(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2022 년 4 월 14 일 (14.04.2022)

WIPO | PCT

(10) 국제공개번호
WO 2022/075563 A1

(51) 국제특허분류:
G06F 21/73 (2013.01) *H04L 9/08* (2006.01)
G06F 21/33 (2013.01) *H04L 9/32* (2006.01)

(21) 국제출원번호: PCT/KR2021/009962

(22) 국제출원일: 2021 년 7 월 30 일 (30.07.2021)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2020-0128757 2020 년 10 월 6 일 (06.10.2020) KR

(71) 출원인: 주식회사 아이씨티케이 홀딩스 (**ICTK HOLDINGS CO., LTD.**) [KR/KR]; 13488 경기도 성남시 분당구 판교로 323, 3층, Gyeonggi-do (KR).

(72) 발명자: 신광조 (**SHIN, Kwang Cho**); 02443 서울시 동대문구 이문로12길 66, 201호, Seoul (KR).

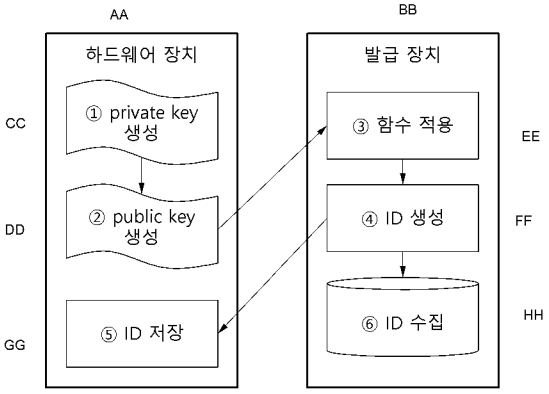
(74) 대리인: 특허법인 무한 (**MUHANN PATENT & LAW FIRM**); 06144 서울시 강남구 언주로 560, 8층 (역삼동, 화물재단빌딩), Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

WO 2022/075563 A1

(54) **Title:** ELECTRONIC DEVICE FOR GENERATING AND AUTHENTICATING IDENTIFICATION INFORMATION OF HARDWARE DEVICE, AND OPERATION METHOD THEREOF

(54) **발명의 명칭:** 하드웨어 장치의 식별 정보를 생성하고 인증하는 전자 장치 및 이의 동작 방법



AA ... Hardware device
BB ... Issuance device
CC ... Generate private key
DD ... Generate public key
EE ... Apply function
FF ... Generate ID
GG ... Store ID
HH ... Collect ID

(57) **Abstract:** Disclosed are an electronic device for generating and authenticating identification information of a hardware device, and an operation method thereof. The disclosed operation method of the electronic device comprises the steps of: determining identification information utilized for authentication of a hardware device, by using a public key of the hardware device, generated from a private key of the hardware device; and managing the identification information.

(57) **요약서:** 하드웨어 장치의 식별 정보를 생성하고 인증하는 전자 장치 및 이의 동작 방법이 개시된다. 개시된 전자 장치의 동작 방법은 하드웨어 장치의 개인 키로부터 생성된 상기 하드웨어 장치의 공개 키를 이용하여, 상기 하드웨어 장치의 인증에 활용되는 식별 정보를 결정하는 단계 및 상기 식별 정보를 관리하는 단계를 포함한다.

[다음 쪽 계속]

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

명세서

발명의 명칭: 하드웨어 장치의 식별 정보를 생성하고 인증하는 전자 장치 및 이의 동작 방법

기술분야

[1] 아래의 설명은 하드웨어 장치의 식별 정보를 생성하고 인증하는 전자 장치 및 이의 동작 방법에 관한 것으로, 보다 구체적으로는 보안 기능을 수행하는 칩, 모듈, 디바이스를 포함하는 하드웨어 장치의 식별 정보를 생성하고, 이에 기반한 인증을 수행하는 방법 및 장치에 관한 것이다.

배경기술

[2] 칩(chip), 모듈(module), 디바이스(device) 등 하드웨어 장치를 생산, 판매, 사용하는 단계에서 해당 하드웨어 장치를 추적 및 관리를 위해서 고유의 ID(identification)와 같은 식별 정보를 필요로 한다. 일반적으로, 식별 정보는 관리를 목적으로 생성되는 정보로서, 생성된 식별 정보는 서버에 저장되고 관리될 수 있다.

[3] 만약 하드웨어 장치가 PKI(Public Key Infrastructure) 기능을 가지고 자신의 개인키(private key)를 통해 보안 기능을 수행하고자 한다면, CA(certificate authority) 서버로부터 인증서를 발급받아 자신이 정당한지를 입증해야 한다. 일반적으로 인증서는 하드웨어 장치의 ID와 공개 키를 묶어서 CA 서버의 비밀 키로 서명함으로써 발급된다.

[4] 다만, 이를 구현하기 위해서는 CA 서버를 하드웨어 장치의 생산 설비에 추가적으로 구축해서 직접 운영하거나, 또는 원격의 CA 서버에 접속하여 인증서를 발급 받기 위해 기존 CA 서버의 운영자와 협약이 요구되는데, 이러한 일련의 과정들이 하드웨어 장치의 생산자나 유통자 등에게는 상당한 비용과 어려움으로 여겨질 수 있다.

발명의 상세한 설명

과제 해결 수단

[5] 일실시예에 따른 전자 장치의 동작 방법은 하드웨어 장치의 개인 키로부터 생성된 상기 하드웨어 장치의 공개 키를 이용하여, 상기 하드웨어 장치의 인증에 활용되는 식별 정보를 결정하는 단계; 및 상기 식별 정보를 관리하는 단계를 포함한다.

[6] 일실시예에 따른 전자 장치의 동작 방법에서 상기 식별 정보를 결정하는 단계는 상기 공개 키 또는 상기 공개 키에 미리 정해진 함수를 적용하여 얻어진 값에 기초하여 상기 식별 정보를 결정할 수 있다.

[7] 일실시예에 따른 전자 장치의 동작 방법에서 상기 함수는 상기 공개 키로부터 미리 정해진 길이의 데이터를 결정하는 암호화 해시 알고리즘(cryptographic hash algorithm), 상기 공개 키를 암호화하는 암호 알고리즘, 상기 공개 키의 일부를

활용하는 함수 또는 이들의 조합에 해당할 수 있다.

[8] 일실시예에 따른 전자 장치의 동작 방법에서 상기 식별 정보를 결정하는 단계는 상기 하드웨어 장치의 생산자 식별 정보, 제품 식별 정보, 생산일자 및 생산장소 중 적어도 하나에 대한 정보를 더 이용하여 상기 식별 정보를 결정할 수 있다.

[9] 일실시예에 따른 전자 장치의 동작 방법에서 상기 하드웨어 장치는 인증 대상이 되는 칩, 모듈, 디바이스 중 어느 하나일 수 있다.

[10] 일실시예에 따른 전자 장치의 동작 방법은 인증이 필요한 하드웨어 장치로부터 수신된 해당 하드웨어 장치의 식별 정보가 기 등록된 식별 정보인지를 확인하는 단계; 및 상기 수신된 식별 정보가 상기 기 등록된 식별 정보인 경우에 응답하여, 상기 수신된 식별 정보로부터 획득한 공개 키 또는 상기 인증이 필요한 하드웨어 장치로부터 수신한 공개 키를 이용하여 상기 인증이 필요한 하드웨어 장치에 대해 PKI 기반 인증을 수행하는 단계를 더 포함할 수 있다.

