(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0015744
(43) 공개일자 2014년02월07일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01)
(21) 출원번호 10-2012-0080360
(22) 출원일자 2012년07월24일
심사청구일자 없음

(71) 출원인
주식회사 비즈모델라인
서울특별시 마포구 와우산로 77, 6층 (서교동, 대창빌딩)
(72) 발명자
김재형
서울 강남구 압구정로 313, 62동 1101호 (압구정동, 한양아파트)
권봉기
경기도 안양시 동안구 관양동 그라테아오피스텔 1214호

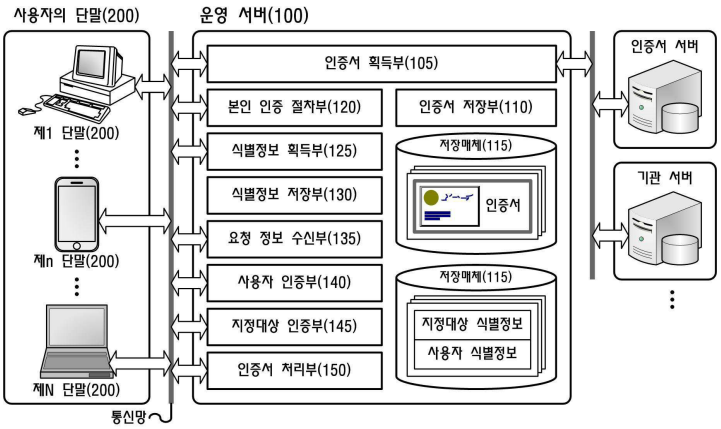
전체 청구항 수 : 총 21 항

(54) 발명의 명칭 **클라우드 방식 인증서 운영 방법**

(57) 요 약

본 발명은 클라우드 방식 인증서 운영 방법에 관한 것으로, 본 발명에 따른 클라우드 방식 인증서 운영 방법은, 서버에 의해 실행되는 클라우드 방식 인증서 운영 방법에 있어서, 사용자에게 발급된 인증서를 지정된 저장매체에 저장하는 제1 단계와, 상기 저장된 인증서를 이용 가능한 N(N≥1)개의 단말을 지정 식별하는 지정대상 식별정보를 저장하는 제2 단계와, 상기 사용자가 이용하는 단말이 상기 지정대상 식별정보에 의해 지정 식별되는 N개의 지정된 단말 중 제n(1≤n≤N) 단말인지 인증하는 제3 단계와, 상기 사용자의 단말이 상기 지정된 제n 단말로 인증된 경우에 상기 저장매체에 저장된 사용자의 인증서가 상기 제n 단말을 통해 이용되도록 처리하는 제4 단계를 포함한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

서버에 의해 실행되는 클라우드 방식 인증서 운영 방법에 있어서,

사용자에게 발급된 인증서를 지정된 저장매체에 저장하는 제1 단계;

상기 저장된 인증서를 이용 가능한 N(N≥1)개의 단말을 지정 식별하는 지정대상 식별정보를 저장하는 제2 단계;

상기 사용자가 이용하는 단말이 상기 지정대상 식별정보에 의해 지정 식별되는 N개의 지정된 단말 중 제n(1≤n≤N) 단말인지 인증하는 제3 단계; 및

상기 사용자의 단말이 상기 지정된 제n 단말로 인증된 경우에 상기 저장매체에 저장된 사용자의 인증서가 상기 제n 단말을 통해 이용되도록 처리하는 제4 단계;를 포함하는 클라우드 방식 인증서 운영 방법.

청구항 2

제 1항에 있어서, 상기 제1 단계는,

상기 저장매체에 저장되는 인증서를 발급받은 사용자에 대한 본인 인증 절차를 수행하는 단계를 더 포함하며,

상기 사용자의 본인 인증이 처리된 경우에 상기 사용자에게 발급된 인증서를 상기 저장매체에 저장하는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 3

제 1항에 있어서, 상기 제1 단계는,

상기 사용자에게 상기 인증서를 발급한 인증서 서버로부터 상기 사용자에게 발급된 인증서를 제공받아 상기 저장매체에 저장하거나,

사용자의 단말로부터 상기 사용자에게 발급된 인증서를 제공받아 상기 저장매체에 저장하는 것 중 적어도 하나를 포함하여 이루어지는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 4

