(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0096691
(43) 공개일자 2017년08월25일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 9/0894 (2013.01)
H04L 9/321 (2013.01)
(21) 출원번호 10-2016-0018219
(22) 출원일자 2016년02월17일
심사청구일자 2016년02월17일

(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

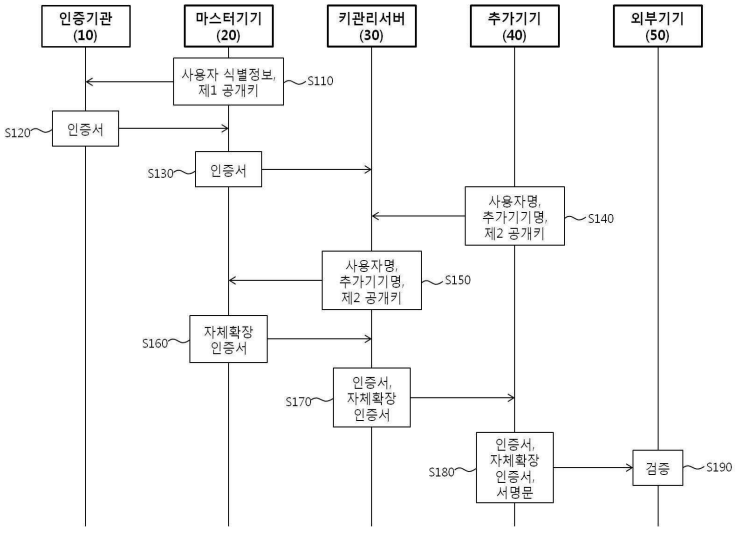
전체 청구항 수 : 총 4 항

(54) 발명의 명칭 **자체확장인증을 이용한 키관리 방법**

(57) 요 약

본 발명은 자체확장인증을 이용한 키관리 방법에 관한 것으로, 하나의 마스터기기가 인증기관으로부터 인증서를 발급받은 뒤 이에 기반하여 자체확장인증서를 발급하여 키관리서버에 전송하고, 추가기기가 상기 키관리서버에 접속하여 외부기기에 사용자 인증을 제공하는데 필요한 인증서 및 자체확장인증서를 다운로드 받을 수 있도록 구성되기 때문에, 사용자가 소유하는 모든 기기에 인증기관으로부터 인증서를 발급받을 필요 없이 사용자 스스로 인증키(보다 구체적으로는, 자체확장인증을 받은 제2 공개키 및 제2 개인키)를 생성하고 관리할 수 있어 키관리의 편의성이 향상된다.

대 표 도 - 도2



(52) CPC특허분류
H04L 9/3263 (2013.01)

명 세 서

청구범위

청구항 1

마스터기기가 제1 공개키 및 제1 개인키를 생성하고, 사용자 식별정보 및 상기 제1 공개키를 인증기관에 전송하는 인증서 발급 신청 단계;

상기 인증기관이 상기 마스터기기에 인증서를 발급하는 인증서 발급 단계;

상기 마스터기기가 상기 인증서를 키관리서버에 전송하는 사용자등록 단계;

추가기기가 상기 키관리서버에 접속하여 제2 공개키 및 제2 개인키를 생성하고, 사용자명, 추가기기명 및 상기 제2 공개키를 상기 키관리서버에 전송하는 기기등록 신청 단계;

상기 마스터기기가 상기 키관리서버에 접속하여 상기 사용자명, 상기 추가기기명 및 상기 제2 공개키에 대한 정보를 획득하는 기기등록 신청정보 획득 단계;

상기 마스터기기가 상기 사용자명, 상기 추가기기명 및 상기 제2 공개키가 포함된 문서에 대해 상기 제1 개인키로 서명한 자체확장인증서를 발급하여 상기 키관리서버에 전송하는 기기등록 허가 단계; 및

상기 추가기기가 상기 키관리서버에 접속하여 상기 인증서 및 상기 자체확장인증서를 다운로드 받는 기기등록 완료 단계;를 포함하는 자체확장인증을 이용한 키관리 방법.

청구항 2

제1항에 있어서,

상기 사용자등록 단계에서, 상기 키관리서버는 상기 마스터기기를 통해 입력되는 사용자 정보에 따라 사용자 계정을 생성하고, 상기 인증서의 유효성을 검증한 후 유효하다고 판단될 경우에만 상기 인증서를 상기 사용자 계정에 저장하고,

상기 기기등록 신청 단계에서, 상기 키관리서버는 상기 사용자명, 상기 추가기기명 및 상기 제2 공개키를 상기 사용자 계정에 저장하며,

상기 기기등록 허가 단계에서, 상기 키관리서버는 상기 자체확장인증서의 유효성을 검증한 후 유효하다고 판단될 경우에만 상기 자체확장인증서를 상기 사용자 계정에 저장하는 것을 특징으로 하는 자체확장인증을 이용한 키관리 방법.

청구항 3

제1항에 있어서,

상기 기기등록 완료 단계 이후에, 상기 추가기기가 외부기기로부터 사용자의 인증을 요청받는 경우 상기 제2 개인키로 서명한 서명문을 생성하고, 상기 인증서, 상기 자체확장인증서 및 상기 서명문을 상기 외부기기에 제공하는 사용자 인증 단계; 및

상기 외부기기는 상기 사용자의 인증을 수행하기 위하여 제공받은 상기 인증서, 상기 자체확장인증서 및 상기 서명문을 검증하는 검증 단계;를 더 포함하는 자체확장인증을 이용한 키관리 방법.

청구항 4

제1항에 있어서,

상기 제1 공개키 및 제1 개인키의 생성은 상기 마스터기기의 내부에 장착되는 하드웨어보안모듈에서 이루어지고,

상기 제2 공개키 및 제2 개인키의 생성은 상기 추가기기의 내부에 장착되는 하드웨어보안모듈에서 이루어지는 것을 특징으로 하는 자체확장인증을 이용한 키관리 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 자체확장인증을 이용한 키관리 방법에 관한 것으로, 보다 상세하게는 하나의 마스터기기가 인증기관(Certification Authority)으로부터 인증서를 발급받은 뒤 자체적으로 생성하는 인증서(즉, 자체확장인증서)를 키관리서버를 통해 추가기기에 발급함으로써, 인증기관으로부터 직접적으로 인증서를 발급받지 않은 추가기기도 외부기기에 사용자 인증을 제공할 수 있도록 구성된 자체확장인증을 이용한 키관리 방법에 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. 구체적으로, 사용자가 자신이 소유하는 기기에서 인증키(certified key)를 사용하기 위해서는, 공개키와 개인키 쌍을 생성한 후 개인키는 기기 내에 안전하게 저장하고 공개키는 인증기관에 제출하여 이에 대해 인증기관으로부터 인증서를 발급받는 것이 일반적인 접근 방법인데, 만일 사용자가 다수의 소유기기를 사용하는 경우에는 각 소유기기마다 사용자의 인증키를 어떻게 설치하고 외부기기에는 사용자 인증을 어떠한 방법으로 제공할 것인지가 매우 중요하다.

