기 인증 매니저 장치

111: 통신부

126: 제어부

121: 인증 코드 요청 신호 암호화부

122: 암호화된 인증 코드 요청 신호 송신부

123: 암호화된 서명된 인증 코드 수신부

124: 암호화된 서명된 인증 코드 복호화부

125: 인증 코드 저장 요청 신호 송신부

130: 전자 기기 칩 정보 수신부

131: 전자 기기 칩 정보 응답 신호 수신부

132: 전자 기기 칩 버전 응답 신호 수신부

140: 근거리 무선 통신 접속 허용부

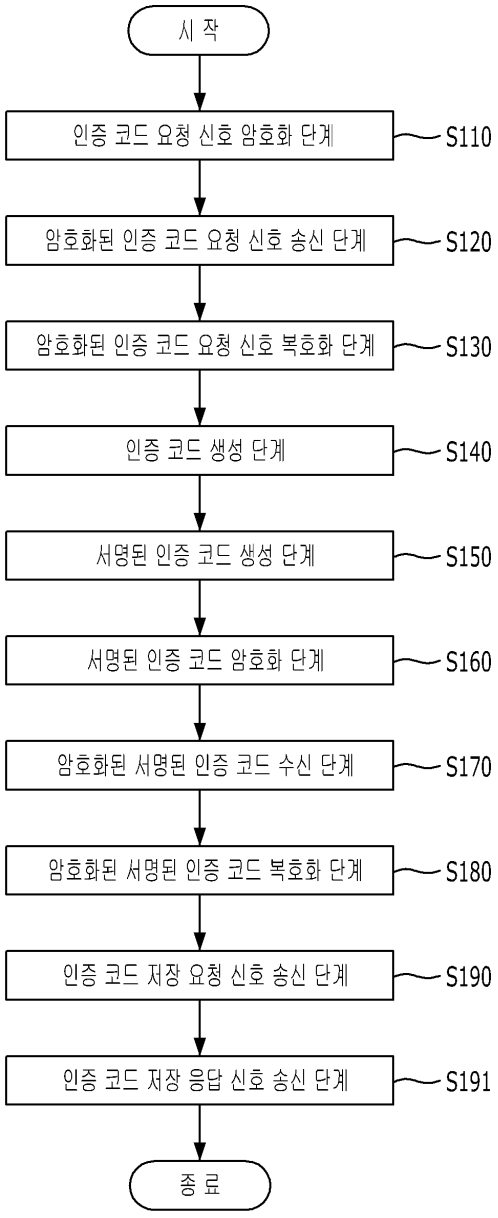
141: 임의값 응답 신호 수신부

142: 전자 기기 정보 응답 신호 수신부

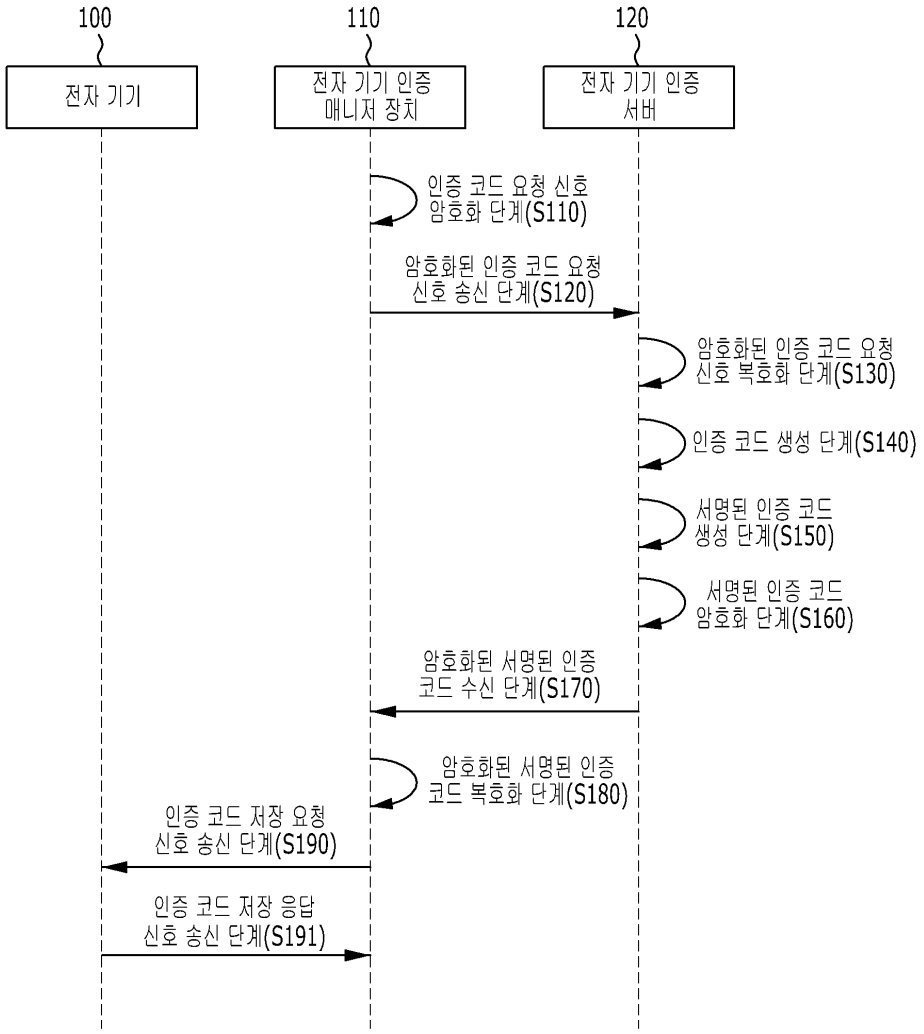
120: 전자 기기 인증 서버

