(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0094128
(43) 공개일자 2016년08월09일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/14* (2006.01)
(52) CPC특허분류
H04L 9/3247 (2013.01)
H04L 9/14 (2013.01)
(21) 출원번호 10-2015-0015329
(22) 출원일자 2015년01월30일
심사청구일자 2015년01월30일

(71) 출원인
중부대학교 산학협력단
충청남도 금산군 추부면 대학로 201
주식회사 드림시큐리티
서울특별시 송파구 중대로8길 8 (문정동)
(72) 발명자
이병천
대전광역시 유성구 엑스포로 448 엑스포아파트 409-1501
범진규
서울특별시 강남구 도산대로92길 10 청담대우유로카운티 104동 504호
(74) 대리인
특허법인 플러스

전체 청구항 수 : 총 3 항

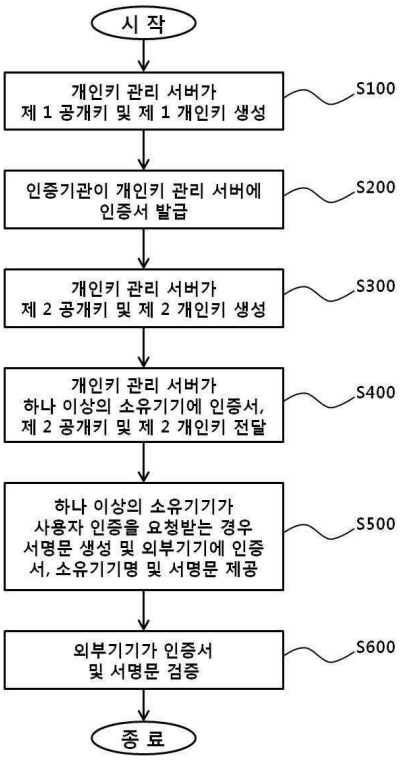
(54) 발명의 명칭 **ID 기반 암호화 방식을 이용한 키관리 및 사용자 인증방법**

(57) 요 약

본 발명에 의한 ID 기반 암호화 방식을 이용한 키관리 및 사용자 인증방법은, 개인 키관리 서버가 사용자의 인증을 위한 제 1 공개키 및 제 1 개인키를 생성하는 단계; 상기 개인 키관리 서버가 사용자 식별정보 및 상기 생성된 제 1 공개키를 인증기관에 전송하여 상기 인증기관으로부터 인증서를 발급받는 단계; 하나 이상의 소유기기가

(뒷면에 계속)

대 표 도 - 도2



상기 개인 키관리 서버에 접속되는 경우, 상기 개인 키관리 서버가 사용자명 및 소유기기명을 이용해서 제 2 공개키를 생성하고, 상기 생성된 제 2 공개키 및 제 1 개인키를 이용해서 제 2 개인키를 생성하는 단계; 상기 개인 키관리 서버가 상기 하나 이상의 소유기기에 상기 발급받은 인증서와 함께, 상기 생성된 제 2 공개키 및 제 2 개인키를 전달하는 단계; 상기 하나 이상의 소유기기가 외부기기로부터 상기 사용자의 인증을 요청받는 경우 상기 전달받은 제 2 공개키 및 제 2 개인키를 이용해서 서명문을 생성하고, 상기 인증서, 소유기기명 및 서명문을 상기 외부기기에 제공하는 단계; 및 상기 외부기기가 상기 사용자의 인증을 수행하기 위하여 상기 제공받은 인증서 및 서명문을 검증하는 단계;를 포함한다.

(52) CPC특허분류
H04L 9/3263 (2013.01)

명 세 서

청구범위

청구항 1

개인 키관리 서버가 사용자의 인증을 위한 제 1 공개키 및 제 1 개인키를 생성하는 단계;

상기 개인 키관리 서버가 사용자 식별정보 및 상기 생성된 제 1 공개키를 인증기관에 전송하여 상기 인증기관으로부터 인증서를 발급받는 단계;

하나 이상의 소유기기가 상기 개인 키관리 서버에 접속되는 경우, 상기 개인 키관리 서버가 사용자명 및 소유기기명을 이용해서 제 2 공개키를 생성하고, 상기 생성된 제 2 공개키 및 제 1 개인키를 이용해서 제 2 개인키를 생성하는 단계;

상기 개인 키관리 서버가 상기 하나 이상의 소유기기에 상기 발급받은 인증서와 함께, 상기 생성된 제 2 공개키 및 제 2 개인키를 전달하는 단계;

상기 하나 이상의 소유기기가 외부기기로부터 상기 사용자의 인증을 요청받는 경우 상기 전달받은 제 2 공개키 및 제 2 개인키를 이용해서 서명문을 생성하고, 상기 인증서, 소유기기명 및 서명문을 상기 외부기기에 제공하는 단계; 및

상기 외부기기가 상기 사용자의 인증을 수행하기 위하여 상기 제공받은 인증서 및 서명문을 검증하는 단계;를 포함하는 ID 기반 암호화 방식을 이용한 키관리 및 사용자 인증방법.