[0003] 우선, 사용자는 다수의 소유기기 중에서 어느 하나의 소유기기에만 인증서를 발급받고, 상기 인증서를 발급받은 소유기기에서 인증키(즉, 인증기관으로부터 인증받은 공개키와 개인키)를 복사하여 다른 소유기기에 전송하는 방법을 생각해 볼 수 있다. 하지만 이 방법은 개인키가 통신을 통해 소유기기의 외부로 전송되기 때문에 외부 공격자의 공격에 의해 탈취되기 쉽다는 문제점이 있다. 또한, 이 방식은 하나의 소유기기에서 개인키가 탈취되면 다른 모든 소유기기에서도 그 개인키를 사용할 수 없게 된다는 문제점이 있다. 만일, 스마트카드, 신뢰플랫폼모듈(Trusted Platform Module; TPM), 범용가입자식별모듈(Universal Subscriber Identity Module; USIM), NFC(Near Field Communication) 칩, USB 보안토큰 등의 하드웨어보안모듈에서 키쌍을 생성하고 이에 대해 인증서를 발급받는 경우에는 개인키를 그 하드웨어보안모듈의 외부로 복사할 수 없으므로 인증키를 다른 소유기기에 복사하여 사용하는 방식 자체를 적용할 수 없다는 문제점도 존재하게 된다.

[0004] 다음으로, 각 소유기기마다 인증기관으로부터 별도의 인증서를 발급받아 사용하는 방법을 생각해 볼 수 있다. 하지만 이 경우 사용자는 자신이 소유하는 기기의 수만큼 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 이들 모두를 안전하게 관리하는 것은 매우 어려운 문제가 될 수 있다. 게다가, 기기의 분실이나 파손 등의 경우에 사용자는 인증기관에게 인증서 취소를 신청하고, 인증기관은 인증서 취소목록을 발행하는 등 인증서 취소 절차를 수행해야 하는데, 이것은 사용자나 인증기관 모두에게 매우 복잡하고 번거로운 일이 아닐 수 없다.

[0005] 현재 국내의 공인인증 시스템에 대해서는 많은 비판들이 존재하는데, 그 주된 비판 요소는 액티브엑스와 같은 비표준 부가프로그램을 브라우저에 설치해야 한다는 점, 특정 브라우저에만 종속된다는 점, 그리고 보다 근본적인 문제로는 컴퓨터 내부에 개인키를 안전하게 보관하고 사용하기 어려워 각종 해킹 공격에 취약하다는 점 등을 들 수 있다. 이러한 문제를 해결하기 위하여 USIM이 장착된 스마트폰에 인증키를 저장하여 사용하고 비밀번호를 대체하기 위해 생체인식기술을 이용하는 FIDO(Fast IDentity Online) 등의 접근방법이 연구개발되고 있으나, 이러한 접근 방법은 인증서 기반의 시스템이 아니기 때문에 다수의 소유기기에 대한 인증키 배포와 관련하여 근본적인 대책이 마련될 필요가 있다.

[0006] 즉, 현재까지는 사용자가 다수의 소유기기를 사용하는 유비쿼터스 환경에서 인증키를 안전하고 효율적으로 관리할 수 있는 체계적인 방안이 제시되지 못하고 있는 실정이고, 사용자 인증을 외부의 인증기관에만 의존하는 복잡하고 경직된 방법을 취하고 있어, 사용자가 다수의 소유기기에 인증키를 직접 배포하고 편리하게 관리할 수 있으면서도 외부기기에 사용자 인증을 제공할 수 있는 기술적 기반이 마련될 필요가 있다.

[0007] 한편, 사용자 소유의 다수의 기기에서 사용자 인증이 가능하도록 하는 방안이 비특허문헌 1에 개시되어 있다. 구체적으로, 비특허문헌 1에 의하면 사용자의 인증서 및 개인키를 구비하고 있는 사용자 소유의 키관리서버가 사용자 소유의 다른 기기들에게 확장인증서명을 발행함으로써 타인 소유의 기기들에 사용자 인증을 제공할 수 있음이 개시되어 있다. 하지만 비특허문헌 1에 개시된 키관리서버는 인증키(특히, 인증기관으로부터 인증받은 사용자의 개인키)를 보유하고 있기 때문에 외부 공격자에 의한 집중적인 공격대상이 될 것으로 예상되는데, 비

전문가인 일반 사용자가 이러한 키관리서버를 직접 안전하게 운영하는 것은 매우 어려운 일이다. 그리고 사용자가 이러한 기능을 갖는 키관리서버를 직접 운영하는 것은 경제적으로도 큰 부담이 된다는 문제점이 존재한다.

선행기술문헌

비특허문헌

[0008] (비특허문헌 0001) 이병천, "자체확장인증과 하드웨어보안모듈을 이용한 하이브리드 키관리(Hybrid Key Management Using Self-Extended Certification and Hardware Security Module)", 보안공학연구논문지, (2014), Vol.11, No.4, pages 273-286

발명의 내용

해결하려는 과제

[0009] 본 발명은 상기와 같은 문제점을 해결하기 위하여 안출된 것으로서, 사용자가 몇 개의 소유기기를 사용하든 상관없이 인증기관에 의존하지 않고 외부기기에 사용자 인증을 제공할 수 있는 키관리 방법을 제공함에 그 목적이 있다. 보다 구체적으로, 본 발명은 사용자가 인증기관으로부터 인증서를 발급받은 하나의 마스터기기를 가지고 있다는 것을 가정하고 있는데, 이런 경우 마스터기기에서 생성하는 사용자의 개인키를 상기 마스터기기에만 저장하고 키관리서버에는 보유시킬 필요가 없도록 함으로써, 외부 공격자가 키관리서버를 공격하여 사용자의 개인키를 탈취할 가능성을 없애고, 그와 동시에 다수의 사용자가 키관리서버를 공동으로 이용할 수 있도록 하는 키관리 방법을 제공함에 그 목적이 있다.

