(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0059643
(43) 공개일자 2015년06월01일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/3263 (2013.01)
H04L 9/0825 (2013.01)
(21) 출원번호 10-2015-0060013(분할)
(22) 출원일자 2015년04월28일
심사청구일자 없음
(62) 원출원 특허 10-2013-0142088
원출원일자 2013년11월21일

(71) 출원인
주식회사 씽크풀
서울특별시 영등포구 국제금융로 70, 15층(여의도동, 미원빌딩)
(72) 발명자
김동진
서울특별시 서초구 서초중앙로 200, 12동 901호 (서초동, 삼풍아파트)
김대진
서울특별시 종로구 평창12길 8-22, 금강파크빌리지 1동 101호 (평창동)
(뒷면에 계속)
(74) 대리인
심충섭

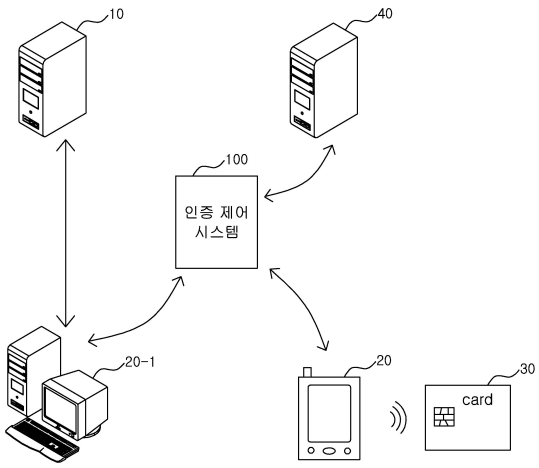
전체 청구항 수 : 총 18 항

(54) 발명의 명칭 **비대칭 암호화 방식의 인증 제어방법 및 인증제어시스템**

(57) 요 약

비대칭 암호화 방식의 인증 제어방법 및 이를 위한 시스템이 개시된다. 상기 비대칭 암호화 방식의 인증 제어방법은 인증제어시스템이, 인증요청 장치로부터 출력된 비대칭 암호화방식을 이용한 인증요청을 수신하는 단계 및 상기 인증제어시스템이, 수신된 상기 인증요청을 소정의 인증조건의 만족여부에 따라 선택적으로 인증기관 시스템으로 전송함으로써 상기 인증요청에 상응하는 인증이 선택적으로 수행되도록 인증제어를 수행하는 단계를 포함하며, 상기 인증조건은 상기 인증요청에 상응하는 사용자의 단말기로부터 상기 단말기에 소정의 이벤트가 발생한 경우에 출력되는 이벤트 발생신호가 수신되는지 여부인 것을 특징으로 한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/3247 (2013.01)
(72) 발명자
심충섭
서울특별시 용산구 효창원로15길 16, 102동 307호 (신창동, 세방리버하이빌)
고진숙
경기 부천시 원미구 소향로 206, 907동 1506호 (중동, 미리내마을아파트)

명 세 서

청구범위

청구항 1

인증제어시스템이, 인증요청 장치로부터 출력된 비대칭 암호화방식을 이용한 인증요청을 수신하는 단계; 및

상기 인증제어시스템이, 수신된 상기 인증요청을 소정의 인증조건의 만족여부에 따라 선택적으로 인증기관 시스템으로 전송함으로써 상기 인증요청에 상응하는 인증이 선택적으로 수행되도록 인증제어를 수행하는 단계를 포함하며,

상기 인증조건은,

상기 인증요청에 상응하는 사용자의 단말기로부터 상기 단말기에 소정의 이벤트가 발생한 경우에 출력되는 이벤트 발생신호가 수신되는지 여부인 것을 특징으로 하는 비대칭 암호화 방식의 인증 제어방법.

청구항 2

제1항에 있어서, 상기 비대칭 암호화 방식의 인증 제어방법은,

상기 인증제어시스템이 상기 인증요청을 수신하기 전에 상기 이벤트 발생신호를 상기 단말기로부터 수신하는 단계를 더 포함하며,

상기 인증요청에 상응하는 인증이 선택적으로 수행되도록 인증제어를 수행하는 단계는,

상기 인증제어시스템이 상기 이벤트 발생신호에 기초하여 설정되는 소정의 인증 가능기간 내에 상기 인증요청이 수신되어야 상기 인증조건을 만족했다고 판단하는 단계를 포함하는 비대칭 암호화 방식의 인증 제어방법.

청구항 3

제2항에 있어서, 상기 인증 가능기간은,

상기 이벤트 발생신호가 상기 인증제어시스템으로 수신된 시점 또는 상기 이벤트가 발생한 시점으로부터 미리 결정된 기간 내이거나,

상기 단말기로부터 입력된 소정의 기간정보에 상응하는 기간인 것을 특징으로 하는 비대칭 암호화 방식의 인증 제어방법.

청구항 4

제2항에 있어서, 상기 인증요청에 상응하는 인증이 선택적으로 수행되도록 인증제어를 수행하는 단계는,

상기 인증제어시스템이 상기 인증 가능기간에 복수의 인증요청이 수신되어도, 미리 결정된 우선순위에 해당하는 인증요청에 대해서만 인증제어를 수행하는 것을 특징으로 하는 비대칭 암호화 방식의 인증 제어방법.

청구항 5

제1항에 있어서, 상기 비대칭 암호화 방식의 인증 제어방법은,

상기 인증제어시스템 또는 상기 인증요청을 위해 상기 인증 요청장치에 설치된 인증서 클라이언트가 상기 이벤트의 실행을 상기 단말기 또는 상기 인증 요청장치에 요청하는 단계; 및

상기 요청에 응답하여 상기 인증제어시스템은 상기 단말기로부터 상기 이벤트 발생신호를 수신하는 단계를 더

포함하는 비대칭 암호화 방식의 인증 제어방법.

청구항 6

제1항에 있어서, 상기 비대칭 암호화 방식의 인증 제어방법은,

상기 인증제어시스템이 수신된 상기 이벤트 발생신호에 기초하여 인증이 허용될 상기 사용자를 특정하는 단계를 더 포함하며,

상기 인증요청에 상응하는 인증이 선택적으로 수행되도록 인증제어를 수행하는 단계는,

상기 인증요청이 특정된 상기 사용자에 상응하여야, 상기 인증요청에 대한 인증제어를 수행하는 단계를 포함하는 비대칭 암호화 방식의 인증 제어방법.

청구항 7

제6항에 있어서, 상기 인증제어시스템이 수신된 상기 이벤트 발생신호에 기초하여 인증이 허용될 상기 사용자를 특정하는 단계는,

상기 인증제어시스템이 상기 이벤트 발생신호를 전송한 상기 단말기의 명의자를 상기 사용자로 특정하는 단계; 또는

상기 인증제어시스템이 상기 이벤트의 발생을 위해 상기 단말기와 근거리 무선통신을 수행하는 근거리 무선통신 장치의 명의자를 상기 사용자로 특정하는 단계를 포함하는 비대칭 암호화 방식의 인증 제어방법.

청구항 8

제1항에 있어서, 상기 비대칭 암호화 방식의 인증 제어방법은,

상기 인증제어시스템이 수신된 상기 인증요청이 미리 설정된 필터링 조건을 만족하는지를 판단하는 단계를 더 포함하며,

상기 인증제어시스템은 상기 필터링 조건을 만족하는 인증요청에 대해서만 인증조건을 만족하여야 상기 인증요청을 상기 인증기관 시스템으로 전송하는 상기 인증제어를 수행하고, 상기 필터링 조건을 만족하지 않는 인증요청에 대해서는 상기 인증조건의 만족여부와 무관하게 상기 인증요청을 상기 인증기관 시스템으로 전송하는 비대칭 암호화 방식의 인증 제어방법.

청구항 9

제8항에 있어서, 상기 필터링 조건은,

상기 인증 요청장치의 속성, 상기 인증 요청장치와 연결된 서비스 시스템의 속성, 인증요청 시간, 또는 상기 인증요청에 상응하는 금액 중 적어도 하나에 의해 결정되는 것을 특징으로 하는 비대칭 암호화 방식의 인증 제어방법.

청구항 10

제1항에 있어서, 상기 특정 이벤트는,

상기 단말기와 소정의 근거리 무선통신장치가 근거리 무선통신을 하는 이벤트; 또는

상기 단말기 또는 상기 단말기와 유무선 네트워크를 통해 연결된 소정의 인증시스템에 의해 상기 사용자가 인증되는 이벤트;

중 적어도 하나를 포함하는 것을 특징으로 하는 비대칭 암호화 방식의 인증 제어방법.

청구항 11

제1항에 있어서, 상기 단말기는,

상기 인증요청 장치와는 별개의 상기 사용자의 단말기인 것을 특징으로 하는 비대칭 암호화 방식의 인증 제어방법.

청구항 12

제1항 내지 제11항 중 어느 한 항에 기재된 방법을 수행하기 위한 프로그램을 기록한 컴퓨터 판독가능한 기록매체.

청구항 13

인증요청 장치로부터 출력된 인증요청을 수신하기 위한 요청 처리부;

상기 인증요청에 상응하는 사용자의 단말기로부터 상기 단말기에 소정의 이벤트가 발생한 경우에 출력되는 이벤트 발생신호를 수신하기 위한 이벤트 처리부;

상기 이벤트 발생신호가 수신되는지 여부에 따라 소정의 인증조건의 만족여부를 판단하는 판단부; 및

상기 인증조건의 만족여부에 따라 상기 인증요청을 선택적으로 인증기관 시스템으로 전송함으로써 상기 인증요청에 상응하는 인증이 선택적으로 수행되도록 인증제어를 수행하는 제어부를 포함하는 인증제어시스템.

청구항 14

제13항에 있어서, 상기 이벤트 처리부는,

상기 인증요청을 수신하기 전에 상기 이벤트 발생신호를 상기 단말기로부터 수신하며,

상기 판단부는,

상기 이벤트 발생신호에 기초하여 설정되는 소정의 인증 가능기간 내에 상기 인증요청이 수신되어야 상기 인증조건을 만족했다고 판단하는 인증제어시스템.

청구항 15

제14항에 있어서, 상기 제어부는,

상기 인증 가능기간에 수신된 복수의 인증요청 중 미리 결정된 우선순위에 해당하는 인증요청만 상기 인증기관 시스템으로 전송하는 것을 특징으로 하는 인증제어시스템.

청구항 16

제13항에 있어서, 상기 이벤트 처리부는,

상기 인증요청 장치에 설치된 인증서 클라이언트 또는 상기 단말기에 설치된 클라이언트 시스템을 통해 상기 이벤트의 실행을 요청하고, 상기 요청에 응답하여 상기 단말기로부터 상기 이벤트 발생신호를 수신하는 인증제어시스템.

청구항 17

제13항에 있어서, 상기 판단부는,

수신된 상기 이벤트 발생신호에 기초하여 인증이 허용될 상기 사용자를 특정하고,

상기 제어부는,

상기 인증요청이 특정된 상기 사용자에 상응하여야, 상기 인증요청에 대한 인증제어를 수행하는 인증제어시스템.

청구항 18

제13항에 있어서, 상기 판단부는,

수신된 상기 인증요청이 미리 설정된 필터링 조건을 만족하는지를 판단하고,

상기 제어부는,

상기 필터링 조건을 만족하는 인증요청에 대해서만 인증조건을 만족하여야 상기 인증요청을 상기 인증기관 시스템으로 전송하는 상기 인증제어를 수행하고, 상기 필터링 조건을 만족하지 않는 인증요청에 대해서는 상기 인증조건의 만족여부와 무관하게 상기 인증요청을 상기 인증기관 시스템으로 전송하는 인증제어시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 비대칭 암호화 방식의 인증 제어방법 및 그 시스템에 관한 것으로, 보다 상세하게는 비대칭 암호화 방식을 통한 인증을 수행할 때 인증이 가능한 상황을 제한적으로 설정함으로써 보안성을 높일 수 있는 인증 제어방법 및 그 시스템에 관한 것이다.

[0002] 특히 인증을 수행하는 시스템이 집중되어 있는 환경(예컨대, 공인 인증서를 이용한 인증 등)에 적합한 인증 제어방법 및 그 시스템에 관한 것이다.

배 경 기 술

[0003] 네트워크의 발달로 인해 많은 사람이 네트워크 시스템에 접속하여 다양한 서비스 또는 기능들을 이용하고 있다. 이러한 다양한 서비스를 이용하면서 서비스를 요청하는 사용자의 정당성을 인증하는 것에 대한 중요성은 갈수록 커지고 있다.

[0004] 이러한 사용자의 정당성의 인증 즉, 서비스를 요청하는 자가 상기 서비스의 사용을 허락받은 정당한 사용자임을 인증하는 방식으로는 대칭 암호화 방식 및 비대칭 암호화 방식이 있다.

[0005] 대칭형 암호화 방식은 동일한 키를 공유하고 있는 양당사자 간에 인증을 수행하는 방식으로 종래의 다양한 인증 방식(예컨대, 비밀번호, 비밀패턴, 생체정보 등)에 이용되어 왔다. 하지만 이러한 대칭형 암호화 방식이 갖는 상대적인 보안상의 취약점으로 인해 최근에는 비대칭형 암호화 방식을 이용한 사용자 인증이 널리 이용되고 있다.

[0006] 비대칭형 암호화 방식은 서로 다른 키를 가지고 있는 양당사자간에 인증을 수행하는 방식으로, 현재 전자상거래 등에 널리 사용되는 공인인증서 등을 이용한 사용자 인증이 그 대표적인 일예라 할 수 있다.

[0007] 비대칭형 암호화 방식의 일예로 서로 쌍을 이루는 공개키와 개인키를 이용하여 양당사자를 인증하는 방식이 존재하는데, 이러한 비대칭 암호화 방식은 공개키만을 제3자에게 공유하고 개인키는 별도로 타인에게 유통할 필요가 없어서, 상대적으로 대칭키를 타인에게 유통해야 하는 대칭형 암호화 방식에 비해 상대적으로 보안성이 높은 방식으로 알려져 있다.

[0008] 하지만, 이러한 비대칭 암호화 방식 역시 공격자(예컨대, 해커 등)에 의해 부정하게 인증이 성공하는 사례가 빈번히 발생하고 있어서 그 피해는 매우 심각한 수준에 이르고 있다. 비대칭 암호화 방식의 보안성의 취약점으로

는 개인키가 한번 유출되면, 더 이상 정상적인 인증 기능을 수행하지 못한다는 데에 있다.