청구항 2

제 1 항에 있어서,

상기 제 2 공개키(Q_{AM_i})는 하기 수학식:

$Q_{AM_i}=H_1(A, M_i)$ (여기서, A는 사용자명이고, M_i는 소유기기명이며, H_1은 해쉬함수임)과 같이 생성되고,

상기 제 2 개인키(D_{AM_i})는 하기 수학식:

$D_{AM_i}=s_A Q_{AM_i}$ (여기서, s_A는 상기 제 1 개인키이고, Q_{AM_i}은 상기 제 2 공개키임)과 같이 생성되는 것을 특징으로 하는 ID 기반 암호화 방식을 이용한 사용자 인증방법.

청구항 3

제 1 항에 있어서,

상기 제 1 공개키 및 제 1 개인키의 생성, 그리고 상기 제 2 공개키 및 제 2 개인키의 생성은 상기 개인 키관리 서버의 내부에 장착되는 하드웨어 보안 모듈에서 이루어지고, 상기 하나 이상의 소유기기가 전달받은 상기 제 2 공개키 및 제 2 개인키는 상기 하나 이상의 소유기기 내부에 장착되는 하드웨어 보안 모듈에 저장하는 것을 특징으로 하는 ID 기반 암호화 방식을 이용한 키관리 및 사용자 인증방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 키관리 및 사용자 인증방법에 관한 것으로, 보다 상세하게는 인증기관(Certification Authority)으로부터 인증서를 발급받은 사용자의 개인 키관리 서버(Personal Key Management Server)가 ID 기반 암호화 방식(Identity Based Encryption; IBE)을 이용해 공개키 및 개인키를 생성한 후, 그 생성된 키쌍을 사용자의 소유기기에 전달함으로써, 인증기관으로부터 직접적으로 인증서를 발급받지 않은 소유기기도 외부기기에 사용자 인증을 제공할 수 있도록 하는 ID 기반 암호화 방식을 이용한 키관리 및 사용자 인증방법에 관한 것이다.

배 경 기 술

[0002] 사용자가 다수의 소유기기(데스크탑, 노트북, 스마트폰, 태블릿 PC와 같은 컴퓨팅기기)들을 사용하는 유비쿼터스 환경에서 인증기관으로부터 인증서를 발급받아 이를 안전하게 사용하고 관리하는 일은 매우 어려운 문제이다. 즉, 사용자가 자신이 소유하는 기기에서 인증키(certified key)를 사용하기 위해서는 인증기관으로부터 인증서를 발급받아 사용하는 것이 일반적인데, 만일 사용자가 다수의 소유기기를 사용하는 경우 각 소유기기마다 외부기기(다른 사용자의 컴퓨팅기기)에 어떠한 방법으로 사용자 인증을 제공할 것인지가 매우 중요하다.

[0003] 우선, 사용자는 다수의 소유기기 중 하나의 소유기기에만 인증서를 발급받고, 그 소유기기의 인증키를 다른 소유기기에 복사 및 전송하는 방법을 생각해 볼 수 있다. 하지만 이 방법은 개인키가 소유기기의 외부로 복사되고 통신을 통해 전송되며 소유기기의 메모리에 로드되어 관리되기 때문에 공격자에 의해 탈취되기 쉽다는 문제점이 있다. 또한, 이 방식은 하나의 소유기기에서 공격자가 개인키를 탈취할 경우 다른 소유기기에서도 그 개인키를 사용할 수 없게 된다는 문제점이 있다. 만일, 하드웨어 보안 모듈에서 키쌍을 생성하고 이에 대해 인증서를 발급받는 경우에는, 개인키를 그 하드웨어 보안 모듈 외부로 복사할 수 없으므로 인증키를 다른 소유기기에 복사하여 사용하는 방식 자체를 적용할 수 없다는 문제점도 존재하게 된다.

[0004] 다음으로, 각 소유기기마다 인증기관으로부터 별도의 인증서를 발급받는 방법을 생각해 볼 수 있다. 하지만 이 경우 사용자는 자신이 소유하는 기기의 수만큼 별도의 인증서를 발급받기 위하여 인증서 발급 프로세스에 여러 번 관여해야 한다는 문제점이 있다. 또한, 발급받은 여러 개의 인증서와 이들이 저장된 소유기기를 모두 개별적으로 관리해야 하는데, 사용자가 소유하는 기기의 수가 많아질수록 이를 안전하게 관리하는 것은 매우 어려운 문제가 될 수 있다.

[0005] 현재까지는 사용자가 다수의 소유기기를 사용하는 유비쿼터스 환경에서 인증키를 효율적으로 관리할 수 있는 체계적인 방안이 제시되지 못하고 있는 실정이고, 사용자의 소유기기에 대해 외부기관에 의존하는 복잡하고 경직된 방법을 취하고 있어, 개인이 직접 키를 관리하고 외부기기와 사용자 인증을 수행할 수 있도록 하는 방안이 마련될 필요가 있다.

[0006] 한편, 최근 들어 안전한 키관리 도구로서 하드웨어 보안 모듈을 활용할 수 있는 환경이 크게 확대되고 있다. 요즘 발매되는 최신형 컴퓨터들은 메인보드에 하드웨어 기반의 보안칩인 신뢰플랫폼모듈(Trusted Platform Module; TPM)이 장착된 형태로 출시되고 있다. 그리고 스마트폰이나 태블릿 PC 등의 이동통신 단말기들은 통신회사에서 가입자 관리를 위해 이용하는 범용가입자식별모듈인 USIM(Universal Subscriber Identity Module)을 장착하여 사용하게 되는데, 이러한 USIM은 키관리를 비롯해서 여러 가지 보안기능을 구현하는 데 활용될 수 있다. 또한, 최근에는 근거리 통신기능과 보안기능이 결합된 NFC(Near Field Communication)칩이 내장된 스마트폰의 보급이 확대되고 있으며, 국내에서는 USB 형태의 인터페이스에 스마트카드칩이 내장된 형태인 USB 보안토큰을 공인인증서의 안전한 저장장치로서 널리 보급하기 위해 노력 중에 있다.