도면

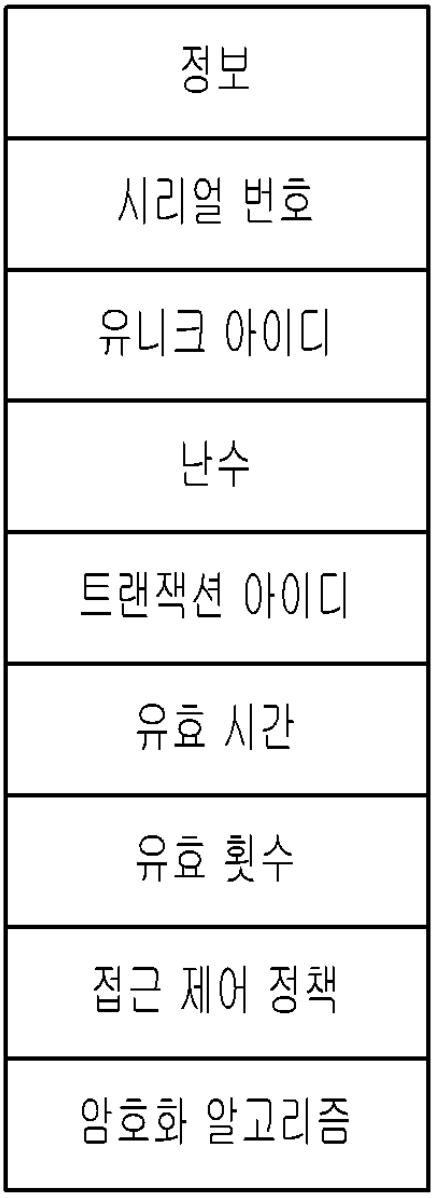
도면1



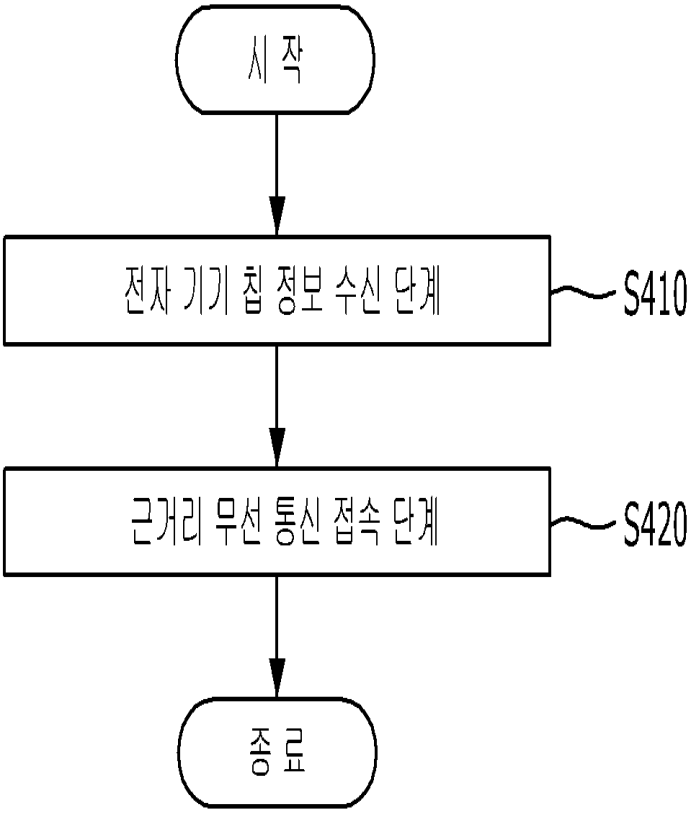
도면2


100
110
120
전자 기기
전자 기기 인증 매니저 장치
전자 기기 인증 서버
인증 코드 요청 신호 암호화 단계(S110)
암호화된 인증 코드 요청 신호 송신 단계(S120)
암호화된 인증 코드 요청 신호 복호화 단계(S130)
인증 코드 생성 단계(S140)
서명된 인증 코드 생성 단계(S150)
서명된 인증 코드 암호화 단계(S160)
암호화된 서명된 인증 코드 수신 단계(S170)
암호화된 서명된 인증 코드 복호화 단계(S180)
인증 코드 저장 요청 신호 송신 단계(S190)
인증 코드 저장 응답 신호 송신 단계(S191)