[0009] 그런데 최근 들어 모바일 디바이스(예컨대, USB 저장장치, 스마트 폰 등)의 다양화로 인해 개인키 자체를 저장하고 있는 디바이스가 다양해지고 있어서 개인키(예컨대, 공인인증서 등) 자체가 유출될 위험이 매우 증가하고 있는 실정이다. 또한, 비록 개인키 자체가 암호화된 상태로 다양한 디바이스들에 저장되고는 있지만, 암호화된 개인키로부터 개인키를 추출하기 위한 패스워드가 다양한 공격기법(예컨대, 키 로깅(key logging), 메모리 해킹, 피싱(pishing) 또는 파밍(pharming) 등)에 의해 노출될 가능성이 있다. 따라서 설령 암호화되어 있더라도 개인키 자체가 유출되는 경우에는 심각한 보안상의 위협이 될 수 있다. 특히 개인키를 보관하는 디바이스가 다수화 또는 다양화됨으로 인해 위험은 배가 되고 있는 실정이다.

[0010] 더구나, 비대칭 암호화 방식 중 대표적으로 많이 쓰이고 있는 공인인증서는 금융기관의 금융거래 또는 전자상거래 등과 같이 다양한 용도에 범용적으로 사용될 수 있는 환경으로 설계가 되어 있고, 이로 인해 거래 상대방 또는 전자서명을 인증하는 주체가 개인이라기보다는 공인된 기관 또는 주체에 의해 수행된다는 특징이 있다. 따라서 공인인증서를 이용한 인증의 경우에는, 제한된 개인들끼리 서로를 인증하기 위한 환경이 아니라, 인증측에서는 다수의 불특정 사용자를 인증하게 되므로 특히 개인키를 포함하고 있는 인증서가 유출되는 경우에는 매우 심각한 보안상의 위협이 된다.

[0011] 즉, 공격자는 사용자의 공인인증서 및 공인인증서의 인증 비밀번호까지 획득하게 되면 언제든지 상기 사용자를 사칭한 전자서명을 할 수 있게 된다. 그리고 공인인증서 및 인증 비밀번호가 탈취되고 사용자를 사칭한 공격자의 공격이 발생하는 경우, 이에 대해 방어를 할 수 있는 방법이 마땅히 마련되지 못하고 있는 실정이다.

[0012] 이러한 문제점을 해결하기 위해 공인인증서를 재발급할 수 있는 단말기를 특정 단말기(지정 단말기)로 제한하는 방식이 강제적으로 시행되고 있기도 하다. 하지만 이러한 방식 역시 이미 공인인증서가 탈취된 상태이고, 정당 사용자가 이를 인지하지 못하거나 공인인증서를 재발급 받지 않는 경우에는 부정 인증을 막지 못하는 문제점이 여전히 존재하게 된다.

선행기술문헌

특허문헌

[0013] (특허문헌 0001) 1. 한국특허출원 공개번호 10-2010-0110064 "공인인증서 사용제한 시스템 및 그 방법"

(특허문헌 0002) 2. 한국특허출원 공개번호 10-2010-0125518 "공인인증서 사용제한 시스템 및 그 방법"

발명의 내용

해결하려는 과제

[0014] 따라서 본 발명이 이루고자 하는 기술적인 과제는 비대칭 암호화 방식을 통한 인증방법에 있어서, 인증을 수행하겠다는 의사표시를 정당한 사용자가 명시적으로 수행한 경우에만 제한적으로 상기 인증이 수행될 수 있도록 함으로써, 개인키가 유출된 경우에도 이러한 의사표시가 없는 경우에는 인증이 수행되지 않도록 하는 방법 및 시스템을 제공하는 것이다.

[0015] 또한, 이러한 의사표시를 비교적 간단하면서도 보안성이 높은 방식으로 정당한 사용자가 서비스 제어시스템에 전달할 수 있는 방법 및 시스템을 제공하는 것이다.

[0016] 또한, 인증요청 중에서도 특정 조건(예컨대, 필터링 조건)을 만족하는 요청에 대해서만 선택적으로 본 발명의 기술적 사상이 적용될 수 있도록 함으로써, 사용자의 인증 이용 형태에 맞추어 적응적으로 본 발명의 기술적 사상에 따른 보안 정책을 설정할 수 있는 방법 및 시스템을 제공하는 것이다.

[0017] 또한, 사용의사를 표현하는데 사용되는 단말기를 인증을 요청하는 장치와 별개의 사용자 명의의 단말기로 설정할 수 있도록 함으로써, 인증을 요청하는 장치가 공격을 당하는 경우에 허위의 사용의사를 표현하는 것을 차단할 수 있으며, 2팩터 인증 또는 그 이상의 보안성이 높은 인증이 수행될 수 있도록 하는 방법 및 시스템을 제공하는 것이다.

과제의 해결 수단

[0018] 상기 기술적 과제를 해결하기 위한 본 발명의 실시 예에 따른 비대칭 암호화 방식의 인증 제어방법은 인증제어시스템이, 인증요청 장치로부터 출력된 비대칭 암호화방식을 이용한 인증요청을 수신하는 단계 및 상기 인증제어시스템이, 수신된 상기 인증요청을 소정의 인증조건의 만족여부에 따라 선택적으로 인증기관 시스템으로 전송함으로써 상기 인증요청에 상응하는 인증이 선택적으로 수행되도록 인증제어를 수행하는 단계를 포함하며, 상기 인증조건은 상기 인증요청에 상응하는 사용자의 단말기로부터 상기 단말기에 소정의 이벤트가 발생한 경우에 출력되는 이벤트 발생신호가 수신되는지 여부인 것을 특징으로 한다.

[0019] 상기 비대칭 암호화 방식의 인증 제어방법은 상기 인증제어시스템이 상기 인증요청을 수신하기 전에 상기 이벤트 발생신호를 상기 단말기로부터 수신하는 단계를 더 포함하며, 상기 인증요청에 상응하는 인증이 선택적으로 수행되도록 인증제어를 수행하는 단계는, 상기 인증제어시스템이 상기 이벤트 발생신호에 기초하여 설정되는 소정의 인증 가능기간 내에 상기 인증요청이 수신되어야 상기 인증조건을 만족했다고 판단하는 단계를 포함할 수 있다.

[0020] 상기 인증 가능기간은 상기 이벤트 발생신호가 상기 인증제어시스템으로 수신된 시점 또는 상기 이벤트가 발생한 시점으로부터 미리 결정된 기간 내이거나, 상기 단말기로부터 입력된 소정의 기간정보에 상응하는 기간인 것을 특징으로 할 수 있다.

[0021] 상기 인증요청에 상응하는 인증이 선택적으로 수행되도록 인증제어를 수행하는 단계는 상기 인증제어시스템이 상기 인증 가능기간에 복수의 인증요청이 수신되어도, 미리 결정된 우선순위에 해당하는 인증요청에 대해서만 인증제어를 수행하는 것을 특징으로 할 수 있다.

[0022] 상기 비대칭 암호화 방식의 인증 제어방법은 상기 인증제어시스템 또는 상기 인증요청을 위해 상기 인증 요청장치에 설치된 인증서 클라이언트가 상기 이벤트의 실행을 상기 단말기 또는 상기 인증 요청장치에 요청하는 단계 및 상기 요청에 응답하여 상기 인증제어시스템은 상기 단말기로부터 상기 이벤트 발생신호를 수신하는 단계를 더 포함할 수 있다.

[0023] 상기 비대칭 암호화 방식의 인증 제어방법은 상기 인증제어시스템이 수신된 상기 이벤트 발생신호에 기초하여 인증이 허용될 상기 사용자를 특정하는 단계를 더 포함하며, 상기 인증요청에 상응하는 인증이 선택적으로 수행되도록 인증제어를 수행하는 단계는 상기 인증요청이 특정된 상기 사용자에 상응하여야, 상기 인증요청에 대한 인증제어를 수행하는 단계를 포함할 수 있다.

[0024] 상기 인증제어시스템이 수신된 상기 이벤트 발생신호에 기초하여 인증이 허용될 상기 사용자를 특정하는 단계는 상기 인증제어시스템이 상기 이벤트 발생신호를 전송한 상기 단말기의 명의자를 상기 사용자로 특정하는 단계 또는 상기 인증제어시스템이 상기 이벤트의 발생을 위해 상기 단말기와 근거리 무선통신을 수행하는 근거리 무선통신장치의 명의자를 상기 사용자로 특정하는 단계를 포함할 수 있다.

[0025] 상기 비대칭 암호화 방식의 인증 제어방법은 상기 인증제어시스템이 수신된 상기 인증요청이 미리 설정된 필터링 조건을 만족하는지를 판단하는 단계를 더 포함하며, 상기 인증제어시스템은 상기 필터링 조건을 만족하는 인증요청에 대해서만 인증조건을 만족하여야 상기 인증요청을 상기 인증기관 시스템으로 전송하는 상기 인증제어를 수행하고, 상기 필터링 조건을 만족하지 않는 인증요청에 대해서는 상기 인증조건의 만족여부와 무관하게 상기 인증요청을 상기 인증기관 시스템으로 전송할 수 있다.

[0026] 상기 필터링 조건은 상기 인증 요청장치의 속성, 상기 인증 요청장치와 연결된 서비스 시스템의 속성, 인증요청 시간, 또는 상기 인증요청에 상응하는 금액 중 적어도 하나에 의해 결정되는 것을 특징으로 할 수 있다.

[0027] 상기 특정 이벤트는 상기 단말기와 소정의 근거리 무선통신장치가 근거리 무선통신을 하는 이벤트 또는 상기 단말기 또는 상기 단말기와 유무선 네트워크를 통해 연결된 소정의 인증시스템에 의해 상기 사용자가 인증되는 이벤트 중 적어도 하나를 포함하는 것을 특징으로 할 수 있다.

[0028] 상기 단말기는 상기 인증요청 장치와는 별개의 상기 사용자의 단말기인 것을 특징으로 할 수 있다. 상기 비대칭 암호화 방식의 인증 제어방법은 프로그램을 기록한 컴퓨터 판독가능한 기록매체에 기록될 수 있다.

[0029] 상기 기술적 과제를 해결하기 위한 인증제어 시스템은 인증요청 장치로부터 출력된 인증요청을 수신하기 위한 요청 처리부, 상기 인증요청에 상응하는 사용자의 단말기로부터 상기 단말기에 소정의 이벤트가 발생한 경우에

출력되는 이벤트 발생신호를 수신하기 위한 이벤트 처리부, 상기 이벤트 발생신호가 수신되는지 여부에 따라 소정의 인증조건의 만족여부를 판단하는 판단부, 및 상기 인증조건의 만족여부에 따라 상기 인증요청을 선택적으로 인증기관 시스템으로 전송함으로써 상기 인증요청에 상응하는 인증이 선택적으로 수행되도록 인증제어를 수행하는 제어부를 포함한다.

[0030] 상기 이벤트 처리부는 상기 인증요청을 수신하기 전에 상기 이벤트 발생신호를 상기 단말기로부터 수신하며, 상기 판단부는 상기 이벤트 발생신호에 기초하여 설정되는 소정의 인증 가능기간 내에 상기 인증요청이 수신되어야 상기 인증조건을 만족했다고 판단할 수 있다.

[0031] 상기 제어부는 상기 인증 가능기간에 수신된 복수의 인증요청 중 미리 결정된 우선순위에 해당하는 인증요청만 상기 인증기관 시스템으로 전송하는 것을 특징으로 할 수 있다.

[0032] 상기 이벤트 처리부는 상기 인증요청 장치에 설치된 인증서 클라이언트 또는 상기 단말기에 설치된 클라이언트 시스템을 통해 상기 이벤트의 실행을 요청하고, 상기 요청에 응답하여 상기 단말기로부터 상기 이벤트 발생신호를 수신할 수 있다.

[0033] 상기 판단부는 수신된 상기 이벤트 발생신호에 기초하여 인증이 허용될 상기 사용자를 특정하고, 상기 제어부는 상기 인증요청이 특정된 상기 사용자에 상응하여야, 상기 인증요청에 대한 인증제어를 수행할 수 있다.

[0034] 상기 판단부는 수신된 상기 인증요청이 미리 설정된 필터링 조건을 만족하는지를 판단하고, 상기 제어부는 상기 필터링 조건을 만족하는 인증요청에 대해서만 인증조건을 만족하여야 상기 인증요청을 상기 인증기관 시스템으로 전송하는 상기 인증제어를 수행하고, 상기 필터링 조건을 만족하지 않는 인증요청에 대해서는 상기 인증조건의 만족여부와 무관하게 상기 인증요청을 상기 인증기관 시스템으로 전송할 수 있다.

발명의 효과

[0035] 본 발명의 기술적 사상에 의하면, 사용자가 인증을 수행하겠다는 의사를 밝히는 경우에만(예컨대, 사용자의 단말기에 특정 이벤트가 발생한 경우에만) 인증이 가능하도록 함으로써, 부정한 사용자에게 인증을 받을 수 있는 가능성을 큰 폭으로 줄일 수 있는 효과가 있다.

[0036] 또한, 사용자가 인증 수행 의사를 사용자 명의의 장치(예컨대, 핸드폰 및/또는 IC 카드, OTP장치 등)를 적어도 하나 소지하고 있거나, 또는 사용자 본인의 생체정보를 통해서만 밝힐 수 있도록 함으로써, 다중 팩터 인증(2팩터 인증 또는 3팩터 인증 등)이 가능한 효과가 있다. 즉, 공격자가 온라인 등을 통해 공인인증서 등의 개인키를 탈취하고 있더라도 정당 사용자의 인증 수행 의사를 밝힐 수 있는 장치(예컨대, 단말기)를 소지할 수 없으므로 공격자가 인증이 성공하는 것을 방어할 수 있는 효과가 있다.

[0037] 또한, 본 발명의 기술적 사상에 따르면 개인키가 유출되는 경우라도 인증기관 또는 인증기관의 전단에서 한번 더 인증이 수행되는 효과가 있으므로, 인증의 수행이 중앙집중식으로 이루어질 수 있는 환경에 특히 유리하게 적용될 수 있는 효과가 있다.