[0007] 이러한 하드웨어 보안 모듈들은 인증키의 안전한 저장소로서의 역할 뿐 아니라, 개인키의 외부 누출 없이 키생성, 암호화, 전자서명, 해쉬, 난수생성 등의 보안기능을 수행할 수 있는 사용 환경을 제공할 수 있다.

[0008] ID 기반 암호화 방식(Identity Based Encryption; IBE)은 사용자의 이름 등과 같이 공개할 수 있는 ID 정보를 공개키로 사용할 수 있는 암호기술로 공개키와 쌍이 되는 개인키는 키생성기관(Key Generation Center; KGC)이라는 외부기관에서 생성하여 사용자에게 제공하는 방식이다. 본 발명에서는 이러한 ID 기반 암호화 방식을 기존의 인증서 기반 암호화 방식과 결합하여 사용함으로써 사용자의 키관리 및 인증을 효율적으로 구성할 수 있도록 하고자 하는 것이다.

선행기술문헌

비특허문헌

[0009] (비특허문헌 0001) Dan Boneh와 Matthew K.Franklin의 논문 "Identity-Based Encryption from the Weil Pairing" Advances in Cryptology-Proceedings of CRYPTO 2001(2001)

(비특허문헌 0002) 차재춘과 천정희의 논문 Cha, J. & Cheon, J. (2003). An Identity-Based Signature from Gap Diffie-Hellman Groups. Practice and Theory in Public Key Cryptography PKC'2003, LNCS 2567, pp. 1830, Springer-Verlag.

발명의 내용

해결하려는 과제

[0010] 본 발명은 상기와 같은 문제점을 해결하기 위하여 안출된 것으로서, 인증기관으로부터 인증서를 발급받은 사용자의 개인 키관리 서버가 ID 기반 암호화 방식을 이용해 공개키 및 개인키를 생성한 후 상기 생성한 키쌍을 사용자의 소유기기에 전달함으로써, 인증기관으로부터 직접적으로 인증서를 발급받지 않은 소유기기도 외부기기에 사용자 인증을 제공할 수 있도록 하는 데 그 목적이 있다.

[0011] 또한, 본 발명은 개인 키관리 서버에서 공개키와 개인키를 생성하고, 하나 이상의 소유기기에서 공개키와 개인키를 저장함에 있어서, 그 개인 키관리 서버 및 하나 이상의 소유기기 내부에 각각 장착되는 하드웨어 보안 모듈을 활용하도록 하여 안전한 키쌍의 생성, 저장 및 활용을 도모하는 데 그 목적이 있다.

과제의 해결 수단

[0012] 상기와 같은 목적을 달성하기 위하여, 본 발명에 의한 ID 기반 암호화 방식을 이용한 키관리 및 사용자 인증방법은, 개인 키관리 서버가 사용자의 인증을 위한 제 1 공개키 및 제 1 개인키를 생성하는 단계; 상기 개인 키관리 서버가 사용자 식별정보 및 상기 생성된 제 1 공개키를 인증기관에 전송하여 상기 인증기관으로부터 인증서를 발급받는 단계; 하나 이상의 소유기기가 상기 개인 키관리 서버에 접속되는 경우, 상기 개인 키관리 서버가 사용자명 및 소유기기명을 이용해서 제 2 공개키를 생성하고, 상기 생성된 제 2 공개키 및 제 1 개인키를 이용해서 제 2 개인키를 생성하는 단계; 상기 개인 키관리 서버가 상기 하나 이상의 소유기기에 상기 발급받은 인증서와 함께, 상기 생성된 제 2 공개키 및 제 2 개인키를 전달하는 단계; 상기 하나 이상의 소유기기가 외부기기로부터 상기 사용자의 인증을 요청받는 경우 상기 전달받은 제 2 공개키 및 제 2 개인키를 이용해서 서명문을 생성하고, 상기 인증서, 소유기기명 및 서명문을 상기 외부기기에 제공하는 단계; 및 상기 외부기기가 상기 사용자의 인증을 수행하기 위하여 상기 제공받은 인증서 및 서명문을 검증하는 단계;를 포함한다.

[0013] 이 때, 상기 제 2 공개키(Q_{AM_i})는 수학식: $Q_{AM_i}=H_1(A, M_i)$ (여기서, A는 사용자명이고, M_i는 소유기기명이며, H_1은 해쉬함수임)과 같이 생성되고, 상기 제 2 개인키(D_{AM_i})는 수학식: $D_{AM_i}=s_A Q_{AM_i}$ (여기서, s_A는 상기 제 1 개인키이고, Q_{AM_i}은 상기 제 2 공개키임)과 같이 생성되는 것을 특징으로 한다.