[11] 일실시예에 따른 전자 장치의 동작 방법에서 상기 PKI 기반 인증을 수행하는 단계는 CA 서버에 의해 발급된 인증서 없이, 상기 획득한 공개 키 또는 상기 수신한 공개 키를 이용하여 PKI 기반 인증을 수행할 수 있다.

[12] 일실시예에 따른 전자 장치의 동작 방법에서 상기 PKI 기반 인증을 수행하는 단계는 상기 획득한 공개 키 또는 상기 수신한 공개 키를 이용하여, 상기 전자 장치가 생성한 랜덤 값에 대한 PKI 서명을 생성할 수 있는지 여부에 기반하여 상기 PKI 기반 인증을 수행할 수 있다.

[13] 일실시예에 따른 전자 장치의 동작 방법에서 상기 PKI 기반 인증을 수행하는 단계는 상기 획득한 공개 키에 기반하여 암호화된 데이터를 상기 인증이 필요한 하드웨어 장치가 복호화할 수 있는지 여부에 기반하여 상기 PKI 기반 인증을 수행할 수 있다.

[14] 일실시예에 따른 전자 장치의 동작 방법에서 상기 PKI 기반 인증을 수행하는 단계는 상기 획득한 공개 키 또는 상기 수신한 공개 키를 이용하여, PKI 기반 세션 생성이 성공하는지 여부에 기반하여 상기 PKI 기반 인증을 수행할 수 있다.

[15] 일실시예에 따른 전자 장치의 동작 방법에서 상기 PKI 기반 인증을 수행하는 단계는 상기 획득한 공개 키로, 상기 인증이 필요한 하드웨어 장치로부터 수신한 서명 문서의 서명을 검증할 수 있는지 여부에 기반하여 상기 PKI 기반 인증을 수행할 수 있다.

[16] 일실시예에 따른 전자 장치의 동작 방법에서 상기 PKI 기반 인증을 수행하는 단계는 상기 수신된 식별 정보로부터 공개 키를 유효하게 생성할 수 없는 경우에 응답하여, 상기 수신한 공개 키로부터 획득한 식별 정보가 상기 수신된 식별 정보에 대응하는지 여부에 기반하여 인증을 수행할 수 있다.

[17] 일실시예에 따른 전자 장치의 동작 방법은 인증이 필요한 하드웨어 장치로부터 해당 하드웨어 장치의 식별 정보를 수신하는 단계; 상기 수신된 식별 정보가 기 등록된 식별 정보인지를 확인하는 단계; 및 상기 수신된 식별 정보가 상기 기

등록된 식별 정보인 경우에 응답하여, CA 서버에 의해 발급된 인증서 없이 상기 수신된 식별 정보로부터 획득한 공개 키 또는 상기 인증이 필요한 하드웨어 장치로부터 수신한 공개 키를 이용하여 상기 인증이 필요한 하드웨어 장치에 대해 PKI 기반 인증을 수행하는 단계를 포함한다.

[18] 일실시예에 따른 전자 장치는 프로세서; 및 상기 프로세서에 의해 실행 가능한 적어도 하나의 명령어를 포함하는 메모리를 포함하고, 상기 적어도 하나의 명령어가 상기 프로세서에서 실행되면, 상기 프로세서는 하드웨어 장치의 개인 키로부터 생성된 상기 하드웨어 장치의 공개 키를 이용하여, 상기 하드웨어 장치의 인증에 활용되는 식별 정보를 결정하고, 상기 식별 정보를 관리한다.

[19] 일실시예에 따른 전자 장치에서 상기 프로세서는 상기 공개 키 또는 상기 공개 키에 미리 정해진 함수를 적용하여 얻어진 값에 기초하여 상기 식별 정보를 결정할 수 있다.

[20] 일실시예에 따른 전자 장치에서 상기 함수는 상기 공개 키로부터 미리 정해진 길이의 데이터를 결정하는 암호화 해시 알고리즘, 상기 공개 키를 암호화하는 암호 알고리즘, 상기 공개 키의 일부를 활용하는 함수 또는 이들의 조합에 해당할 수 있다.

[21] 일실시예에 따른 전자 장치에서 상기 프로세서는 상기 하드웨어 장치의 생산자 식별 정보, 제품 식별 정보, 생산일자 및 생산장소 중 적어도 하나에 대한 정보를 더 이용하여 상기 식별 정보를 결정할 수 있다.

[22] 일실시예에 따른 전자 장치에서 상기 하드웨어 장치는 인증 대상이 되는 칩, 모듈, 디바이스 중 어느 하나일 수 있다.

[23] 일실시예에 따른 전자 장치에서 상기 프로세서는 인증이 필요한 하드웨어 장치로부터 수신된 해당 하드웨어 장치의 식별 정보가 기 등록된 식별 정보인지를 확인하고, 상기 수신된 식별 정보가 상기 기 등록된 식별 정보에 해당하는 경우에 응답하여, 상기 수신된 식별 정보로부터 획득한 공개 키 또는 상기 인증이 필요한 하드웨어 장치로부터 수신한 공개 키를 이용하여 상기 인증이 필요한 하드웨어 장치에 대해 PKI 기반 인증을 수행할 수 있다.

발명의 효과

[24] 일실시예에 따르면, CA 서버로부터 인증서를 발급 받지 않고 하드웨어 장치의 공개 키에 기반하여 식별 정보를 생성함으로써, 비교적 단순한 시스템을 통해서도 하드웨어의 무결성을 유효하게 검증할 수 있다. 식별 정보는 외부에 공개되는 공개 키에 기반하여 생성되므로, 식별 정보 자체가 외부에 노출되는 것이 보안과 무관할 수 있다.

[25] 일실시예에 따르면, CA 서버로부터 인증서 발급 없이 식별 정보가 해당 하드웨어 장치의 공개 키로부터 생성됨으로써, CA 서버를 직접 운영하거나, 원격으로 기존 CA 서버에 접속해서 인증서를 발급 받아야 하는 어려움이나 비용 발생을 방지하면서도, 하드웨어 장치의 무결성(integrity)을 유효하게 입증할 수

있는 식별 정보를 얻을 수 있다. 또한, 인증서에 기반한 무거운 데이터 처리가 불필요하므로, 상대적으로 가벼운 보안 처리만으로 하드웨어 장치의 무결성을 효과적으로 입증할 수 있다.

[26] 일실시예에 따르면, 인증서를 발급 받아 사용하는 기존 시스템에서도 관리 목적으로 ID를 추출하여 저장하는 경우라면 인증서 발급 과정만 생략한 채 본 명세서에서 설명한 것을 그대로 적용할 수 있다.

도면의 간단한 설명

[27] 도 1 내지 도 3은 일실시예에 따른 식별 정보를 발급하는 과정을 설명하기 위한 도면이다.

[28] 도 4는 일실시예에 따른 식별 정보에 기반하여 하드웨어 장치를 인증하는 과정을 설명하기 위한 도면이다.

[29] 도 5는 일실시예에 따른 전자 장치를 설명하기 위한 도면이다.

발명의 실시를 위한 최선의 형태

[30] 실시예들에 대한 특정한 구조적 또는 기능적 설명들은 단지 예시를 위한 목적으로 개시된 것으로서, 다양한 형태로 변경되어 구현될 수 있다. 따라서, 실제 구현되는 형태는 개시된 특정 실시예로만 한정되는 것이 아니며, 본 명세서의 범위는 실시예들로 설명한 기술적 사상에 포함되는 변경, 균등물, 또는 대체물을 포함한다.

