(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2012 년 9 월 13 일 (13.09.2012)

WIPO | PCT

(10) 국제공개번호
WO 2012/121497 A2

(51) 국제특허분류:
H04L 9/32 (2006.01) *H04W 12/06* (2009.01)

(21) 국제출원번호: PCT/KR2012/001246

(22) 국제출원일: 2012 년 2 월 20 일 (20.02.2012)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2011-0019204 2011 년 3 월 4 일 (04.03.2011) KR

(71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **(주) 잉카인터넷 (INCA INTERNET CO., LTD.)** [KR/KR]; 서울특별시 구로구 구로 3 동 235-2 에이스하이엔드타워 1201 호, 152-740 Seoul (KR).

(72) 발명자; 겸
(75) 발명자/출원인 (US 에 한하여): **정영석 (JUNG, Young Suk)** [KR/KR]; 경기도 안양시 만안구 박달 2 동 대림한숲타운 105 동 102 호, 430-702 Gyeonggi-do (KR). **한형덕 (HAN, Hyung-Deok)** [KR/KR]; 경기도 광명시 소하 1 동 소하휴먼시아 5 단지 503 동 1002 호, 423-051 Gyeonggi-do (KR). **황 재 연 (HWANG, Jae Yeon)** [KR/KR]; 서울특별시 동작구 상도동 509-11 번지, 156-030 Seoul (KR).

(74) 대리인: **특허법인 우인 (WOOIN PATENT & LAW FIRM)**; 서울특별시 강남구 역삼동 648-15 신원빌딩 3 층, 135-911 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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

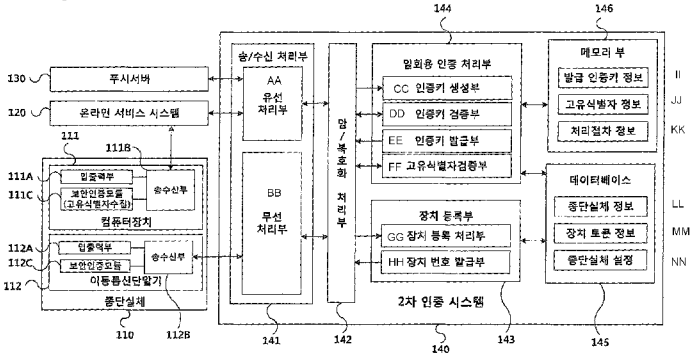
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS,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

[다음 쪽 계속]

(54) Title: DISTINCT IDENTIFIER-BASED AUTHENTICATION SYSTEM AND METHOD

(54) 발명의 명칭 : 고유식별자 기반 인증시스템 및 방법

[Fig. 2]



AA ... Wired processing unit
BB ... Wireless processing unit
CC ... Authentication key generation unit
DD ... Authentication key verification unit
EE ... Authentication key issue unit
FF ... Distinct identifier verification unit
GG ... Device registration processing unit
HH ... Device number issue unit
II ... Issued authentication key information
JJ ... Distinct identifier information
KK ... Processing procedure information
LL ... End entity information
MM ... Device token information
NN ... End entity setup
110 ... End entity

111 ... Computer device
111A, 112A ... Input and output unit
111B, 112B ... Transmission and reception unit
111C ... Security authentication module (collection of distinct identifier)
112 ... Mobile communication terminal
112C ... Security authentication module
120 ... Online service system
130 ... Push server
140 ... Second-authentication system
141 ... Transmission/reception processing unit
142 ... Encoding/decoding processing unit
143 ... Device registration unit
144 ... Disposable authentication processing unit
145 ... Database
146 ... Memory unit

(57) **Abstract**: A distinct identifier-based authentication system according to the present invention comprises: a device registration unit with which end entity information required for second authentication and a mobile communication terminal matched with the end entity information are registered; a transmission and reception processing unit which communicates with an online service system to receive a distinct identifier of a first-authenticated computer device with the end entity information, a distinct identifier of a second-authentication attempt computer device which attempts a second authentication with the end entity information, and a disposable authentication key inputted from the second-authentication attempt computer device; a distinct identifier verification unit which verifies whether or not the first-authenticated computer device and the second-authentication attempt computer device are identical with each other using the distinct identifier of the first-authenticated computer device and the distinct identifier of the second-authentication attempt computer device; an authentication key issue unit which issues and transmits a disposable authentication key to the mobile communication terminal through the transmission and reception processing unit; and an authentication key verification unit which verifies whether or not the disposable authentication key issued by the authentication key issue unit and the disposable authentication key inputted to the transmission and reception processing unit are identical with each other.

(57) 요약서:

[다음 쪽 계속]

WO 2012/121497 A2

공개:

— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

이 발명에 따른 고유식별자 기반 인증시스템은, 2 차 인증에 필요한 종단실체 정보와 상기 종단실체 정보와 매칭되는 이동통신단말기를 등록하는 장치등록부와; 온라인 서비스 시스템과 통신하여 상기 종단실체 정보로 1 차 인증된 컴퓨터장치의 고유식별자와 상기 종단실체 정보로 2 차 인증을 시도하는 2 차 인증 시도 컴퓨터장치의 고유식별자와 상기 2 차 인증 시도 컴퓨터장치로부터 입력되는 일회용 인증키를 수신하는 송수신처리부와; 상기 1 차 인증된 컴퓨터장치의 고유식별자와 상기 2 차 인증 시도 컴퓨터장치의 고유식별자를 이용하여 상기 1 차 인증된 컴퓨터장치와 상기 2 차 인증 시도 컴퓨터장치의 동일 여부를 검증하는 고유식별자검증부와; 상기 이동통신단말기에 일회용 인증키를 발급하여 상기 송수신처리부를 통해 송신하는 인증키 발급부와; 상기 인증키 발급부에서 발급한 일회용 인증키와 상기 송수신처리부로 입력된 일회용 인증키의 동일 여부를 검증하는 인증키 검증부를 포함한다.

명세서

발명의 명칭: 고유식별자 기반 인증시스템 및 방법

기술분야

[1] 이 발명은 인증시스템 및 방법에 관한 것으로서, 보다 상세하게는 1차 인증된 컴퓨터장치의 고유식별자와 2차 인증을 시도하는 컴퓨터장치의 고유식별자를 비교한 후 사용자 인증이 이루어지도록 하는 고유식별자 기반 인증시스템 및 방법에 관한 것이다.

배경기술

[2] 오늘날 인터넷의 발달에 힘입어 다양한 종류의 온라인 서비스가 제공되고 있다. 대부분의 온라인 서비스 시스템들은 인터넷을 통해 해당 시스템에 접근하는 클라이언트 컴퓨터장치가 해당 온라인 서비스를 이용할 자격을 가지는지 여부를 인증하고 있다.

[3] 가장 보편적으로 사용되는 사용자 인증방법은 사용자 아이디와 비밀번호를 이용한 인증방법으로서, 사용자가 온라인 서비스 시스템에 회원으로 가입할 때 사용자 아이디와 비밀번호를 등록하고, 추후 해당 사용자가 해당 시스템에 접속하고자 할 때 기등록한 사용자 아이디와 비밀번호를 입력받아 그 사용자의 본인 여부를 검증한다.

[4] 그러나, 이러한 아이디와 비밀번호를 이용한 인증방법은 인증 정보(사용자 아이디와 비밀번호)가 도용되거나 해킹되기 쉬우며, 인증 정보가 노출될 경우 악의적인 접근 시도를 차단할 수 없는 문제점이 있다.

[5] 온라인 서비스 시스템에는 다양한 개인 정보들이 관리되고 있고, 최근 온라인 서비스 시스템을 통한 무형의 자산(예컨대, 온라인 게임에서의 아이템, 사이버 머니 등)이 증가함에 따라, 보다 강력한 본인 인증방법들이 요구되고 있다.

[6] 이러한 요구에 따라 상술한 사용자 아이디와 비밀번호에 의한 1차 인증 후의 다양한 2차 인증방식들이 시도되고 있는데, 특히 사용자의 이동통신단말기를 이용한 일회용 인증키 기반 2차 인증방식이 널리 사용되고 있다. 이 일회용 인증키 기반 인증방식은 통상 다음과 같은 절차로 진행된다. 먼저, 온라인 서비스 시스템은 1차 인증 절차(예컨대, 사용자 아이디와 비밀번호 확인)를 진행하고, 1차 인증 후, 2차인증서버에게 2차 인증을 요청한다. 2차인증서버는 사용자의 이동통신단말기에 일회용 인증키가 포함된 문자메시지(SMS)를 발송한다. 온라인 서비스 시스템은 사용자의 컴퓨터장치를 통해 그 일회용 인증키를 입력받아 2차인증서버에게 전달한다. 그러면 2차인증서버는 사용자의 이동통신단말기에 발송한 일회용 인증키와 온라인 서비스 시스템을 통해 입력받은 일회용 인증키가 동일한 지를 검증한다.

[7] 이러한 일회용 인증키 기반 2차인증방식은 본인 인증 보안 강도를 어느 정도 강화시킬 수는 있으나, 아래와 같은 원거리 해킹이나 근거리 해킹에 의한

취약점이 여전히 존재한다.

[8] 즉, 원거리 해킹 기법으로서, 사용자가 일회용 인증키를 온라인 서비스 시스템으로 전송할 때 해커가 네트워크 스푸핑을 통해 일회용 인증키를 가로채거나, 해커가 사용자의 컴퓨터장치에 미리 키로거를 설치하고 원격에서 사용자의 컴퓨터장치에 입력되는 일회용 인증키를 모니터링하여 빼내거나, 사용자가 온라인 서비스 시스템이 아닌 피싱사이트에 접속하도록 유도하여 피싱사이트로 입력되는 일회용 인증키를 갈취하는 방법 등을 통해 인증키가 갈취될 수 있다. 예로서, 2006년 7월 미국의 한 은행에서 원거리 해킹 기법인 피싱사이트를 통해 갈취한 인증키로 은행 계좌에 침투한 사례가 있다.

[9] 또한, 근거리 해킹 기법으로서, 사용자 근처에서 숄더서핑(shoulder surfing)이나 사회공학(social engineering) 등의 기법을 통해 사용자의 이동통신단말기에 전송된 일회용 인증키를 알아내어 도용하기도 한다.

[10] 따라서, 일회용 인증키를 이용한 2차 인증방식으로서, 원거리 해킹 기법이나 근거리 해킹 기법 등에 의해 해커에게 일회용 인증키가 갈취되더라도, 이에 저항할 수 있는 보다 강력한 본인 인증기술이 필요하다.