[0010] 이와 함께, 본 발명은 사용자 자신이 아닌 서버 전문가가 키관리서버를 운영할 수 있는 키관리 프로토콜을 제공함으로써 사용자가 키관리서버를 직접 운영함에 따라 초래될 수 있는 불편함을 해소하고, 키관리서버가 전문가에 의해 안정적으로 운영될 수 있도록 하며, 키관리서버 운영에 소요되는 사용자의 경제적 부담을 해소시킬 수 있는 키관리 방법을 제공함에 그 목적이 있다.

과제의 해결 수단

[0011] 상기와 같은 목적을 달성하기 위하여, 본 발명에 따른 자체확장인증을 이용한 키관리 방법은, 마스터기기가 제1 공개키 및 제1 개인키를 생성하고, 사용자 식별정보 및 상기 제1 공개키를 인증기관에 전송하는 인증서 발급 신청 단계; 상기 인증기관이 상기 마스터기기에 인증서를 발급하는 인증서 발급 단계; 상기 마스터기기가 상기 인증서를 키관리서버에 전송하는 사용자등록 단계; 추가기기가 상기 키관리서버에 접속하여 제2 공개키 및 제2 개인키를 생성하고, 사용자명, 추가기기명 및 상기 제2 공개키를 상기 키관리서버에 전송하는 기기등록 신청 단계; 상기 마스터기기가 상기 키관리서버에 접속하여 상기 사용자명, 상기 추가기기명 및 상기 제2 공개키에 대한 정보를 획득하는 기기등록 신청정보 획득 단계; 상기 마스터기기가 상기 사용자명, 상기 추가기기명 및 상기 제2 공개키가 포함된 문서에 대해 상기 제1 개인키로 서명한 자체확장인증서를 발급하여 상기 키관리서버에 전송하는 기기등록 허가 단계; 및 상기 추가기기가 상기 키관리서버에 접속하여 상기 인증서 및 상기 자체확장인증서를 다운로드 받는 기기등록 완료 단계;를 포함한다.

[0012] 이 때, 상기 사용자등록 단계에서, 상기 키관리서버는 상기 마스터기기를 통해 입력되는 사용자 정보에 따라 사용자 계정을 생성하고, 상기 인증서의 유효성을 검증한 후 유효하다고 판단될 경우에만 상기 인증서를 상기 사용자 계정에 저장하고, 상기 기기등록 신청 단계에서, 상기 키관리서버는 상기 사용자명, 상기 추가기기명 및 상기 제2 공개키를 상기 사용자 계정에 저장하며, 상기 기기등록 허가 단계에서, 상기 키관리서버는 상기 자체확장인증서의 유효성을 검증한 후 유효하다고 판단될 경우에만 상기 자체확장인증서를 상기 사용자 계정에 저장하는 것을 특징으로 한다.

[0013] 또한, 본 발명에 따른 자체확장인증을 이용한 키관리 방법은, 상기 기기등록 완료 단계 이후에, 상기 추가기기가 외부기기로부터 사용자의 인증을 요청받는 경우 상기 제2 개인키로 서명한 서명문을 생성하고, 상기 인증서, 상기 자체확장인증서 및 상기 서명문을 상기 외부기기에 제공하는 사용자 인증 단계; 및 상기 외부기기는 상기 사용자의 인증을 수행하기 위하여 제공받은 상기 인증서, 상기 자체확장인증서 및 상기 서명문을 검증하는 검증 단계;를 더 포함한다.

[0014] 그리고 본 발명에 따른 자체확장인증을 이용한 키관리 방법에서, 상기 제1 공개키 및 제1 개인키의 생성은 상기

마스터기기의 내부에 장착되는 하드웨어보안모듈에서 이루어지고, 상기 제2 공개키 및 제2 개인키의 생성은 상기 추가기기의 내부에 장착되는 하드웨어보안모듈에서 이루어지는 것을 특징으로 한다.

발명의 효과

[0015] 본 발명에 의하면, 하나의 마스터기기가 인증기관으로부터 인증서를 발급받은 뒤 이에 기반하여 자체확장인증서를 발급하여 키관리서버에 전송하고, 추가기기가 상기 키관리서버에 접속하여 외부기기에 사용자 인증을 제공하는데 필요한 인증서 및 자체확장인증서를 다운로드 받을 수 있도록 구성되기 때문에, 사용자는 자신이 소유하는 모든 기기에 인증기관으로부터 인증서를 발급받을 필요 없이 사용자 스스로 인증키(보다 구체적으로는, 자체확장인증을 받은 제2 공개키 및 제2 개인키)를 생성하고 관리할 수 있어 키관리의 편의성이 향상된다.

[0016] 마스터기기에서 발급되어 키관리서버에 전송되는 자체확장인증서는 유효기간, 폐기 메커니즘 등의 가변적인 정보가 필요 없기 때문에, 외부기기에서 한 번만 서명검증을 하면 인증서의 유효기간까지 추가적인 서명검증 없이 사용할 수 있게 된다.

[0017] 또한 본 발명에 의하면, 키관리서버가 사용자의 개인키를 저장할 필요 없이 자체확장인증서를 발급하는 마스터기기 및 자체확장인증서를 발급받는 추가기기 사이의 통신을 중개하는 역할만을 수행하기 때문에, 사용자가 직접 키관리 서버를 운영할 필요없이 별도의 서버 전문가로 하여금 키관리서버를 운영하도록 할 수 있다. 그리고 이와 같이 전문가가 운영하는 키관리서버가 존재하는 경우에는, 사용자가 자신의 소유기기에 자체확장인증서를 발급하는데 있어서 상기 키관리서버를 클라이언트 입장에서 이용할 수 있기 때문에 사용상의 편의성 및 운영상의 안정성이 보장될 수 있고, 키관리서버 운영에 소요되는 사용자의 경제적 부담을 해소시킬 수 있게 된다.

[0018] 또한, 본 발명에 의하면 사용자의 개인키는 마스터기기 및 추가기기에서 각각 생성하고 보유하되 키관리서버에는 이를 보유시키지 않기 때문에, 사용자가 마스터기기 및 추가기기에서 생성하는 개인키만 관리하면 외부 공격자에 의해 사용자의 개인키가 탈취될 가능성이 크게 감소될 수 있다. 이에 따라, 본 발명에 의하면 키관리서버를 다수의 사용자들도 안심하고 이용할 수 있어 사용자들의 편의성이 크게 증진될 수 있다. 게다가, 마스터기기는 자체확장인증서의 발급 시에만 사용하고 외부기기와의 일상적인 통신에서는 사용하지 않고 꺼놓을 수 있으며, 이 경우에는 제1 개인키가 외부 공격자로부터 탈취될 가능성이 더욱 감소되어 안전한 키관리를 실현할 수 있게 된다.