[31] 제1 또는 제2 등의 용어를 다양한 구성요소들을 설명하는데 사용될 수 있지만, 이런 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 해석되어야 한다. 예를 들어, 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소는 제1 구성요소로도 명명될 수 있다.

[32] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다.

[33] 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 설명된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함으로 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[34] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 해당 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[35] 이하, 실시예들을 첨부된 도면들을 참조하여 상세하게 설명한다. 첨부 도면을 참조하여 설명함에 있어, 도면 부호에 관계없이 동일한 구성 요소는 동일한 참조 부호를 부여하고, 이에 대한 중복되는 설명은 생략하기로 한다.

[36]

[37] 도 1 내지 도 3은 일실시예에 따른 식별 정보를 발급하는 과정을 설명하기 위한 도면이다.

[38] 도 1을 참조하면, 일실시예에 따른 전자 장치에 구비된 프로세서의 제어를 통해 식별 정보를 결정하고 관리하는 방법이 도시된다.

[39] 단계(110)에서, 전자 장치는 하드웨어 장치의 개인 키로부터 생성된 하드웨어 장치의 공개 키를 이용하여, 하드웨어 장치의 인증에 활용되는 식별 정보를 결정한다. 식별 정보는 고유하게 부여되어 해당 하드웨어 장치가 다른 하드웨어 장치와 구별될 수 있게 하는 정보로서, 이러한 식별 정보가 생성되는 과정에 대해서는 도 2 및 도 3을 통해 상세히 설명한다.

[40] 하드웨어 장치는 생산되어 사용자에게 판매된 후 해당 사용자에 의해 사용될 때 무결성 입증이 요구되는 장치로서, 예를 들어, 칩, 모듈, 디바이스 등을 포함할 수 있다. 여기서, 칩이나 모듈은 완제품에 해당하는 디바이스 내에 포함되어 일정한 기능을 담당하는 구성요소를 의미할 수 있다. 디바이스는, 예를 들어 스마트 폰, 태블릿, 랩탑, 퍼스널 컴퓨터 등 다양한 컴퓨팅 장치, 스마트 시계, 스마트 안경, 스마트 의류 등 다양한 웨어러블 기기, 스마트 스피커, 스마트 TV, 스마트 냉장고 등 다양한 가전장치, 스마트 자동차, 스마트 키오스크, IoT(Internet of Things) 기기, WAD(Walking Assist Device), 드론, 로봇 등을 포함할 수 있다.

[41] 아래에서 상세히 설명되겠으나, CA 서버로부터 인증서 발급 없이 식별 정보가 해당 하드웨어 장치의 공개 키로부터 생성됨으로써, CA 서버를 직접 운영하거나, 원격으로 기존 CA 서버에 접속해서 인증서를 발급 받아야 하는 어려움이나 비용 발생을 방지하면서도, 하드웨어 장치의 무결성을 유효하게 입증할 수 있는 식별 정보를 얻을 수 있다. 또한, 인증서에 기반한 무거운 데이터 처리가 불필요하므로, 상대적으로 가벼운 보안 처리만으로 하드웨어 장치의 무결성을 효과적으로 입증할 수 있다.

[42] 이러한 식별 정보를 생성하는 전자 장치는 하드웨어 장치로부터 공개 키 등을 추출하여 식별 정보를 생성하는 발급 장치나, 하드웨어 자체일 수 있으나, 실시예가 이로 한정되는 것은 아니다. 여기서, 발급 장치는 하드웨어 장치를 생산하는 시설에 구비되어 해당 시설에서 하드웨어 장치가 생산될 때마다 해당 장치의 식별 정보를 발급하는 장치일 수 있으나, 발급 장치의 실시예가 이에 한정되는 것은 아니다.

[43] 단계(120)에서, 전자 장치는 식별 정보를 관리한다. 예를 들어, 전자 장치가 발급 장치라면, 여러 하드웨어 장치들 각각에 대해 식별 정보를 결정해서 리스트로 관리할 수 있다. 전자 장치가 하드웨어 자체라면, 자신의 식별 정보를 내부에 저장하고, 외부의 데이터베이스로도 전송하여 여러 식별 정보들이 함께

관리되게끔 할 수 있다.

[44] 일실시예에서, 식별 정보들을 수집한 엔티티(entity)(예컨대, 칩이나 모듈 생산자 등)가 다른 엔티티(예컨대, 칩이나 모듈을 제공 받아 디바이스를 생산하는 자 등)로 식별 정보 리스트를 전달함으로써, 추후 설명할 인증 과정을 수행할 주체가 변경될 수도 있다. 식별 정보 리스트를 전달 받은 엔티티가 또 다른 엔티티로 해당 리스트를 이관시킬 수도 있음은 물론이다.

[45] 만약 특정 하드웨어 장치에 분실, 도난, 폐기 등의 이벤트가 발생하면, 해당 하드웨어 장치의 식별 정보를 식별 정보 리스트에서 삭제하거나, 폐기 리스트에 추가하여 별도로 관리함으로써, 해당 하드웨어 장치가 무단으로 사용되거나, 도용되는 것을 효과적으로 막을 수 있다.

[46] 이하, 설명의 편의를 위해 식별 정보가 발급 장치에서 결정되는 예시를 기준으로 설명하겠으나, 아래의 설명이 하드웨어 장치에서 식별 정보가 결정되는 예시에도 마찬가지로 적용될 수 있으므로, 보다 상세한 설명은 생략한다.

[47]

[48] 도 2를 참조하면, 일실시예에 따라 하드웨어 장치와 발급 장치 간 동작을 설명하기 위한 블록도가 도시된다.

[49] 먼저, 하드웨어 장치는 자신의 비밀 키를 결정할 수 있다. 예를 들어, 하드웨어 장치는 PUF 값에 기반하여 비밀 키를 생성하거나, RNG(random number generator)에서 생성된 랜덤 값에 기반하여 비밀 키를 생성할 수도 있다. 다만, 비밀 키를 생성하는 예시를 한정하는 것은 아니고, 비밀 키를 생성할 수 있는 다른 방법에도 본 명세서의 설명이 적용될 수 있다.

[50] 그리고, 하드웨어 장치는 PKI에 기반하여 비밀 키로부터 공개 키를 생성할 수 있다. 하드웨어 장치는 식별 정보의 생성을 위해 공개 키를 발급 장치로 전송할 수 있다. 본 명세서에서 식별 정보는 설명의 편의를 위해 ID로도 지칭될 수 있다.

[51] 발급 장치는 하드웨어 장치의 공개 키를 이용하여 해당 하드웨어 장치의 ID를 생성할 수 있으며, 이때 함수가 추가적으로 이용될 수도 있다.

[52] 도 3을 참조하여 식별 키 생성에 대해 상세하게 설명하면, 식별 정보는 공개 키 또는 공개 키에 일정한 함수를 적용시킨 값에 기반하여 결정될 수 있다. 함수 적용 없이 공개 키로 식별 정보를 결정하는 경우에도, 공개 키의 전체 또는 일부가 식별 정보 결정에 이용될 수 있다.