발명의 상세한 설명

기술적 과제

[11] 상술한 종래기술의 문제점을 해결하기 위하여 안출된 이 발명의 목적은, 1차인증이 완료된 컴퓨터장치의 고유식별자와 2차 인증을 시도하는 컴퓨터장치의 고유식별자를 비교하여 사용자 인증을 함으로써, 원거리 해킹 기법 또는 근거리 해킹 기법을 통한 일회용 인증키 갈취에 저항할 수 있는 고유식별자 기반 인증시스템 및 방법을 제공하기 위한 것이다.

과제 해결 수단

[12] 상기한 목적을 달성하기 위한 이 발명에 따른 고유식별자 기반 인증시스템은, 2차 인증에 필요한 종단실체 정보와 상기 종단실체 정보와 매칭되는 이동통신단말기를 등록하는 장치등록부와; 온라인 서비스 시스템과 통신하여 상기 종단실체 정보로 1차 인증된 컴퓨터장치의 고유식별자와 상기 종단실체 정보로 2차 인증을 시도하는 2차 인증 시도 컴퓨터장치의 고유식별자와 상기 2차 인증 시도 컴퓨터장치로부터 입력되는 일회용 인증키를 수신하는 송수신처리부와; 상기 1차 인증된 컴퓨터장치의 고유식별자와 상기 2차 인증 시도 컴퓨터장치의 고유식별자를 이용하여 상기 1차 인증된 컴퓨터장치와 상기 2차 인증 시도 컴퓨터장치의 동일 여부를 검증하는 고유식별자검증부와; 상기 이동통신단말기에 일회용 인증키를 발급하여 상기 송수신처리부를 통해 송신하는 인증키 발급부와; 상기 인증키 발급부에서 발급한 일회용 인증키와 상기 송수신처리부로 입력된 일회용 인증키의 동일 여부를 검증하는 인증키 검증부를 포함한 것을 특징으로 한다.

[13]

[14] 또한, 이 발명에 따른 고유식별자 기반 인증방법은, 2차 인증 시스템이 2차 인증에 필요한 종단실체 정보와 상기 종단실체 정보와 매칭되는 이동통신단말기를 등록하는 장치등록단계와; 온라인 서비스 시스템과 통신하여 상기 종단실체 정보로 1차 인증된 컴퓨터장치의 고유식별자와 2차 인증 요청이 수신되면, 상기 2차 인증 시스템이 상기 이동통신단말기에 일회용 인증키를 발급하는 인증키 발급단계와; 상기 2차 인증 시스템이 상기 온라인 서비스 시스템과 통신하여 상기 종단실체 정보로 2차 인증을 시도하는 2차 인증 시도 컴퓨터장치의 고유식별자와 상기 2차 인증 시도 컴퓨터장치로부터 입력되는 일회용 인증키를 수신하는 2차 인증 시도단계와; 상기 2차 인증 시스템이 상기 1차 인증된 컴퓨터장치의 고유식별자와 상기 2차 인증 시도 컴퓨터장치의 고유식별자를 이용하여 상기 1차 인증된 컴퓨터장치와 상기 2차 인증 시도 컴퓨터장치의 동일 여부를 검증하는 고유식별자 검증단계와; 상기 2차 인증 시스템이 상기 인증키 발급단계에서 발급한 일회용 인증키와 상기 2차 인증 시도단계에서 입력된 일회용 인증키의 동일 여부를 검증하는 인증키 검증단계를 포함한 것을 특징으로 한다.

[15]

[16] 또한, 이 발명에 따른 고유식별자 기반 인증방법은, 이동통신단말기가 보안인증모듈을 설치하는 제1단계와; 상기 이동통신단말기가 2차 인증 시스템에 접속하여 2차 인증에 필요한 종단실체 정보와 상기 이동통신단말기의 시스템 정보를 전송하는 제2단계와; 상기 이동통신단말기가 푸시서버에 접속하여 상기 보안인증모듈의 인증서와 상기 이동통신단말기의 고유정보를 전송하며 장치토큰 발급을 요청하는 제3단계와; 상기 이동통신단말기가 상기 푸시서버로부터 상기 장치토큰이 발급되면 상기 발급된 장치토큰을 상기 2차 인증 시스템에게 전달하는 제4단계와; 상기 푸시서버로부터 푸시메시지가 입력되면, 상기 이동통신단말기가 상기 2차 인증 시스템과 통신하여 상기 2차 인증 시스템으로부터 일회용 인증키를 수신하여 화면에 출력하는 제5단계를 포함한 것을 특징으로 한다.

[17]

[18] 또한, 이 발명에 따른 고유식별자 기반 인증방법은, 사용자로부터 1차 인증을 위한 종단실체 정보가 입력되면, 컴퓨터장치는 상기 컴퓨터장치의 고유식별자를 생성하는 제1단계와; 상기 컴퓨터장치가 상기 제1단계에서 생성된 상기 컴퓨터장치의 고유식별자와 상기 1차 인증을 위한 종단실체 정보를 온라인 서비스 시스템에게 전송하는 제2단계와; 사용자로부터 2차 인증을 위한 일회용 인증키가 입력되면, 상기 컴퓨터장치가 상기 컴퓨터장치의 고유식별자를 생성하는 제3단계와; 상기 컴퓨터장치가 상기 제3단계에서 생성된 상기 컴퓨터장치의 고유식별자와 상기 2차 인증을 위한 일회용 인증키를 상기 온라인 서비스 시스템에게 전송하는 제4단계를 포함한 것을 특징으로 한다.

발명의 효과

[19] 이상과 같이 이 발명에 따르면, 1차 인증이 완료된 컴퓨터장치의 고유식별자와 2차 인증을 시도하는 컴퓨터장치의 고유식별자가 동일한 경우에만 사용자 인증을 하기 때문에, 인증 보안이 더욱 강화되는 효과가 있다.

도면의 간단한 설명

[20] 도 1은 이 발명에 따른 고유식별자 기반 인증시스템의 개략적인 구성 블록도이다.

[21] 도 2는 이 발명에 따른 고유식별자 기반 인증시스템의 상세 구성 블록도이다.

[22] 도 3은 이 발명의 한 실시예에 따른 이동통신단말기의 동작을 도시한 동작 흐름도이다.

[23] 도 4는 이 발명에 따른 컴퓨터장치의 보안인증모듈이 컴퓨터장치의 고유식별자를 수집하는 동작을 도시한 동작 흐름도이다.

[24] 도 5는 이 발명에 따른 2차 인증 시스템의 동작을 도시한 동작 흐름도이다.

[25] 도 6은 이 발명에 따른 2차 인증 시스템이 종단실체에 일회용 인증키를 갱신 발급하는 과정을 도시한 동작 흐름도이다.

[26] [부호의 설명]

[27] 110 : 종단실체 111 : 컴퓨터장치

[28] 112 : 이동통신단말기 120 : 온라인 서비스 시스템

[29] 130 : 푸시서버 140 : 2차 인증 시스템

[30] 141 : 송수신처리부 142 : 암복호화 처리부

[31] 143 : 장치등록부 144 : 일회용인증처리부

[32] 145 : 데이터베이스 146 : 메모리부

발명의 실시를 위한 최선의 형태

[33] 이하, 첨부된 도면을 참조하여 이 발명에 따른 고유식별자 기반 인증시스템 및 방법을 보다 상세하게 설명한다.

[34] 최근 온라인 서비스 시스템이 아이디와 비밀번호를 기반으로 한 1차 인증과, 일회용 인증키를 기반으로 한 2차 인증을 모두 통과한 사용자에게 온라인 서비스를 제공함에 따라, 타인의 온라인 서비스 아이디를 도용하는 해킹 방법도 진화하고 있다.

[35] 이러한 온라인 서비스 아이디 도용 해킹은 여러 대의 컴퓨터장치가 설치된 피씨방에서 이루어지는 경우가 많은데, 해커는 정상 사용자가 사용할 컴퓨터장치(이하, 해킹 대상 컴퓨터장치라 함)에 스파이웨어나 키로거 등의 해킹 프로그램을 설치한 후, 근방의 컴퓨터장치(이하, 해킹 컴퓨터장치라 함)에서 그 해킹 대상 컴퓨터장치를 해킹한다.

[36] 이때, 정상 사용자가 해킹 프로그램이 설치된 해킹 대상 컴퓨터장치를 이용하여 온라인 서비스 시스템에 아이디와 비밀번호를 입력하여 1차 인증하고, 자신의 이동통신단말기로 일회용 인증키를 수신받아 2차 인증을 시도하면,

해커는 해킹 컴퓨터장치를 통해 이 모든 과정에서 입력되는 정보를 갈취할 수 있다. 정상 사용자가 해킹 대상 컴퓨터장치에 아이디와 비밀번호를 입력하여 1차 인증을 완료하면, 해커는 해킹 컴퓨터장치로도 해당 아이디와 비밀번호를 입력하여 1차 인증을 완료하고(아이디와 비밀번호를 이용한 중복 로그인이 가능함), 정상 사용자가 해킹 대상 컴퓨터장치에 2차 인증을 위한 일회용 인증키를 입력하면 해커도 그 일회용 인증키를 갈취하여 해킹 컴퓨터장치에 입력한다.

[37] 그러나, 정상 사용자가 해킹 대상 컴퓨터장치를 통해 입력한 일회용 인증키는 온라인 서비스 시스템에 전달되는 과정에서 차단되고, 대신 해커가 해킹 컴퓨터장치를 통해 입력한 일회용 인증키가 온라인 서비스 시스템에 전달된다. 이로써 정상 사용자가 사용중인 해킹 대상 컴퓨터장치는 온라인 서비스 시스템에 접속되지 못하고, 해커가 사용중인 해킹 컴퓨터장치가 온라인 서비스 시스템에 접속되는 불상사가 발생한다. 즉, 1차 인증은 해킹 대상 컴퓨터장치에서 이루어지지만, 2차 인증은 해킹 컴퓨터장치에서 이루어지고 결국 해킹 컴퓨터장치가 온라인 서비스 시스템에 접속된다. 이 발명은 이러한 상황에서 보다 강력한 본인 인증을 수행하는 방법을 제안한다.

발명의 실시를 위한 형태

[38] 도 1은 이 발명에 따른 고유식별자 기반 인증시스템의 개략적인 구성 블록도이다.