도면의 간단한 설명

[0019] 도 1은 본 발명을 구현시킬 수 있는 키관리 시스템의 구성을 예시적으로 나타낸 도면이다.

도 2는 본 발명에 따른 자체확장인증을 이용한 키관리 방법을 나타낸 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0020] 이하, 첨부한 도면들을 참조하여 본 발명에 따른 자체확장인증을 이용한 키관리 방법에 대해 상세하게 설명한다. 첨부한 도면들은 통상의 기술자에게 본 발명의 기술적 사상이 충분히 전달될 수 있도록 하기 위해 제공되는 것으로서, 본 발명은 첨부한 도면들만으로 한정되는 것이 아니라 본 발명의 기술적 사상을 변화시키지 않는 범위 내에서 다른 형태로 구체화될 수 있다. 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능 및 구성에 대해서는 그 상세한 설명을 생략하기로 한다.

[0021] 도 1은 본 발명을 구현시킬 수 있는 키관리 시스템의 구성을 예시적으로 나타낸 도면이고, 도 2는 본 발명에 따른 자체확장인증을 이용한 키관리 방법을 나타낸 흐름도이다.

[0022] 본 발명은 사용자가 몇 개의 소유기기를 사용하든 상관없이 인증기관에 의존하지 않고 외부기기에 사용자 인증을 제공할 수 있는 키관리 방법을 제공함에 그 목적이 있다.

[0023] 이를 위해, 본 발명을 구현시킬 수 있는 키관리 시스템은, 도 1에 도시된 바와 같이 인증기관(10), 마스터기기(20), 키관리서버(30) 및 추가기기(40)를 포함하며, 외부기기(50)를 더 포함하여 구성될 수 있다.

[0024] 인증기관(10)은 사용자의 신원을 확인한 뒤 인증서를 발급하는 기관을 말한다.

[0025] 마스터기기(20)는 사용자의 소유기기들 중에서 인증기관(10)에 인증서 발급을 요청하여 그로부터 인증서를 발급받으며, 인증받은 제1 개인키를 이용하여 자체확장인증서를 발급하는 컴퓨팅기기를 의미한다.

[0026] 추가기기(40)는 사용자의 소유기기들 중에서 인증기관(10)으로부터 직접적으로 인증서를 발급받지 않으며, 외부

기기(50)에 사용자 인증을 제공하기 위해 키관리서버(30)로부터 인증서 및 자체확장인증서를 다운로드 받는 컴퓨팅기기를 의미한다.

[0027] 그리고 외부기기(50)는 제3자가 소유하는 컴퓨팅기기 또는 제3자가 운영하는 서버로서, 인증서, 자체확장인증서 및 서명문을 이용하여 추가기기(40)에 대한 사용자의 인증을 수행하는 기기를 의미한다.

[0028] 그리고 키관리서버(30)는 마스터기기(20)와 추가기기(40) 사이에서 인증서의 전달 및 자체확장인증서의 발급 프로세스를 중개하며, 인증서 및 자체확장인증서를 저장하고 관리하기 위해 사용자 계정을 생성할 수 있다. 즉, 키관리서버(30)는 마스터기기(20)로부터 인증서 및 자체확장인증서를 전송받아 이를 사용자 계정에 저장한 뒤 추가기기(40)에 제공하고, 추가기기(40)로부터는 사용자명, 추가기기명 및 제2 공개키를 전송받아 이를 상기 사용자 계정에 저장한 뒤 마스터기기(20)에 제공할 수 있다.

[0029] 만일 마스터기기(20)에서 자체확장인증서를 발급하여 추가기기(40)에 직접적으로 전송하는 형태를 취하게 하려면, 마스터기기(20) 또는 추가기기(40)가 항상 동작하면서 외부의 접속을 기다리고 있다가 요청이 있으면 응답하는 서버로서의 기능을 가져야 하는데, 이와 같은 경우에는 외부 공격자도 마스터기기(20) 또는 추가기기(40)에 접속을 쉽게 시도할 수 있어서 공격을 받기 쉬워진다는 문제점이 있다.

[0030] 이에 따라, 본 발명에서는 별도의 키관리서버(30)를 두어 이 키관리서버(30)가 마스터기기(20)와 추가기기(40) 사이에서 인증서의 전달 및 자체확장인증서의 발급을 위한 통신을 중개하는 역할을 수행하도록 한다. 즉, 마스터기기(20)와 추가기기(40)는 키관리서버(30)에 대해 클라이언트 입장에서 인증서의 전달 및 자체확장인증서의 발급 프로세스를 수행하도록 하고 있다.

[0031] 도 1에서 점선으로 나타낸 박스는 마스터기기(20) 및 추가기기(40)가 사용자 소유의 컴퓨팅기기임을 의미하며, 비록 도 1에서는 추가기기(40)의 수가 하나인 것으로 도시하였지만 이는 본 발명의 일 실시예를 나타낸 것일 뿐 추가기기(40)의 수는 복수개일 수 있다.

[0032] 본 발명에서는 인증기관(10)으로부터 직접적으로 인증서를 발급받지 않은 추가기기(40)가 외부기기(50)에 사용자 인증을 제공할 수 있도록 하기 위해 추가기기(40)에 인증서의 전달 및 자체확장인증서의 발급 방안에 대해 제안하며, 이하에서는 도 2를 참고하여 보다 상세히 설명하기로 한다.

[0033] 도 2에 나타낸 바와 같이, 본 발명의 일 실시예에 따른 자체확장인증을 이용한 키관리 방법은, 우선 인증서 발급 신청 단계로서, 마스터기기(20)가 제1 공개키 및 제1 개인키를 생성(즉, 제1 키쌍을 생성)하고, 사용자 식별정보 및 상기 제1 공개키를 인증기관에 전송한다(S110).