[0014] 이 때, 상기 제 1 공개키 및 제 1 개인키의 생성, 그리고 상기 제 2 공개키 및 제 2 개인키의 생성은 상기 개인키 관리 서버의 내부에 장착되는 하드웨어 보안 모듈에서 이루어지고, 상기 하나 이상의 소유기기가 전달받은 상기 제 2 공개키 및 제 2 개인키는 상기 하나 이상의 소유기기 내부에 장착되는 하드웨어 보안 모듈에 저장하는 것을 특징으로 한다.

발명의 효과

[0015] 본 발명에 의하면, 인증기관으로부터 인증서를 발급받은 사용자의 개인 키관리 서버가 ID 기반 암호화 방식을 이용해 제 2 공개키 및 제 2 개인키를 생성한 후, 상기 생성된 제 2 키쌍을 인증기관으로부터 인증서를 발급받지 않은 소유기기에 전달하여 그 소유기기와 외부기기 사이에 사용자의 인증을 수행하도록 하기 때문에, 사용자

가 소유하는 모든 기기에 인증기관으로부터 인증서를 발급받을 필요가 없어 키관리의 편의성이 향상된다.

[0016] 개인 키관리 서버에서 생성하는 제 1 개인키는 인증기관에 인증서 발급을 요청할 때 및, 소유기기에 전달할 제 2 공개키 및 제 2 개인키를 생성할 때에만 사용하고 외부기기와의 통신에는 사용하지 않도록 할 수 있기 때문에, 인증기관으로부터 직접적으로 인증받는 제 1 개인키에 대한 공격을 최소화할 수 있다.

[0017] 개인 키관리 서버가 생성하는 제 2 공개키 및 제 2 개인키는 사용자가 필요할 때 언제든지 생성하고 삭제할 수 있기 때문에, 사용자는 소유기기를 분실했을 때 또는 소유기기의 접근 암호를 분실했을 때 언제든지 제 2 키쌍을 삭제하고 재생성할 수 있다.

[0018] 개인 키관리 서버의 내부에 장착된 하드웨어 보안 모듈에서 제 1 키쌍 및 제 2 키쌍을 생성하고, 하나 이상의 소유기기 내부에 장착된 하드웨어 보안 모듈에 제 2 키쌍을 저장하면 공격자의 침입으로부터 개인키의 안전한 관리가 보장될 수 있다.

도면의 간단한 설명

[0019] 도 1은 본 발명의 일 실시예에 의한 ID 기반 암호화 방식을 이용한 키관리 및 사용자 인증 시스템의 구성을 도시한 도면이다.

도 2는 본 발명의 일 실시예에 의한 ID 기반 암호화 방식을 이용한 키관리 및 사용자 인증방법의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0020] 이하에서는 첨부한 도면을 참조하여 본 발명의 일 실시예에 의한 ID 기반 암호화 방식을 이용한 키관리 및 사용자 인증방법에 대하여 설명한다.

[0021] 도 1은 본 발명의 일 실시예에 의한 ID 기반 암호화 방식을 이용한 키관리 및 사용자 인증 시스템의 구성을 도시한 도면이고, 도 2는 본 발명의 일 실시예에 의한 ID 기반 암호화 방식을 이용한 키관리 및 사용자 인증방법의 흐름도이다.

[0022] 본 발명의 일 실시예에 의한 ID 기반 암호화 방식을 이용한 키관리 및 사용자 인증 시스템은 도 1에 도시된 바와 같이, 인증기관(10), 개인 키관리 서버(20), 소유기기(30) 및 외부기기(40)를 포함하여 구성될 수 있다.

[0023] 본 발명에서 인증기관(10)은 사용자의 신원을 확인한 뒤 인증서를 발급하는 기관을 말한다. 개인 키관리 서버(20)는 인증기관(10)에 인증서 발급을 요청하여 그로부터 인증서를 발급받으며 사용자의 소유기기(30)에 제 2 공개키 및 제 2 개인키를 생성하여 전달하는 사용자의 컴퓨팅기기를 의미하고, 소유기기(30)는 인증기관(10)으로부터 직접적으로 인증서를 발급받지 않으며 개인 키관리 서버(20)로부터 제 2 키쌍을 전달받는 사용자의 컴퓨팅기기로서 하나 이상일 수 있다. 그리고 외부기기(40)는 제 3 자가 소유하는 컴퓨팅기기를 의미한다.

[0024] 도 1에 점선으로 나타낸 박스는 개인 키관리 서버(20) 및 소유기기(30)가 사용자의 컴퓨팅기기임을 의미하며, 도 1에서는 소유기기(30)의 수를 하나인 것으로 도시하였지만 이는 본 발명의 일 실시예를 나타낸 것일 뿐 소유기기(30)의 수는 복수 개일 수 있다.

[0025] 도 1을 참고하여 본 발명에 의한 사용자 인증방법에 대해 개략적으로 설명하면, 사용자가 소유하는 개인 키관리 서버(20)가 제 1 공개키 및 제 1 개인키를 생성해서 인증기관(10)에 사용자 식별정보 및 상기 생성된 제 1 공개키를 전송(인증서 발급 요청)하면 인증기관(10)이 개인 키관리 서버(20)에 인증서를 발급한다. 그 후, 개인 키관리 서버(20)는 제 2 공개키 및 제 2 개인키를 생성해서 하나 이상의 소유기기(30)에 상기 발급받은 인증서와 함께 상기 생성된 제 2 공개키 및 제 2 개인키를 전달한다. 그 후, 소유기기(30)는 외부기기(40)로부터 사용자의 인증을 요청받는 경우 제 2 공개키 및 제 2 개인키를 이용해서 서명문을 생성하고 그 외부기기(40)에 인증서, 소유기기명 및 서명문을 제공함으로써 외부기기(40)가 인증서 및 서명문을 검증하여 사용자의 인증을 수행할 수 있도록 한다.