제 1항에 있어서, 상기 저장매체에 저장되는 인증서는,

상기 사용자에게 발급된 인증서의 전체 구성을 포함하거나, 또는

상기 사용자에게 발급된 인증서의 일부 구성을 포함하는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 5

제 4항에 있어서,

상기 저장매체에 저장된 인증서에 일부 구성이 포함되는 경우,

상기 저장된 인증서의 일부 구성을 제외한 나머지 구성은,

상기 N개의 지정된 단말에 저장되거나, 또는

상기 N개의 지정된 단말을 통해 이용될 인증서를 저장하는 사용자 소유의 휴대 매체에 저장되는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 6

제 1항에 있어서, 상기 인증서를 저장하는 저장매체는,

상기 인증서의 발급기관이 운영하는 저장매체,

상기 인증서의 등록기관이 운영하는 저장매체,

상기 서버에 구비된 저장매체,

상기 서버에서 접근 가능한 네트워크 상의 저장매체 중 적어도 하나인 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 7

제 1항에 있어서, 상기 제2 단계는,

상기 인증서를 발급받은 사용자가 상기 인증서가 이용될 단말을 지정 등록하는지에 대한 사용자 본인 인증 절차를 수행하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 8

제 1항에 있어서, 상기 제2 단계는,

상기 인증서를 발급받은 사용자를 고유 인증하는 사용자 식별정보를 획득하는 단계를 더 포함하며,

상기 N개의 지정대상 식별정보는, 사용자 식별정보와 매핑되어 저장되는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 9

제 1항에 있어서, 상기 지정대상 식별정보는,

지정된 단말의 읽기/쓰기 메모리에 저장된 정보, 지정된 단말에 구비된 IC칩에 저장된 정보, 지정된 단말의 읽기전용 메모리에 기록된 정보, 지정된 단말의 하드웨어적 구성품에 할당된 정보, 지정된 단말의 통신식별 정보, 지정된 단말에서 생성된 정보, 지정된 단말에서 입력된 정보, 지정된 단말에 구비된 프로그램을 식별하는 정보, 지정된 코드생성모듈을 통해 동적 생성된 정보 중 적어도 하나 또는 둘 이상의 조합으로 이루어지는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 10

제 1항에 있어서,

상기 인증서가 이용될 단말로 등록 가능한 각 단말의 종류, 통신망 및 플랫폼 중 적어도 하나를 기준으로 각 단말의 지정대상 식별정보로 이용 가능한 M(M≥1)개의 지정 정보를 지정하는 지정대상 식별정보 조건이 설정되는 단계를 더 포함하며,

상기 제2 단계는, 상기 등록되는 단말의 지정대상 식별정보 조건에 부합하는 M개의 지정 정보 중에서 m(1≤m≤M)개의 지정 정보를 포함하는 지정대상 식별정보를 획득하는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 11

제 1항에 있어서, 상기 제2 단계는,

단말 지정 등록을 위해 접속한 사용자의 단말을 상기 인증서를 이용 가능한 단말로 지정 등록하는 경우,

상기 사용자의 단말로부터 지정된 하나 이상의 지정 정보를 포함하는 지정대상 식별정보를 수신하거나,

상기 사용자의 단말을 관리하는 관리서버로부터 상기 사용자의 단말에 지정된 하나 이상의 지정 정보를 포함하는 지정대상 식별정보를 수신하는 것 중,

적어도 하나 또는 둘 이상의 조합을 통해 상기 사용자의 단말을 상기 저장된 인증서가 이용될 단말로 지정하는 지정대상 식별정보를 획득하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 12

제 1항에 있어서, 상기 제2 단계는,

단말 지정 등록을 위해 접속한 사용자의 단말 이외에 상기 사용자가 이용 가능한 다른 단말을 상기 인증서를 이용 가능한 단말로 지정 등록하는 경우,

상기 사용자의 단말로부터 상기 인증서를 이용 가능한 단말로 등록되는 대상 단말에 지정된 하나 이상의 지정 정보를 포함하는 지정대상 식별정보를 수신하거나,

상기 사용자의 단말로부터 제공되는 상기 대상 단말에 대한 단말정보를 근거로 상기 대상 단말로부터 지정된 하나 이상의 지정 정보를 포함하는 지정대상 식별정보를 수신하거나,