[53] 또한, 함수는 공개 키로부터 미리 정해진 길이의 데이터를 결정하는 암호화 해시 알고리즘(cryptographic hash algorithm), 공개 키를 암호화하는 암호 알고리즘, 공개 키의 일부를 활용하는 함수 또는 이들의 조합에 해당할 수 있다. 공개 키가 너무 긴 경우(예컨대, RSA(Rivest Shamir Adleman)나 PQC(post quantum cryptography)가 사용되는 경우 등), 이를 일정 길이의 데이터로 줄일 수 있는 암호화 해시 알고리즘이 함수로 식별 키에 적용되어 상대적으로 짧은 길이의 식별 정보가 얻어질 수 있다. 또는, 공개 키에 암호화 알고리즘을

적용시키거나, 공개 키의 일부를 자르거나(trim), 공개 키에 XOR(Exclusive OR) 연산을 적용시켜서 얻어진 값에 기초하여 식별 정보가 결정될 수도 있다. 경우에 따라서는, 앞서 설명한 함수들 둘 이상을 조합하여 공개 키에 적용시킴으로써 식별 정보가 결정될 수도 있다. 또한, 함수에 공개 키 전체가 입력될 수도 있으나, 실시예에 따라서는 공개 키의 일부만 함수에 입력되거나, 공개 키에 다른 특정 값을 추가한 결과가 함수에 입력될 수도 있다.

[54] 또한, 식별 정보가 공개 키 또는 공개 키에 함수를 적용시킨 값에 기반하여 결정될 때, 부가 정보가 추가적으로 고려될 수 있다. 예를 들어, 부가 정보는 하드웨어 장치의 생산자 식별 정보, 제품 식별 정보, 생산일자 및 생산장소 중 적어도 하나에 대한 정보를 포함할 수 있다. 다시 말해, 공개 키 또는 공개 키에 함수를 적용시킨 값과 같은 하드웨어 장치마다 상이한 개별 정보뿐만 아니라 생산자 식별 정보, 제품 식별 정보, 생산일자 및 생산장소에 대한 정보와 같이 함께 생성된 복수의 하드웨어 장치들이 공통적으로 가지는 고정 정보도 식별 정보 생성에 이용될 수 있다.

[55] 도 2로 돌아와서, 생성된 ID는 발급 장치에 의해 데이터베이스에 수집 및 저장되어 식별 정보 리스트로 관리될 수 있다. 식별 정보 리스트는 추후 하드웨어 장치의 무결성을 인증하는 인증 서버에 의해 활용될 수 있다.

[56] 또한, 생성된 ID는 하드웨어 장치로 전송되어 저장될 수 있다.

[57]

[58] 도 4는 일실시예에 따른 식별 정보에 기반하여 하드웨어 장치를 인증하는 과정을 설명하기 위한 도면이다.

[59] 도 4를 참조하면, 일실시예에 따른 전자 장치에 구비된 프로세서의 제어를 통해 하드웨어 장치를 인증하는 방법이 도시된다.

[60] 하드웨어 장치가 생산되어 사용자에게 판매된 경우, 해당 사용자는 하드웨어 장치에 기반한 서비스 이용을 위해 해당 서비스를 제공하는 서비스 서버에 접속할 수 있다. 서비스 서버는 정식 생산시설에서 실제 생산된 하드웨어 장치를 구매한 사용자에게만 서비스를 제공하기 위하여, 접속된 하드웨어 장치의 무결성 또는 유효성을 검증할 수 있다. 이때, 앞서 설명한 방식으로 생성된 식별 정보가 이용될 수 있다. 이후에 상세히 설명하겠으나, 이러한 무결성 또는 유효성 검증에 CA 서버에서 발급된 인증서가 요구되지 않아 상대적으로 적은 비용과 단순한 검증 방식으로도 손쉽게 검증이 수행될 수 있다. 본 명세서에서 하드웨어 장치의 무결성이나 유효성을 검증하는 서비스 서버는 설명의 편의를 위해 인증 서버로도 지칭될 수 있다.

[61] 만약 하드웨어 장치에 해당하는 칩(예컨대, SoC(System On Chip) 등)이 칩 제조사에서 생산되어 디바이스 제조사로 전달된 경우, 칩 제조사는 전달하는 하드웨어 장치들에 대한 식별 정보 리스트도 함께 디바이스 제조사로 전달함으로써, 디바이스 제조사는 칩의 진위 여부를 식별 정보 리스트를 통해 손쉽게 확인할 수 있다. 또한, 디바이스 제조사는 칩을 이용해 디바이스를

만들어 사용자에게 판매한 후, 해당 사용자가 디바이스를 통해 디바이스 제조사가 운영하는 서버에 접속하면 칩의 식별 정보를 통해 칩의 진위 여부뿐만 아니라 디바이스의 식별 정보를 통해 디바이스의 진위 여부를 용이하게 확인할 수 있고, 무결성이 검증된 칩이 적용된 디바이스나 무결성이 입증된 디바이스에게만 자신의 서비스를 제공할 수 있다.

[62] 이하, 하드웨어 장치를 인증하는 방법에 대해 상세히 설명하며, 인증 동작을 수행하는 서비스 서버 또는 인증 서버는 전자 장치로도 지칭될 수 있다.

[63] 단계(410)에서, 전자 장치는 인증이 필요한 하드웨어 장치로부터 해당 하드웨어 장치의 식별 정보를 수신한다.

[64] 단계(420)에서, 전자 장치는 수신된 식별 정보가 기 등록된 식별 정보인지를 확인한다. 전자 장치는 하드웨어 장치로부터 수신된 식별 정보가 리스트에 기 등록된 식별 정보인지를 확인할 수 있다. 또는, 전자 장치는 하드웨어 장치로부터 수신된 식별 정보가 폐기 리스트에 등록된 식별 정보인지를 확인할 수도 있다. 만약 수신된 식별 정보가 유효 리스트에 기 등록된 식별 정보에 해당하지 않는다면, 전자 장치는 하드웨어 장치의 인증을 거부하고 동작을 종료할 수 있다. 반대로, 수신된 식별 정보가 유효 리스트에 기 등록된 식별 정보에 해당한다면, 단계(430)가 이어서 수행될 수 있다.

[65] 단계(430)에서, 전자 장치는 수신된 식별 정보로부터 획득한 공개 키 또는 인증이 필요한 하드웨어 장치로부터 수신한 공개 키를 이용하여 인증이 필요한 하드웨어 장치에 대해 PKI 기반 인증을 수행한다. 이러한 PKI 기반 인증에는 CA 서버에 의해 발급된 인증서가 이용되지 않으므로, CA 서버로부터 인증서를 발급받는 과정도 요구되지 않는다. 앞서 설명한 공개 키로부터 식별 정보를 결정하는 방식을 반대로 적용하여, 식별 정보로부터 공개 키가 획득될 수도 있다.

[66] 만약 식별 정보에 공개 키가 모두 포함되지 않아 식별 정보로부터 온전한 공개 키를 생성하기 어려운 경우라면, 하드웨어 장치로부터 수신된 공개 키에 동일한 방식을 적용하여 식별 정보를 생성하고, 생성된 식별 정보가 단계(410)에서 수신된 식별 정보와 일치하는지 여부로 인증을 수행할 수도 있다. 특히, 해시 알고리즘이 적용된 경우라면 해시 알고리즘 특성에 의해 공개 키의 유효성을 보다 명확하게 확인할 수 있다.

[67] 예를 들어, 획득한 공개 키 또는 수신한 공개 키를 이용하여 전자 장치가 생성한 랜덤 값에 대한 PKI 서명을 생성할 수 있는지 여부에 기초하여 PKI 기반 인증이 수행될 수 있다.

[68] 또한, 획득한 공개 키에 기반하여 암호화된 데이터를 하드웨어 장치가 복호화할 수 있는지 여부에 기반하여 PKI 기반 인증이 수행될 수 있다. 만약 하드웨어 장치가 유효한 식별 정보를 도용하여 인증을 시도한 경우라면, 해당 하드웨어 장치는 정당한 개인 키를 가지고 있지 않으므로 해당 식별 정보로부터 획득된 공개 키로 암호화된 데이터를 복호화할 수 없다는 특성을 이용한 인증 방법이다.