[0026] 본 발명에서는 인증기관(10)으로부터 직접적으로 인증서를 발급받지 않은 하나 이상의 소유기기(30)가 외부기기(40)에 사용자 인증을 제공하는 방법에 대해 제안하며, 이하에서는 도 2를 참고하여 보다 상세히 설명하도록 한다.

[0027] 도 2에 나타낸 본 발명의 일 실시예에 의한 ID 기반 암호화 방식을 이용한 키관리 및 사용자 인증방법은 우선,

개인 키관리 서버(20)가 사용자의 인증을 위한 제 1 공개키 및 제 1 개인키를 생성하며(S100), 이 때, 개인 키관리 서버(20)는 비특허문헌 1에서 설명된 겹선형 페어링(bilinear pairing)을 이용하여 제 1 키쌍을 생성한다.

[0028] 이하, ID 기반 암호화 방식에서 사용하는 키생성 및 암호 기법들에 대해 설명한다.

[0029] 인증기관(10)은 다음과 같은 시스템 파라미터를 생성한다. G_1은 큰 소수 q를 위수로 갖는 덧셈군이며, G_2는 같은 위수 q를 갖는 곱셈군이다. P는 그룹 G_1의 생성자이다. $e:G_1 \times G_1 \rightarrow G_2$는 겹선형 페어링(bilinear pairing)을 나타내는 맵이다. H_1, H_2는 해쉬함수를 나타낸다. 인증기관(10)은 위수 q보다 작은 난수값 s_0를 생성하고 $P_0 = s_0 P$를 계산한다. 이 때, s_0는 인증기관(10)의 개인키, P_0는 인증기관(10)의 공개키가 된다.

[0030] 개인의 ID(즉, 사용자명)를 A라고 하자. 개인 키관리 서버(20)는 위에서와 마찬가지 방법으로 위수 q보다 작은 난수값 s_A를 생성하고 $P_A = s_A P$를 계산한다. 이 때, s_A는 개인 키관리 서버(20)의 제 1 개인키, P_A는 개인 키관리 서버(20)의 제 1 공개키가 된다.

[0031] 여기서, 개인 키관리 서버(20)는 그 내부에 하드웨어 보안 모듈을 장착하고 그 하드웨어 보안 모듈에서 상기 제 1 공개키 및 제 1 개인키를 생성할 수 있으며, 이와 같은 하드웨어 보안 모듈에서의 키쌍의 생성에 대해서는 후술한다.

[0032] 상기 S100 이후에는, 개인 키관리 서버(20)가 사용자 식별정보 및 상기 생성된 제 1 공개키를 인증기관(10)에 전송하여 상기 인증기관(10)으로부터 인증서를 발급받는다(S200).

[0033] 개인 키관리 서버(20)가 생성하는 제 1 키쌍 중 제 1 개인키는 개인 키관리 서버(20) 내부에 저장하고 외부로 누출되지 않도록 하며, 제 1 공개키만 사용자 식별정보와 함께 인증기관(10)에 전송한다. 여기서, 인증서 발급에 필요한 사용자 식별정보는 사용자명을 포함한다.

[0034] 인증기관(10)이 개인 키관리 서버(20)로부터 사용자 식별정보 및 제 1 공개키를 전송받는 경우, 그 인증기관(10)은 사용자의 신원을 확인한 뒤 자신이 가지고 있는 개인키 s_0로 서명한 문서 즉, 인증서를 개인 키관리 서버(20)에 발급한다.

[0035] 이 때, 인증기관(10)이 개인 키관리 서버(20)에 발급하는 인증서($Cert_A$)는 하기 수학식 1에 의해 얻어지는 형태일 수 있다.

수학식 1

[0036] $$Cert_A = s_0 H_1(CI_A, P_A)$$

[0037] 여기서 CI_A는 사용자명 A, 유효기간, 확장필드 등 인증서 발급에 필요한 사용자의 인증정보들을 총칭하여 나타낸 것이다. 즉, 사용자의 인증정보 CI_A와 사용자의 제 1 공개키 P_A의 해쉬값에 대해 인증기관이 자

신의 개인키 s_0로 서명한 것이 인증서 $Cert_A$가 된다.

[0038] 이와 같이, 인증기관(10)이 개인 키관리 서버(20)에 발급하는 인증서에는 상기 제 1 공개키 P_A 및 사용자명 A 등이 포함되어 있으며, 그 밖에도 공공의 네트워크에서 인증기관(10)이 사용자에게 부여하는 속성을 제한하기 위해 유효기간, 키이용 목적, 확장필드 등의 복잡한 필드들이 포함되어 있다.

[0039] 개인 키관리 서버(20)가 인증서를 발급받음에 따라, 상기 S100에서 생성한 제 1 키쌍은 인증기관(10)에 의해 인증받은 인증키쌍이 된다.

[0040] 다음으로, 하나 이상의 소유기기(30)가 개인 키관리 서버(20)에 접속되는 경우, 개인 키관리 서버(20)가 사용자명 및 소유기기명을 이용해서 제 2 공개키를 생성하고, 상기 생성된 제 2 공개키 및 제 1 개인키를 이용해서 제 2 개인키를 생성한다(S300).