[0034] 사용자가 자신의 컴퓨팅기기를 개방형 네트워크에서 사용하기 위해서는 공개키 암호방식(public key cryptography)을 사용할 것이 요구되며, 그 공개키 암호방식은 특정 엔티티(entity)의 공개키가 그 엔티티의 것이 맞는지 확인하기 위하여 공개키 기반구조(Public Key Infrastructure; PKI) 기술을 이용한 인증서와 함께 사용되어야 한다. PKI 환경에서 널리 사용되는 공개키 암호 알고리즘에는 RSA 암호기술과 ECC 암호기술이 있으며, 그 중 RSA 암호기술은 알고리즘이 직관적이고 암호화 및 서명을 동일한 알고리즘으로 처리할 수 있다는 점에서 장점을 갖고 있어서 널리 사용되고 있다.

[0035] 이에 따라, 상기 S110 단계에서 마스터기기(20)가 제1 공개키 및 제1 개인키를 생성할 때에는 이러한 RSA 암호기술을 이용할 수 있다. 이 때, 마스터기기(20)는 그 내부에 하드웨어보안모듈을 장착하고 그 하드웨어보안모듈 내부에서 제1 키쌍을 생성할 수 있다.

[0036] 즉, 하드웨어보안모듈이 장착된 마스터기기(20)가 생성하는 제1 키쌍 중 제1 개인키는 그 하드웨어보안모듈 내부에 저장하고 외부로 누출되지 않도록 하며, 제1 공개키만 사용자 식별정보와 함께 인증기관(10)에 전송할 수 있다. 여기서, 마스터기기(20)는 인증기관(10)에 사용자명(예를 들어, 사용자의 ID)을 비롯하여 인증기관의 정책에 따라 요구되는 사용자 식별정보를 전송하게 되는데, 이는 인증기관(10)이 인증서를 발급하기 전에 사용자의 신원을 확인할 수 있도록 하기 위함이다.

[0037] 인증서 신청이 이루어진 다음에는, 인증서 발급 단계로서, 인증기관(10)이 마스터기기(20)에 인증서를 발급한다(S120). 즉, 인증기관(10)이 마스터기기(20)로부터 사용자 식별정보 및 제1 공개키를 전송받을 경우에는 사용자의 신원을 확인하고, 그 후 상기 사용자 식별정보 및 제1 공개키가 포함된 문서에 인증기관의 개인키로 서명한 문서, 즉 인증서를 마스터기기(20)에 발급한다.

[0038] 인증기관(10)이 마스터기기(20)에 발급하는 인증서에는 사용자명 및 제1 공개키가 포함되어 있으며, 그 밖에도 공공의 네트워크에서 인증기관(10)이 사용자에게 부여하는 속성을 제한하기 위하여 유효기간, 키이용 목적, 확

장필드와 같은 복잡한 필드들이 포함되어 있다. 마스터기기(20)가 인증기관(10)으로부터 인증서를 발급받음에 따라, 상기 S110에서 생성된 제1 키쌍은 인증기관(10)에 의해 인증받은 인증키쌍이 된다.

[0039] 마스터기기(20)에 인증서 발급이 이루어진 뒤에는, 사용자등록 단계로서, 마스터기기(20)가 키관리서버(30)에 접속하여 인증서를 그 키관리서버(30)에 전송한다(S130). 즉, 사용자는 마스터기기(20)를 통해 키관리서버(30)에 접속하여 인증기관(10)으로부터 발급받은 인증서를 그 키관리서버(30)에 전송시킬 수 있으며, 이와 같은 인증서의 전송은 마스터기기(20)의 사용자를 키관리서버(30)에 알려줌으로써 키관리서버(30)에 사용자등록을 신청하는 것으로 이해될 수 있다.

[0040] 키관리서버(30)에 전송된 인증서는 키관리서버(30)의 사용자 계정 데이터베이스(미도시)에 저장될 수 있다. 구체적으로, 마스터기기(20)가 키관리서버(30)에 접속될 때, 상기 키관리서버(30)는 사용자 계정을 생성하기 위한 프로그램을 실행시켜 마스터기기(20)의 화면에 제공할 수 있다. 그 뒤 키관리서버(30)는 마스터기기(20)의 키패드나 터치패드 등을 통해 입력되는 사용자 정보(예를 들어, 사용자 ID와 비밀번호)에 따라 데이터베이스에 사용자 계정을 생성한 뒤, 그 사용자 계정에 인증서를 저장할 수 있다. 이와 같이 키관리서버(30)가 사용자 계정에 인증서를 저장하는 것으로 구성할 경우에는, 다수의 사용자가 키관리서버(30)를 함께 사용하는데 있어서 그들 각각의 사용자 정보를 별도의 저장공간에 저장할 수 있기 때문에 효율적인 키관리가 가능해진다.

[0041] 한편, 키관리서버(30)가 마스터기기(20)로부터 인증서를 전송받을 때에는 그 인증서의 유효성을 검증할 수 있다. 인증서의 유효성 검증은 인증기관(10)의 공개키를 이용하여 이루어질 수 있다. 키관리서버(30)는 인증서 검증을 통해 인증서가 유효하다고 판단될 경우에만 인증서를 사용자 계정에 저장하고, 그렇지 않을 경우에는 인증서를 저장하지 않을 수 있다. 키관리서버(30)가 이와 같이 인증서의 유효성을 검증함으로써, 향후 인증서 및 자체확장인증서를 다운로드 받는 추가기기(40)가 외부기기(50)에 대하여 신뢰성 높은 사용자 인증을 제공할 수 있게 된다.

[0042] 키관리서버(30)에 인증서 전송이 이루어진 뒤에는 추가기기(40)에 인증서의 전달 및 자체확장인증서의 발급이 이루어지게 되는데, 이는 기기등록 신청 단계, 기기등록 신청정보 획득 단계, 기기등록 허가 단계 및 기기등록 완료 단계를 거쳐 이루어지게 된다.

[0043] 우선, 기기등록 신청 단계로서, 추가기기(40)가 키관리서버(30)에 접속하여 제2 공개키 및 제2 개인키(즉, 제2 키쌍을 생성)를 생성하고, 사용자명, 추가기기명 및 제2 공개키를 키관리서버(30)에 전송한다(S140). 즉, 사용자는 그 소유기기들 중에서 외부기기(50)에 사용자 인증을 제공하기를 원하는 기기(즉, 인증서 및 자체확장인증서를 다운로드 받기를 원하는 기기)를 통해 키관리서버(30)에 접속할 수 있다. 추가기기(40)에서는 제2 공개키 및 제2 개인키를 생성한 뒤 상기 제2 공개키를 사용자명, 추가기기명과 함께 전송하게 되는데, 이는 마스터기기(20)로 하여금 자체확장인증서를 발급할 수 있도록 하기 위함이다. 그리고 이와 같이 추가기기(40)가 키관리서버(30)에 사용자명, 추가기기명을 전송하는 것은, 추가기기(40)의 사용자 및 기기명을 키관리서버(30)에 알려줌으로써 키관리서버(30)에 그 추가기기(40)의 등록을 신청하는 것을 의미한다.