[0038] 또한, 특정 조건에 해당하는 인증요청에 대해서만 선택적으로 본 발명의 기술적 사상을 적용할 수 있으므로, 사용자는 자신의 인증이용 행태에 따라 적응적인 보안정책의 설정이 가능하며 서비스 이용에도 불편함을 줄일 수 있는 효과가 있다.

[0039] 또한, 인증을 수행하겠다는 의사표시가 근거리 무선통신인 경우, 간단히 근거리 무선통신을 통해 상기 인증 수행 의사를 밝힐 수 있으므로, 사용자의 입장에서도 절차적으로 간편한 효과가 있다.

도면의 간단한 설명

[0040] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 간단한 설명이 제공된다.

도1은 본 발명의 실시 예에 따른 비대칭 암호화 방식의 인증 제어방법을 위한 개략적인 시스템을 나타낸다.

도2는 본 발명의 실시 예에 따른 필터링 조건을 설명하기 위한 도면이다.

도3은 본 발명의 실시 예에 따른 인증제어시스템의 개략적인 구성을 설명하기 위한 도면이다.

도4는 본 발명의 일 실시 예에 따른 클라이언트 시스템의 개략적인 구성을 설명하기 위한 도면이다.

도5는 본 발명의 일 실시 예에 따른 비대칭 암호화 방식의 인증 제어방법의 개략적인 과정을 설명하기 위한 플로우차트이다.

도6은 본 발명의 다른 실시 예에 따른 비대칭 암호화 방식의 인증 제어방법의 개략적인 과정을 설명하기 위한 플로우차트이다.

발명을 실시하기 위한 구체적인 내용

[0041] 본 발명과 본 발명의 동작상의 이점 및 본 발명의 실시에 의하여 달성되는 목적을 충분히 이해하기 위해서는 본 발명의 바람직한 실시 예를 예시하는 첨부 도면 및 첨부 도면에 기재된 내용을 참조하여야만 한다.

[0042] 또한, 본 명세서에 있어서는 어느 하나의 구성요소가 다른 구성요소로 데이터를 '전송'하는 경우에는 상기 구성요소는 상기 다른 구성요소로 직접 상기 데이터를 전송할 수도 있고, 적어도 하나의 또 다른 구성요소를 통하여 상기 데이터를 상기 다른 구성요소로 전송할 수도 있는 것을 의미한다.

[0043] 반대로 어느 하나의 구성요소가 다른 구성요소로 데이터를 '직접 전송'하는 경우에는 상기 구성요소에서 다른 구성요소를 통하지 않고 상기 다른 구성요소로 상기 데이터가 전송되는 것을 의미한다.

[0044] 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시 예를 설명함으로써, 본 발명을 상세히 설명한다. 각 도면에 제시된 동일한 참조부호는 동일한 부재를 나타낸다.

[0045] 본 발명의 기술적 사상은 반드시 비대칭 암호화 방식의 인증시에만 이용되어야 하는 것은 아니며, 어떠한 인증 방식에도 이용될 수 있음은 당업자에게 용이하게 추론될 수 있을 것이다. 이하에서는 설명의 편의를 위해 비대칭 암호화 방식으로 인증을 수행하는 경우를 일 예로 설명하도록 한다.

[0046] 도1은 본 발명의 실시 예에 따른 비대칭 암호화 방식의 인증 제어방법을 위한 개략적인 시스템을 나타낸다.

[0047] 도1을 참조하면, 본 발명의 실시 예에 따른 비대칭 암호화 방식의 인증 제어방법(이하, '인증 제어방법')을 구현하기 위해서는 인증제어시스템(100)이 구비될 수 있다. 상기 인증제어시스템(100)은 소정의 데이터 프로세싱 장치(예컨대, 서버 등)에 설치되어 구현될 수 있다. 상기 인증제어시스템(100)이 상기 데이터 프로세싱 장치에 설치된다고 함은, 상기 인증제어시스템(100)의 기능을 구현하기 위한 소프트웨어가 상기 데이터 프로세싱 장치에 설치되어, 상기 소프트웨어와 상기 데이터 프로세싱 장치의 하드웨어가 유기적으로 결합되어 본 발명의 기술적 사상을 구현함을 의미할 수 있다.

[0048] 일 실시 예에 의하면, 상기 인증제어시스템(100)은 인증요청이 수신되면, 수신된 인증요청에 대해 비대칭 암호화 방식으로 인증을 수행하는 인증기관 시스템에 설치될 수도 있다. 즉, 상기 인증제어시스템(100)은 인증기관 시스템(40)의 데이터 프로세싱 장치에 설치될 수도 있다. 이러한 경우, 상기 인증제어시스템(100)은 상기 인증기관 시스템(40)과는 동일한 적어도 하나의 물리적 장치를 이용하면서도, 기능적으로는 독립적인 시스템으로 취급될 수 있다. 이러한 경우 상기 인증제어시스템(100)과 상기 인증기관 시스템(40)은 소정의 함수 호출, 클래스(class) 또는 라이브러리(library)의 공유, 파라미터(parameter)의 전달을 통해 필요한 정보 또는 신호를 교환할 수 있다.

[0049] 물론 구현 예에 따라서는 도1에 도시된 바와 같이 상기 인증제어시스템(100)은 상기 인증기관 시스템(40)과는 별개의 독립적인 데이터 프로세싱 장치에 설치될 수도 있다. 이러한 경우에는 상기 인증제어시스템(100) 즉, 상기 데이터 프로세싱 장치와 상기 인증기관 시스템(40)은 유선 또는 무선 네트워크를 통해 통신을 수행하면서 본 발명의 기술적 사상을 구현할 수 있다.

[0050] 또한, 구현 예에 따라서는, 상기 인증제어시스템(100)의 일부의 구성은 상기 인증기관 시스템(40)에 설치되고, 나머지 일부의 구성은 상기 인증기관 시스템(40)과는 별개의 데이터 프로세싱 장치로 구현될 수도 있다. 따라서 본 명세서에서 정의되는 상기 인증제어시스템(100)의 일부의 기능은 상기 인증기관 시스템(40)에서 구현될 수도 있음은 본 발명의 기술분야의 평균적 전문가는 용이하게 추론할 수 있을 것이다.

[0051] 이하에서는 설명의 편의를 위해 상기 인증제어시스템(100)은 상기 인증기관 시스템(40)과는 별개의 물리적 장치인 데이터 프로세싱 장치에 설치되어 구현되는 경우를 일예로 설명하지만, 본 발명의 권리범위는 이에 한정되지는 않는다.

[0052] 이하 본 명세서에서는 설명의 편의를 위해 비대칭 암호화 방식을 이용한 인증의 일예로 공인인증서를 이용하는

경우를 주로 설명하지만, 그 밖에 다양한 비대칭 암호화 방식을 이용한 인증에도 본 발명의 기술적 사상이 적용될 수 있음은 물론이다.

[0053] 공인인증서를 이용한 인증의 경우에는 인증이 공인된 인증기관 시스템에 의해 수행되므로, 다수의 인증 요청장치(예컨대, 20-1)로부터 출력된 다수의 인증요청은 상기 인증기관 시스템(40)으로 집중되는 구조를 가질 수 있다. 이처럼 인증요청이 특정 주체 또는 특정 시스템으로 집중되는 환경에서 본 발명의 기술적 사상은 더욱 효과적으로 적용될 수 있다. 왜냐하면, 종래의 비대칭 암호화 방식은 개인키는 정당한 사용자만이 소지하고 있다는 가정을 가지며 이러한 가정이 어긋나는 경우(즉, 개인키가 타인에게 유출되는 경우)에는 유효한 인증을 수행할 수 없는 반면, 도1에 도시된 바와 같이 본 발명의 기술적 사상에 의하면 상기 인증기관 시스템(40)으로 인증요청이 집중되는 경우에는 본 발명의 기술적 사상에 의한 인증제어시스템(100)을 통해 중앙집중식으로 추가적인 보안 수단이 구비되는 것과 같은 효과를 얻을 수 있다.

[0054] 종래에는 소정의 인증요청장치(이하, '요청장치', 20-1)가 소정의 서비스 시스템(예컨대, 10)에 접속하여 서비스(예컨대, 로그인, 전자상거래, 금융거래, 증명서의 발급 등)를 이용하고자 하는 경우, 상기 서비스 시스템(10)은 공인인증서를 이용한 인증(본 명세서에서는 공인인증서를 이용한 전자서명을 포함하는 의미로 정의됨)을 상기 요청장치(예컨대, 20-1)로 요구하였다. 상기 요청장치(예컨대, 20-1)에는 개인키를 포함하는 공인인증서가 저장되어 있거나, 또는 상기 공인인증서를 저장하고 있는 디바이스가 상기 요청장치(예컨대, 20-1)에 연결될 수 있다. 그러면 상기 요청장치(예컨대, 20-1)에는 인증을 위한 인증서 클라이언트가 실행되고, 상기 인증서 클라이언트를 통해 사용자가 인증서의 비밀번호를 입력하면, 상기 인증서 클라이언트는 상기 비밀번호를 이용하여 개인키를 복호화하고 복호화된 개인키를 상기 인증기관 시스템(40)으로 전송할 수 있다. 복호화된 개인키는 상기 인증기관 시스템(40)에 저장된 공개키를 통해 인증이 될 수 있으며, 인증이 성공하면 상기 인증기관 시스템(40)은 상기 요청장치(예컨대, 20-1) 즉, 상기 인증서 클라이언트로 인증이 성공하였음을 통지하게 되고, 상기 인증서 클라이언트는 상기 서비스 시스템(예컨대, 10)으로 인증완료 신호를 전송하거나 전자서명을 하게 된다.

[0055] 본 발명의 기술적 사상에 의하면, 상기 요청장치(예컨대, 20-1)로부터 복호화된 개인키를 포함하는 인증요청이 출력되면 상기 인증요청은 요청장치(예컨대, 20-1)와 상기 인증기관 시스템(40) 사이에 존재하는 상기 인증제어시스템(100)으로 전송될 수 있다. 그리고 상기 인증제어시스템(100)은 본 발명의 기술적 사상에 따라 소정의 인증조건이 만족하는 경우에만, 상기 인증요청을 상기 인증기관 시스템(40)으로 전송할 수 있다. 이처럼 본 발명의 기술적 사상에 따라 인증요청이 소정의 인증조건을 만족하는지 여부를 판단하고, 판단결과에 따라 선택적으로 수신된 인증요청을 상기 인증기관 시스템(40)으로 전송하는 과정을 본 명세서에서는 인증제어로 정의하기로 한다.

[0056] 이처럼 상기 인증제어시스템(100)에 의해 수행되는 인증제어를 통해 본 발명의 기술적 사상은 구현될 수 있다. 상기 인증제어가 성공되기 위해서는 인증요청에 상응하는 정당한 사용자로부터 출력된 인증수행 의사가 상기 인증제어시스템(100)에 수신되어야 할 수 있다. 따라서 정당한 사용자로부터 상기 인증수행 의사가 출력되지 않은 이상, 인증요청은 거부될 수 있다. 결국, 부정한 사용자가 개인키를 소지하고 있다고 하더라도(즉, 인증서를 소지하고 인증서의 비밀번호를 알고 있다고 하더라도), 정당한 사용자가 인증수행 의사를 출력하지 않은 이상 부정한 사용자에 의한 인증은 허용되지 않을 수 있다.

[0057] 또한, 본 발명의 기술적 사상에 의한 인증제어는 모든 인증요청에 대해 수행되는 것이 아니라, 미리 정해진 소정의 조건(이하, 필터링 조건)에 부합하는 인증요청에 대해서만 수행될 수도 있다. 따라서 상기 필터링 조건에 부합하지 않는 인증요청은 종래와 같이 인증조건의 만족여부와 무관하게 상기 인증기관시스템(40)으로 전송되어 인증이 될 수도 있다. 이처럼 상기 필터링 조건을 만족하는 인증요청에 대해서만 인증제어를 수행함으로써 사용자가 자주 사용하는 인증행태에 대해서는 종래의 방식대로 인증이 수행되고, 사용자가 특별히 보안성을 높여야겠다고 판단한 인증행태에 대해서만 인증제어가 수행되도록 할 수도 있다. 이를 통해 사용자의 사용성이 크게 저하되지 않고도 높은 보안성을 제공할 수 있는 효과가 있다.

[0058] 사용자의 인증수행 의사는 사용자의 단말기(예컨대, 20)를 이용하여 사용자가 특정 행위를 수행함으로써 표현될 수 있다. 즉, 상기 단말기(예컨대, 20)에서 상기 특정 행위에 상응하는 소정의 이벤트가 발생한 경우에 상기 사용자는 인증수행 의사를 표현한 것으로 취급될 수 있다. 상기 단말기(예컨대, 20)는 상기 인증제어시스템(100)에 미리 등록된 특정 단말기이거나, 상기 사용자 명의의 단말기일 수 있다. 또한, 상기 이벤트는 상기 단말기(예컨대, 20)와 소정의 근거리 무선통신장치(30)가 근거리 무선통신을 수행하는 이벤트일 수도 있다. 물론, 이외에도 상기 단말기(예컨대, 20)를 통해 정당한 사용자가 상기 이벤트를 수행한 것임을 특정할 수 있는 다양한 이벤트가 본 발명에 적용될 수 있다. 상기 이벤트가 상기 단말기(예컨대, 20)에서 발생하면 상기

단말기(예컨대, 20)는 이벤트 발생신호를 상기 인증제어시스템(100)으로 출력할 수 있다.

[0059] 상기 인증기관시스템(40)은 공인인증서를 이용한 인증을 수행하는 인증기관에 상응하는 시스템일 수 있다. 상기 인증기관시스템(40)은 구현 예에 따라서는 상기 서비스시스템(예컨대, 10)과 동일한 시스템일 수도 있다. 즉, 서비스시스템(예컨대, 10)이 직접 인증서를 이용한 인증요청을 인증할 수도 있다. 예컨대, 상기 인증기관시스템(40)은 소정의 웹서비스(예컨대, 온라인 금융서비스)를 제공하는 웹서비스 주체의 시스템(예컨대, 금융기관 시스템)일 수도 있고, 상기 웹서비스 주체의 시스템(예컨대, 금융기관 시스템)과 연동하여 인증을 수행하는 공인인증서의 공인인증기관 시스템(예컨대, 금융결제원, 증권전산 등의 시스템)일 수도 있다. 서비스의 종류에 따라 인증기관시스템(40)의 구현 예 또한 다양할 수 있음을 본 발명의 기술분야의 평균적 전문가는 용이하게 추론할 수 있을 것이다.