[0041] 여기서, 개인 키관리 서버(20)가 제 2 공개키 및 제 2 개인키를 생성하는 것은, 이 제 2 키쌍을 하나 이상의 소유기기(30)에 전달하여 외부기기(40)에 사용자 인증을 제공할 수 있도록 하기 위함이다.

[0042] 우선, 사용자 A의 소유기기(30)의 명칭을 M_i라고 하자. 이 때, 개인 키관리 서버(20)가 생성하는 제 2 공개키($Q_{A.Mi}$)는 하기 수학식 2와 같이 생성할 수 있다.

수학식 2

[0043] $$Q_{A.Mi}=H_1(A, M_i)$$

[0044] 여기서, 개인 키관리 서버(20)가 생성하는 제 2 공개키는 사용자명 A와 소유기기명 M_i를 해쉬함수 H_1에 입력하여 얻은 해쉬값으로서 모두 공개된 정보에 해당한다.

[0045] 여기서 사용자명 A는 상기 S200에서 개인 키관리 서버(20)가 인증기관(10)으로부터 발급받은 인증서에 포함되어 있는 사용자명과 동일한 정보를 이용해야 한다. 그리고 소유기기명 M_i는 하나 이상의 소유기기(30)가 개인 키관리 서버(20)에 접속될 때 그 하나 이상의 소유기기(30)에서 개인 키관리 서버(20)로 전송되거나, 또는 사용자가 개인 키관리 서버(20)에 소유기기명 M_i를 직접 입력(예를 들어, 하나 이상의 소유기기에 대해 pc1, pc2 등으로 구분하여 입력)할 수도 있다.

[0046] 종래 ID 기반 암호화 방식에서는 외부의 신뢰기관인 키생성기관(KGC)에서 사용자 A에게 개인키를 발급하였으며, 이 때, 사용자명에 해당하는 A만에 대한 해쉬값(즉, $H_1(A)$)을 공개키로서 생성하고 있었다.

[0047] 이와 비교하여 본 발명은 개인 키관리 서버(20)가 키생성기관의 역할을 하도록 하는 방식으로서, 인증기관(10)으로부터 직접적으로 인증서를 발급받지 않은 소유기기(30)가 외부기기(40)에 사용자 인증을 제공하기 위해서는, 그 소유기기(30)가 과연 사용자의 기기인지 검증할 수 있도록 하여야 하므로, 개인 키관리 서버(20)에서 제 2 공개키를 생성할 때 사용자명 A와 소유기기명 M_i를 해쉬함수에 함께 입력하여 해쉬값을 구하는 것을 특징으로 한다.

[0048] 한편, 제 2 개인키(D_{AM_i})는 하기 수학식 3과 같이 생성할 수 있다.

수학식 3

[0049] $$D_{AM_i} = s_A Q_{AM_i}$$

[0050] 수학식 3에서 s_A는 상기 S100에서 개인 키관리 서버(20)가 생성하여, 상기 S200에서 인증기관(10)에 의해 인증된 제 1 개인키이고, Q_{AM_i}는 상기 생성된 제 2 공개키이며, 이 때, 개인 키관리 서버(20)가 생성하는 제 2 개인키 D_{AM_i}는 상기 제 1 개인키 s_A로 상기 제 2 공개키 Q_{AM_i}를 서명한 값에 해당한다.

[0051] 상술한 바와 같이, 상기 제 1 공개키 및 제 1 개인키의 생성은 개인 키관리 서버(20)에 내장된 하드웨어 보안 모듈에서 이루어질 수 있으며, 상기 제 2 공개키 및 제 2 개인키의 생성 역시 개인 키관리 서버(20)에 내장된 하드웨어 보안 모듈에서 이루어질 수 있다.

[0052] 다음으로, 개인 키관리 서버(20)는 하나 이상의 소유기기(30)에 상기 발급받은 인증서와 함께, 상기 생성된 제 2 공개키 및 제 2 개인키를 전달한다(S400).

[0053] 하나 이상의 소유기기(30)는 인증기관(10)으로부터 직접적으로 인증서를 발급받지 않아 외부기기(40)에 사용자 인증을 제공할 수 없기 때문에, 개인 키관리 서버(20)는 하나 이상의 소유기기(30)에 인증서를 각각 전달하여야 한다.

[0054] 그리고 개인 키관리 서버(20)는 상기 인증서를 전달하면서 상기 S300에서 생성한 제 2 공개키 및 제 2 개인키도 함께 전달하여, 하나 이상의 소유기기(30)가 서명문을 생성할 수 있도록 한다.

[0055] 개인 키관리 서버(20)가 하나 이상의 소유기기(30)에 제 2 공개키 및 제 2 개인키를 전달하는 경우, 하나 이상의 소유기기(30)는 이를 안전하게 저장하여야 하며, 이 때, 제 2 개인키가 외부로 누출되는 것을 방지하기 위하여, 상기 제 2 키쌍은 하나 이상의 소유기기(30) 내부에 장착되는 하드웨어 보안 모듈에 저장하는 것이 바람직하다.