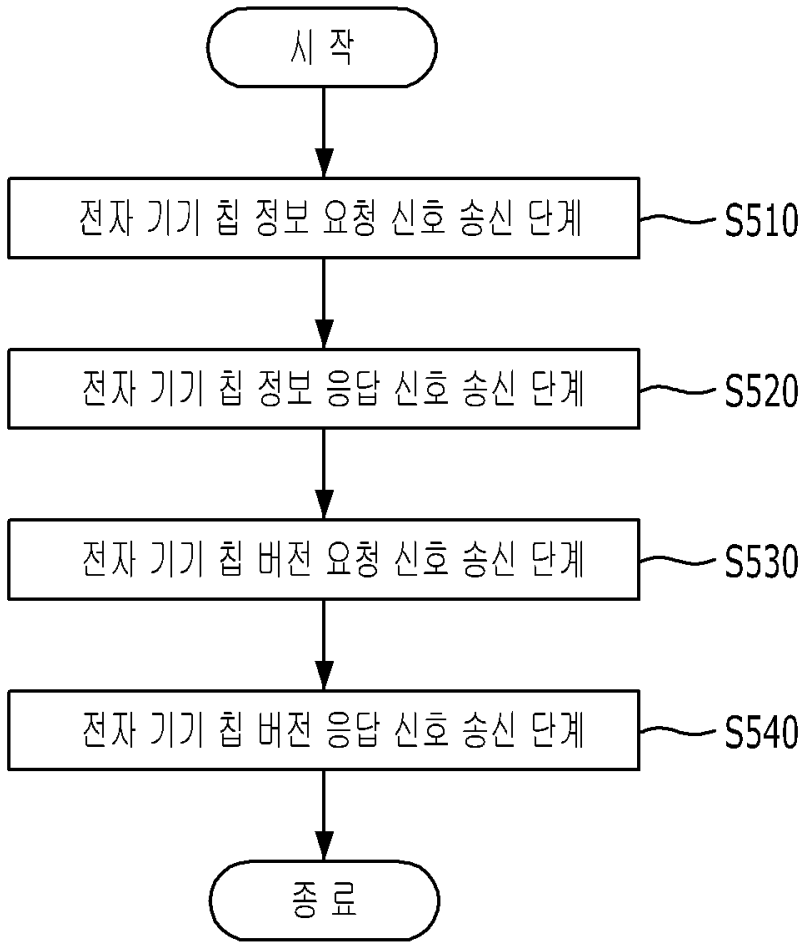
도면3



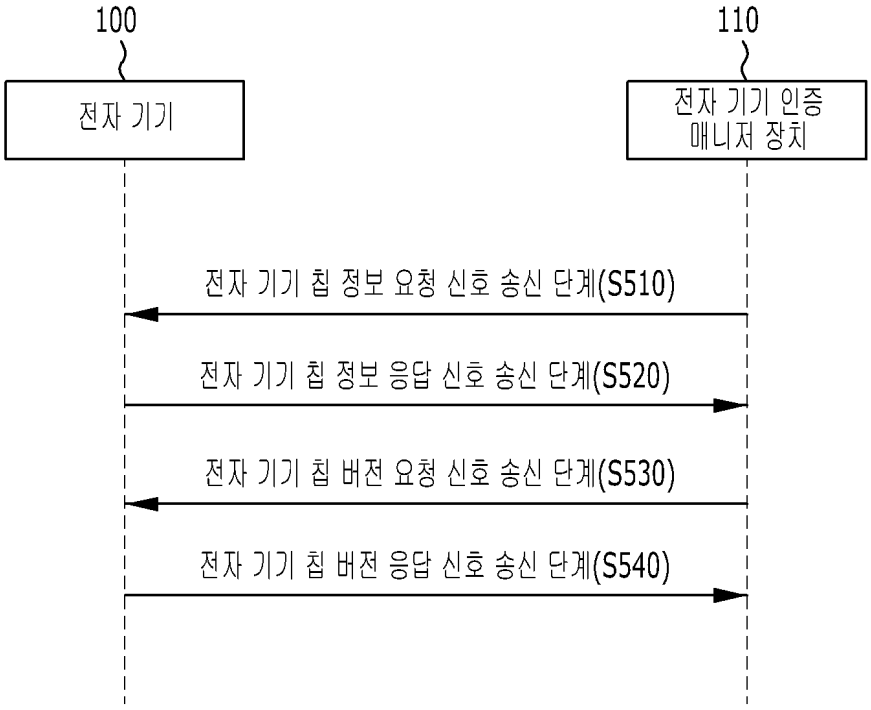
도면4



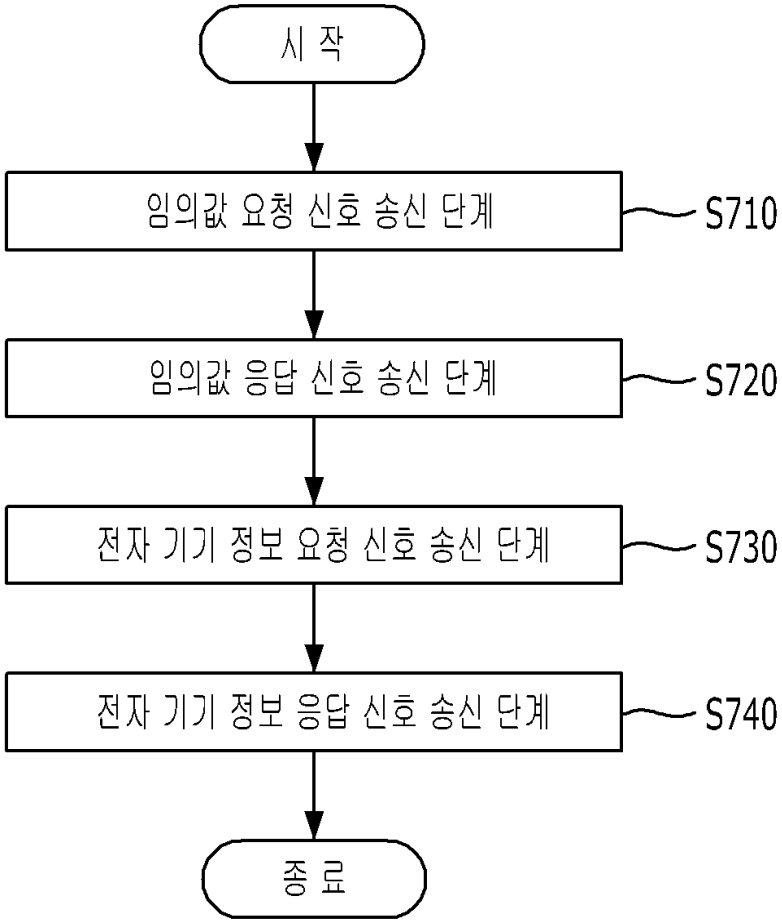
도면5


시 작
전자 기기 칩 정보 요청 신호 송신 단계
S510
전자 기기 칩 정보 응답 신호 송신 단계
S520
전자 기기 칩 버전 요청 신호 송신 단계
S530
전자 기기 칩 버전 응답 신호 송신 단계
S540
종 료