상기 대상 단말을 관리하는 관리서버로부터 상기 대상 단말에 지정된 하나 이상의 지정대상 식별정보를 수신하는 것 중,

적어도 하나 또는 둘 이상의 조합을 통해 상기 사용자가 이용 가능한 단말을 상기 저장된 인증서가 이용될 단말로 지정하는 지정대상 식별정보를 획득하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 13

제 1항에 있어서, 상기 제3 단계는,

상기 인증서를 발급받은 사용자가 상기 저장된 인증서를 요청하는지에 대한 사용자 본인 인증 절차와, 상기 N개의 단말을 등록한 사용자가 상기 저장된 인증서를 요청하는지에 대한 사용자 본인 인증 절차 중, 적어도 하나의 본인 인증 절차를 수행하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 14

제 1항에 있어서, 상기 제3 단계는,

상기 사용자를 고유 인증하는 사용자 식별정보가 상기 지정대상 식별정보와 매핑되어 저장된 경우, 상기 사용자의 단말로부터 수신되는 사용자 식별정보와 상기 저장된 사용자 식별정보를 비교하여 상기 사용자를 인증하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 15

제 1항에 있어서, 상기 제3 단계는,

상기 사용자의 단말로부터 상기 저장된 지정대상 식별정보에 포함된 하나 이상의 지정 정보와 매칭되는 지정대

상 식별정보를 수신하는 단계; 및

상기 수신된 지정대상 식별정보와 상기 저장된 지정대상 식별정보를 비교하여 상기 사용자의 단말을 상기 지정된 제n 단말로 인증하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 16

제 1항에 있어서, 상기 제3 단계는,

지정대상 식별정보로 이용 가능한 M(M≥1)개의 지정 정보 중에서 상기 사용자의 단말을 지정 식별하는데 이용되는 m(1≤m≤M)개의 지정 정보를 포함하는 지정대상 식별정보의 구성을 확인하는 단계;

상기 사용자의 단말로부터 상기 m개의 지정 정보를 포함하는 지정대상 식별정보를 수신하는 단계; 및

상기 수신된 지정대상 식별정보와 상기 저장된 지정대상 식별정보를 비교하여 상기 사용자의 단말을 상기 지정된 제n 단말로 인증하는 단계;를 더 포함하여 이루어지는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 17

제 1항에 있어서,

상기 지정대상 식별정보는, 지정된 단말에 고정 유지된 둘 이상의 지정 정보를 포함하며,

상기 지정된 단말에 고정 유지된 둘 이상의 정보 중 일부는 인증되고 나머지 일부는 인증되지 않는 경우에 상기 지정대상 식별정보에 대한 폐기 절차 또는 재등록 절차를 수행하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 18

제 1항에 있어서, 상기 제4 단계는,

상기 저장된 사용자의 인증서를 상기 제n 단말로 제공하는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 19

제 1항에 있어서, 상기 제4 단계는,

상기 사용자에게 발급된 인증서의 일부 구성을 상기 제n 단말로 제공하는 것을 특징으로 하며,

상기 제n 단말은, 상기 제공되는 인증서의 일부 구성을 제외한 나머지 구성이 구비되어 있거나, 상기 사용자 소유의 휴대 매체에 구비된 상기 인증서의 나머지 구성을 이용 가능한 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 20

제 19항에 있어서,

상기 인증서의 일부 구성은,

N개의 지정된 단말에 대하여 동일하거나, 또는

N개의 지정된 단말 별로 서로 다른 것을 특징으로 하며,

상기 인증서의 나머지 구성은,

N개의 지정된 단말에 대하여 동일하거나, 또는

N개의 지정된 단말 별로 서로 다른 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

청구항 21

제 1항에 있어서, 상기 제4 단계는,

상기 저장된 사용자의 인증서를 통해 상기 제n 단말의 인증서 처리를 대행하는 것을 특징으로 하는 클라우드 방식 인증서 운영 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 네트워크 상의 지정된 저장매체에 사용자에게 발급된 인증서를 저장한 후에, 상기 사용자가 이용하는 단말이 통신망을 통해 상기 저장매체에 저장된 사용자의 인증서를 상기 단말에 구비된 인증서처럼 이용할 수 있도록 처리하는 것이다.

배 경 기 술

[0002] 통신망을 이용한 비대면 방식으로 뱅킹거래를 이용하거나, 또는 일정 금액 이상의 지불결제를 이용하기 위해서는 사용자에게 발급된 공인인증서를 이용한 인증서 처리가 수반되어야 한다.