[39] 종단실체(110)는 이 발명을 통한 인증 절차를 이용하는 최종 사용자이다. 이 종단실체(110)는 통신망(100)을 통해 온라인 서비스 시스템(120)에서 온라인 서비스를 제공받기 위해 이 발명에 따른 인증 절차를 이용한다. 종단실체(110)는 온라인 서비스 시스템(120)의 온라인 서비스를 제공받고 온라인 서비스 시스템(120)과의 통신을 통해 이 발명에 따른 1차 인증과 2차 인증을 수행하는 컴퓨터장치(111)와, 2차 인증을 수행하기 위한 이동통신단말기(112)를 포함한다.

[40] 컴퓨터장치(111)는 데스크탑, 노트북과 같은 다양한 컴퓨터 환경을 포함한다. 컴퓨터장치(111)는 이 발명에 따른 보안인증모듈을 포함하는데, 이 보안인증모듈은 1차 인증을 수행하는 과정과 2차 인증을 수행하는 과정에서 각각 해당 컴퓨터장치(111)의 고유식별자를 추출하여, 온라인 서비스 시스템(120)에게 전송한다.

[41] 이동통신단말기(112)는 일반 피처폰(feature phone) 또는 운영체제(OS)를 탑재하고 다양한 어플리케이션(응용프로그램)의 설치 및 구동이 가능한 스마트폰을 포함한다. 이 발명을 구현하기 위한 컴퓨터장치(111)와 이동통신단말기(112)의 내부 상세 구성과, 컴퓨터장치(111)의 보안인증모듈이 컴퓨터장치의 고유식별자를 추출하는 과정은 후술하기로 한다.

[42] 온라인 서비스 시스템(120)은 통신망(100)을 통해 다수의 사용자들에게 온라인 서비스를 제공하는 웹 상의 시스템으로서, 종단실체(110)에 대한 1차 인증을

수행한다. 통상적으로 온라인 서비스 시스템(120)은 로그인 처리 시스템(121)을 구비하고, 이 로그인 처리 시스템(121)에서 종단실체(110)에 대한 1차 인증을 수행한다. 1차 인증은 지식기반인증, 소유기반인증, 존재(신체)기반인증 등의 모든 단일요소인증(Single Factor Authentication) 형태를 포함한다. 온라인 서비스 시스템(120)은 1차 인증된 컴퓨터장치(111)의 고유식별자를 2차 인증 시스템(140)에게 전달하며 1차 인증된 종단실체에 대해 2차 인증을 요청한다. 그리고, 온라인 서비스 시스템(120)은 컴퓨터장치(111)로부터 2차 인증을 위해 입력되는 일회용 인증키와 그 컴퓨터장치(111)의 고유식별자를 2차 인증 시스템(140)에게 전달한다.

[43] 2차 인증 시스템(140)은 1차 인증이 수행된 임의의 컴퓨터장치에 대해 온라인 서비스 시스템(120)으로부터 2차 인증이 요청되면, 1차 인증된 컴퓨터장치의 고유식별자를 입력받고, 1차 인증된 종단실체의 이동통신단말기(112)에게 일회용 인증키를 발급한다. 그리고, 이 2차 인증 시스템(140)은 온라인 서비스 시스템(120)을 통해 일회용 인증키 및 일회용 인증키가 입력된(2차 인증 시도) 컴퓨터장치의 고유식별자를 입력받는다. 2차 인증 시스템(140)은 1차 인증된 컴퓨터장치의 고유식별자와 2차 인증 시도 컴퓨터장치의 고유식별자를 이용하여 1차 인증된 컴퓨터장치와 2차 인증 시도 컴퓨터장치가 동일한지를 검증하고, 종단실체(110)의 이동통신단말기(112)에게 발급한 일회용 인증키와 일회용 인증키 입력 컴퓨터장치를 통해 입력된 일회용 인증키가 동일한지를 검증하며, 그 검증결과를 온라인 서비스 시스템에게 통보한다.

[44] 이동통신단말기가 일반 피쳐폰이거나 푸시서비스를 위한 장치토큰이 등록되지 않은 스마트폰인 경우, 2차 인증 시스템(140)은 에스엠에스(SMS) 서버를 통해 해당 이동통신단말기에게 일회용 인증키를 발급한다. 한편, 이동통신단말기가 푸시서비스를 위한 장치토큰이 등록된 스마트폰인 경우, 2차 인증 시스템(140)은 푸시서버(130)를 이용하여 해당 이동통신단말기에게 일회용 인증키를 발급한다. 2차 인증 시스템(140)이 에스엠에스 서버를 통해 이동통신단말기에게 일회용 인증키를 발급하는 과정은 통상적인 절차이므로, 상세한 설명은 생략한다. 이 명세서에서는 2차 인증 시스템(140)이 푸시서버를 이용하여 이동통신단말기에게 일회용 인증키를 발급하는 과정에 대해 상세하게 설명한다.

[45] 푸시(PUSH)서버는 종단실체의 이동통신단말기의 제조업체에서 제공하는 서비스로서, 이동통신단말기는 임의의 어플리케이션에 대해 푸시서비스를 제공받고자 할 경우, 먼저 푸시서버로부터 해당 어플리케이션에 대응하는 장치토큰을 발급받는다. 그러면, 푸시서버는 이동통신단말기에 푸시메시지를 전송하여 이동통신단말기를 깨우고(wakeup), 해당 토큰장치에 대응되는 어플리케이션(이 발명의 이동통신단말기의 보안인증모듈)을 활성화시키는 역할을 수행한다.

[46] 즉, 2차 인증 시스템(140)이 종단실체(110)의 이동통신단말기(111)에게 일회용

인증키를 발급하고자 할 때, 2차 인증 시스템(140)의 이동통신단말기(111)의 장치토큰을 푸시(PUSH)서버(130)에게 전달하고, 그러면 푸시(PUSH)서버(130)는 이동통신단말기(111)에게 푸시메시지를 출력하여 이동통신단말기(111)가 깨어나서 2차 인증 시스템(140)과 통신하도록 한다.

[47] 이동통신단말기가 푸시(PUSH)서버로부터 장치토큰을 발급받는 것에 대한 상세한 설명은 후술하기로 한다. 푸시서버의 예로서, iOS계열은 애플에서 제공하는 APNs(Apple Push Notification Service)를 푸시서버로 사용하고, 안드로이드 계열은 구글에서 제공하는 C2DM(Cloud To Device Messaging)를 푸시서버로 사용한다.

[48] 컴퓨터장치에 설치된 보안인증모듈은 각 컴퓨터장치마다 유일한 고유식별자를 추출한다. 이때, 고유식별자는 오픈 소프트웨어 파운데이션(Open Software Foundation, OSF)에서 표준으로 지정한 범용고유식별자(Universally Unique Identifier, UUID) 또는 전역고유식별자(Globally unique identifier, GUID)를 기반으로 생성됨으로써, 컴퓨터장치의 고유식별자에 대한 유일성을 제공한다.

[49] 도 2는 이 발명에 따른 고유식별자 기반 인증시스템의 상세 구성 블록도이다.

[50] 이 발명에 따른 종단실체(110)의 컴퓨터장치(111)는 입출력부(111A)와, 송수신부(111B)와, 보안인증모듈(111C)을 포함한다. 입출력부(111A)는 통상적인 키보드, 마우스, 모니터 등으로서, 사용자와의 인터페이스를 수행한다. 송수신부(111B)는 유선 통신망을 통해 온라인 서비스 시스템(120)과 접속한다. 보안인증모듈(111C)는 컴퓨터장치(111)에 설치되어 동작하는 소프트웨어로서, 컴퓨터장치의 고유식별자를 수집하는 고유식별자수집부와 수집된 고유식별자를 암호화하여 송수신부(111B)를 통해 출력하는 암호화처리부를 포함한다. 고유식별자수집부는 오픈 소프트웨어 파운데이션(Open Software Foundation, OSF)에서 표준으로 지정한 범용고유식별자(Universally Unique Identifier, UUID) 또는 전역고유식별자(Globally unique identifier, GUID)를 기반으로 해당 컴퓨터장치의 고유식별자를 생성한다.

[51] 이 발명에 따른 종단실체(110)의 이동통신단말기(112)는 입출력부(112A)와, 송수신부(112B)와, 보안인증모듈(112C)을 포함한다. 입출력부(112A)는 통상적인 터치패드 등으로서, 사용자와의 인터페이스를 수행한다. 송수신부(112B)는 이동 통신망을 통해 이 발명에 따른 2차 인증 시스템(140) 및 푸시서버(130)와 통신한다. 보안인증모듈(112C)는 푸시서버(130)로부터 해당 보안인증모듈(112C)에 대응하는 장치토큰을 발급받고, 그 발급된 장치토큰을 2차 인증 시스템(140)에 등록하며, 푸시서버(130)로부터 푸시메시지가 전달된 후 2차 인증 시스템(140)으로부터 일회용 인증키가 수신되면, 그 수신된 일회용 인증키를 입출력부(112A)의 화면에 출력한다.

[52] 이 발명에 따른 온라인 서비스 시스템(120)은 종단실체(110)의 1차 인증에 필요한 정보를 저장하고, 1차 인증이 완료된 종단실체(110)에 대해 2차 인증 시스템(140)에게 2차 인증을 요청하고, 2차 인증 시스템(140)으로부터 그 결과를

입력받는다. 즉, 온라인 서비스 시스템(120)은 종단실체(110)를 1차 인증하고, 해당 종단실체(110)로부터 2차 인증을 위한 일회용 인증키를 입력받아 2차 인증 시스템(140)에게 전달한다. 아울러, 온라인 서비스 시스템(120)은 종단실체의 1차 인증된 컴퓨터장치의 고유식별자와 2차 인증 시도 컴퓨터장치의 고유식별자를 2차 인증 시스템(140)에게 전달한다.

[53] 이 발명에 따른 2차 인증 시스템(140)은 종단실체(110)와 온라인 서비스 시스템(120)과 푸시서버(130)와의 데이터 송수신을 위한 송수신처리부(141)와, 송수신되는 데이터를 암호화 또는 복호화하는 암복호화 처리부(142)와, 종단실체(110) 정보와 이동통신단말기(112)의 정보(예컨대, 전화번호, 장치토큰 발급 여부, 장치토큰 정보)를 매칭하여 등록하는 장치등록부(143)와, 1차 인증된 종단실체의 기등록된 이동통신단말기에 일회용 인증키를 생성하고 발급하여 2차 인증하고 동일 종단실체에 대해 1차 인증된 컴퓨터장치의 고유식별자와 2차 인증 시도 컴퓨터장치의 고유식별자를 비교하여 1차 인증된 컴퓨터장치와 2차 인증 시도 컴퓨터장치의 동일 여부를 검증하는 일회용 인증 처리부(144)와, 종단실체 정보와 장치토큰 정보와 각 종단실체별 설정 사항을 저장하는 데이터베이스(145)와, 일회용 인증 처리부(144)에서 발급된 일회용 인증키와 1차 인증된 컴퓨터장치의 고유식별자와 처리절차 정보 등을 저장한 메모리부(146)를 포함한다.