[69] 또한, 획득한 공개 키 또는 수신한 공개 키를 이용하여, PKI 기반 세션 생성이 성공하는지 여부에 기반하여 PKI 기반 인증이 수행될 수 있다.

[70] 또한, 획득한 공개 키로, 하드웨어 장치로부터 수신한 서명 문서의 서명을 검증할 수 있는지 여부에 기반하여 PKI 기반 인증이 수행될 수 있다. 만약 하드웨어 장치가 유효한 식별 정보를 도용하여 인증을 시도한 경우라면, 해당 하드웨어 장치는 정당한 개인 키를 가지고 있지 않으므로 정당한 개인 키로 서명한 서명 문서를 생성할 수 없다. 따라서, 하드웨어 장치로부터 수신된 서명 문서의 서명이 획득한 공개 키로 검증할 수 없으며, 이러한 특성을 이용한 인증 방법이다.

[71]

[72] 도 5는 일실시예에 따른 전자 장치를 설명하기 위한 도면이다.

[73] 도 5를 참조하면, 일실시예에 따른 전자 장치(500)는 메모리(510) 및 프로세서(520)를 포함한다. 메모리(510) 및 프로세서(520)는 버스(bus)(530)를 통하여 서로 통신할 수 있다. 도 5에서는 다른 디바이스와 유선 및/또는 무선 네트워크를 통해 통신을 수행하는 통신부가 생략될 수 있다. 전자 장치(500)는 앞서 설명한 하드웨어 장치, 발급 장치, 서비스 서버 또는 인증 서버로 구현될 수 있다.

[74] 메모리(510)는 컴퓨터에서 읽을 수 있는 명령어를 포함할 수 있다. 프로세서(520)는 메모리(510)에 저장된 명령어가 프로세서(520)에서 실행됨에 따라 앞서 언급된 동작들을 수행할 수 있다. 메모리(510)는 휘발성 메모리 또는 비휘발성 메모리일 수 있다.

[75] 프로세서(520)는 명령어들, 혹은 프로그램들을 실행하거나, 전자 장치(500)를 제어하는 장치로서, 예를 들어, CPU(Central Processing Unit) 및 GPU(Graphic Processing Unit) 등을 포함할 수 있다.

[76] 전자 장치(500)가 하드웨어 장치 또는 발급 장치로 구현되는 경우에, 프로세서(520)는 하드웨어 장치의 개인 키로부터 생성된 하드웨어 장치의 공개 키를 이용하여, 하드웨어 장치의 인증에 활용되는 식별 정보를 결정하고, 식별 정보를 관리한다.

[77] 전자 장치(500)가 서비스 서버 또는 인증 서버로 구현되는 경우에, 프로세서(520)는 인증이 필요한 하드웨어 장치로부터 해당 하드웨어 장치의 식별 정보를 수신하고, 수신된 식별 정보가 기 등록된 식별 정보인지를 확인하며, 수신된 식별 정보가 기 등록된 식별 정보인 경우에 응답하여, CA 서버에 의해 발급된 인증서 없이 수신된 식별 정보로부터 획득한 공개 키 또는 인증이 필요한 하드웨어 장치로부터 수신한 공개 키를 이용하여 인증이 필요한 하드웨어 장치에 대해 PKI 기반 인증을 수행한다.

[78] 실시예들은, 기존의 칩, 모듈, 디바이스에 인증, 추적 등의 목적으로 보안이 필요한 경우 CA 서버로부터 인증서를 발급 받아 사용하는 불편함을 해소하기 위해 ID를 공개 키에 기반하여 생성함으로써, 칩, 모듈, 디바이스의 유효성을

증명하는데 비용이나 노력을 효과적으로 감소시킬 수 있다. 특히, 인증서를 발급 받아 사용하는 기존 시스템에서도 관리 목적으로 ID를 추출하여 저장하는 경우라면 인증서 발급 과정만 생략한 채 본 명세서에서 설명한 것을 그대로 적용할 수 있다.

[79] 그 밖에, 전자 장치(500)에 관해서는 상술된 동작을 처리할 수 있다.

[80]

[81] 이상에서 설명된 실시예들은 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치, 방법 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[82] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[83] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있으며 매체에 기록되는 프로그램 명령은 실시예를 위하여

특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[84] 위에서 설명한 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 또는 복수의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[85] 이상과 같이 실시예들이 비록 한정된 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 이를 기초로 다양한 기술적 수정 및 변형을 적용할 수 있다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[86] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

청구범위

[청구항 1] 하드웨어 장치의 개인 키로부터 생성된 상기 하드웨어 장치의 공개 키를 이용하여, 상기 하드웨어 장치의 인증에 활용되는 식별 정보를 결정하는 단계; 및
상기 식별 정보를 관리하는 단계
를 포함하는
전자 장치의 동작 방법.

[청구항 2] 제1항에 있어서,
상기 식별 정보를 결정하는 단계는
상기 공개 키 또는 상기 공개 키에 미리 정해진 함수를 적용하여 얻어진 값에 기초하여 상기 식별 정보를 결정하는,
전자 장치의 동작 방법.

[청구항 3] 제2항에 있어서,
상기 함수는
상기 공개 키로부터 미리 정해진 길이의 데이터를 결정하는 암호화 해시 알고리즘(cryptographic hash algorithm), 상기 공개 키를 암호화하는 암호 알고리즘, 상기 공개 키의 일부를 활용하는 함수 또는 이들의 조합에 해당하는,
전자 장치의 동작 방법.

[청구항 4] 제1항에 있어서,
상기 식별 정보를 결정하는 단계는
상기 하드웨어 장치의 생산자 식별 정보, 제품 식별 정보, 생산일자 및 생산장소 중 적어도 하나에 대한 정보를 더 이용하여 상기 식별 정보를 결정하는,
전자 장치의 동작 방법.

[청구항 5] 제1항에 있어서,
상기 하드웨어 장치는
인증 대상이 되는 칩, 모듈, 디바이스 중 어느 하나인,
전자 장치의 동작 방법.

[청구항 6] 제1항에 있어서,
인증이 필요한 하드웨어 장치로부터 수신된 해당 하드웨어 장치의 식별 정보가 기 등록된 식별 정보인지를 확인하는 단계; 및
상기 수신된 식별 정보가 상기 기 등록된 식별 정보인 경우에 응답하여, 상기 수신된 식별 정보로부터 획득한 공개 키 또는 상기 인증이 필요한 하드웨어 장치로부터 수신한 공개 키를 이용하여 상기 인증이 필요한 하드웨어 장치에 대해 PKI 기반 인증을 수행하는 단계
를 더 포함하는,

전자 장치의 동작 방법.

[청구항 7] 제6항에 있어서,
상기 PKI 기반 인증을 수행하는 단계는
CA 서버에 의해 발급된 인증서 없이, 상기 획득한 공개 키 또는 상기 수신한 공개 키를 이용하여 PKI 기반 인증을 수행하는,
전자 장치의 동작 방법.

[청구항 8] 제6항에 있어서,
상기 PKI 기반 인증을 수행하는 단계는
상기 획득한 공개 키 또는 상기 수신한 공개 키를 이용하여, 상기 전자 장치가 생성한 랜덤 값에 대한 PKI 서명을 생성할 수 있는지 여부에 기반하여 상기 PKI 기반 인증을 수행하는,
전자 장치의 동작 방법.