[0044] 한편, 추가기기(40)가 제2 공개키 및 제2 개인키를 생성할 때에는 상기 S110에서와 같이 RSA 암호기술을 이용할 수 있으며, 이러한 제2 키쌍의 생성은 추가기기(40)의 내부에 장착된 하드웨어보안모듈에서 이루어지는 것이 바람직하다.

[0045] 하드웨어보안모듈이란 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.

[0046] 구체적으로, 요즘 발매되는 최신형 컴퓨터들은 메인보드에 하드웨어 기반의 보안칩인 신뢰플랫폼모듈(TPM)이 장착된 형태로 출시되고 있다. 그리고 스마트폰이나 태블릿 PC 등의 이동통신 단말기들은 통신회사에서 가입자 관리를 위해 이용하는 범용가입자식별모듈인 USIM을 장착하여 사용하게 되는데, 이러한 USIM은 키관리를 비롯해서 여러 가지 보안기능을 구현하는 데에 활용될 수 있다. 또한, 최근에는 근거리 통신기능과 보안기능이 결합된 NFC 칩이 내장된 스마트폰의 보급이 확대되고 있으며, 국내에서는 USB 형태의 인터페이스에 스마트카드칩이 내장된 형태인 USB 보안토큰을 공인인증서의 안전한 저장장치로서 널리 보급하기 위해 노력 중에 있다.

[0047] 이러한 하드웨어보안모듈은 키쌍의 안전한 저장소로서의 역할뿐 아니라 개인키의 외부 누출 없이 키쌍 생성, 전자서명, 서명검증 등이 그 장치 내부에서 안전하게 수행될 수 있도록 한다.

[0048] 이에 따라, 상기 S110 단계에서 이루어지는 제1 공개키 및 제1 개인키의 생성은 마스터기기(20)의 내부에 장착된 하드웨어보안모듈 내부에서 이루어지도록 하고, 상기 S140 단계에서 이루어지는 제2 공개키 및 제2 개인키의

생성은 추가기기(40)의 내부에 장착된 하드웨어보안모듈 내부에서 이루어지도록 하면, 제1 개인키 및 제2 개인키를 외부 공격자의 공격으로부터 보다 안전하게 방어할 수 있게 된다.

[0049] 추가기기(40)가 생성하는 제2 키쌍 중 제2 개인키는 추가기기(40) 내부에 저장하고 외부로 누출되지 않도록 하며, 제2 공개키만 키관리서버(30)에 전송한다.

[0050] 그리고 추가기기(40)가 제2 공개키를 키관리서버(30)에 전송할 때에는 사용자명 및 추가기기명을 함께 전송한다. 예를 들어, 사용자가 추가기기(40)를 통해 키관리서버(30)에 접속할 경우 추가기기(40)의 화면에는 키관리서버(30)에 의해 사용자명과 추가기기명을 각각 입력할 수 있는 창이 제공될 수 있다. 이에 따라, 사용자는 추가기기(40)를 통해 자신을 식별시킬 수 있는 사용자명(예를 들어, 사용자 ID)과, 추가기기(40)를 식별시킬 수 있는 추가기기명(예를 들어, pc1, pc2, phone1, phone2)을 입력할 수 있다. 키관리서버(30)가 추가기기(40)로부터 사용자명, 추가기기명 및 제2 공개키를 전송받을 경우에는, 이를 상기 S130 단계에서 생성한 사용자 계정에 저장할 수 있다.

[0051] 한편, 추가기기(40)가 키관리서버(30)에 사용자명, 추가기기명 및 제2 공개키를 전송할 때에는, 제2 공개키 정보의 유효성과 제2 개인키를 소유하고 있다는 것을 증명하기 위하여 상기 사용자명, 기기명 및 제2 공개키를 제2 개인키로 서명하여 전송할 수도 있다.

[0052] 기기등록 신청이 이루어진 뒤에는, 기기등록 신청정보 획득 단계로서, 마스터기기(20)가 키관리서버(30)에 접속하여 상기 사용자명, 기기명 및 제2 공개키에 대한 정보를 획득한다(S150).

[0053] 구체적으로, 마스터기기(20)가 키관리서버(30)에 접속하게 되면, 마스터기기(20)의 화면에는 상기 S140 단계에서 사용자가 추가기기(40)로 수행한 기기등록 신청 내역이 제공될 수 있다. 이에 따라 사용자는 자신이 추가기기(40)를 이용하여 신청했던 내역과 동일한지 확인(즉, 사용자명이 맞는지, 추가기기명이 맞는지 등을 확인)할 수 있으며, 신청 내역과 동일하다면 키관리서버(30)로부터 마스터기기(20)로 상기 사용자명, 추가기기명 및 제2 공개키에 대한 정보를 다운로드 할 수 있다.

[0054] 마스터기기(20)가 기기등록 신청정보를 획득한 다음에는, 기기등록 허가 단계로서, 마스터기기(20)가 상기 사용자명, 추가기기명 및 제2 공개키가 포함된 문서에 대해, 상기 S110 단계에서 생성되어 상기 S120 단계에서 인증기관(10)에 의해 인증받은 제1 개인키로 서명한 자체확장인증서를 발급하여 이를 키관리서버(30)에 전송한다(S160).

[0055] 여기서, 마스터기기(20)가 자체확장인증서를 발급하는 것은 추가기기(40)의 등록을 허가하는 것을 의미한다.

[0056] 마스터기기(20)가 발급하는 자체확장인증서에는 상기 사용자명, 추가기기명 및 제2 공개키가 포함되어 있으며, 다만 자체확장인증서는 사용자가 소유하는 기기들에 사용자 인증을 자체적으로 확장하기 위해 발급하는 문서이기 때문에 인증서처럼 복잡한 필드들로 구성될 필요는 없다(예를 들어, 자체확장인증서에는 유효기간을 제한할 필요가 없음).