[54] 여기서, 송수신처리부(141)는 유선 통신망을 통해 온라인 서비스 시스템(120)와 푸시서버(130) 및 도시되지 않은 에스엠에스(SMS)서버와 통신하는 유선처리부와, 무선 통신망을 통해 이동통신단말기(110)와 통신하는 무선처리부를 포함한다. 장치등록부(143)는 각 이동통신단말기에 대해 장치 등록을 처리하는 장치등록처리부와, 등록된 이동통신단말기에 대해 번호를 발급하는 장치번호발급기를 포함한다. 일회용 인증 처리부(144)는 1차 인증 완료된 컴퓨터장치의 고유식별자를 메모리부에 저장해놓고 2차 인증을 시도하는 컴퓨터장치의 고유식별자를 검증하는 고유식별자검증부와, 일회용 인증키를 생성하는 인증키 생성부와, 1차 인증 완료된 종단실체에 매칭된 이동통신단말기에게 상기 일회용 인증키를 발급하는 인증키 발급부와, 2차 인증 시도 컴퓨터장치에 입력된 일회용 인증키를 온라인 서비스 시스템을 통해 입력받아 상기 발급된 일회용 인증키와 입력된 일회용 인증키를 비교하여 검증하는 인증키 검증부를 포함한다.

[55] 여기서, 인증키 생성부는 1차 인증 완료된 컴퓨터장치의 고유식별자를 기반으로 일회용 인증키를 생성할 수 있다.

[56] 일회용 인증키는 1차 인증된 종단실체에 대해 2차 인증이 요청되면, 인증키 생성부에서 생성되고, 인증키 발급부에서 활성되며, 인증키 검증부에서 검증된 후 소멸된다. 종래에는 2차 인증이 요청되어 일회용 인증키가 생성되고 정상적으로 소멸되기 전에라도 2차 인증이 다시 요청되면 새로운 일회용 인증키가 중복 발급되었다. 그러나, 이럴 경우 악의적인 목적을 가진 해커가

정당한 종단실체의 보안인증 절차에 개입하여 정당한 종단실체가 2차 인증을 통과하지 못하도록 방해하는 등의 문제가 발생할 수 있다. 이러한 이유로 말미암아 이 발명은 원칙적으로는 일회용 인증 처리부(144)가 일회용 인증키가 생성, 활성, 소멸까지 순차적으로 진행되도록 하고, 동일한 종단실체에 대해 일회용 인증키가 중복 발급되지 않도록 한다. 한편, 특정 이유에 의해 정당한 종단실체의 일회용 인증키가 갱신되어야 할 경우, 초기 일회용 인증키 발급을 요청한 종단실체 컴퓨터장치와 인증키 갱신을 요청한 종단실체 컴퓨터장치를 비교하여 동일할 경우 기발급된 일회용 인증키를 폐기하고 새로운 일회용 인증키를 생성 및 활성화할 수 있다.

[57]

[58] 도 3은 이 발명의 한 실시예에 따른 이동통신단말기의 동작을 도시한 동작 흐름도이다.

[59] 이동통신단말기(112)의 보안인증모듈(112C)은 이동통신단말기(112)에 탑재된 운영체제를 기반으로 제작되어, 이 발명에 따른 인증 절차를 수행하는 응용프로그램(어플리케이션)이다. 도 3은 이동통신단말기가 푸시서버로부터 장치토큰을 발급받고, 이 장치토큰을 이용하여 일회용 인증키를 수신하기 위해 필요한 절차이다.

[60] 먼저, 종단실체의 이동통신단말기에 보안인증모듈(112C)을 설치한다(S301). 이 보안인증모듈(112C)은 인증 수행을 위한 종단실체 정보(온라인 서비스 시스템에 접속하기 위한 사용자 아이디, 이동통신단말기의 시스템 정보 등)를 2차 인증 시스템에게 전송하고 이로써 2차 인증 시스템은 이동통신단말기를 통해 종단실체 정보를 수집한다(S302).

[61] 다음, 2차 인증 시스템은 수집된 종단실체 정보를 확인하고, 이동통신단말기 자체에 대한 실명인증 및 본인인증을 수행하고, 그 결과를 이동통신단말기에게 전송하는데, 2차 인증 시스템으로부터 실명인증 및 본인인증 실패 결과가 수신되면(S303), 장치 등록 실패로 인식하고 종료한다(S304).

[62] 한편, 2차 인증 시스템으로부터 이동통신단말기에 대한 실명인증 및 본인인증 성공 결과가 수신되면(S303), 이동통신단말기의 보안인증모듈은 푸시서버에 접속하여 보안인증모듈의 인증서와 이동통신단말기 고유정보를 푸시서버에게 전송하면서 장치토큰 발급을 요청한다(S305).

[63] 푸시서버로부터 장치토큰이 발급되면(S306), 이동통신단말기의 보안인증모듈은 그 발급된 장치토큰을 2차 인증 시스템에게 전달한다(S307). 그러면 2차 인증 시스템은 해당 종단실체 정보와 함께 이동통신단말기의 장치토큰을 데이터베이스에 등록한다.

[64] 이 후, 푸시서버로부터 푸시메시지가 수신되면(S308), 이동통신단말기의 보안인증모듈이 활성화되어 2차 인증 시스템과 통신한다(S309). 다음, 2차 인증 시스템으로부터 일회용 인증키가 수신되면(S310), 그 일회용 인증키를 입출력부의 화면에 출력한다(S311).

[65]

[66] 도 4는 이 발명에 따른 컴퓨터장치의 보안인증모듈이 컴퓨터장치의 고유식별자를 수집하는 동작을 도시한 동작 흐름도이다. 이 발명에 따른 컴퓨터장치의 보안인증모듈은 온라인 서비스 시스템에 접속하는 컴퓨터장치에 설치되어 구동하는 응용프로그램이다.

[67] 컴퓨터장치의 고유식별자는 오픈 소프트웨어 파운데이션(Open Software Foundation, OSF)에서 표준으로 지정한 범용고유식별자(UUID) 혹은 전역고유식별자(GUID)를 기반으로 생성된다. 범용고유식별자의 목적은 분산시스템에서 각 컴퓨터장치를 유일하게 식별하기 위한 것이다. 따라서 어떠한 개체(컴퓨터장치)의 식별을 위해 생성된 범용고유식별자는 다른 개체(컴퓨터장치)의 식별을 위해 생성된 범용고유식별자와 동일한 경우가 거의 없다. 물론 아주 드문 확률로 동일한 경우가 있을 수는 있으나, 1차 인증된 컴퓨터장치의 UUID와 2차 인증을 시도하는 해커 컴퓨터장치의 UUID가 동일한 경우는 거의 불가능하기 때문에 UUID 기반의 고유식별자의 유일성은 신뢰할 수 있다. 본 발명에서는 이 UUID를 본 발명의 목적에 맞추어 응용하여 사용한다.

[68] 이 발명에서 사용되는 컴퓨터장치의 고유식별자의 구성요소는 고유식별자의 재사용 공격에 대응하기 위해 고유식별자의 일회성을 제공하는 타임스탬프, 온라인서비스 시스템의 식별을 제공하는 서비스 파일의 정보, 해당 컴퓨터장치의 고유정보로 이루어진다. 이 컴퓨터장치의 고유정보는 UUID를 포함하고, 추가적으로 컴퓨터장치의 시스템 하드웨어의 고유정보를 포함할 수 있다.

[69] 종단실체 컴퓨터장치의 보안인증모듈에 고유식별자 수집요청이 발생하면, 고유식별자수집부는 협정세계시(Universal Time Clock, UTC) 기반의 타임스탬프를 생성하고(S401), 온라인 서비스 시스템에서 제공하는 서비스 파일의 정보를 수집한다(S402). 서비스 파일의 정보는 기본적인 파일 정보 외에 파일의 메시지 다이제스트와 같이 가공되어 생성된 파일 정보를 포함한다. 온라인 서비스 시스템이 제공하는 서비스 파일의 정보 수집이 끝나면, 종단실체 컴퓨터장치의 고유정보를 수집한다(S403).

[70] 이 수집된 컴퓨터장치의 고유정보는 종단실체의 정보 제공 동의 여부에 따라 재가공될 수 있다. 종단실체가 수집된 컴퓨터장치의 고유정보를 2차 인증 시스템에 전달하는 것을 동의하면(S404), 단계 S401에서 연산한 타임스탬프와, 단계 S402에서 수집한 온라인 서비스 시스템의 서비스 파일 정보와, 단계 S403에서 수집한 종단실체 컴퓨터장치의 고유정보를 병합하여 고유식별자를 생성하고(S405), 생성한 고유식별자를 대칭키 암호화 알고리즘으로 암호화한다(S406). 상기 대칭키 암호화 알고리즘의 암호화 키는 다양한 키공유 알고리즘을 통해 2차 인증 시스템과 공유하며, 암호화된 고유식별자는 온라인 서비스 시스템을 경유하여 2차 인증 시스템으로 전송된다(S407).

[71] 단계 404에서, 만약 종단실체가 수집된 컴퓨터장치의 고유정보를 2차 인증

시스템에 제공하기를 원치 않는다면, 단계 S403에서 수집된 컴퓨터장치의 고유정보를 단일 방향 암호화 알고리즘인 해시(HASH)값을 산출하고(S408), 수집된 컴퓨터장치의 고유정보를 그 산출된 해시값으로 대처하여 단계 S405에 제공한다(S409).

[72]

[73] 도 5는 이 발명에 따른 2차 인증 시스템의 동작을 도시한 동작 흐름도이다.