[청구항 9] 제6항에 있어서,
상기 PKI 기반 인증을 수행하는 단계는
상기 획득한 공개 키에 기반하여 암호화된 데이터를 상기 인증이 필요한 하드웨어 장치가 복호화할 수 있는지 여부에 기반하여 상기 PKI 기반 인증을 수행하는,
전자 장치의 동작 방법.

[청구항 10] 제6항에 있어서,
상기 PKI 기반 인증을 수행하는 단계는
상기 획득한 공개 키 또는 상기 수신한 공개 키를 이용하여, PKI 기반 세션 생성이 성공하는지 여부에 기반하여 상기 PKI 기반 인증을 수행하는,
전자 장치의 동작 방법.

[청구항 11] 제6항에 있어서,
상기 PKI 기반 인증을 수행하는 단계는
상기 획득한 공개 키로, 상기 인증이 필요한 하드웨어 장치로부터 수신한 서명 문서의 서명을 검증할 수 있는지 여부에 기반하여 상기 PKI 기반 인증을 수행하는,
전자 장치의 동작 방법.

[청구항 12] 제6항에 있어서,
상기 PKI 기반 인증을 수행하는 단계는
상기 수신된 식별 정보로부터 공개 키를 유효하게 생성할 수 없는 경우에 응답하여, 상기 수신한 공개 키로부터 획득한 식별 정보가 상기 수신된 식별 정보에 대응하는지 여부에 기반하여 인증을 수행하는,
전자 장치의 동작 방법.

[청구항 13] 인증이 필요한 하드웨어 장치로부터 해당 하드웨어 장치의 식별 정보를 수신하는 단계;
상기 수신된 식별 정보가 기 등록된 식별 정보인지를 확인하는 단계; 및

상기 수신된 식별 정보가 상기 기 등록된 식별 정보인 경우에 응답하여, CA 서버에 의해 발급된 인증서 없이 상기 수신된 식별 정보로부터 획득한 공개 키 또는 상기 인증이 필요한 하드웨어 장치로부터 수신한 공개 키를 이용하여 상기 인증이 필요한 하드웨어 장치에 대해 PKI 기반 인증을 수행하는 단계

를 포함하는

전자 장치의 동작 방법.

[청구항 14] 제1항 내지 제13항 중에서 어느 하나의 항의 방법을 실행시키기 위한 프로그램이 기록된 컴퓨터 판독 가능한 저장 매체.

[청구항 15] 프로세서; 및

상기 프로세서에 의해 실행 가능한 적어도 하나의 명령어를 포함하는 메모리

를 포함하고,

상기 적어도 하나의 명령어가 상기 프로세서에서 실행되면, 상기 프로세서는

하드웨어 장치의 개인 키로부터 생성된 상기 하드웨어 장치의 공개 키를 이용하여, 상기 하드웨어 장치의 인증에 활용되는 식별 정보를 결정하고,

상기 식별 정보를 관리하는,

전자 장치.

[청구항 16] 제15항에 있어서,

상기 프로세서는

상기 공개 키 또는 상기 공개 키에 미리 정해진 함수를 적용하여 얻어진 값에 기초하여 상기 식별 정보를 결정하는,

전자 장치.

[청구항 17] 제16항에 있어서,

상기 함수는

상기 공개 키로부터 미리 정해진 길이의 데이터를 결정하는 암호화 해시 알고리즘(cryptographic hash algorithm), 상기 공개 키를 암호화하는 암호 알고리즘, 상기 공개 키의 일부를 활용하는 함수 또는 이들의 조합에 해당하는,

전자 장치.

[청구항 18] 제15항에 있어서,

상기 프로세서는

상기 하드웨어 장치의 생산자 식별 정보, 제품 식별 정보, 생산일자 및 생산장소 중 적어도 하나에 대한 정보를 더 이용하여 상기 식별 정보를 결정하는,

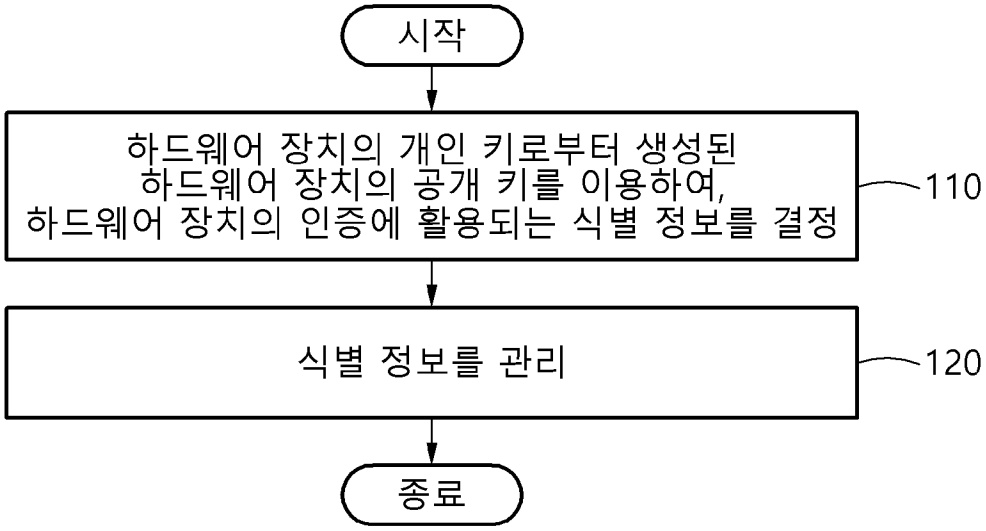
전자 장치.

[청구항 19] 제15항에 있어서,

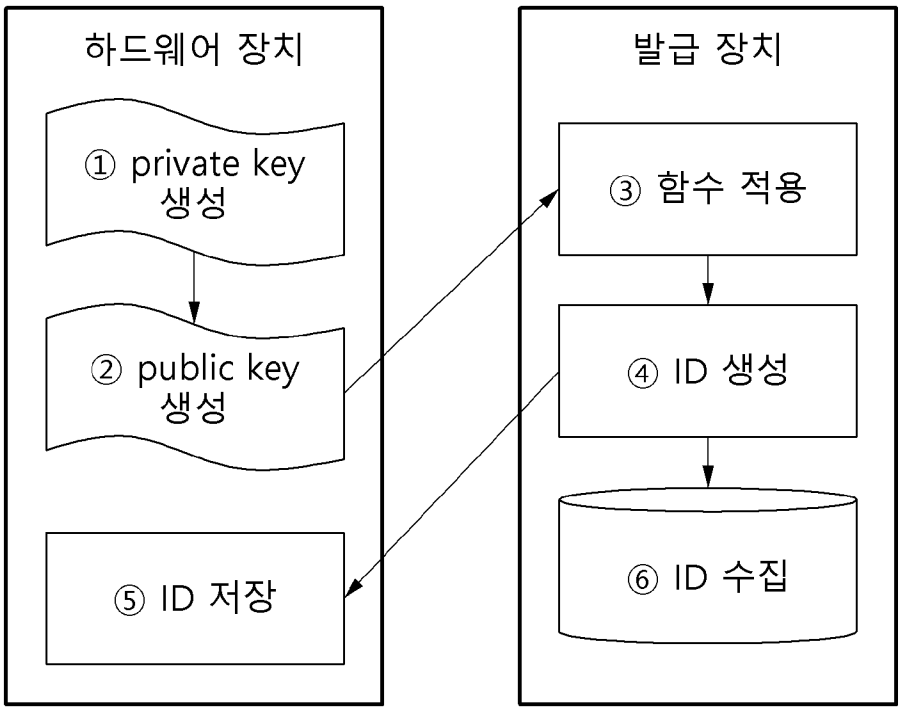
상기 하드웨어 장치는
인증 대상이 되는 칩(chip), 모듈(module), 디바이스 중 어느 하나인,
전자 장치.