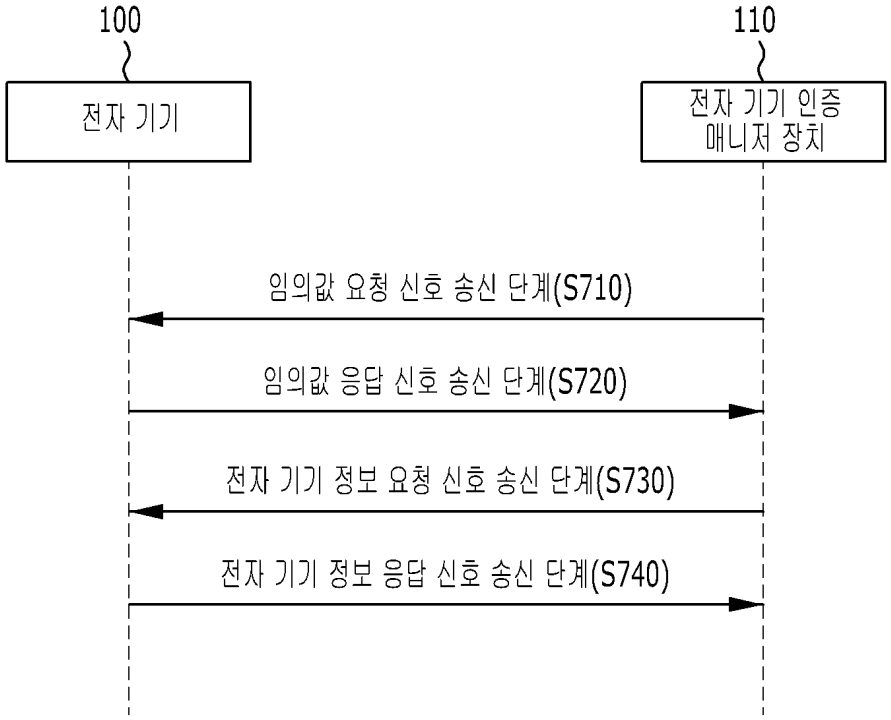
도면6


100
전자 기기
110
전자 기기 인증
매니저 장치
전자 기기 칩 정보 요청 신호 송신 단계(S510)
전자 기기 칩 정보 응답 신호 송신 단계(S520)
전자 기기 칩 버전 요청 신호 송신 단계(S530)
전자 기기 칩 버전 응답 신호 송신 단계(S540)

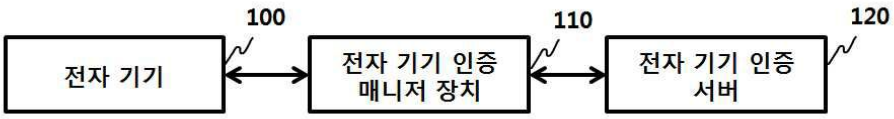
도면7


시 작
임의값 요청 신호 송신 단계
S710
임의값 응답 신호 송신 단계
S720
전자 기기 정보 요청 신호 송신 단계
S730
전자 기기 정보 응답 신호 송신 단계
S740
종 료