[74] 종단실체 컴퓨터장치가 온라인 서비스 시스템에 접근하면, 온라인 서비스 시스템은 이 종단실체 컴퓨터장치에 대해 1차 인증을 수행한다. 이때, 컴퓨터장치는 인증에 필요한 종단실체 정보와 도 4를 통해 생성된 컴퓨터장치의 고유식별자를 온라인 서비스 시스템에게 전송한다. 1차 인증에 성공하면, 온라인 서비스 시스템은 종단실체 정보와 1차 인증된 컴퓨터장치의 고유식별자를 2차 인증 시스템에게 전달하며 2차 인증을 요청한다.

[75] 2차 인증 시스템은 온라인 서비스 시스템으로부터 종단실제 정보와 1차 인증된 컴퓨터장치의 고유식별자가 입력되며 2차 인증이 요청되면(S501), 수신된 종단실체 정보에 대응하는 이동통신단말기가 등록되어 있는지를 확인한다(S502). 이동통신단말기가 등록되어 있으면(S503), 일회용 인증키를 생성하고(S504), 생성된 일회용 인증키를 이동통신단말기에게 발급한다(S505).

[76] 이때, 단계 S504의 일회용 인증키는 1차 인증된 컴퓨터장치의 고유식별자를 기반으로 생성할 수 있고, 일회용 인증키의 중복 확률을 낮추기 위해서 1차 인증된 고유식별자외에 시간/랜덤수 등의 다른 요소를 더 기반하여 생성할 수 있다.

[77] 생성된 일회용 인증키는 단계 S505에서, 에스엠에스(SMS) 서버를 통해 일회용 인증키가 포함된 문자메시지 형태로 이동통신단말기에게 발급될 수 있고, 푸시서버에 의해 활성화된 이동통신단말기와 2차 인증 시스템이 서버/클라이언트 통신을 통해 해당 이동통신단말기에게 발급될 수 있다.

[78] 푸시서버를 이용하는 경우, 2차 인증 시스템은 해당 이동통신단말기의 장치토큰과 이동통신단말기와의 통신을 메시지를 푸시서버에게 전달한다. 그러면, 푸시서버는 2차 인증 시스템으로부터 전달받은 장치토큰으로부터 푸시메시지를 전달할 이동통신단말기를 파악하고, 해당 이동통신단말기에 푸시메시지를 전달하여 이동통신단말기와 이 이동통신단말기의 보안인증모듈을 활성화시킨다. 활성화된 보안인증모듈은 2차 인증 시스템과 서버/클라이언트 통신을 수행하며, 2차 인증 시스템은 이 보안인증모듈에게 일회용 인증키를 발급한다.

[79] 생성된 일회용 인증키는 통신망을 통해 정당 종단실체의 이동통신단말기로 전송되어 화면에 출력된다. 이 상태에서 정당한 종단실체 또는 해커가 이동통신단말기에 출력된 일회용 인증키를 2차 인증 시도 컴퓨터장치에 입력하면, 그 2차 인증 시도 컴퓨터장치의 고유식별자가 수집된다(S506).

[80] 단계 S506에서 2차 인증 시도 컴퓨터에 입력된 일회용 인증키와 2차 인증 시도

컴퓨터장치의 고유식별자는 온라인 서비스 시스템을 경유하여 2차 인증 시스템으로 전달된다(S507).

[81] 2차 인증 시스템은 단계 S505에서 발급한 일회용 인증키와 단계 S507에서 수신한 일회용 인증키를 비교하여(S508) 일회용 인증키에 대한 인증을 수행한다. 발급한 일회용 인증키와 수신한 일회용 인증키가 일치하면(S508), 1차 인증된 컴퓨터장치의 고유식별자와 2차 인증 시도 컴퓨터장치의 고유식별자를 비교하여(S509) 2차 인증 시도 컴퓨터장치가 1차 인증된 컴퓨터장치와 동일한지에 대한 검증을 수행한다. 두 컴퓨터장치가 동일하면(S509), 인증 승인으로 처리하고(S510) 그 결과를 온라인 서비스 시스템에게 전송한다(S511).

[82] 한편, 단계 S503에서 등록되지 않은 이동통신단말기이면 미등록 이동통신단말기로 처리하고(S512), 미등록 이동통신단말기임을 온라인 서비스 시스템에 통보한다(S511). 또한, 단계 S508에서 발급한 일회용 인증키와 수신한 일회용 인증키가 일치하지 않거나, 단계 S509에서 두 컴퓨터장치가 일치하지 않으면, 인증 실패 처리하고(S513) 온라인 서비스 시스템에게 그 결과를 통보한다(S511).

[83]

[84] 도 6은 이 발명에 따른 2차 인증 시스템이 종단실체에 일회용 인증키를 갱신 발급하는 과정을 도시한 동작 흐름도이다.

[85] 종단실체는 2차 인증시 발급된 일회용 인증키를 갱신해야 되는 경우가 발생할 수 있다. 예를 들면 통신망의 장애로 인해 2차 인증 시스템에서 발급한 일회용 인증키가 이동통신단말기에 전달되지 않고 소실된 경우 혹은 2차 인증을 시도할 컴퓨터장치의 물리적 결함으로 인해 발급받은 일회용 인증키를 부분적으로 입력할 수 없는 경우 등에는 일회용 인증키를 다른 값으로 갱신해야 한다.

[86] 종단실체로부터 온라인 서비스 시스템을 통해 일회용 인증키 갱신 발급이 요청되면, 2차 인증 시스템은 일회용 인증키 갱신 발급을 요청한 종단실체가 정당한 종단실체인지 혹은 악의적인 목적을 가진 종단실체가 보안인증 절차에 개입하는 것인지를 판단할 필요가 있다. 따라서, 2차 인증 시스템은 일회용 인증키의 갱신 요청과 함께 그 갱신 요청 컴퓨터장치의 고유식별자를 온라인 서비스 시스템을 경유하여 수신받고, 일회용 인증키의 최초 요청 컴퓨터장치와 갱신 요청 컴퓨터장치가 동일한지를 검증한다. 이를 상세하게 설명한다.

[87] 2차 인증 시스템은 갱신 요청 컴퓨터장치로부터 종단실체 정보와 일회용 인증키 갱신 요청 및 고유식별자를 수신받는다(S601). 수신된 종단실체 정보에 매칭되는 이동통신단말기에 기발급된 일회용 인증키가 존재하는 지를 확인한다(S602). 해당 이동통신단말기가 기발급된 일회용 인증키가 존재하면(S603), 상기 일회용 인증키를 기발급한 인증키 발급 컴퓨터장치의 고유식별자와 갱신 요청 컴퓨터장치의 고유식별자를 비교하여, 인증키 발급 컴퓨터장치와 갱신 요청 컴퓨터가 동일한지를 검증한다(S604). 두 컴퓨터장치가 동일하면(S604), 일회용 인증키를 갱신하여 해당 종단실체 정보에 매칭되는

이동통신단말기에게 재발급하고(S605), 온라인 서비스 시스템으로부터 해당 재발급된 일회용 인증키가 수신되기까지 대기한다(S606). 단계 S603에서 기발급된 일회용 인증키가 존재하지 않거나 단계 S604에서 두 컴퓨터장치가 동일하지 않으면 일회용 인증키 갱신 실패로 판단하고 로그를 수집한다(S607).

[88]

청구범위

[청구항 1] 2차 인증에 필요한 종단실체 정보와 상기 종단실체 정보와 매칭되는 이동통신단말기를 등록하는 장치등록부와;
온라인 서비스 시스템과 통신하여 상기 종단실체 정보로 1차 인증된 컴퓨터장치의 고유식별자와 상기 종단실체 정보로 2차 인증을 시도하는 2차 인증 시도 컴퓨터장치의 고유식별자와 상기 2차 인증 시도 컴퓨터장치로부터 입력되는 일회용 인증키를 수신하는 송수신처리부와;
상기 1차 인증된 컴퓨터장치의 고유식별자와 상기 2차 인증 시도 컴퓨터장치의 고유식별자를 이용하여 상기 1차 인증된 컴퓨터장치와 상기 2차 인증 시도 컴퓨터장치의 동일 여부를 검증하는 고유식별자검증부와;
상기 이동통신단말기에 일회용 인증키를 발급하여 상기 송수신처리부를 통해 송신하는 인증키 발급부와;
상기 인증키 발급부에서 발급한 일회용 인증키와 상기 송수신처리부로 입력된 일회용 인증키의 동일 여부를 검증하는 인증키 검증부를 포함한 것을 특징으로 하는 고유식별자 기반 인증시스템.

[청구항 2] 제 1 항에 있어서, 상기 컴퓨터장치의 고유식별자는 범용고유식별자(UUID)를 포함한 것을 특징으로 하는 고유식별자 기반 인증시스템.

[청구항 3] 제 1 항에 있어서, 상기 컴퓨터장치의 고유식별자는 전역고유식별자(GUID)를 포함한 것을 특징으로 하는 고유식별자 기반 인증시스템.

[청구항 4] 제 1 항에 있어서, 상기 컴퓨터장치의 고유식별자는 범용고유식별자(UUID)의 해쉬값을 포함한 것을 특징으로 하는 고유식별자 기반 인증시스템.

[청구항 5] 제 1 항에 있어서, 상기 컴퓨터장치의 고유식별자는 전역고유식별자(GUID)의 해쉬값을 포함한 것을 특징으로 하는 고유식별자 기반 인증시스템.

[청구항 6] 제 2 항 내지 제 5 항 중 어느 한 항에 있어서, 상기 컴퓨터장치의 고유식별자는 타임스탬프를 더 포함한 것을 특징으로 하는 고유식별자 기반 인증시스템.

[청구항 7] 제 2 항 내지 제 5 항 중 어느 한 항에 있어서, 상기 컴퓨터장치의 고유식별자는 상기 온라인 서비스 시스템의 서비스 파일 정보를 더 포함한 것을 특징으로 하는 고유식별자 기반 인증시스템.

[청구항 8] 제 1 항에 있어서, 상기 인증키 발급부에서 발급하는 일회용

인증키는 상기 1차 인증된 컴퓨터장치의 고유식별자로부터 생성되는 것을 특징으로 하는 고유식별자 기반 인증시스템.

[청구항 9] 제 1 항에 있어서, 상기 장치등록부는 상기 종단실체 정보와 매칭되는 이동통신단말기의 장치토큰을 등록하고, 상기 인증키 발급부는 상기 종단실체 정보와 매칭되는 이동통신단말기의 장치토큰을 이용하여 상기 이동통신단말기를 활성화시킨 후 상기 이동통신단말기와 통신하여 상기 이동통신단말기에 일회용 인증키를 발급하는 것을 특징으로 하는 고유식별자 기반 인증시스템.