[청구항 20] 제15항에 있어서,
상기 프로세서는
인증이 필요한 하드웨어 장치로부터 수신된 해당 하드웨어 장치의 식별 정보가 기 등록된 식별 정보인지를 확인하고,
상기 수신된 식별 정보가 상기 기 등록된 식별 정보에 해당하는 경우에 응답하여, 상기 수신된 식별 정보로부터 획득한 공개 키 또는 상기 인증이 필요한 하드웨어 장치로부터 수신한 공개 키를 이용하여 상기 인증이 필요한 하드웨어 장치에 대해 PKI 기반 인증을 수행하는
전자 장치.

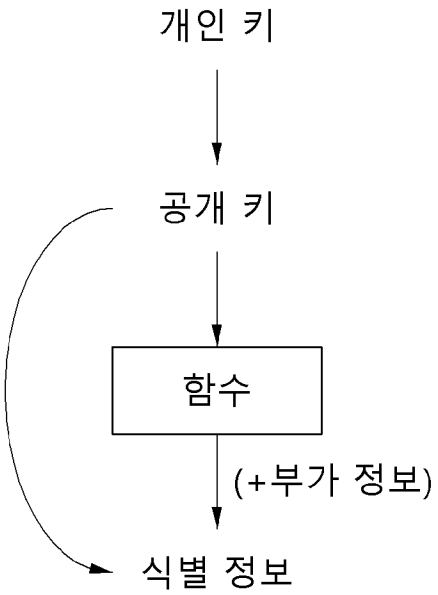
[도1]


시작
하드웨어 장치의 개인 키로부터 생성된
하드웨어 장치의 공개 키를 이용하여,
하드웨어 장치의 인증에 활용되는 식별 정보를 결정
110
식별 정보를 관리
120
종료

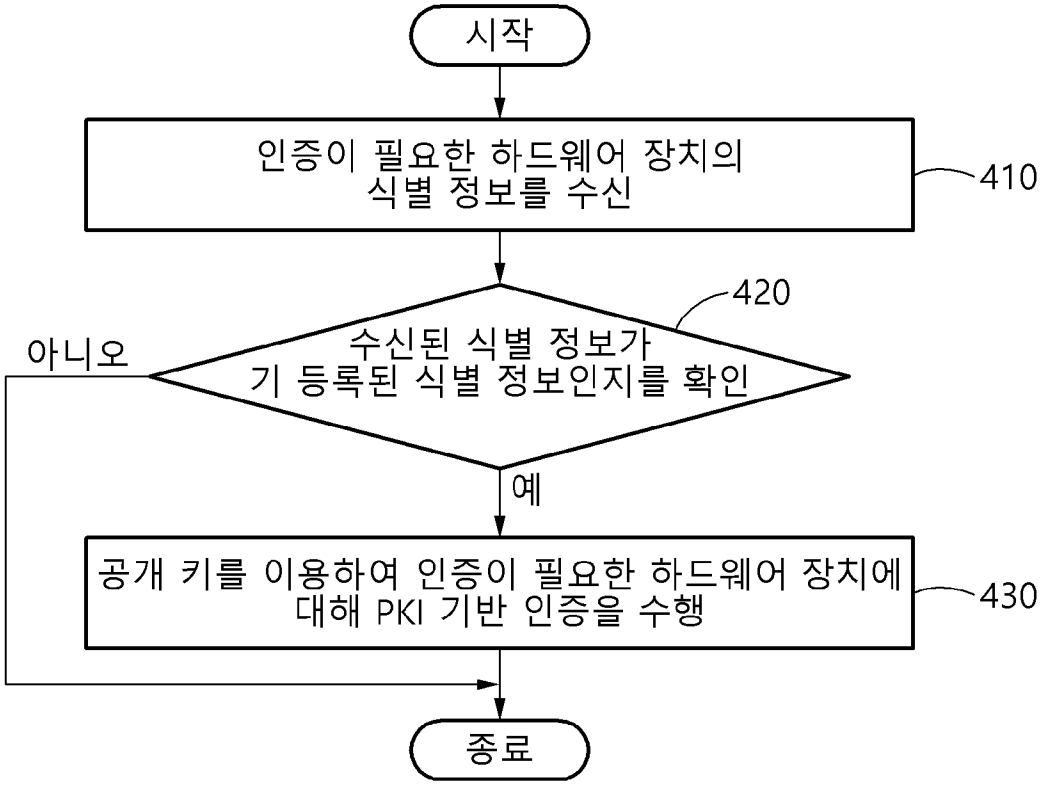
[도2]


하드웨어 장치
① private key 생성
② public key 생성
⑤ ID 저장
발급 장치
③ 함수 적용
④ ID 생성
⑥ ID 수집

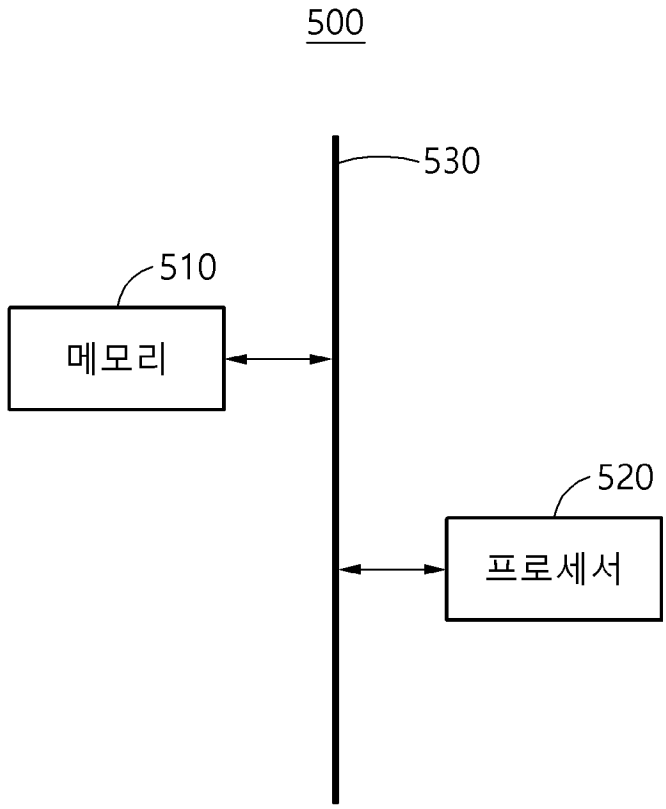
[도3]


개인 키
공개 키
함수
(+부가 정보)
식별 정보

[도4]


시작
인증이 필요한 하드웨어 장치의
식별 정보를 수신
410
420
수신된 식별 정보가
기 등록된 식별 정보인지를 확인
아니오
예
공개 키를 이용하여 인증이 필요한 하드웨어 장치에
대해 PKI 기반 인증을 수행
430
종료