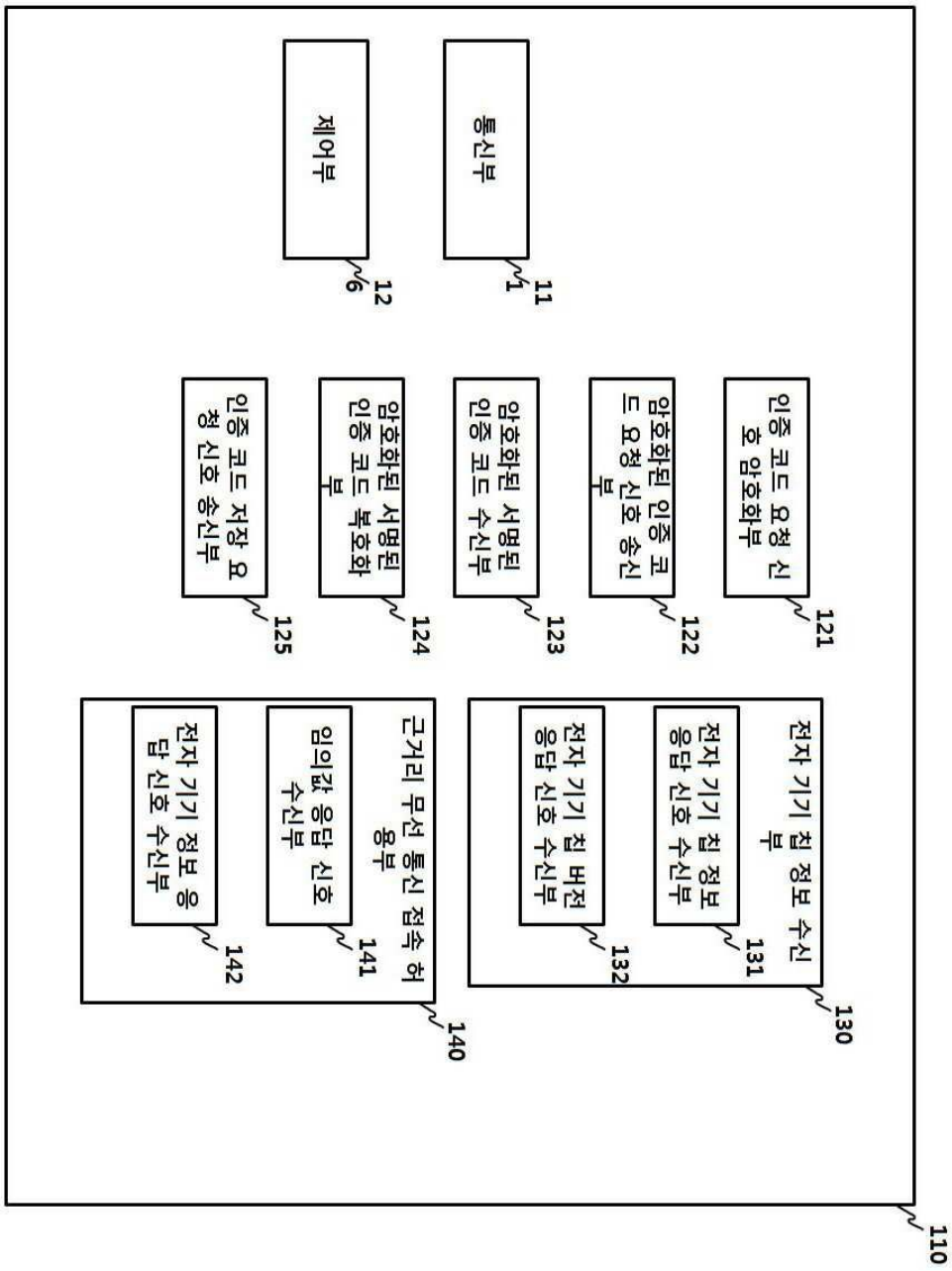
도면8


100
110
전자 기기
전자 기기 인증
매니저 장치
임의값 요청 신호 송신 단계(S710)
임의값 응답 신호 송신 단계(S720)
전자 기기 정보 요청 신호 송신 단계(S730)
전자 기기 정보 응답 신호 송신 단계(S740)

도면9


100
110
120
전자 기기
전자 기기 인증
매니저 장치
전자 기기 인증
서버

도면10


110
통신부
11
제어부
12
인증 코드 요청 신호 암호화부
121
암호화된 인증 코드 요청 신호 송신부
122
암호화된 서명된 인증 코드 수신부
123
암호화된 서명된 인증 코드 복호화부
124
인증 코드 저장 요청 신호 송신부
125
전자 기기 칩 정보 수신부
130
전자 기기 칩 정보 응답 신호 수신부
131
전자 기기 칩 버전 응답 신호 수신부
132
근거리 무선 통신 접속 허용부
140
임의값 응답 신호 수신부
141
전자 기기 정보 응답 신호 수신부
142