[청구항 10] 제 1 항에 있어서, 상기 인증키 발급부는 에스엠에스(SMS)서버를 통해 상기 상기 이동통신단말기에 일회용 인증키를 발급하는 것을 특징으로 하는 고유식별자 기반 인증시스템.

[청구항 11] 2차 인증 시스템이 2차 인증에 필요한 종단실체 정보와 상기 종단실체 정보와 매칭되는 이동통신단말기를 등록하는 장치등록단계와;

온라인 서비스 시스템과 통신하여 상기 종단실체 정보로 1차 인증된 컴퓨터장치의 고유식별자와 2차 인증 요청이 수신되면, 상기 2차 인증 시스템이 상기 이동통신단말기에 일회용 인증키를 발급하는 인증키 발급단계와;

상기 2차 인증 시스템이 상기 온라인 서비스 시스템과 통신하여 상기 종단실체 정보로 2차 인증을 시도하는 2차 인증 시도 컴퓨터장치의 고유식별자와 상기 2차 인증 시도 컴퓨터장치로부터 입력되는 일회용 인증키를 수신하는 2차 인증 시도단계와;

상기 2차 인증 시스템이 상기 1차 인증된 컴퓨터장치의 고유식별자와 상기 2차 인증 시도 컴퓨터장치의 고유식별자를 이용하여 상기 1차 인증된 컴퓨터장치와 상기 2차 인증 시도 컴퓨터장치의 동일 여부를 검증하는 고유식별자 검증단계와;

상기 2차 인증 시스템이 상기 인증키 발급단계에서 발급한 일회용 인증키와 상기 2차 인증 시도단계에서 입력된 일회용 인증키의 동일 여부를 검증하는 인증키 검증단계를 포함한 것을 특징으로 하는 고유식별자 기반 인증방법.

[청구항 12] 제 11 항에 있어서, 상기 컴퓨터장치의 고유식별자는 범용고유식별자(UUID)를 포함한 것을 특징으로 하는 고유식별자 기반 인증방법.

[청구항 13] 제 11 항에 있어서, 상기 컴퓨터장치의 고유식별자는 전역고유식별자(GUID)를 포함한 것을 특징으로 하는 고유식별자 기반 인증방법.

[청구항 14] 제 11 항에 있어서, 상기 컴퓨터장치의 고유식별자는 범용고유식별자(UUID)의 해쉬값을 포함한 것을 특징으로 하는 고유식별자 기반 인증방법.

[청구항 15] 제 11 항에 있어서, 상기 컴퓨터장치의 고유식별자는 전역고유식별자(GUID)의 해쉬값을 포함한 것을 특징으로 하는 고유식별자 기반 인증방법.

[청구항 16] 제 12 항 내지 제 15 항 중 어느 한 항에 있어서, 상기 컴퓨터장치의 고유식별자는 타임스탬프를 더 포함한 것을 특징으로 하는 고유식별자 기반 인증방법.

[청구항 17] 제 12 항 내지 제 15 항 중 어느 한 항에 있어서, 상기 컴퓨터장치의 고유식별자는 상기 온라인 서비스 시스템의 서비스 파일 정보를 더 포함한 것을 특징으로 하는 고유식별자 기반 인증방법.

[청구항 18] 제 11 항에 있어서, 상기 인증키 발급단계에서 발급된 일회용 인증키는 상기 1차 인증된 컴퓨터장치의 고유식별자로부터 생성되는 것을 특징으로 하는 고유식별자 기반 인증방법.

[청구항 19] 제 11 항에 있어서, 상기 장치등록단계는 상기 종단실체 정보와 매칭되는 이동통신단말기의 장치토큰을 등록하고, 상기 인증키 발급단계는 상기 종단실체 정보와 매칭되는 이동통신단말기의 장치토큰을 이용하여 상기 이동통신단말기를 활성화시킨 후 상기 이동통신단말기와 통신하여 상기 이동통신단말기에 일회용 인증키를 발급하는 것을 특징으로 하는 고유식별자 기반 인증방법.

[청구항 20] 제 11 항에 있어서, 상기 인증키 발급부는 에스엠에스(SMS)서버를 통해 상기 상기 이동통신단말기에 일회용 인증키를 발급하는 것을 특징으로 하는 고유식별자 기반 인증방법.

[청구항 21] 이동통신단말기가 보안인증모듈을 설치하는 제1단계와,
상기 이동통신단말기가 2차 인증 시스템에 접속하여 2차 인증에 필요한 종단실체 정보와 상기 이동통신단말기의 시스템 정보를 전송하는 제2단계와,
상기 이동통신단말기가 푸시서버에 접속하여 상기 보안인증모듈의 인증서와 상기 이동통신단말기의 고유정보를 전송하며 장치토큰 발급을 요청하는 제3단계와,
상기 이동통신단말기가 상기 푸시서버로부터 상기 장치토큰이 발급되면 상기 발급된 장치토큰을 상기 2차 인증 시스템에게 전달하는 제4단계와,
상기 푸시서버로부터 푸시메시지가 입력되면, 상기 이동통신단말기가 상기 2차 인증 시스템과 통신하여 상기 2차 인증 시스템으로부터 일회용 인증키를 수신하여 화면에 출력하는

제5단계를 포함한 것을 특징으로 하는 고유식별자 기반 인증방법.

[청구항 22] 사용자로부터 1차 인증을 위한 종단실체 정보가 입력되면, 컴퓨터장치는 상기 컴퓨터장치의 고유식별자를 생성하는 제1단계와;
상기 컴퓨터장치가 상기 제1단계에서 생성된 상기 컴퓨터장치의 고유식별자와 상기 1차 인증을 위한 종단실체 정보를 온라인 서비스 시스템에게 전송하는 제2단계와;
사용자로부터 2차 인증을 위한 일회용 인증키가 입력되면, 상기 컴퓨터장치가 상기 컴퓨터장치의 고유식별자를 생성하는 제3단계와;
상기 컴퓨터장치가 상기 제3단계에서 생성된 상기 컴퓨터장치의 고유식별자와 상기 2차 인증을 위한 일회용 인증키를 상기 온라인 서비스 시스템에게 전송하는 제4단계를 포함한 것을 특징으로 하는 고유식별자 기반 인증방법.

[청구항 23] 제 22 항에 있어서, 상기 컴퓨터장치의 고유식별자는 범용고유식별자(UUID)를 포함한 것을 특징으로 하는 고유식별자 기반 인증방법.

[청구항 24] 제 22 항에 있어서, 상기 컴퓨터장치의 고유식별자는 전역고유식별자(GUID)를 포함한 것을 특징으로 하는 고유식별자 기반 인증방법.

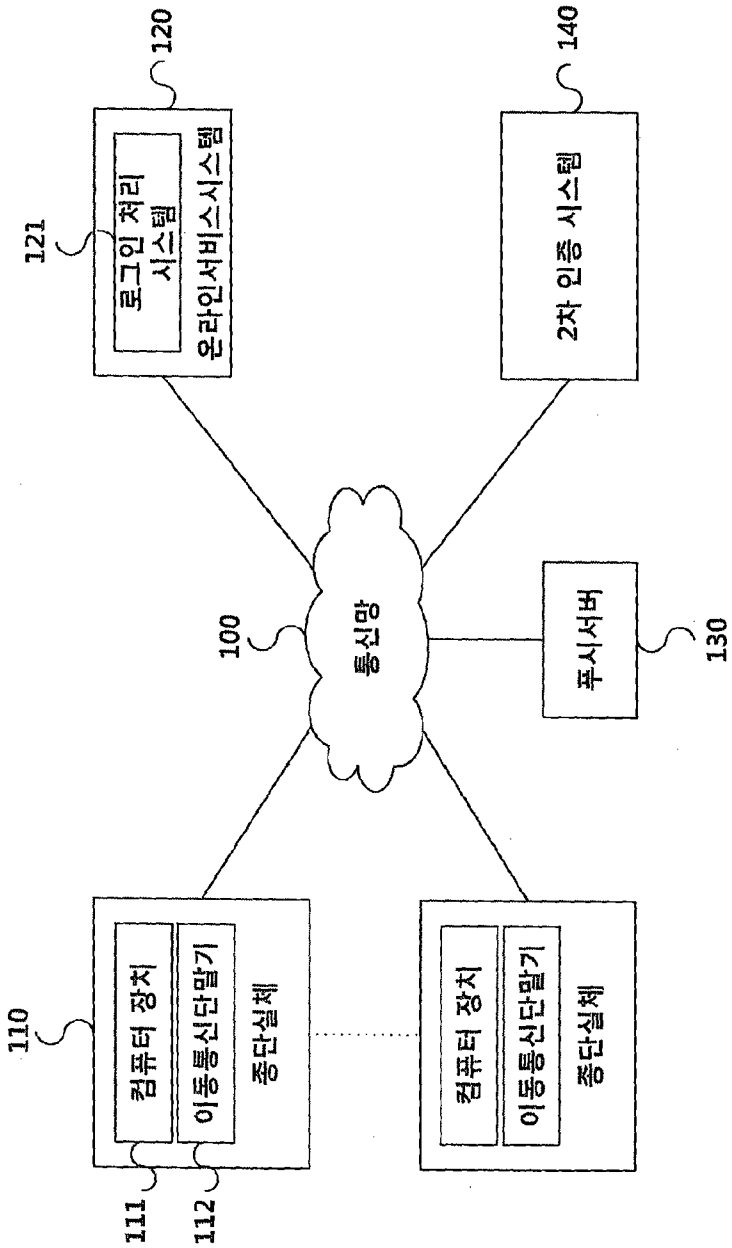
[청구항 25] 제 22 항에 있어서, 상기 컴퓨터장치의 고유식별자는 범용고유식별자(UUID)의 해쉬값을 포함한 것을 특징으로 하는 고유식별자 기반 인증방법.

[청구항 26] 제 22 항에 있어서, 상기 컴퓨터장치의 고유식별자는 전역고유식별자(GUID)의 해쉬값을 포함한 것을 특징으로 하는 고유식별자 기반 인증방법.