[0060] 또한, 본 발명의 기술적 사상을 구현하기 위해서는 사용자의 단말기(20 또는 20-1)가 구비될 수 있다. 또한 실시 예에 따라 상기 사용자의 단말기(20 또는 20-1)와 근거리 무선통신을 수행할 수 있는 근거리 무선통신장치(30)가 더 구비될 수 있다.

[0061] 상기 인증제어시스템(100)은 상기 인증기관시스템(40)을 제어하여, 요청장치(예컨대, 20-1)로부터 상기 인증기관시스템(40)으로 출력되는 인증요청이 인증되도록 할지 또는 인증이 아예 수행되지 않도록 할지를 제어할 수 있다.

[0062] 이를 위해 상기 인증제어시스템(100)은 요청장치(예컨대, 20-1)로부터 인증기관시스템(40)으로 출력되는 인증요청을 수신하고, 수신된 인증요청을 상기 인증기관 시스템(40)으로 전달하도록 구현될 수 있다. 이러한 경우에는 상기 인증요청를 전달하는지 여부에 따라 인증이 수행되도록 할지여부를 제어할 수 있다. 따라서 상기 인증기관시스템(40)은 특별한 변경을 하지 않아도 본 발명의 기술적 사상이 적용될 수 있는 효과가 있다.

[0063] 다른 구현 예에 의하면, 상기 인증요청은 상기 인증제어시스템(100)을 거쳐서 상기 인증기관시스템(40)으로 전송되는 것이 아니라, 상기 인증기관시스템(40)으로 직접 전송될 수도 있다. 이러한 경우에는, 상기 인증기관시스템(40)으로 이미 전송된 인증요청 또는 전송될 인증요청에 대해 인증을 수행할지 여부를 제어하기 위한 제어신호를 상기 인증제어시스템(100)이 상기 인증기관시스템(40)으로 전송함으로써, 상기 인증제어시스템(100)은 상기 인증기관시스템(40)을 제어할 수도 있다. 물론, 이러한 경우에는 상기 인증제어시스템(100)은 상기 인증기관시스템(40)으로부터 상기 인증요청이 언제 수신되었는지 또는 어떤 사용자 명의의 인증요청인지에 대한 정보를 수신할 수도 있다. 또는, 상기 제어신호에 상기 이벤트 발생신호가 수신된 시점에 대한 정보 또는 이벤트 발생시점에 대한 정보를 포함하여 전송함으로써, 최종적으로는 상기 인증기관시스템(40)이 수신된 정보에 기초하여 상기 인증요청을 인증할지 여부를 결정할 수도 있다.

[0064] 필요에 따라 상기 인증제어시스템(100)은 상기 인증요청의 수신시점을 확인할 수 있다. 상기 수신시점은 상기 인증요청이 상기 인증기관시스템(40)으로 직접 전송되는 경우에는 상기 인증기관시스템(40)에 수신된 시점을 의미할 수 있으며, 상기 인증요청이 상기 인증제어시스템(100)으로 수신되는 경우에는 상기 인증제어시스템(100)에 수신된 시점을 의미할 수 있다.

[0065] 그러면 상기 인증제어시스템(100)은 상기 수신시점이 후술할 바와 같은 이벤트 발생신호에 기초하여 설정되는 인증 가능기간 내에 포함되는 경우에만 상기 인증기관시스템(40)이 인증을 수행하도록 제어할 수 있다.

[0066] 상기 인증제어시스템(100)은 소정의 단말기(예컨대, 20)로부터 수신되는 이벤트 발생신호가 수신되어야만 소정의 인증 가능기간을 설정하고, 상기 인증 가능기간 내에 상기 인증요청이 상기 인증제어시스템(100) 또는 상기 인증기관 시스템(40)으로 수신되어야만 인증을 하도록 제어함으로써 본 발명이 목적하는 보안성을 취득할 수 있다. 따라서 상기 인증 가능기간이 아니면 정당한 사용자에 의한 인증요청이든 부정한 사용자에 의한 인증요청이든 관계없이 인증은 수행되지 않을 수 있다.

[0067] 상기 이벤트 발생신호를 출력하는 사용자의 단말기(예컨대, 20)는 요청장치(예컨대, 20-1)와 독립적인 단말기일 수 있다. 이처럼 인증을 요청하는 요청장치(예컨대, 20-1)와 별도의 단말기(예컨대, 20)를 통해 이벤트 발생신호를 출력하도록 함으로써, 2팩터 인증이 가능한 효과가 있다. 구현 예에 따라서는, 상기 이벤트 발생신호가 상기 단말기(예컨대, 20)뿐만 아니라 사용자 명의의 다른 장치, 예컨대, 근거리 무선통신장치(사용자의 신용카드, IC 카드, OTP 장치 등)까지 소지하고 있어야만 출력되도록 구현될 수도 있다. 예컨대, 상기 단말기(예컨대, 20)와 상기 근거리 무선통신장치가 근거리 무선통신을 수행하는 이벤트가 발생하여야 상기 단말기(예컨대, 20)가 이벤트 발생신호를 출력하도록 구현될 수도 있다. 이러한 경우에는 3팩터 인증이 가능해지므로 매우 뛰어난 보안성이 제공될 수 있는 효과가 있다.

[0068] 물론, 상기 단말기(예컨대, 20)에 의해 사용자가 인증되면 상기 이벤트 발생신호가 상기 인증제어시스템(100)으로 출력될 수도 있다. 예컨대, 상기 단말기(예컨대, 20)에 본 발명의 기술적 사상을 구현하기 위한 소정의 클라이언트(소프트웨어)가 설치되어 있으며, 상기 클라이언트에 의해 사용자가 소정의 방식으로 인증될 수도 있다. 그리고 인증이 되면 상기 단말기(예컨대, 20)는 상기 인증제어시스템(100)으로 이벤트 발생신호를 출력할 수 있다.

[0069] 상기 소정의 방식은 예컨대, 상기 단말기(예컨대, 20)에 소정의 인증정보가 미리 저장되어 있고, 상기 인증정보를 이용하여 인증이 되는 방식일 수 있다. 상기 인증정보는 대칭키(예컨대, 비밀번호, 비밀패턴, 생체정보 등)를 이용한 인증일 수도 있다. 구현 예에 따라서는 비대칭키를 이용한 인증방식이 이용될 수도 있다. 이러한 경우에는 상기 단말기(예컨대, 20)가 소정의 인증시스템(미도시)과 통신을 함으로써 사용자가 인증될 수도 있다. 상기 비대칭키를 이용한 인증방식 이외에도 OTP 등을 이용한 방식이 존재할 수 있다. 어떠한 경우든 상기 단말기(예컨대, 20)는 상기 사용자의 인증에 참여할 수 있다.

[0070] 이처럼 사용자 명의의 상기 단말기(예컨대, 20)를 통해 사용자가 인증되면, 상기 이벤트 발생신호는 상기 인증제어시스템(100)으로 출력될 수 있다.

[0071] 결국, 본 발명의 기술적 사상에 의하면 사용자의 인증수행 의사는 사용자가 상기 인증기관시스템(40)에 접속하여 소정의 방식으로 자신을 인증한 후 서비스를 사용할 의사표시를 표현하는 것이 아니라, 사용자 명의의 단말기(예컨대, 20)에 의해 소정의 이벤트를 발생시키는지 여부에 따라 수행될 수 있다. 즉, 사용자가 소정의 단말기(예컨대, 20)를 통해 인증기관시스템(40)에 접속하여 사용자 인증(예컨대, 로그인, 공인인증서, OTP 등)을 거친 후, 사용자가 인증이 되면 서비스를 사용하겠다는 의사표시를 하는 것인 경우에는, 상기 사용자 인증이 뚫리는 경우(즉, 공격자에 의한 인증이 성공하는 경우) 공격자가 얼마든지 임의로 인증 수행의사를 할 수 있으므로 종래의 사용자 인증방식으로 사용자를 인증한 후 서비스를 제공하는 것에 비해 큰 효과가 없을 수 있다.

[0072] 하지만, 본 발명의 기술적 사상에 의하면, 상기 인증기관시스템(40) 또는 상기 인증제어시스템(100)에 접속하여 인증을 수행하는 것이 아니라, 정당한 사용자가 상기 단말기(예컨대, 20)를 통해 인증수행 의사를 표시 하지 않은 경우에는 인증이 수행되지 않게 된다. 따라서 본 발명의 기술적 사상에 의하면 사용자 명의의 단말기(예컨대, 20)를 소지하고 있지 않은 이상 상기 사용자의 대칭키 또는 비대칭키가 유출된다고 하더라도 인증이 정상적으로 수행되지 못하게 할 수 있는 효과가 있다.

[0073] 상기 이벤트 발생신호는 하나의 신호가 아니라, 본 명세서에서 정의되는 기능을 수행하는 복수의 신호들의 조합일 수 있다. 즉, 이벤트 발생신호는 1회성으로 상기 인증제어시스템(100)으로 전송될 필요는 없다.

[0074] 한편, 전술한 필터링 조건에 대해서는 도2를 참조하여 설명하도록 한다.

[0075] 도2는 본 발명의 실시 예에 따른 필터링 조건을 설명하기 위한 도면이다.

[0076] 도2를 참조하면, 상기 필터링 조건을 정의하기 위한 속성으로 인증을 요청하는 요청장치(예컨대, 20-1)의 속성, 상기 서비스 시스템(예컨대, 10)의 속성, 또는 서비스 요청시간, 서비스에 상응하는 금액이 특정될 수 있는 경우에는 상기 금액 등이 포함될 수 있다.

[0077] 예컨대, 요청장치(예컨대, 20-1)의 속성(예컨대, 요청 단말기의 IP가 해외 IP인지 여부 등)이 필터링 조건으로 설정될 수 있다. 구현 예에 따라서는, 상기 서비스 시스템(예컨대, 10)의 속성(예컨대, 웹 서비스를 제공하는 웹 서비스 시스템의 종류(예컨대, 온라인 쇼핑몰 시스템, 게임사 시스템, 금융기관 시스템, 이동통신사 시스템 등))의 속성이 상기 필터링 조건으로 설정될 수도 있다. 상기 서비스 시스템(예컨대, 10)은 예컨대, 온라인 결제 등과 같이 상기 요청장치(예컨대, 20-1)가 접속해 있는 상태에서 상기 요청장치(예컨대, 20-1)로 인증을 요청하는 시스템을 의미할 수 있다.

[0078] 따라서 사용자는 이러한 서비스 시스템(예컨대, 10)의 속성을 필터링 조건을 정의하는 속성으로 정의할 수 있으므로, 예컨대, 사용자는 온라인 쇼핑몰에 대해서는 본 발명의 기술적 사상이 적용되지 않도록 할 수 있고, 게임 사이트에서는 본 발명의 기술적 사상이 적용되도록 설정할 수 있다.

[0079] 예컨대, 도2에 도시된 바와 같이 상기 요청장치(예컨대, 20-1)로 인증을 요구하는 서비스 시스템(예컨대, 금융기관 시스템, 웹 서비스 시스템 등, 10)이 존재할 수도 있다. 이러한 경우에는 상기 서비스 시스템(예컨대, 10)의 속성이 필터링 조건으로 설정될 수도 있다.

[0080] 또한, 상기 필터링 조건은 도2에 도시된 바와 같이 공인인증서들(예컨대, 인증서1 및 인증서2) 각각에 대해 설

정될 수도 있음은 물론이다.

[0081] 또한, 상기 필터링 조건의 속성으로 인증요청 시간이 포함될 수도 있다. 예컨대, 인증서1에 대해서는 인증요청 시간이 21시에서 06시까지는 원칙적으로 본 발명의 기술적 사상에 따라 인증제어가 수행되는 시간으로 설정될 수 있으며, 인증서2에 대해서는 인증요청 시간이라는 속성으로는 필터링 조건이 설정되어 있지 않을 수 있다. 즉, 인증서2를 이용한 인증요청은 서비스 시스템(예컨대, 10)이 해외 시스템 또는 은행 시스템인 경우에만 본 발명의 기술적 사상에 따른 인증제어가 수행되도록 설정될 수도 있다.

[0082] 또한, 상기 필터링 조건의 속성으로 인증금액(예컨대, 전자상거래, 결제 또는 이체 등의 거래의 가치)이 포함될 수도 있다. 물론, 인증금액에 따라 필터링 조건을 정의하는 경우에는, 기존의 공인인증서를 이용한 인증의 경우에는 인증대상(즉, 거래대상)의 정보를 인증기관이 알 수 없는 경우도 있지만, 본 발명의 기술적 사상을 위해 거래대상(즉, 전자서명의 대상이 되는 거래)에 대한 정보가 인증기관 즉, 인증기관 시스템(40)으로 전송되도록 구현될 수도 있다.

[0083] 도2에서는 서비스가 공인인증서를 이용한 인증 서비스인 경우를 일예로 설명하였지만, 서비스의 종류 또는 구현예에 따라 필터링 조건을 정의하는 속성은 다양할 수 있음은 물론이다.

[0084] 결국, 요청장치(예컨대, 20-1)의 속성 또는 서비스 시스템(예컨대, 10)의 속성에 따라 다양한 필터링 조건이 정의될 수 있다. 또한, 본 발명의 기술적 사상은 사용자 또는 인증제어시스템(100)에 의해 상기 필터링 조건이 정의될 수 있다. 따라서 사용자는 자신의 인증 이용행태에 따라 적응적으로 필터링 조건을 정의할 수 있는 효과도 있다. 왜냐하면, 비록 본 발명의 기술적 사상에 따른 인증수행 의사 표시가 비교적 간단한 절차(예컨대, 단말기(예컨대, 20)와 근거리 무선통신장치(30)의 근거리 무선통신)만으로도 수행될 수 있더라도, 자주 사용하는 인증 또는 크게 중요하지 않은 인증을 위해 매번 인증수행 의사 표시를 해야 하는 경우에는 번거로움이 있을 수도 있기 때문이다. 따라서 사용자는 자신이 잘 이용하지 않는 인증행태 또는 특히 보안성이 필요한 인증행태를 상기 필터링 조건으로 정의함으로써 가능한 한 서비스 이용에 불편을 느끼지 않으면서도 보안성은 높일 수 있는 효과가 있다.