[0056] 하드웨어 보안 모듈이란 난수생성, 키생성, 키의 안전한 저장, 암호화 및 복호화, 전자서명 및 서명검증 등의 기능을 수행할 수 있는 하드웨어 칩을 말하며, 컴퓨팅기기에 내장된 신뢰플랫폼모듈(TPM), 이동통신기기에 내장된 범용가입자식별모듈(USIM), NFC 칩 및 USB 보안토큰 등을 그 예로 들 수 있다.

[0057] 이러한 하드웨어 보안 모듈은 키쌍의 안전한 저장소로서의 역할 뿐 아니라 개인키의 외부 누출 없이 키쌍 생성, 전자서명, 서명검증 등이 그 장치 내부에서 안전하게 수행될 수 있도록 한다.

[0058] 이에 따라, 본 발명의 S100에서 상기 제 1 공개키 및 제 1 개인키의 생성, S300에서 상기 제 2 공개키 및 제 2 개인키의 생성은 개인 키관리 서버(20)의 내부에 장착되는 하드웨어 보안 모듈에서 이루어지도록 하고, S400에서 하나 이상의 소유기기(30)가 상기 제 2 공개키 및 제 2 개인키를 전달받을 경우, 그 제 2 키쌍을 하나 이상의 소유기기(30) 내부에 장착되는 하드웨어 보안 모듈에 저장하도록 함으로써, 제 1 개인키 및 제 2 개인키를 공격자의 침입으로부터 보다 안전하게 방어할 수 있다.

[0059] 다음으로, 하나 이상의 소유기기(30)가 외부기기(40)로부터 상기 사용자의 인증을 요청받는 경우 상기 전달받은 제 2 공개키 및 제 2 개인키를 이용해서 서명문을 생성하고, 상기 인증서, 소유기기명 및 서명문을 외부기기(40)에 제공한다(S500).

[0060] 서명문을 생성하기 위해서는 ID 기반 암호키를 이용하는 어떤 전자서명 기법이라도 이용할 수 있으며, 상기 비특허문헌 2에 개시된 방식을 이용하는 사례는 하기 수학식 4와 같이 나타낼 수 있다.

수학식 4

[0061] $$k \in_R Z_q^*,\ U = kQ_{AM_i},\ V = (k + H_2(M, U))D_{AM_i}$$

[0062] 소유기기(30)는 위수 q보다 작은 임의의 난수 k를 선택해서 제 2 공개키 Q_{AM_i}에 곱해 U를 계산하고, 메세지 M과 상기 U를 해쉬함수 H_2에 입력하여 얻어지는 해쉬값에 난수 k를 더한 후 제 2 개인키 D_{AM_i}에 곱해 V를 계산하며, 상기 U와 V가 서명문 $sig = (U, V)$가 된다.

[0063] 하나 이상의 소유기기(30)는 외부기기(40)로부터 상기 사용자의 인증을 요청받는 경우 이와 같은 방식으로 제 2 공개키 및 제 2 개인키를 이용하여 서명문을 생성할 수 있으며, 그 생성된 서명문을 인증서 및 소유기기명과 함께 외부기기(40)에 제공한다.

[0064] 다음으로, 외부기기(40)는 상기 사용자의 인증을 수행하기 위하여 상기 제공받은 인증서 및 서명문을 다음과 같이 검증한다(S600).

[0065] 구체적으로, 외부기기(40)는 상기 제공받은 인증서를 인증기관(10)의 공개키 P_0를 이용하여 검증함으로써 사용자의 신원을 확인하고, 이에 따라 사용자의 인증서에 포함된 제 1 공개키 P_A의 유효성을 확인할 수 있다.

[0066] 그리고 외부기기(40)는 상기 제공받은 서명문을 하기 수학식 5를 사용하여 검증할 수 있다.

수학식 5

[0067] $$e(P, V) = e(P_A, U)e(P_A, H_2(M, U)Q_{AM_i})$$

[0068] 수학식 5에 의하면, 좌변항과 우변항의 값이 같으면 서명문이 유효한 것으로 판정한다. 외부기기(40)가 서명문을 검증하기 위해서는 개인 키관리 서버(20)가 생성한 제 1 공개키 P_A 및 제 2 공개키 Q_{AM_i}등이 사용된다.

[0069] 이 때, 제 1 공개키 P_A는 상기 S500에서 제공되는 인증서에 포함되어 있으므로 이를 이용할 수 있다.

[0070] 그리고 제 2 공개키 Q_{AM_i}는 사용자명 A 및 소유기기명 M_i의 해쉬값에 해당하는 것으로서, 여기서 사용자명 A는 상기 S500에서 제공되는 인증서에 포함되어 있고, 소유기기명 M_i는 상기 S500에서 인증서 및 서명문 제공 시 함께 제공되므로, 이 사용자명 A 및 소유기기명 M_i를 이용해서 상기 서명문을 검증할 수 있다.

[0071] 외부기기(40)는 상기와 같은 검증 과정을 거침으로써 하나 이상의 소유기기(30)에 대해 사용자를 인증할 수 있게 된다.

[0072] 본 발명에 의하면, 사용자는 개인 키관리 서버(20)에 하나의 인증서만 발급받으면, 인증서를 발급받지 않은 소유기기(30)에 대해서도 제 2 공개키 및 제 2 개인키를 생성하여 전달함으로써 외부기기(40)에 사용자 인증을 제공할 수 있게 된다. 그리고 이 경우 제 1 개인키(개인 키관리 서버(20)에서 생성하여 인증기관(10)으로부터 인증받은 개인키)는 개인 키관리 서버(20)에 저장해 놓고 외부로 복사 및 전송하지 않으므로, 제 1 개인키가 공격자로부터 탈취되는 위험을 없앨 수 있다.