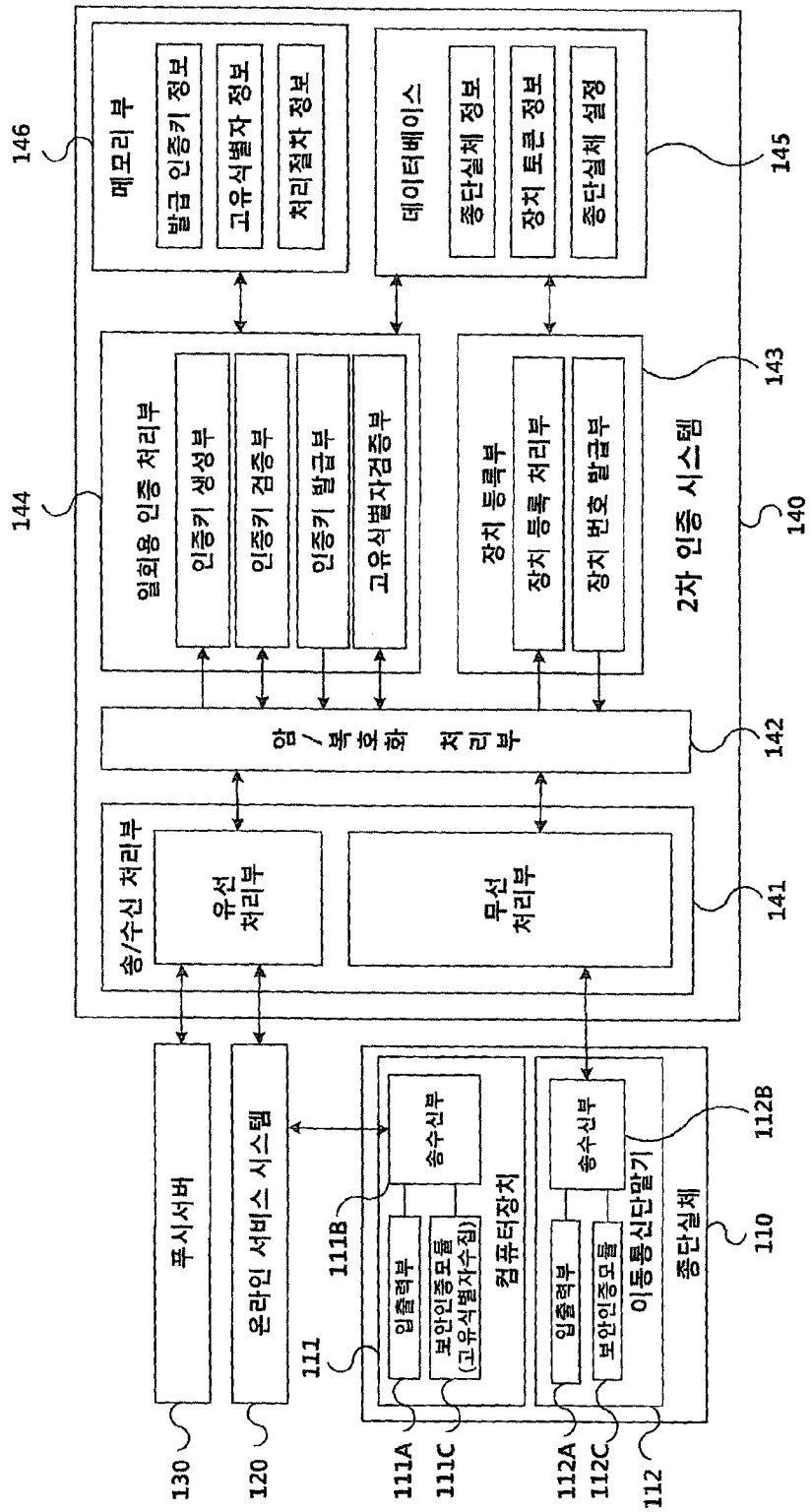
[청구항 27] 제 23 항 내지 제 26 항 중 어느 한 항에 있어서, 상기 컴퓨터장치의 고유식별자는 타임스탬프를 더 포함한 것을 특징으로 하는 고유식별자 기반 인증방법.

[청구항 28] 제 23 항 내지 제 26 항 중 어느 한 항에 있어서, 상기 컴퓨터장치의 고유식별자는 상기 온라인 서비스 시스템의 서비스 파일 정보를 더 포함한 것을 특징으로 하는 고유식별자 기반 인증방법.

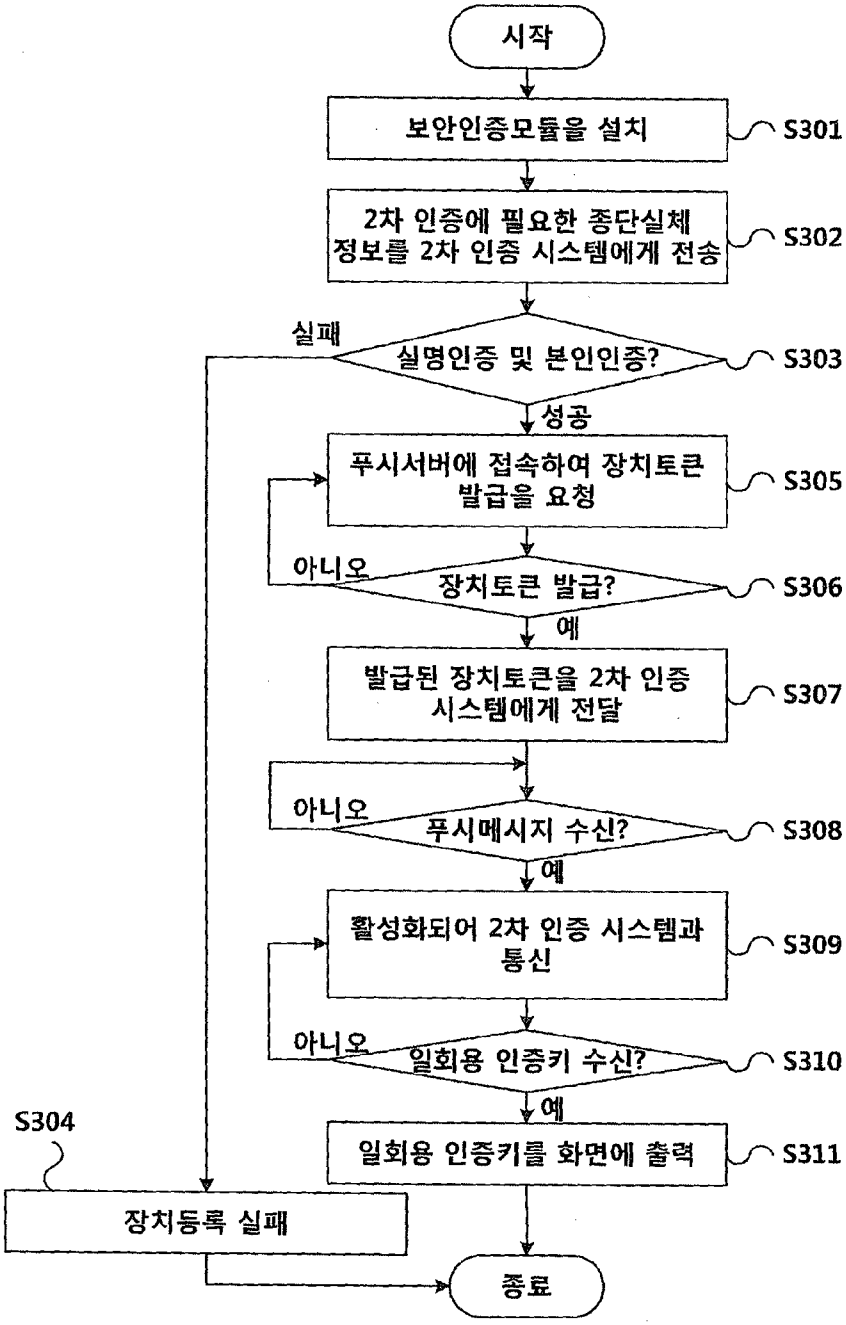
[Fig. 1]


120
140
121
로그인 처리 시스템
온라인서비스시스템
2차 인증 시스템
100
통신망
푸시서버
130
110
컴퓨터 장치
이동통신단말기
종단실체
컴퓨터 장치
이동통신단말기
종단실체
111
112

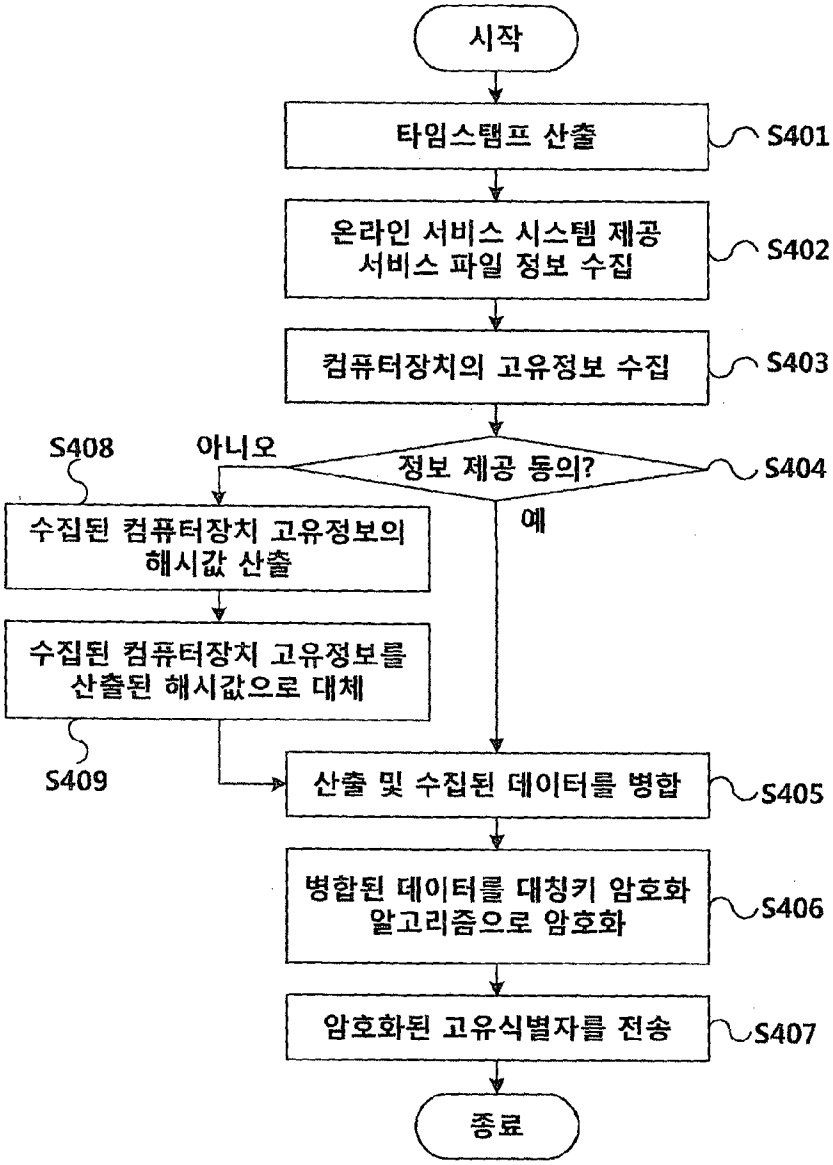
[Fig. 2]