[0085] 상기 인증제어시스템(100)은 사용자의 인증수행 의사가 표시된 것임을 나타내는 신호 즉, 이벤트 발생신호가 수신되면, 상기 이벤트 발생신호에 기초하여 인증 가능기간을 설정할 수 있다.

[0086] 상기 인증 가능기간은 상기 인증제어시스템(100)이 제한적으로 인증을 허용하도록 상기 인증기관 시스템(40)을 제어하는 제한된 기간을 의미할 수 있다. 즉, 상기 인증 가능기간에 인증요청이 상기 인증제어시스템(100) 또는 상기 인증기관 시스템(40)으로 수신되어야 상기 인증제어시스템(100)은 수신된 인증요청을 인증할 수 있다.

[0087] 일예에 의하면, 사용자는 인증요청을 하기 전에 인증수행 의사의 표시를 수행하여야 할 수 있다. 즉, 상기 인증요청의 수신시점 전에 이벤트 발생신호가 수신되어야 할 수 있다. 이러한 경우에는 인증 가능기간은 상기 이벤트 발생신호가 수신된 시점으로부터 미리 설정된 기간일 수 있으며, 수초, 수분, 또는 수십 분으로 설정될 수 있다.

[0088] 구현 예에 따라서는, 상기 사용자는 스스로 인증 가능기간을 설정할 수도 있다. 이러한 경우 사용자는 후술할 바와 같이 본 발명의 기술적 사상을 위한 클라이언트 시스템을 통해 인증 가능기간으로 설정할 기간정보를 입력할 수 있으며, 입력된 기간정보는 상기 이벤트 발생신호에 포함되어 또는 이벤트 발생신호와는 별개로 상기 인증제어시스템(100)으로 전송될 수 있다. 그러면, 상기 인증제어시스템(100)은 상기 기간정보에 상응하는 기간을 인증 가능기간으로 설정할 수 있다. 이러한 경우에는 상대적으로 긴 시간(예컨대, 몇 시간 또는 며칠 등) 동안 사용자가 해당 서비스를 이용하고자 하는 경우일 수 있다. 그리고 상기 인증 가능기간이 상대적으로 긴 시간일 수 있으므로, 상기 인증 가능기간 동안에는 다시 사용자가 인증 수행의사 표시를 위해 특정 이벤트를 수행하여야 할 필요는 없을 수도 있다. 물론, 인증 가능기간이 도과하면, 다시 인증은 수행되지 않을 수 있다.

[0089] 사용자는 이벤트 발생신호를 상기 인증제어시스템(100)으로 출력하기 위해 소정의 이벤트에 상응하는 특정 행위를 상기 사용자의 단말기(예컨대, 20)를 통해 수행하여야 할 수 있다. 상기 특정 행위는 상기 특정 행위가 정당한 사용자(카드(30) 명의자 또는 단말기(예컨대, 20)의 명의자에 의해 수행되는 것임을 파악할 수 있는 행위이면 족하다. 사용자가 자신의 단말기(예컨대, 20)를 이용하여 특정 행위를 수행하면, 결과적으로 상기 단말기(예컨대, 20)에는 상기 특정 행위에 상응하는 특정 이벤트가 발생할 수 있다.

[0090] 상기 특정 행위는 후술할 클라이언트 시스템(200)이 사용자를 인증하기 위해 수행하여야할 행위일 수 있다. 상기 클라이언트 시스템(200)은 미리 등록된 인증정보(예컨대, 비밀번호, 비밀패턴, 생체정보 등)를 이용하여 사

용자를 인증할 수 있다.

[0091] 구현 예에 따라, 상기 특정 행위는 상기 클라이언트 시스템(200)과 연결될 수 있는 소정의 네트워크 시스템(미도시)에 의해 사용자가 인증되기 위해 수행하여야할 행위일 수도 있다. 예컨대, 공인인증서, OTP, 또는 보안카드를 이용한 인증 등이 수행될 수 있다. 사용자는 상기 단말기(예컨대, 20)를 통해 상기의 인증을 수행할 수 있다.

[0092] 한편, 상기 특정 행위는 소정의 근거리 무선통신장치(30)가 상기 사용자의 단말기(20)와 근거리 무선통신(예컨대, NFC 통신)이 수행되는 행위일 수도 있다. 그러면, 상기 특정 행위에 상응하는 이벤트는 상기 단말기(20)가 상기 근거리 무선통신장치(30)와 근거리 무선통신을 수행하는 이벤트일 수 있다.

[0093] 이러한 경우에는 상기 특정 행위를 수행한 사용자가 상기 근거리 무선통신장치(30)와 상기 단말기(20)를 모두 소지하고 있음이 인증되는 효과가 있다. 사용자는 단말기(20)와 상기 근거리 무선통신장치(30)를 단순히 근거리 무선통신(예컨대, NFC 태깅)하는 행위만 수행하여 본 발명의 기술적 사상에 따라 인증을 수행하겠다는 의사표시를 할 수 있으므로, 사용자의 입장에서는 절차적으로 매우 간편한 효과가 있다.

[0094] 상기 단말기(예컨대, 20) 즉, 클라이언트 시스템(200)은 상기 근거리 무선통신장치(30)가 정당한 장치 즉, 사용자 명의의 장치인지를 인증할 수도 있다. 예컨대, 상기 클라이언트 시스템(200)에 미리 상기 사용자 명의의 근거리 무선통신장치(30)의 식별정보가 저장되어 있을 수 있으며, 상기 클라이언트 시스템(200)은 상기 근거리 무선통신장치(30)와 근거리 무선통신을 수행하면 근거리 무선통신장치(30)의 식별정보를 확인함으로써 근거리 무선통신장치(30)의 정당성을 인증할 수도 있다. 또는 종래의 스마트카드에 사용되는 크립토그램(cryptogram)을 이용하는 인증이 이용될 수도 있다. 또는 IC카드 등에 1회성 정보(예컨대, 랜덤 넘버 또는 OTP 등)를 생성할 수 있는 모듈이 탑재되고, 상기 1회성 정보를 이용한 인증이 이용될 수도 있다. 이처럼 상기 클라이언트 시스템(200)에 의해 상기 근거리 무선통신장치(30)가 인증되어야 상기 이벤트 발생신호가 상기 인증제어시스템(100)으로 출력될 수도 있다.

[0095] 이러한 기술적 사상을 구현하기 위한 본 발명의 실시 예에 따른 인증제어시스템(100)의 개략적인 구성은 도 3에 도시된다.

[0096] 도3은 본 발명의 실시 예에 따른 인증제어시스템의 개략적인 구성을 설명하기 위한 도면이다.

[0097] 도3을 참조하면, 본 발명의 실시 예에 따른 인증제어시스템(100)은 제어부(110), 이벤트 처리부(120), 요청 처리부(130), 및 판단부(140)를 포함할 수 있다.

[0098] 상기 인증제어시스템(100)은 본 발명의 기술적 사상을 구현하기 위해 필요한 하드웨어 리소스(resource) 및/또는 소프트웨어를 구비할 수 있으며, 반드시 하나의 물리적인 구성요소를 의미하거나 하나의 장치를 의미하는 것은 아니다. 즉, 상기 인증제어시스템(100)은 본 발명의 기술적 사상을 구현하기 위해 구비되는 하드웨어 및/또는 소프트웨어의 논리적인 결합을 의미할 수 있으며, 필요한 경우에는 서로 이격된 장치에 설치되어 각각의 기능을 수행함으로써 본 발명의 기술적 사상을 구현하기 위한 논리적인 구성들의 집합으로 구현될 수도 있다. 또한, 상기 인증제어시스템(100)은 본 발명의 기술적 사상을 구현하기 위한 각각의 기능 또는 역할별로 별도로 구현되는 구성들의 집합을 의미할 수도 있다. 예컨대, 상기 인증제어시스템(100)은 상기 인증기관 시스템(40)에 일부가 구비되어 구현될 수도 있다.

[0099] 또한, 본 명세서에서 '~부' 또는 '모듈'이라 함은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 '~부' 또는 모듈은 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스(resource)의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것은 아님은 본 발명의 기술분야의 평균적 전문가에게는 용이하게 추론될 수 있다.

[0100] 상기 제어부(110)는 본 발명의 기술적 사상을 구현하기 위하여 다른 구성요소들(예컨대, 이벤트 처리부(120), 요청 처리부(130), 및/또는 판단부(140) 등)의 리소스 및/또는 기능을 제어할 수 있다.

[0101] 상기 이벤트 처리부(120)는 상기 사용자의 단말기(예컨대, 20)와 통신을 수행할 수 있다. 특히 상기 이벤트 처리부(120)는 상기 단말기(예컨대, 20)로부터 이벤트 발생신호를 수신할 수 있다. 상기 이벤트 발생신호는 전술한 바와 같이 사용자가 인증을 수행하겠다는 의사표시를 나타내는 신호일 수 있다. 상기 이벤트 발생신호는 상기 단말기(예컨대, 20)에 특정 이벤트가 발생한 경우에만 상기 단말기(예컨대, 20)로부터 상기 이벤트 처리부(120)로 출력되는 신호일 수 있다.

[0102] 상기 요청 처리부(130)는 상기 요청장치(예컨대, 20-1)로부터 상기 인증기관 시스템(40)으로 출력되는 인증요청을 수신할 수 있다. 또는 상기 요청 처리부(130)는 상기 인증요청의 수신시점을 확인할 수 있다. 일예에 의하면, 상기 인증요청은 상기 인증제어시스템(100)으로 수신될 수도 있고, 이러한 경우에 상기 수신시점은 상기 인증제어시스템(100)이 수신한 수신시점일 수도 있다. 구현에 따라서는 상기 인증요청은 상기 인증기관 시스템(40)으로 전송될 수도 있다. 이러한 경우에는 상기 수신시점은 상기 인증기관 시스템(40)이 상기 인증요청을 수신한 시점일 수도 있다.

[0103] 상기 판단부(140)는 수신된 인증요청이 인증조건을 만족하는지 여부를 확인할 수 있다. 상기 인증조건은 단순히 상기 인증요청에 상응하는 사용자의 단말기(예컨대, 20)로부터 상기 이벤트 발생신호가 수신되었는지 여부만일 수도 있다. 구현 예에 따라서는, 상기 인증요청이 상기 이벤트 발생신호에 기초하여 설정되는 인증 가능기간에 수신되었는지 여부에 의해 상기 인증조건의 만족여부가 판단될 수도 있다. 이를 위해 상기 판단부(140)는 상기 이벤트 발생신호가 수신되면, 수신된 상기 이벤트 발생신호에 기초하여 상기 인증 가능기간을 설정할 수 있다.

[0104] 상기 판단부(140)는 상기 이벤트 발생신호의 수신시점 이후 또는 수신시점 이후 소정의 기간 내(예컨대, 수초 또는 수분 등)를 상기 인증 가능기간으로 설정할 수 있다. 즉, 상기 이벤트 발생신호가 수신된 후 또는 상기 이벤트 발생신호가 수신된 후 소정의 기간 내에 상기 인증요청이 상기 인증제어시스템(100) 또는 상기 인증기관 시스템(40)으로 수신되면 서비스를 허용하도록 허용제어를 수행할 수 있다. 이러한 경우에는 사용자가 능동적으로 상기 이벤트 발생신호를 출력시키므로, 어떠한 공격자라도 상기 인증 가능기간을 미리 알 수 없게 되는 효과가 있다.

[0105] 다른 실시 예에 의하면, 상기 이벤트 발생신호에는 소정의 기간정보가 포함될 수도 있다. 예컨대, 후술할 클라이언트 시스템(200)은 상기 단말기에 이벤트가 발생했다고 판단하면 소정의 UI를 제공할 수 있다. 사용자는 상기 UI를 통해 서비스를 사용할 기간정보를 입력할 수 있다. 그러면, 상기 클라이언트 시스템(200)은 상기 기간정보를 포함하는 상기 이벤트 발생신호를 상기 인증제어시스템(100)으로 출력할 수도 있다.

[0106] 실시 예에 따라서는 사용자가 본 발명의 기술적 사상에 의한 서비스를 신청할 때에 미리 기간정보를 설정해둘 수도 있다. 그러면 상기 클라이언트 시스템(200)은 상기 이벤트 발생신호를 상기 인증제어시스템(100)으로 출력하고, 상기 인증제어시스템(100)에서 이벤트 발생신호에 상응하는 기간정보를 산정할 수도 있다.

[0107] 사용자가 별도로 기간정보를 설정하지 않는 경우에는, 상기 판단부(140)는 비교적 짧은 시간(예컨대, 수초 또는 수분)동안을 인증 가능기간으로 설정할 수 있다. 따라서 사용자는 서비스를 이용할 때마다 서비스 이용을 위한 의사표시 즉, 특정 행위를 수행하여야 할 수 있다.

[0108] 하지만, 공격자가 이러한 짧은 시간동안에 허위로 서비스 요청을 하는 경우가 존재할 수도 있다. 이러한 경우를 대비해 상기 제어부(110)는 상기 인증 가능기간동안이라도 소정의 우선순위에 해당하는 인증요청에 대해서만 한정적으로 인증제어를 수행할 수도 있다. 예컨대, 상기 우선순위는 인증요청의 수신순서에 의해 결정될 수 있다. 예컨대, 첫 번째(또는 미리 정해진 수 번째까지) 수신된 인증요청에 대해서만 인증제어를 수행할 수도 있다. 그리고 첫 번째(또는 미리 정해진 수 번째까지) 인증요청에 응답하여 인증을 수행하도록 상기 인증기관 시스템(40)을 제어한 후에는 인증 가능기간이 남은 경우라도 이후에 수신되는 인증요청에 대해서는 인증제어를 수행하지 않을 수도 있다. 다양한 우선순위의 실시 예가 존재할 수 있다.

[0109] 본 발명의 기술적 사상에 의하면 공격자는 사용자가 언제 특정행위를 수행할지 알지 못하므로, 짧은 시간동안만 인증 가능기간으로 설정되는 경우에, 상기 인증 가능기간에 허위의 인증요청을 할 수 있는 확률이 매우 낮아질 수 있다. 공격자가 인증 가능기간임을 알게 되는 경우라 하더라도, 첫 번째(또는 미리 정해진 수 번째까지)의 인증요청에 대해서만 서비스를 제공하는 경우에는 일반적으로 사용자가 공격자보다 먼저 인증요청을 하게 될 확률이 매우 크므로, 혹시 있을지 모를 인증 가능기간동안의 공격에도 이를 차단할 수 있는 효과를 얻을 수 있다.