[0057] 마스터기기(20)가 생성하는 자체확장인증서는 키관리서버(30)로 전송되어 키관리서버(30)의 데이터베이스에 저장될 수 있다. 이 때, 키관리서버(30)는 자체확장인증서를 상기 S130 단계에서 생성한 사용자 계정에 저장함으로써 효율적인 키관리가 이루어지도록 할 수 있으며, 이에 따라 키관리서버(30)가 생성한 사용자 계정에는 마스터기기(20)가 인증기관(10)으로부터 발급받은 사용자의 인증서 및 마스터기기(20)가 자체적으로 발급한 사용자의 자체확장인증서가 저장되게 된다.

[0058] 그리고 키관리서버(30)가 자체확장인증서를 전송받을 때에는, 그 자체확장인증서의 유효성을 검증할 수 있다. 자체확장인증서의 유효성 검증은 인증서에 포함되어 있는 제1 공개키를 이용하여 이루어질 수 있다. 키관리서버(30)는 자체확장인증서 검증을 통해 자체확장인증서가 유효하다고 판단될 경우에만 자체확장인증서를 사용자 계정에 저장하고, 그렇지 않을 경우에는 자체확장인증서를 저장하지 않을 수 있다. 키관리서버(30)가 이와 같이 자체확장인증서의 유효성을 검증함으로써, 향후 인증서 및 자체확장인증서를 다운로드 받는 추가기기(40)가 외부기기(50)에 대하여 신뢰성 높은 사용자 인증을 제공할 수 있게 된다.

[0059] 기기등록 허가가 이루어진 뒤에는, 기기등록 완료 단계로서, 추가기기(40)가 키관리서버(30)에 접속하여 인증서 및 자체확장인증서를 다운로드 받는다(S170).

[0060] 구체적으로, 사용자는 기기 등록을 신청했던 추가기기(40)로 키관리서버(30)에 접속한 뒤 사용자명(예를 들어, 사용자 ID)과 추가기기명(예를 들어, pc1)을 입력할 수 있다. 이에 따라, 추가기기(40)의 화면에는 기기등록 허가 내역으로서 마스터기기(20)에 의해 발급이 이루어진 자체확장인증서가 표시될 수 있으며, 키관리서버(30)로

부터 추가기기(40)로 상기 자체확장인증서를 다운로드할 수 있다.

[0061] 추가기기(40)가 키관리서버(30)를 통해 자체확장인증서를 발급받음에 따라, 상기 S140 단계에서 생성된 제2 키쌍은 마스터기기(20)에 의해 자체적으로 인증받은 자체확장인증키쌍이 된다.

[0062] 자체확장인증서는 인증서에 논리적으로 연결되어 있어서 항상 인증서와 함께 사용되므로, 추가기기(40)는 외부기기(50)에 사용자 인증을 제공하기 위해 인증서를 자체확장인증서와 함께 다운로드 받을 필요가 있다. 이에 따라 추가기기(40)에는 인증서 및 자체확장인증서가 저장될 수 있으며, 이로써 기기등록 절차가 모두 완료된다.

[0063] 추가기기(40)는 상기와 같이 발급받은 인증서와 자체확장인증서를 가지고 외부기기(50)에 대하여 사용자 인증을 제공할 수 있다.

[0064] 대표적인 사례로서 전자서명 로그인을 들 수 있다. 예를 들어, 사용자가 추가기기(40)를 통해 제3자가 운영하는 서버(외부기기(50))의 로그인 페이지에 접속할 경우, 그 외부기기(50)에서는 추가기기(40)에 사용자 인증을 요청할 수 있다. 이 경우, 추가기기(40)는 인증기관(10)으로부터 직접적으로 인증서를 발급받은 기기가 아니기 때문에, 외부기기(50)로 하여금 사용자의 신원 및 추가기기(40)가 사용자의 소유임을 확인할 수 있도록 하여야 한다.

[0065] 이에 따라, 추가기기(40)가 외부기기(50)로부터 사용자의 인증을 요청받는 경우(예를 들어, 추가기기(40)는 외부기기(50)로부터 로그인을 요청받을 수 있다)에는 추가기기(40)가 그 외부기기(50)에 사용자 인증을 제공한다. 즉, 사용자 인증 단계로서, 추가기기(40)는 상기 S170 단계에서 자체확장인증을 받은 제2 개인키로 서명한 서명문(즉, 전자서명)을 생성할 수 있으며, 그 서명문을 상기 S170 단계에서 다운로드 받은 인증서 및 자체확장인증서와 함께 외부기기(50)에 제공하게 된다(S180).

[0066] 이 경우, 외부기기(50)는 추가기기(40)에 대한 사용자 인증을 수행하기 위하여 검증 단계를 거치게 된다(S190). 즉, 외부기기(50)는 추가기기(40)로부터 제공받은 인증서, 자체확장인증서 및 서명문을 검증한 후에 로그인을 허용(사용자 검증)할 수 있다.

[0067] 구체적으로, 외부기기(50)는 추가기기(40)로부터 제공받은 인증서를 인증기관(10)의 공개키를 이용하여 검증함으로써 사용자의 신원을 확인할 수 있다.

[0068] 그리고 외부기기(50)는 추가기기(40)로부터 제공받은 자체확장인증서를 상기 인증서에 포함된 제1 공개키를 이용하여 검증함으로써 추가기기(40)가 사용자의 소유임을 확인할 수 있다.

[0069] 마지막으로 외부기기(50)는 추가기기(40)로부터 제공받은 서명문을 상기 자체확장인증서에 포함된 제2 공개키를 이용하여 검증함으로써 그 서명문의 유효성을 확인할 수 있다.

[0070] 외부기기(50)는 상기와 같은 3단계 검증 과정을 거침으로써, 사용자가 추가기기(40)를 사용하고 있는 환경에서도 사용자를 인증할 수 있게 된다.

[0071] 이상에서 살펴본 바와 같이, 본 발명에 의하면 하나의 마스터기기(20)가 인증기관(10)으로부터 인증서를 발급받은 뒤 이에 기반하여 자체확장인증서를 발급하여 키관리서버(30)에 전송하고, 추가기기(40)가 상기 키관리서버(30)에 접속하여 외부기기(50)에 사용자 인증을 제공하는데 필요한 인증서 및 자체확장인증서를 다운로드 받을 수 있도록 구성되기 때문에, 사용자는 자신이 소유하는 모든 기기에 인증기관(10)으로부터 인증서를 발급받을 필요 없이 사용자 스스로 인증키(보다 구체적으로는, 자체확장인증을 받은 제2 공개키 및 제2 개인키)를 생성하고 관리할 수 있어 키관리의 편의성이 향상된다.