[도5]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2021/009962

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/73(2013.01)i; **G06F 21/33**(2013.01)i; **H04L 9/08**(2006.01)i; **H04L 9/32**(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/73(2013.01); G06F 21/44(2013.01); G06F 21/70(2013.01); H04L 29/08(2006.01); H04L 9/08(2006.01); H04L 9/14(2006.01); H04L 9/32(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models: IPC as above
Japanese utility models and applications for utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & keywords: 하드웨어(hardware), 식별(identification), 인증(authentication), 개인 키(private key), 공개 키(public key), 함수(function), 암호화 해시 알고리즘(cryptographic hash algorithm), 칩(chip), 모듈(module), 디바이스(device), PKI(Public Key Infrastructure), CA(certificate authority), 서버(server)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2015-0080579 A (INTEL CORPORATION) 09 July 2015 (2015-07-09) See paragraphs [0006], [0008] and [0035]; claims 1 and 6-7; and figure 2.	1-5,14-19
Y		6-13,20
Y	KR 10-2017-0087678 A (SAMSUNG ELECTRONICS CO., LTD.) 31 July 2017 (2017-07-31) See paragraphs [0032], [0057], [0096]-[0097] and [0118]; and figures 1 and 5.	6-13,20
A	KR 10-2019-0002388 A (ICTK HOLDINGS CO., LTD.) 08 January 2019 (2019-01-08) See paragraphs [0021]-[0025] and [0072]-[0078]; and figures 4 and 6.	1-20
A	KR 10-2013-0129334 A (ICTK CO., LTD.) 28 November 2013 (2013-11-28) See paragraphs [0099]-[0103]; and figure 4.	1-20

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 January 2022	**11 January 2022**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **Government Complex-Daejeon Building 4, 189 Cheongsa-ro, Seo-gu, Daejeon 35208**	
Facsimile No. **+82-42-481-8578**	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2021/009962

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-1599995 B1 (KOREA UNIVERSITY RESEARCH AND BUSINESS FOUNDATION) 07 March 2016 (2016-03-07) See claims 1 and 6.	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2021/009962

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
KR 10-2015-0080579 A	09 July 2015	CN 104838385 A	12 August 2015
		CN 104838385 B	02 March 2018
		EP 2939171 A1	04 November 2015
		EP 2939171 A4	10 August 2016
		KR 10-1723006 B1	04 April 2017
		US 2014-0189890 A1	03 July 2014
		US 8938792 B2	20 January 2015
		WO 2014-105310 A1	03 July 2014
KR 10-2017-0087678 A	31 July 2017	CN 107070657 A	18 August 2017
		US 10263961 B2	16 April 2019
		US 2017-0214662 A1	27 July 2017
KR 10-2019-0002388 A	08 January 2019	EP 2991267 A1	02 March 2016
		EP 2991267 B1	23 October 2019
		EP 3598696 A1	22 January 2020
		KR 10-1947408 B1	13 February 2019
		KR 10-2014-0126787 A	03 November 2014
		US 2016-0065378 A1	03 March 2016
		US 9876647 B2	23 January 2018
		WO 2014-175538 A1	30 October 2014
KR 10-2013-0129334 A	28 November 2013	CN 103748831 A	23 April 2014
		CN 103748831 B	21 July 2017
		CN 107579828 A	12 January 2018
		EP 2747335 A2	25 June 2014
		EP 2747335 B1	11 January 2017
		EP 3206330 A1	16 August 2017
		EP 3206330 B1	26 December 2018
		ES 2615750 T3	08 June 2017
		JP 2014-528195 A	23 October 2014
		KR 10-1372719 B1	19 March 2014
		KR 10-1952601 B1	03 June 2019
		KR 10-2013-0019358 A	26 February 2013
		TW 201342868 A	16 October 2013
		TW I479870 B	01 April 2015
		US 2014-0310515 A1	16 October 2014
		US 9787670 B2	10 October 2017
		WO 2013-025060 A2	21 February 2013
		WO 2013-025060 A3	11 April 2013
KR 10-1599995 B1	07 March 2016	None	

국 제 조 사 보 고 서

국제출원번호
PCT/KR2021/009962

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/73(2013.01)i; **G06F 21/33**(2013.01)i; **H04L 9/08**(2006.01)i; **H04L 9/32**(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 21/73(2013.01); G06F 21/44(2013.01); G06F 21/70(2013.01); H04L 29/08(2006.01); H04L 9/08(2006.01); H04L 9/14(2006.01); H04L 9/32(2006.01)

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 하드웨어(hardware), 식별(identification), 인증(authentication), 개인키(private key), 공개 키(public key), 함수(function), 암호화 해시 알고리즘(cryptographic hash algorithm), 칩(chip), 모듈(module), 디바이스(device), PKI(Public Key Infrastructure), CA(certificate authority), 서버(server)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	KR 10-2015-0080579 A (인텔 코포레이션) 2015.07.09 단락 [0006], [0008], [0035]; 청구항 1, 6-7; 및 도면 2	1-5,14-19
Y		6-13,20
Y	KR 10-2017-0087678 A (삼성전자주식회사) 2017.07.31 단락 [0032], [0057], [0096]-[0097], [0118]; 및 도면 1, 5	6-13,20
A	KR 10-2019-0002388 A (주식회사 아이씨티케이 홀딩스) 2019.01.08 단락 [0021]-[0025], [0072]-[0078]; 및 도면 4, 6	1-20
A	KR 10-2013-0129334 A ((주) 아이씨티케이) 2013.11.28 단락 [0099]-[0103]; 및 도면 4	1-20
A	KR 10-1599995 B1 (고려대학교 산학협력단) 2016.03.07 청구항 1, 6	1-20

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☑ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌
"D" 본 국제출원에서 출원인이 인용한 문헌
"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌
"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌
"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌
"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌
"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌
"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.
"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.
"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2022년01월10일(10.01.2022)	**2022년01월11일(11.01.2022)**

ISA/KR의 명칭 및 우편주소	심사관
대한민국 특허청 **(35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)**	**양정록**
팩스 번호 **+82-42-481-8578**	전화번호 **+82-42-481-5709**

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2021/009962

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2015-0080579 A	2015/07/09	CN 104838385 A	2015/08/12
		CN 104838385 B	2018/03/02
		EP 2939171 A1	2015/11/04
		EP 2939171 A4	2016/08/10
		KR 10-1723006 B1	2017/04/04
		US 2014-0189890 A1	2014/07/03
		US 8938792 B2	2015/01/20
		WO 2014-105310 A1	2014/07/03
KR 10-2017-0087678 A	2017/07/31	CN 107070657 A	2017/08/18
		US 10263961 B2	2019/04/16
		US 2017-0214662 A1	2017/07/27
KR 10-2019-0002388 A	2019/01/08	EP 2991267 A1	2016/03/02
		EP 2991267 B1	2019/10/23
		EP 3598696 A1	2020/01/22
		KR 10-1947408 B1	2019/02/13
		KR 10-2014-0126787 A	2014/11/03
		US 2016-0065378 A1	2016/03/03
		US 9876647 B2	2018/01/23
		WO 2014-175538 A1	2014/10/30
KR 10-2013-0129334 A	2013/11/28	CN 103748831 A	2014/04/23
		CN 103748831 B	2017/07/21
		CN 107579828 A	2018/01/12
		EP 2747335 A2	2014/06/25
		EP 2747335 B1	2017/01/11
		EP 3206330 A1	2017/08/16
		EP 3206330 B1	2018/12/26
		ES 2615750 T3	2017/06/08
		JP 2014-528195 A	2014/10/23
		KR 10-1372719 B1	2014/03/19
		KR 10-1952601 B1	2019/06/03
		KR 10-2013-0019358 A	2013/02/26
		TW 201342868 A	2013/10/16
		TW I479870 B	2015/04/01
		US 2014-0310515 A1	2014/10/16
		US 9787670 B2	2017/10/10
		WO 2013-025060 A2	2013/02/21
		WO 2013-025060 A3	2013/04/11
KR 10-1599995 B1	2016/03/07	없음	