[0003] 상기와 같은 인증서 처리를 위해서는 비대면 거래를 처리하는 사용자의 단말에 해당 사용자의 인증서가 저장되거나, 또는 상기 사용자의 단말과 연동 가능한 사용자의 휴대 매체(예컨대, USB메모리, IC카드, HSM, 플로피디스크 등)에 상기 사용자의 인증서 저장되어 있어야 한다.

[0004] 그러나 대부분의 사용자가 어느 하나의 특정 단말만을 이용하여 비대면 거래를 처리하는 것은 아니다. 사용자가 이용하는 단말이라면 어떠한 단말이라고 비대면 거래에 이용될 수 있다. 그러나 사용자의 인증서를 사용자가 이용 가능한 모든 단말에 저장하는 것은 보안상 치명적인 문제를 유발한다. 물론 사용자의 휴대 매체에 사용자의 인증서를 저장하고 상기 인증서 처리가 필요할 때마다 상기 휴대 매체로부터 상기 사용자의 인증서를 꺼내 쓸 수는 있다. 그러나 상기 사용자의 휴대 매체가 사용자가 이용하는 모든 단말과 연동 가능한 것은 결코 아니다. 즉 상기 사용자의 휴대 매체와 연동 가능한 모듈을 구비한 단말을 제외한 다른 단말에서는 상기 사용자의 휴대 매체에 저장된 인증서를 꺼내 쓸 수 없다.

발명의 내용

해결하려는 과제

[0005] 상기와 같은 문제점을 해소하기 위한 본 발명의 목적은, 사용자에게 발급된 인증서를 지정된 저장매체에 저장하고, 상기 저장된 인증서를 이용 가능한 N(N≥1)개의 단말을 지정 식별하여 등록한 후, 상기 사용자가 이용하는 단말로부터 상기 저장된 인증서를 이용할 수 있도록 요청되는 경우에 상기 사용자의 단말이 지정 등록된 N개의 단말 중 제n(1≤n≤N) 단말인지 인증하고, 상기 사용자의 단말이 상기 제n 단말로 인증되는 경우에 상기 사용자의 제n 단말을 통해 상기 저장된 인증서기 이용되도록 처리하는 클라우드 방식 인증서 운영 방법을 제공함에 있다.

과제의 해결 수단

[0006] 본 발명에 따른 클라우드 방식 인증서 운영 방법은, 서버에 의해 실행되는 클라우드 방식 인증서 운영 방법에 있어서, 사용자에게 발급된 인증서를 지정된 저장매체에 저장하는 제1 단계와, 상기 저장된 인증서를 이용 가능한 N(N≥1)개의 단말을 지정 식별하는 지정대상 식별정보를 저장하는 제2 단계와, 상기 사용자가 이용하는 단말이 상기 지정대상 식별정보에 의해 지정 식별되는 N개의 지정된 단말 중 제n(1≤n≤N) 단말인지 인증하는 제3 단계와, 상기 사용자의 단말이 상기 지정된 제n 단말로 인증된 경우에 상기 저장매체에 저장된 사용자의 인증서가 상기 제n 단말을 통해 이용되도록 처리하는 제4 단계를 포함한다.

[0007] 본 발명에 따르면, 상기 제1 단계는, 상기 저장매체에 저장되는 인증서를 발급받은 사용자에 대한 본인 인증 절차를 수행하는 단계를 더 포함하며, 상기 사용자의 본인 인증이 처리된 경우에 상기 사용자에게 발급된 인증서를 상기 저장매체에 저장할 수 있다.

[0008] 본 발명에 따르면, 상기 제1 단계는, 상기 사용자에게 상기 인증서를 발급한 인증서 서버로부터 상기 사용자에게 발급된 인증서를 제공받아 상기 저장매체에 저장하거나, 사용자의 단말로부터 상기 사용자에게 발급된 인증서를 제공받아 상기 저장매체에 저장하는 것 중 적어도 하나를 포함할 수 있다.

[0009] 본 발명에 따르면, 상기 저장매체에 저장되는 인증서는, 상기 사용자에게 발급된 인증서의 전체 구성을 포함하거나, 또는 상기 사용자에게 발급된 인증서의 일부 구성을 포함할 수 있다. 한편 상기 저장매체에 저장된 인증서에 일부 구성이 포함되는 경우, 상기 저장된 인증서의 일부 구성을 제외한 나머지 구성은, 상기 N개의 지정된 단말에 저장되거나, 또는 상기 N개의 지정된 단말을 통해 이용될 인증서를 저장하는 사용자 소유의 휴대 매체에 저장될 수 있다.