[0072] 이러한 본 발명은 유무선으로 구성되는 전통적인 컴퓨팅 환경뿐만 아니라, 모바일, 사물인터넷, 클라우드 환경에서 키관리를 수행할 때에도 편리하게 이용될 수 있다.

[0073] 예를 들어, 사물인터넷 환경에서는 센서기기, 게이트웨이, 클라우드 서비스 플랫폼, 사용자 단말기기와 같이 많은 기기들 사이에 상호 인증이 필요하다. 이러한 사물인터넷 환경에서 본 발명을 적용하면, 사용자는 인증기관으로부터 발급받는 인증서 및 그 인증서에 기반하여 발급되는 자체확장인증서에 의해 많은 소유기기들의 멤버십을 체계적으로 관리할 수 있게 된다. 아울러 타인의 센서기기, 단말기 등과도 인증서 및 자체확장인증서에 기반하여 명확한 접근제어 및 권한제어 기능을 제공할 수도 있다.

[0074] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능한 것은 물론이다. 따라서, 본 발명의 기술적 사상은 특허청구범위에 의해서만 파악되어야 하고, 이의 균등

또는 등가적 변형 모두는 본 발명의 기술적 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0075] 10: 인증기관

20: 마스터기기

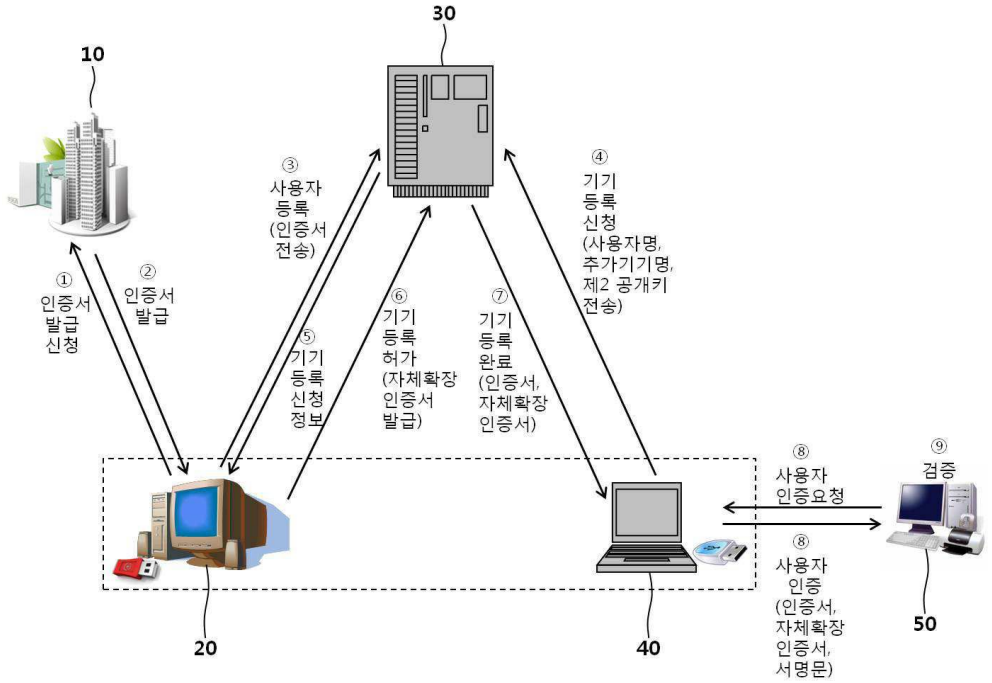
30: 키관리서버

40: 추가기기

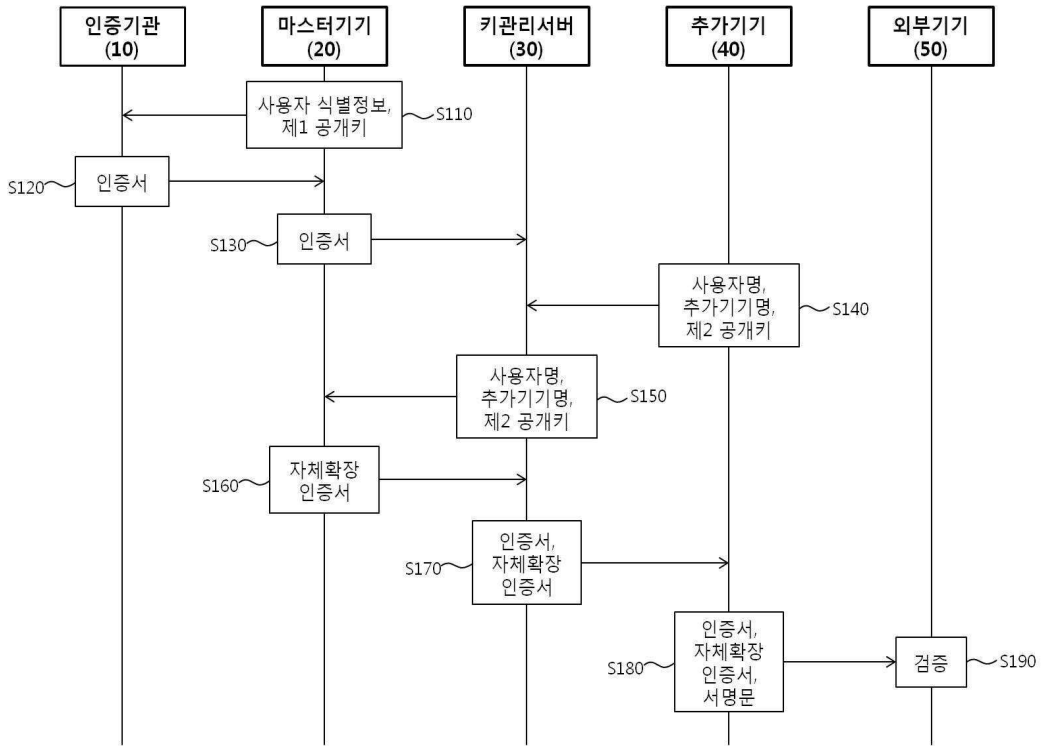
50: 외부기기

도면

도면1



도면2


인증기관
(10)
마스터기기
(20)
키관리서버
(30)
추가기기
(40)
외부기기
(50)
사용자 식별정보,
제1 공개키
S110
S120
인증서
S130
인증서
사용자명,
추가기기명,
제2 공개키
S140
사용자명,
추가기기명,
제2 공개키
S150
S160
자체확장
인증서
S170
인증서,
자체확장
인증서
S180
인증서,
자체확장
인증서,
서명문
검증
S190