146
메모리 부
발급 인증키 정보
고유식별자 정보
처리절차 정보
데이터베이스
종단실체 정보
장치 토큰 정보
종단실체 설정
145
144
입회용 인증 처리부
인증키 생성부
인증키 검증부
인증키 발급부
고유식별자검증부
장치 등록부
장치 등록 처리부
장치 번호 발급부
143
2차 인증 시스템
140
암/복호화 처리부
142
송/수신 처리부
유선 처리부
무선 처리부
141
푸시서버
온라인 서비스 시스템
111
111B
송수신부
입출력부
보안인증모듈 (고유식별자수집)
컴퓨터장치
112B
송수신부
입출력부
보안인증모듈
이동통신단말기
종단실체
110
130
120
111A
111C
112A
112C
112

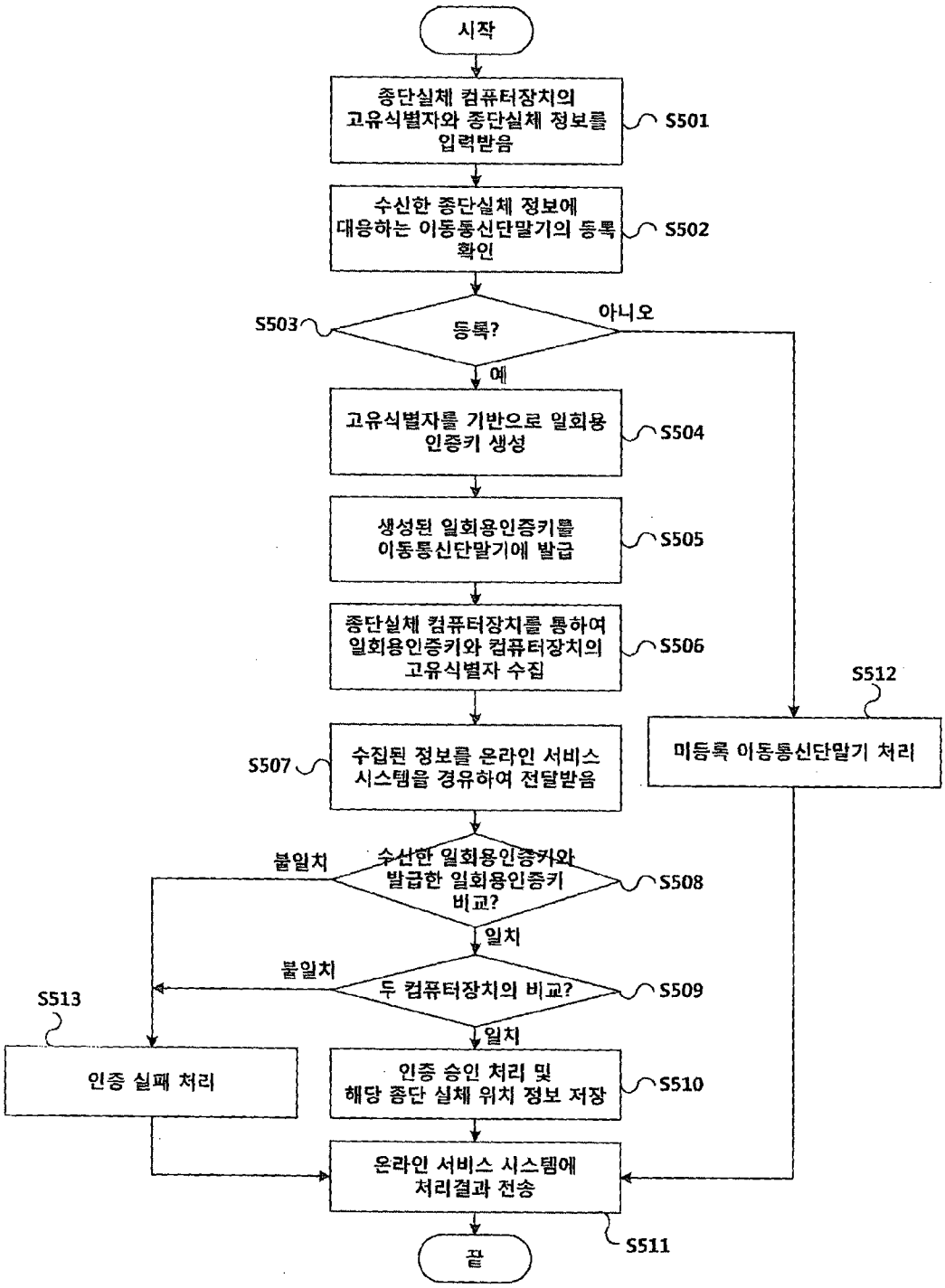
[Fig. 3]


시작
보안인증모듈을 설치
S301
2차 인증에 필요한 종단실체 정보를 2차 인증 시스템에게 전송
S302
실패
실명인증 및 본인인증?
S303
성공
푸시서버에 접속하여 장치토큰 발급을 요청
S305
아니오
장치토큰 발급?
S306
예
발급된 장치토큰을 2차 인증 시스템에게 전달
S307
아니오
푸시메시지 수신?
S308
예
활성화되어 2차 인증 시스템과 통신
S309
아니오
일회용 인증키 수신?
S310
예
일회용 인증키를 화면에 출력
S311
S304
장치등록 실패
종료

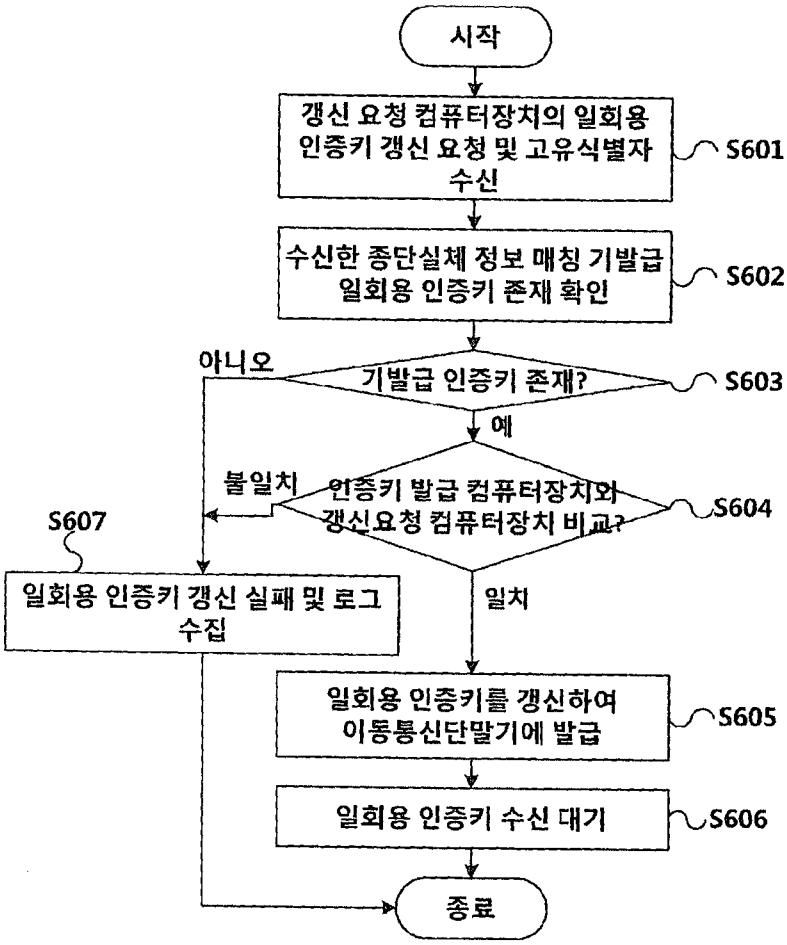
[Fig. 4]


시작
타임스탬프 산출
S401
온라인 서비스 시스템 제공 서비스 파일 정보 수집
S402
컴퓨터장치의 고유정보 수집
S403
정보 제공 동의?
S404
아니오
예
S408
수집된 컴퓨터장치 고유정보의 해시값 산출
수집된 컴퓨터장치 고유정보를 산출된 해시값으로 대체
S409
산출 및 수집된 데이터를 병합
S405
병합된 데이터를 대칭키 암호화 알고리즘으로 암호화
S406
암호화된 고유식별자를 전송
S407
종료

[Fig. 5]


시작
종단실체 컴퓨터장치의 고유식별자와 종단실체 정보를 입력받음
S501
수신한 종단실체 정보에 대응하는 이동통신단말기의 등록 확인
S502
S503
등록?
아니오
예
고유식별자를 기반으로 일회용 인증키 생성
S504
생성된 일회용인증키를 이동통신단말기에 발급
S505
종단실체 컴퓨터장치를 통하여 일회용인증키와 컴퓨터장치의 고유식별자 수집
S506
S512
미등록 이동통신단말기 처리
S507
수집된 정보를 온라인 서비스 시스템을 경유하여 전달받음
불일치
수신한 일회용인증키와 발급한 일회용인증키 비교?
S508
일치
불일치
두 컴퓨터장치의 비교?
S509
S513
일치
인증 실패 처리
인증 승인 처리 및 해당 종단 실체 위치 정보 저장
S510
온라인 서비스 시스템에 처리결과 전송
S511
끝

[Fig. 6]


시작
갱신 요청 컴퓨터장치의 일회용 인증키 갱신 요청 및 고유식별자 수신
S601
수신한 종단실체 정보 매칭 기발급 일회용 인증키 존재 확인
S602
아니오
기발급 인증키 존재?
S603
예
불일치
인증키 발급 컴퓨터장치와 갱신요청 컴퓨터장치 비교?
S604
S607
일회용 인증키 갱신 실패 및 로그 수집
일치
일회용 인증키를 갱신하여 이동통신단말기에 발급
S605
일회용 인증키 수신 대기
S606
종료