[0073] 또한, 개인 키관리 서버(20)에서의 제 1 키쌍 및 제 2 키쌍의 생성, 그리고 하나 이상의 소유기기(30)에서의 제 2 키쌍의 저장이 각각 그 내부에 장착된 하드웨어 보안 모듈에서 이루어질 경우에는 제 1 개인키 및 제 2 개인키가 외부로 누출될 염려가 줄어들어, 개인키가 공격자에 의해 불법적으로 탈취되는 것을 방지할 수 있게 된다.

부호의 설명

[0074] 10: 인증기관

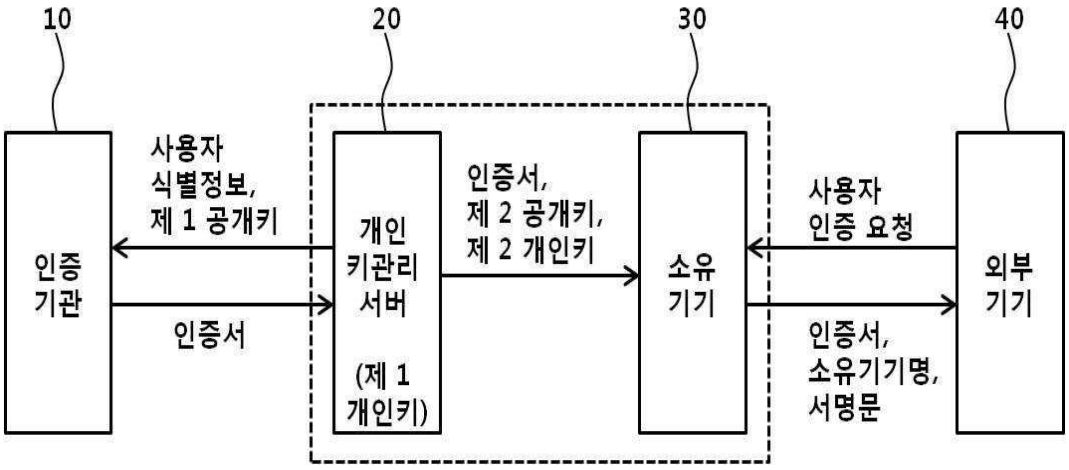
20: 개인 키관리 서버

30: 소유기기

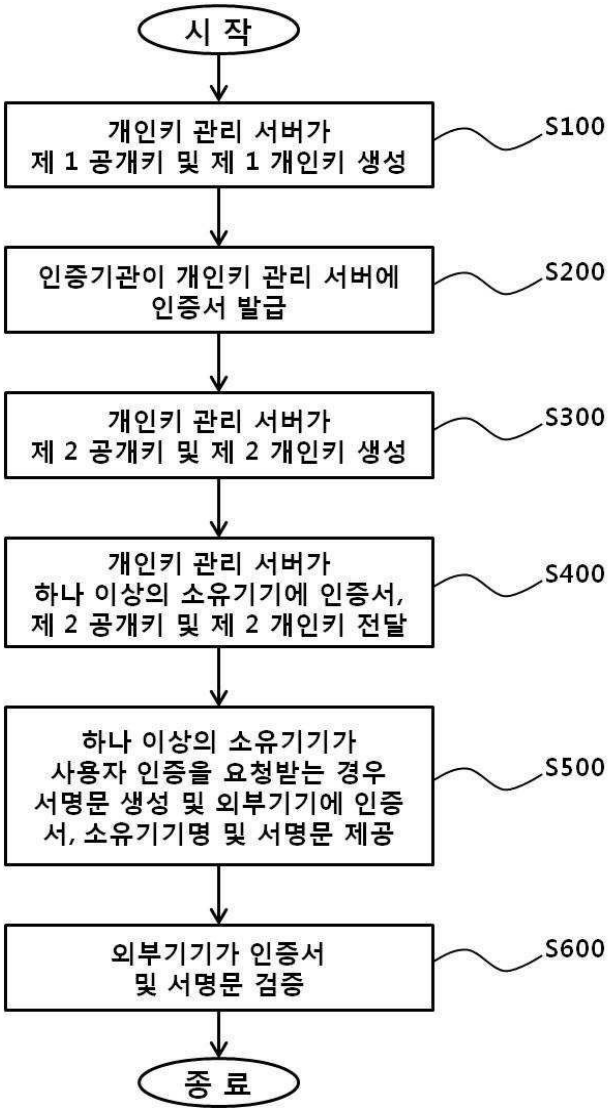
40: 외부기기

도면

도면1



도면2


시 작
개인키 관리 서버가
제 1 공개키 및 제 1 개인키 생성
S100
인증기관이 개인키 관리 서버에
인증서 발급
S200
개인키 관리 서버가
제 2 공개키 및 제 2 개인키 생성
S300
개인키 관리 서버가
하나 이상의 소유기기에 인증서,
제 2 공개키 및 제 2 개인키 전달
S400
하나 이상의 소유기기가
사용자 인증을 요청받는 경우
서명문 생성 및 외부기기에 인증
서, 소유기기명 및 서명문 제공
S500
외부기기가 인증서
및 서명문 검증
S600
종 료