[0110] 상기 판단부(140)에 의해 인증 가능기간이 설정되고, 상기 판단부(140)에 의해 상기 인증요청이 상기 인증 가능기간에 수신되었다고 판단되면, 상기 제어부(110)는 상기 인증요청에 상응하는 서비스를 수행하도록 상기 인증기관 시스템(40)을 제어할 수 있다.

[0111] 상기 제어부(110)는, 상기 판단부(140)에 의해 인증조건이 만족되었다고 판단되면, 상기 인증요청을 상기 인증기관 시스템(40)으로 전달함으로써 인증제어를 수행할 수 있다. 즉, 상기 인증요청은 상기 인증제어시스템(100)으로 수신될 수 있으며, 상기 제어부(110)에 의해 상기 인증요청을 상기 인증기관 시스템(40)으로 전송하는 것에 의해 인증의 수행여부가 제어될 수 있다. 이러한 경우에는 상기 인증기관 시스템(40)의 특별한 변경 없이 본 발명의 기술적 사상이 구현될 수 있는 유리한 효과가 있다.

[0112] 다른 실시 예에 의하면, 상기 인증요청은 상기 요청장치(예컨대, 20-1)로부터 직접 상기 인증기관 시스템(40)으로 전송될 수도 있다. 이때에는 상기 인증요청이, 상기 제어부(110)가 본 발명의 기술적 사상에 따른 제어신호를 상기 인증기관 시스템(40)으로 전송하기 전에, 이미 상기 인증기관 시스템(40)으로 전송되어 있거나 상기 제어신호가 전송된 후에 상기 인증기관 시스템(40)으로 전송될 수도 있다. 즉, 인증요청이 상기 요청장치(예컨대, 20-1)로부터 상기 인증기관 시스템(40)으로 직접 전송되는 경우에는, 이벤트가 인증요청 전에 발생하더라도 네트워크 사정 등 다양한 사정에 의해 인증요청이 상기 인증기관 시스템(40)으로 먼저 전송될 수도 있고, 그렇지 않을 수도 있다. 이러한 경우에는 상기 제어부(110)는 이미 전송되어 있거나 전송될 상기 인증요청의 인증 수행 여부를 나타내는 제어신호를 상기 인증기관 시스템(40)으로 전송함으로써 인증제어를 수행할 수도 있다. 또는 상기 제어신호에 추후에 수신될 상기 인증요청의 인증 수행여부를 판단할 수 있는 정보(예컨대, 이벤트 발생신호의 수신시점, 이벤트 발생시점 등)를 포함시켜 상기 인증기관 시스템(40)으로 전송함으로써, 상기 인증기관 시스템(40)이 상기 제어신호에 응답하여 최종적으로 인증의 수행여부를 결정하도록 할 수도 있다. 구현 예에 따라서는, 상기 인증기관 시스템(40)이 상기 인증요청이 수신된 시점에 대한 정보를 상기 인증제어시스템(100)으로 전송하고, 상기 인증제어시스템(100)은 수신된 정보에 기초하여 상기 인증요청이 인증 가능기간 내에 수신되었는지를 판단할 수도 있다. 다양한 실시 예가 가능할 수 있음을 본 발명의 기술분야의 평균적 전문가가 용이하게 추론할 수 있을 것이다.

[0113] 한편, 상기 인증제어시스템(100)은 소정의 단말기(예컨대, 20)로부터 이벤트 발생신호가 수신된 경우, 상기 이벤트 발생신호가 어떤 사용자의 인증수행 의사 표시인지를 알아야 할 수 있다. 그래야만 상기 사용자 명의의 인증요청에 응답하여 인증을 수행하도록 제어를 수행할 수 있다. 이를 위해 상기 이벤트 발생신호에는 상기 사용자를 식별할 수 있는 정보가 포함될 수 있다. 사용자를 식별할 수 있는 정보로는 상기 단말기(예컨대, 20)의 식별정보, 상기 특정 행위가 상기 단말기(예컨대, 20)와 상기 근거리 무선통신장치(30)와의 근거리 무선통신일 경우에는 상기 근거리 무선통신장치(30)의 식별정보, 또는 사용자가 직접 자신의 식별정보를 입력하는 경우의 사용자 식별정보 중 적어도 하나일 수 있다.

[0114] 상기 판단부(140)는 수신된 상기 이벤트 발생신호에 기초하여 서비스가 제한적으로 허용될 사용자를 특정할 수 있다. 즉, 상기 이벤트 발생신호에 상응하는 사용자를 특정할 수 있다. 그러면, 상기 제어부(110)는 상기 특정된 사용자에 상응하는 인증요청에 대해서만 제한적으로 인증제어를 수행할 수 있다.

[0115] 예컨대, 상기 판단부(140)는 상기 단말기의 식별정보를 확인할 수 있다. 상기 단말기(예컨대, 20)의 식별정보는 상기 이벤트 발생신호에 포함될 수도 있고, 상기 단말기(예컨대, 20)와 상기 인증제어시스템(100)간에 통신에 의해 판단될 수도 있다. 그러면, 상기 판단부(140)는 상기 단말기(예컨대, 20)의 식별정보에 기초하여 상기 단말기(예컨대, 20)의 명의자 즉, 상기 사용자를 특정할 수 있다. 상기 판단부(140)는 상기 단말기(예컨대, 20)의 식별정보를 이용하여 소정의 외부시스템(예컨대, 이동통신사 시스템 등)으로부터 상기 단말기(예컨대, 20)의 명의자에 대한 정보를 획득할 수도 있다. 구현 예에 따라서는, 상기 단말기(예컨대, 20)의 식별정보 및 명의자의 정보가 연계되어 미리 상기 인증제어시스템(100)에 저장되어 있을 수도 있다. 그러면 상기 제어부(110)는 상기 이벤트 발생신호에 상응하는 사용자 명의의 인증요청에 대해서만 인증제어를 수행할 수 있다.

[0116] 구현 예에 따라서, 상기 판단부(140)는 상기 이벤트(예컨대, 근거리 무선통신)의 발생을 위해 상기 단말기(예컨대, 20)와 근거리 무선통신을 수행하는 근거리 무선통신장치(30)의 명의자를 상기 사용자로 특정할 수도 있다. 예컨대, 상기 이벤트 발생신호에는 상기 근거리 무선통신장치(30)의 식별정보가 포함될 수 있다. 그러면, 상기 판단부(140)는 상기 근거리 무선통신장치(30)의 식별정보에 기초하여 상기 사용자를 특정할 수 있다. 상기 근거리 무선통신장치(30)의 식별정보에 대응되는 사용자의 정보가 미리 상기 인증제어시스템(100)에 저장되어 있을 수 있음은 물론이다. 실시 예에 따라서는, 상기 단말기(예컨대, 20)가 상기 근거리 무선통신장치(30)를 인증할 수도 있다. 이러한 경우에는 상기 이벤트 발생신호에 상기 근거리 무선통신장치(30)의 명의자에 대한 정보가 포함될 수도 있다. 다양한 방식으로 상기 단말기(예컨대, 20)의 명의자가 상기 판단부(140)에 의해 특정될 수도 있다.

[0117] 일 실시 예에 의하면, 상기 판단부(140)는 상기 단말기(예컨대, 20)의 명의자와 상기 근거리 무선통신장치(30)의 명의자가 일치하여야 상기 명의자를 상기 사용자로 특정할 수도 있다. 이러한 경우에는 복수의 사용자 명의의 장치(즉, 상기 단말기(예컨대, 20) 및 상기 근거리 무선통신장치(30))를 소지하여야 인증이 수행되므로, 보안성은 매우 높아질 수 있다. 이외에도 다양한 방식으로 상기 판단부(140)는 상기 이벤트 발생신호에 기초하여 상기 사용자를 특정할 수 있다.

[0118] 또한, 사용자가 수행하는 특정 행위가 상술한 근거리 무선통신장치(30)와 상기 단말기(예컨대, 20)의 근거리 무

선통신이 아니라, 상기 단말기(예컨대, 20)를 통한 소정의 인증인 경우라 하더라도 적어도 사용자 명의의 상기 단말기(예컨대, 20)를 소지하여야 하므로 2팩터 인증이 가능한 효과가 있다.

[0119] 한편, 인증을 요청하는 요청장치(예컨대, 20-1)와 상기 의사표시를 수행하는 상기 단말기(예컨대, 휴대폰, 20)는 별개의 단말기일 수도 있다. 즉, 사용자는 상기 요청장치(예컨대, 20-1)를 통해 인증요청을 하고, 인증요청 전 또는 후에 상기 단말기(예컨대, 20)를 통해 상기 특정 행위를 수행할 수도 있다. 물론, 상기 단말기(예컨대, 20)를 통해 인증요청을 하고, 상기 단말기(예컨대, 20)를 통해 상기 특정 행위를 수행할 수도 있다. 이때에는 상기 단말기(예컨대, 20)가 상기 요청장치(예컨대, 20-1)가가 될 수 있음은 물론이다. 물론, 상기 요청장치(예컨대, 20-1)를 통해 인증요청을 하고, 상기 요청장치(예컨대, 20-1)를 통해 특정 행위를 수행할 수도 있다. 이러한 경우에는 상기 요청장치(예컨대, 20-1)가 사용자 명의임을 상기 인증제어시스템(100)이 알 수 있도록 소정의 정보(예컨대, 상기 요청장치(예컨대, 20-1)의 명의자의 정보)가 미리 상기 인증제어시스템(100)에 저장되어 있거나, 구현 예에 따라서는 상기 특정 행위를 수행하는 단말기(예컨대, 20-1)가 사용자 명의이어야 할 요건이 생략될 수도 있다. 이처럼 사용자 명의의 단말기를 통해서만 이벤트 발생신호가 전송되도록 하는 강제조건이 없더라도 본 발명의 기술적 사상은 종래의 공인인증서 방식에 비해 보안성이 뛰어난 효과는 여전히 존재한다.

[0120] 또한, 상기 판단부(140)는 전술한 바와 같이 상기 인증제어시스템(100) 또는 상기 인증기관 시스템(40)으로 수신되는 인증요청이 필터링 조건을 만족하는지 여부를 판단할 수 있다. 그리고 판단결과 상기 인증요청이 상기 필터링 조건을 만족하는 필터링 인증요청인 경우에만, 상기 제어부(110)에 의해 인증제어가 수행되도록 할 수도 있다.

[0121] 예컨대, 상기 인증요청이 상기 인증제어시스템(100)으로 수신되면, 상기 판단부(140)는 상기 인증요청이 필터링 조건을 만족하는 인증요청 즉, 필터링 인증요청인지를 판단하고, 판단결과 필터링 인증요청인 경우에는 인증조건을 만족하는지 여부를 판단하고 판단결과에 따라 인증이 수행되도록 인증제어를 수행할 수 있다.

[0122] 만약, 상기 판단부(140)에 의해 상기 인증요청이 상기 필터링 인증요청이 아니라고 판단되면, 상기 제어부(110)는 상기 인증요청이 상기 인증조건을 만족하는지 여부와 무관하게 상기 인증요청이 인증되도록 상기 인증기관 시스템(40)을 제어할 수 있다.

[0123] 상기 인증요청이 상기 인증기관 시스템(40)으로 직접 전송되는 경우에는, 상기 인증기관 시스템(40)은 상기 인증제어시스템(100)으로부터 소정의 제어신호를 미리 받은 경우에는 인증을 수행하면 되고, 상기 인증제어시스템(100)으로부터 소정의 제어신호를 수신하지 못한 경우에는 상기 인증제어시스템(100)으로부터 소정의 제어신호가 수신되기 전까지 인증을 수행하지 않고 대기할 수 있다. 그러면, 상기 인증요청이 필터링 인증요청인지가 상기 인증기관 시스템(40) 또는 상기 판단부(140)에 의해 판단될 수 있다. 이를 위해 상기 인증기관 시스템(40)은 상기 인증요청에 대한 정보(예컨대, 금액, 요청장치(예컨대, 20-1)의 속성, 서비스 시스템(예컨대, 10)의 속성 등과 같은 필터링 조건의 만족여부를 판단할 수 있는 정보)를 상기 인증제어시스템(100)으로 전송할 수도 있다. 상기 인증요청이 필터링 인증요청으로 판단된 경우, 상기 판단부(140)는 상기 필터링 인증요청이 인증조건을 만족하는지를 판단하고, 판단결과에 따라 상기 제어부(110)는 인증제어를 위한 제어신호를 상기 인증기관 시스템(40)으로 전송할 수 있다. 또한, 상기 제어부(110)는 인증조건을 만족하지 않으면, 상기 인증기관 시스템(40)이 서비스를 거부하도록 하는 제어신호를 상기 인증기관 시스템(40)으로 전송할 수도 있다.

[0124] 만약, 상기 인증기관 시스템(40)으로 수신된 인증요청이 필터링 인증요청이 아니라고 상기 판단부(140)에 의해 판단된 경우, 상기 판단부(140)는 상기 인증요청이 인증조건을 만족하는지를 판단할 필요 없이 상기 제어부(110)가 상기 인증요청을 인증하도록 하는 제어신호를 상기 인증기관 시스템(40)으로 전송할 수도 있다.

[0125] 한편, 본 발명의 기술적 사상을 구현하기 위해서는 상기 단말기(예컨대, 20)에 소정의 클라이언트 즉, 애플리케이션(또는 소프트웨어)이 설치될 수 있다. 상기 애플리케이션이 설치되면, 상기 단말기(예컨대, 20)의 하드웨어와 상기 애플리케이션이 유기적으로 결합하여 본 발명의 기술적 사상에 따른 클라이언트 시스템(200)이 구현될 수 있다.

[0126] 도4는 본 발명의 실시 예에 따른 클라이언트 시스템의 개략적인 구성을 나타낸다.

[0127] 우선 도4를 참조하면, 본 발명의 기술적 사상을 구현하기 위한 클라이언트 시스템(200)은 사용자의 단말기(예컨대, 20)에 포함되어 구현될 수 있다.

[0128] 따라서 상기 단말기(예컨대, 20)가 본 발명의 기술적 사상을 구현하기 위한 소정의 기능을 수행한다고 함은, 상기 단말기(예컨대, 20)에 설치된 상기 클라이언트 시스템(200)이 상기 기능을 수행함을 의미할 수도 있다. 예컨대, 상기 이벤트 발생신호를 출력하거나, 상기 특정 이벤트가 발생함을 판단하는 등의 기능은 상기 클라이언트

시스템(200)에 의해 수행될 수 있다.

[0129] 상기 클라이언트 시스템(200)은 제어모듈(210) 및 판단모듈(220)을 포함할 수 있다. 상기 제어모듈(210)은 상기 판단모듈(220) 및/또는 상기 단말기(예컨대, 20)의 다른 구성들의 기능 및/또는 리소스를 제어할 수 있도록 구현될 수 있다.

[0130] 상기 판단모듈(220)은 상기 단말기(예컨대, 20)에 특정 이벤트가 발생했는지 판단할 수 있다. 상기 특정 이벤트는 전술한 바와 같이 상기 단말기(예컨대, 20)와 상기 근거리 무선통신장치(30)가 근거리 무선통신을 수행하는 이벤트일 수도 있고, 상기 단말기(예컨대, 20)를 통해 소정의 인증정보(예컨대, 비밀번호, 생체정보, OTP, 공인인증서 등)를 이용한 인증 이벤트일 수도 있다. 상기 단말기(예컨대, 20)를 통해 인증 이벤트가 수행되는 경우에는, 상기 인증정보는 상기 단말기(예컨대, 20)에 저장되어 있을 수도 있지만 상기 인증정보를 인증할 수 있는 소정의 네트워크 시스템(예컨대, OTP 인증시스템, 생체정보 인증시스템, 또는 공인인증서 인증시스템 등)에 상기 인증정보가 저장되어 있을 수도 있다. 이러한 경우에는 상기 네트워크 시스템으로부터 인증이 성공했음을 상기 판단모듈(220)이 수신하여야 상기 특정 이벤트가 수행되었다고 판단할 수 있다.

[0131] 상기 판단모듈(220)에 의해 상기 특정 이벤트가 발생했다고 판단되면, 상기 제어모듈(210)은 상기 인증제어시스템(100)으로 이벤트 발생신호를 전송할 수 있으며, 상기 이벤트 발생신호가 상기 제어모듈(210)로부터 상기 인증제어시스템(100)으로 출력되면, 상기 인증제어시스템(100)은 전술한 바와 같이 인증 가능기간동안에만 제한적으로 요청장치(예컨대, 20-1)로부터 수신되는 인증요청에 응답하여 상기 인증기관 시스템(40)이 인증을 수행하도록 인증제어를 수행할 수 있다.

[0132] 상기 제어모듈(210)은 상기 단말기(예컨대, 20)의 식별정보(예컨대, 전화번호, IMEI 등)를 추출할 수 있고, 추출된 정보를 상기 이벤트 발생신호에 포함시킬 수 있다. 구현 예에 따라서는, 상기 특정 이벤트가 상기 단말기(예컨대, 20)와 상기 근거리 무선통신장치(30)의 근거리 무선통신인 경우, 상기 근거리 무선통신장치(30)의 식별정보를 상기 근거리 무선통신을 통해 수신한 후 상기 이벤트 발생신호에 포함시킬 수도 있다. 또는 소정의 방식으로 상기 근거리 무선통신장치(30)의 사용자를 인증하고, 인증결과에 따라 상기 근거리 무선통신장치(30)의 명의자의 정보를 상기 이벤트 발생신호에 포함시킬 수도 있다. 예컨대, 상기 제어모듈(210)은 사용자로부터(상기 단말기(예컨대, 20)로부터) 직접 사용자 식별정보(예컨대, ID, 이름, 주민번호 등)를 입력받고, 입력받은 정보를 상기 이벤트 발생신호에 포함시킬 수도 있다.

[0133] 또한, 전술한 바와 같이 상기 제어모듈(210)은 상기 근거리 무선통신장치(30)를 인증할 수도 있다. 상기 제어모듈(210)이 상기 근거리 무선통신장치(30)를 인증하는 방식은 다양할 수 있다. 예컨대, 상기 근거리 무선통신장치(30)의 식별정보가 미리 상기 단말기(20)에 저장되어 있는 경우에는, 상기 근거리 무선통신을 수행한 상기 근거리 무선통신장치(30)의 식별정보가 상기 단말기(20)에 미리 저장된 식별정보에 상응하는지를 상기 제어모듈(210)이 판단함으로써 상기 제어모듈(210)은 상기 근거리 무선통신장치(30)를 인증할 수 있다. 또한, 보다 높은 보안성을 위해서는 상기 근거리 무선통신장치(예컨대, IC카드, 30)가 소정의 난수(random number)를 생성하고, 생성된 난수를 비대칭 암호화 방식을 통해 인증하는 크립토그램 방식이 이용될 수도 있다. 구현 예에 따라서는 상기 근거리 무선통신장치(30)가 OTP를 생성하는 OTP클라이언트 역할을 수행하고, 상기 제어모듈(210)이 OTP를 인증하는 OTP 서버 역할을 수행할 수도 있다. 다양한 방식으로 상기 제어모듈(210)은 상기 근거리 무선통신장치(30)를 인증할 수 있다. 물론, 상기 근거리 무선통신장치(30)의 인증은 전술한 바와 같이 상기 인증제어시스템(100)에 의해 수행될 수도 있다. 예컨대, 상기 근거리 무선통신장치(30)가 생성한 난수를 비대칭 암호화 방식을 통해 인증하는 두 장치가 상기 인증제어시스템(100) 및 상기 근거리 무선통신장치(30)일 수도 있다. 이러한 경우, 상기 클라이언트 시스템(200)은 단순히 상기 인증제어시스템(100)과 상기 근거리 무선통신장치(30)사이의 통신을 중개하는 기능을 수행할 수도 있다. 상기 근거리 무선통신장치(30)가 OTP 클라이언트 역할을 수행하는 경우에도, 상기 인증제어시스템(100)이 OTP 서버의 역할을 수행하여 상기 근거리 무선통신장치(30)를 인증할 수도 있다.

[0134] 상기 이벤트가 상기 근거리 무선통신인 경우, 사용자는 간단히 자신의 단말기(예컨대, 20) 및/또는 자신의 근거리 무선통신장치(30)를 통해 인증 수행의사 표시를 수행할 수 있고, 이러한 의사표시가 있을 때에만 상기 인증기관 시스템(40)에 의해 인증이 수행될 수 있다.

[0135] 사용자는 비교적 오랜 기간 동안 인증을 수행하고자 할 때 상기 제어모듈(210)이 제공하는 소정의 UI를 통해 기간정보를 입력할 수도 있고, 상기 제어모듈(210)은 상기 기간정보를 상기 이벤트 발생신호에 포함시켜 상기 인증제어시스템(100)으로 전송할 수도 있다. 그러면, 상기 인증 가능기간 동안에는 반복적으로 특정 행위를 수행하지 않더라도 서비스가 수행될 수도 있다.

[0136] 도5는 본 발명의 일 실시 예에 따른 비대칭 암호화 방식의 인증 제어방법의 개략적인 과정을 설명하기 위한 플로우차트이다.

[0137] 도5는 사용자가 인증을 수행하기 전에 사전적으로 특정 행위 즉, 소정의 이벤트를 발생시키는 일예를 도시하고 있다. 도5를 참조하면, 사용자는 인증을 위해 특정 행위를 수행함으로써 특정 이벤트를 상기 단말기(예컨대, 20)에 발생시킬 수 있다. 그러면, 상기 클라이언트 시스템(200)은 상기 특정 이벤트의 발생을 판단하고, 상기 인증제어시스템(100)으로 이벤트 발생신호를 전송할 수 있다(S100). 사용자는 상기 특정 행위를 수행한 후 소정의 서비스 시스템(10)에서 인증(전자서명)을 요구받고(S110), 이에 응답하여 요청장치(예컨대, 20-1)를 이용하여 인증요청을 출력할 수 있다(S120). 상기 인증요청을 출력하기 위해 사용자는 상기 요청장치(예컨대, 20-1)에서 실행되는 인증서 클라이언트에 인증서의 비밀번호를 입력하여야 함은 물론이다. 상기 인증요청에는 인증서의 개인키뿐만 아니라, 인증기관, 다양한 인증서 정보가 포함될 수 있음은 널리 공지된 바와 같다.

[0138] 상기 요청장치(예컨대, 20-1)로부터 출력된 인증요청은 상기 인증제어시스템(100)으로 전송될 수 있다(S120). 상기 인증제어시스템(100)은 수신된 인증요청이 인증조건을 만족하는지 여부를 판단할 수 있다(S130). 그리고 인증조건이 만족한다고 판단한 경우에는 상기 인증요청을 상기 인증기관 시스템(40)으로 전송할 수 있다(S140). 그러면 상기 인증기관 시스템(40)은 수신된 인증요청을 인증하고, 인증결과를 상기 인증제어시스템(100)을 통해서 또는 상기 요청장치(예컨대, 20-1) 즉, 상기 인증서 클라이언트로 직접 전송할 수 있다(S150). 그러면 상기 요청장치(예컨대, 20-1)는 상기 서비스 시스템(10)으로 인증결과를 전송함으로써, 사용자가 인증(또는 요청된 거래가 전자서명)될 수 있다(S160).

[0139] 상기 인증조건이 만족하는 경우는 인증 가능기간에 상기 인증요청이 수신된 경우일 수 있다. 상기 인증 가능기간은 예컨대, 상기 이벤트 발생신호가 수신된 수신시점으로부터 일정 기간 내일 수 있다. 구현 예에 따라서는, 상기 인증요청이 먼저 수신되고 상기 이벤트 발생신호가 수신될 수도 있다. 즉, 사용자는 인증요청을 먼저 출력하고 상기 단말기(20)를 통해 특정 행위를 수행할 수도 있다. 이러한 경우에는 상기 인증 가능기간은 상기 이벤트 발생신호가 수신된 시점 이전의 일정 기간내일 수도 있다. 물론, 상기 이벤트 발생신호에 소정의 기간정보가 포함될 수도 있으며, 이러한 경우에는 상기 기간정보에 상응하는 기간이 인증 가능기간일 수도 있다.

[0140] 일예에 의하면, 사용자는 상기 클라이언트 시스템(200)을 상기 단말기(예컨대, 20)에서 실행시킨 후 상기 특정 행위를 수행할 수 있다. 구현 예에 따라서는, 상기 특정 행위(예컨대, 근거리 무선통신)를 수행하면 자동으로 상기 클라이언트 시스템(200)이 상기 단말기(예컨대, 20)에서 실행될 수도 있다.

[0141] 만약, 상기 인증제어시스템(100)의 판단결과, 상기 인증조건이 만족하지 않는다고 판단되면 상기 인증제어시스템(100)은 수신된 인증요청을 상기 인증기관 시스템(40)으로 전송하지 않을 수 있다. 그럼으로써 상기 인증요청은 인증이 수행되지 않을 수 있다.

[0142] 다른 실시 예에 의하면, 상기 인증요청은 상기 인증제어시스템(100)으로 전송되는 것이 아니라, 직접 상기 인증기관 시스템(40)으로 전송될 수도 있다. 이러한 경우에는 상기 인증기관 시스템(40)은 상기 인증제어시스템(100)의 제어신호에 기초하여 수신되는 인증요청의 인증을 수행할지 여부를 판단할 수 있다.

[0143] 한편, 상기 인증제어시스템(100)은 상기 인증요청이 필터링 조건을 만족하는지 여부를 더 판단할 수도 있다. 그리고 필터링 조건을 만족하는 인증요청에 대해서만 인증조건의 만족여부를 판단하고, 필터링 조건을 만족하지 않는 인증요청에 대해서는 인증조건의 만족여부와 무관하게 인증이 수행되도록 할 수도 있음은 전술한 바와 같다. 또한, 소정의 우선순위를 만족하는 인증요청에 대해서만 인증이 수행되도록 제어할 수 있음도 전술한 바와 같다.

[0144] 도6는 본 발명의 다른 실시 예에 따른 비대칭 암호화 방식의 인증 제어방법의 개략적인 과정을 설명하기 위한 플로우차트이다.

[0145] 도6은 도5와는 달리 사용자가 능동적으로 특정 행위를 수행하는 것이 아니라, 상기 인증제어시스템(100) 또는 클라이언트 시스템(200)에 의해 특정 행위의 요청이 되는 경우를 도시하고 있다.

[0146] 도6을 참조하면, 사용자 즉, 요청장치(예컨대, 20-1)는 소정의 서비스 시스템(10)으로부터 인증(전자서명)을 요구받을 수 있다(S200). 그러면, 상기 요청장치(예컨대, 20-1)에는 인증서 클라이언트가 로딩될 수 있다. 상기 인증서 클라이언트는 사용자로부터 인증서 비밀번호를 입력받기 전 또는 후에 사용자에게 소정의 단말기(20)를 통해 특정 행위를 수행하라는 정보를 상기 요청장치(예컨대, 20-1)에 출력할 수 있다(S210). 그러면 사용자는 상기 특정 행위를 수행함으로써 상기 단말기(20)를 통해 이벤트 발생신호를 상기 인증제어시스템(100)으로 출력

할 수 있다(S230). 이러한 경우에는 상기 인증서 클라이언트가 본 발명의 기술적 사상에 따라 상기 사용자에게 상기 특정 행위를 요청하는 기능을 수행할 수 있도록 구현될 수 있다. 상기 인증서 클라이언트는 상기 단말기(20)에서 상기 특정 행위가 수행되기 전에는 상기 인증요청을 상기 인증제어시스템(100) 또는 상기 인증기관 시스템(40)으로 출력하지 않도록 구현될 수도 있다. 이러한 경우, 상기 인증서 클라이언트는 상기 인증제어시스템(100)으로부터 이벤트 발생신호가 수신되었음을 나타내는 신호를 수신하고, 상기 신호가 수신되어야 개인키를 추출하거나 또는 이미 추출된 개인키를 포함하는 인증요청을 출력할 수도 있다. 물론, 상기 단말기(20)가 상기 요청장치(예컨대, 20-1)인 경우에는 이벤트가 발생하였음을 상기 인증서 클라이언트가 판단할 수 있다. 즉, 이러한 경우에는 상기 인증서 클라이언트가 전술한 바와 같은 클라이언트 시스템(200)의 기능 또는 역할을 수행할 수도 있다.

[0147] 다른 실시 예에 의하면, 상기 인증서 클라이언트를 통해 인증요청이 상기 인증제어시스템(100)으로 출력되면(S220), 상기 인증제어시스템(100)은 상기 인증요청에 상응하는 사용자를 특정하고 특정된 사용자의 상기 단말기(20)에 설치된 클라이언트 시스템(200)을 통해 특정 행위 즉, 이벤트를 요청할 수 있다(S220-1). 그러면 사용자는 요청에 응답하여 이벤트를 발생시키기 위한 상기 특정행위를 수행함으로써 이벤트 발생신호를 상기 인증제어시스템(100)으로 출력할 수 있다(S230).

[0148] 이처럼 사용자에게 특정 행위를 수행하도록 상기 인증제어시스템(100) 또는 상기 인증서 클라이언트가 요청하는 경우에는 요청에 응답하여 상기 이벤트가 발생하는지 여부가 인증조건의 만족여부일 수 있다. 따라서 이러한 경우에는 별도로 인증조건의 만족여부를 판단하지 않을 수도 있다. 물론, 구현 예에 따라서는 일정 시간 내에 상기 이벤트가 발생하는지를 판단함으로써 인증조건의 만족여부를 더 판단할 수도 있다.

[0149] 상기 인증제어시스템(100)은 상기 이벤트 발생신호가 수신되면 상기 요청장치(예컨대, 20-1)로부터 수신된 인증요청을 상기 인증기관 시스템(40)으로 전송할 수 있다(S240).

[0150] 그러면 상기 인증기관 시스템(40)은 인증을 수행하고, 인증결과를 상기 인증제어시스템(100)을 통해 또는 직접 상기 요청장치(예컨대, 20-1)로 출력할 수 있다(S250). 그러면 요청장치(예컨대, 20-1)는 상기 서비스 시스템(10)과 통신을 수행하여 인증(전자서명)을 완료할 수 있다(S260).

[0151] 물론, 도6의 경우에도 필터링 조건을 만족하는지 여부, 미리 설정된 우선순위를 만족하는지 여부 등이 상기 인증제어시스템(100)에 의해 더 판단될 수 있음은 물론이다.

[0152] 결국, 본 발명의 기술적 사상에 따르면 소정의 특정 행위를 수행한 자는 정당한 명의자로 추정이 되고, 상기 명의자의 행위(예컨대, 근거리 무선통신을 수행하는 행위)에 의해 제한적으로 인증이 수행되는 효과가 있다.

[0153] 또한, 서비스 이용을 위한 의사표시가, 상기 인증기관 시스템(40) 또는 상기 인증제어시스템(100)에 의한 사용자 인증을 통해서가 아니라, 의사표시를 하는 자가 사용자 명의의 장치(예컨대, 인증정보를 이용한 인증이 특정 행위인 경우에는 상기 단말기(예컨대, 20), 근거리 무선통신이 특정 행위인 경우에는 상기 단말기(예컨대, 20) 또는 상기 근거리 무선통신장치(30))를 적어도 하나 소지하고 있음이 확인되어야 수행될 수 있으므로 인증기관 시스템(40) 또는 인증제어시스템(100)이 제공하는 사용자 인증(예컨대, 로그인 등)이 공격자에 의해 더 이상 제 기능을 발휘하지 못하는 경우에도 여전히 공격자에게 인증이 수행될 수 있는 것이 차단되는 효과가 있다.

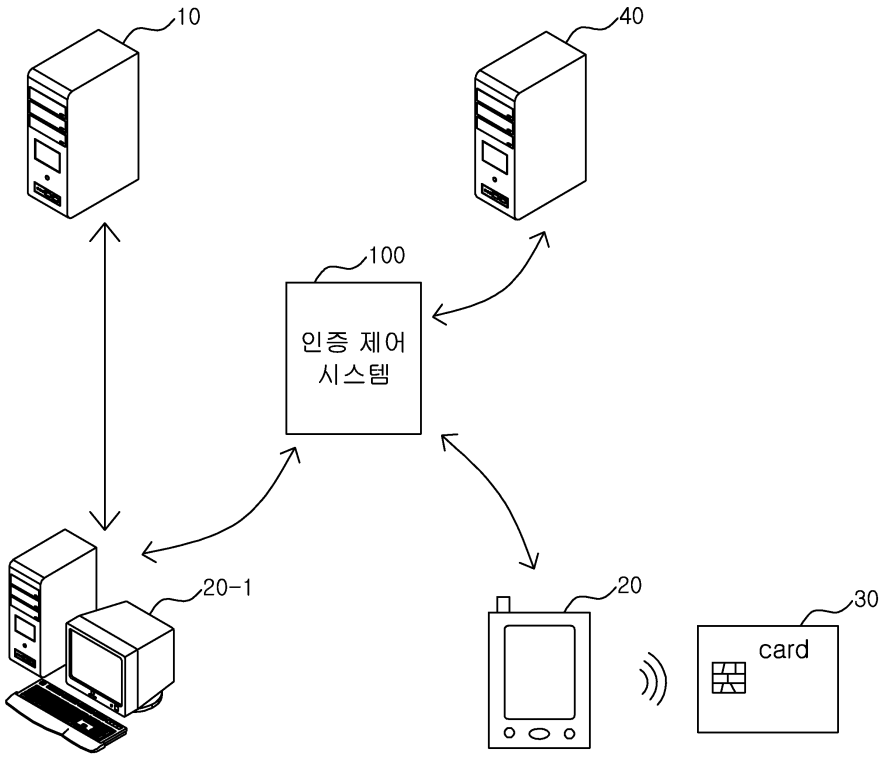
[0154] 더구나 사용자의 입장에서도 비교적 간단한 행위(예컨대, 근거리 무선통신 등)만으로 안전하게 인증요청에 대한 인증 또는 필터링 조건을 만족하는 인증요청에 대한 선택적인 인증이 수행될 수 있는 효과가 있다.

[0155] 본 발명의 실시 예에 따른 인증 제어방법은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 하드 디스크, 플로피 디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어, 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술분야의 프로그래머들에 의해 용이하게 추론될 수 있다.

[0156] 본 발명은 도면에 도시된 일 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면

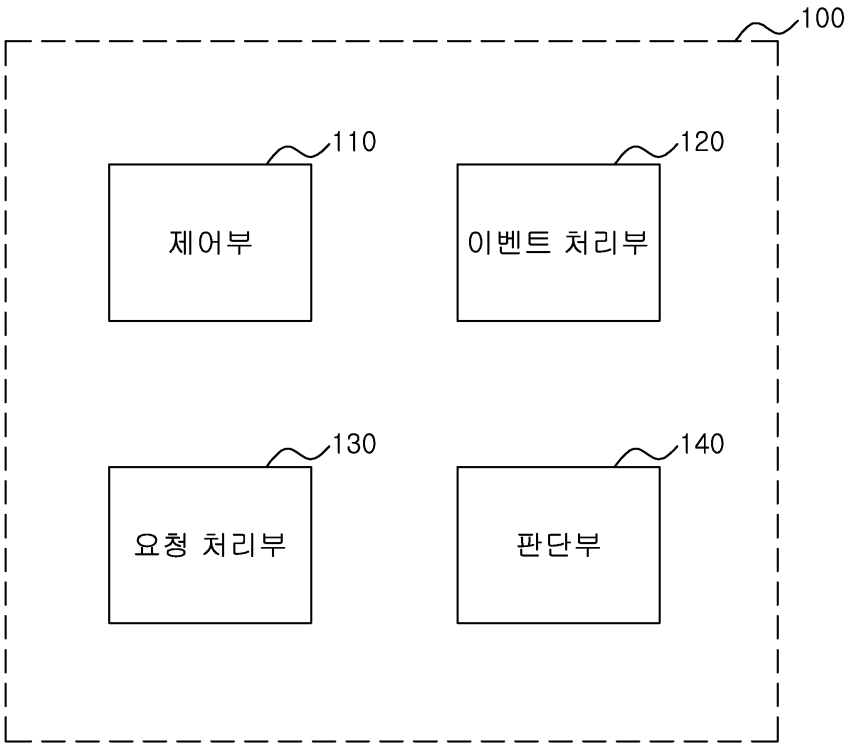
도면1



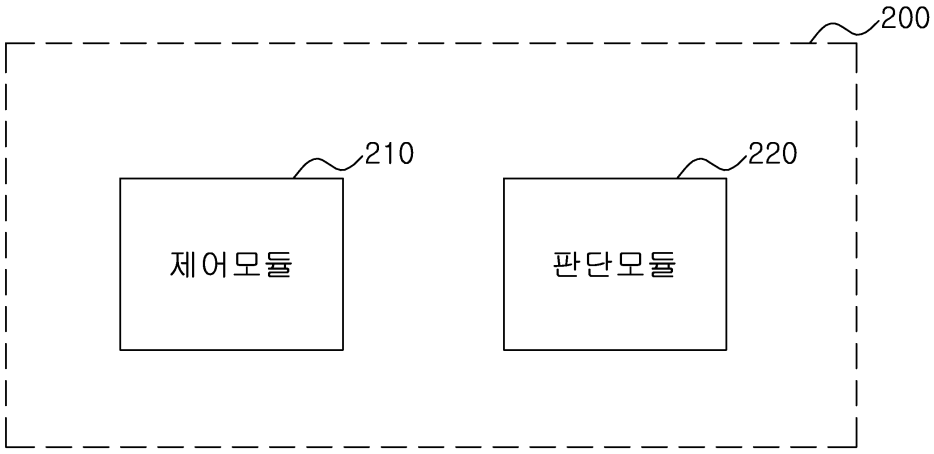
도면2

• 필터링 조건			
인증서	서비스 시스템	시간	서비스 금액
인증서1	• 특정 웹 서비스 시스템	21시 ~ 06시	• 30만원 이상
인증서2	• 해외 시스템 • 은행 시스템	•	•

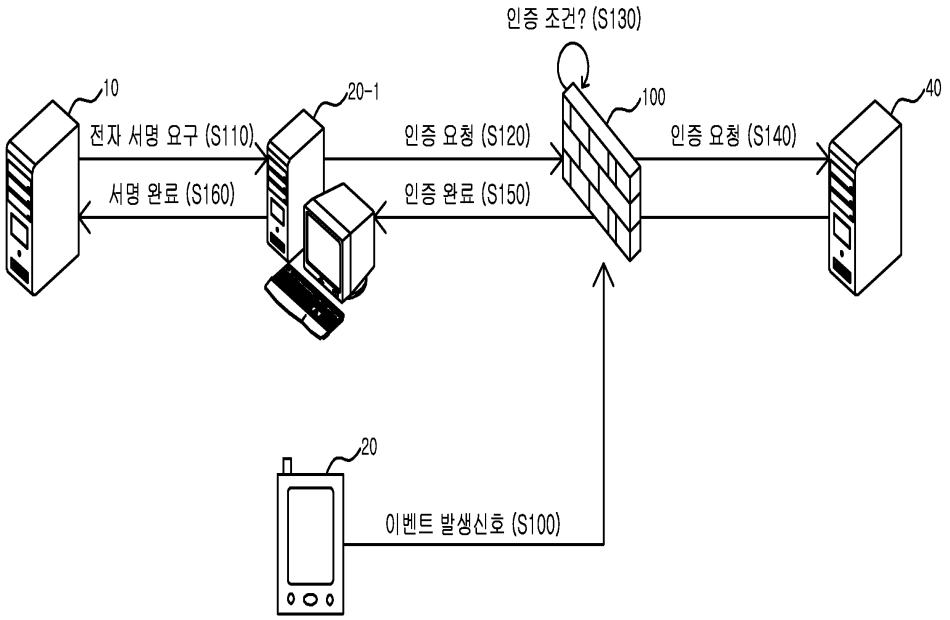
도면3



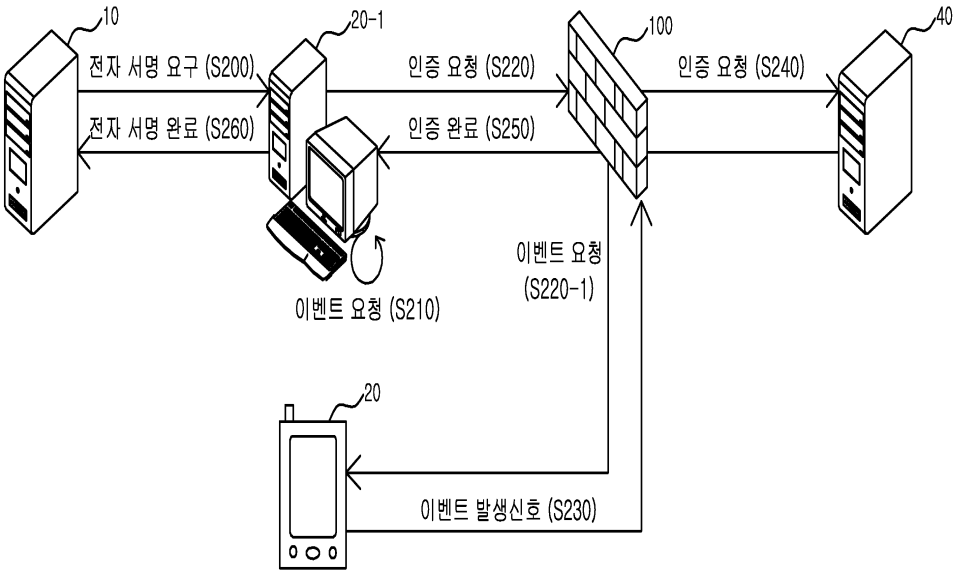
도면4



도면5


인증 조건? (S130)
10
20-1
100
40
전자 서명 요구 (S110)
인증 요청 (S120)
인증 요청 (S140)
서명 완료 (S160)
인증 완료 (S150)
20
이벤트 발생신호 (S100)

도면6


10
20-1
100
40
전자 서명 요구 (S200)
인증 요청 (S220)
인증 요청 (S240)
전자 서명 완료 (S260)
인증 완료 (S250)
이벤트 요청 (S210)
이벤트 요청
(S220-1)
20
이벤트 발생신호 (S230)