[0010] 본 발명에 따르면, 상기 인증서를 저장하는 저장매체는, 상기 인증서의 발급기관이 운영하는 저장매체, 상기 인증서의 등록기관이 운영하는 저장매체, 상기 서버에 구비된 저장매체, 상기 서버에서 접근 가능한 네트워크 상의 저장매체 중 적어도 하나를 포함할 수 있다.

[0011] 본 발명에 따르면, 상기 제2 단계는, 상기 인증서를 발급받은 사용자가 상기 인증서가 이용될 단말을 지정 등록하는지에 대한 사용자 본인 인증 절차를 수행하는 단계를 더 포함할 수 있다.

[0012] 본 발명에 따르면, 상기 제2 단계는, 상기 인증서를 발급받은 사용자를 고유 인증하는 사용자 식별정보를 획득하는 단계를 더 포함하며, 상기 N개의 지정대상 식별정보는, 사용자 식별정보와 매핑되어 저장될 수 있다.

[0013] 본 발명에 따르면, 상기 지정대상 식별정보는, 지정된 단말의 읽기/쓰기 메모리에 저장된 정보, 지정된 단말에 구비된 IC칩에 저장된 정보, 지정된 단말의 읽기전용 메모리에 기록된 정보, 지정된 단말의 하드웨어적 구성품에 할당된 정보, 지정된 단말의 통신식별 정보, 지정된 단말에서 생성된 정보, 지정된 단말에서 입력된 정보, 지정된 단말에 구비된 프로그램을 식별하는 정보, 지정된 코드생성모듈을 통해 동적 생성된 정보 중 적어도 하나 또는 둘 이상의 조합으로 이루어질 수 있다.

[0014] 본 발명에 따르면, 상기 클라우드 방식 인증서 운영 방법은, 상기 인증서가 이용될 단말로 등록 가능한 각 단말의 종류, 통신망 및 플랫폼 중 적어도 하나를 기준으로 각 단말의 지정대상 식별정보로 이용 가능한 M(M≥1)개의 지정 정보를 지정하는 지정대상 식별정보 조건이 설정되는 단계를 더 포함하며, 상기 제2 단계는, 상기 등록되는 단말의 지정대상 식별정보 조건에 부합하는 M개의 지정 정보 중에서 m(1≤m≤M)개의 지정 정보를 포함하는 지정대상 식별정보를 획득할 수 있다.

[0015] 본 발명에 따르면, 상기 제2 단계는, 단말 지정 등록을 위해 접속한 사용자의 단말을 상기 인증서를 이용 가능한 단말로 지정 등록하는 경우, 상기 사용자의 단말로부터 지정된 하나 이상의 지정 정보를 포함하는 지정대상 식별정보를 수신하거나, 상기 사용자의 단말을 관리하는 관리서버로부터 상기 사용자의 단말에 지정된 하나 이상의 지정 정보를 포함하는 지정대상 식별정보를 수신하는 것 중, 적어도 하나 또는 둘 이상의 조합을 통해 상기 사용자의 단말을 상기 저장된 인증서가 이용될 단말로 지정하는 지정대상 식별정보를 획득하는 단계를 더 포함할 수 있다.

[0016] 본 발명에 따르면, 상기 제2 단계는, 단말 지정 등록을 위해 접속한 사용자의 단말 이외에 상기 사용자가 이용 가능한 다른 단말을 상기 인증서를 이용 가능한 단말로 지정 등록하는 경우, 상기 사용자의 단말로부터 상기 인증서를 이용 가능한 단말로 등록되는 대상 단말에 지정된 하나 이상의 지정 정보를 포함하는 지정대상 식별정보를 수신하거나, 상기 사용자의 단말로부터 제공되는 상기 대상 단말에 대한 단말정보를 근거로 상기 대상 단말로부터 지정된 하나 이상의 지정 정보를 포함하는 지정대상 식별정보를 수신하거나, 상기 대상 단말을 관리하는 관리서버로부터 상기 대상 단말에 지정된 하나 이상의 지정대상 식별정보를 수신하는 것 중, 적어도 하나 또는 둘 이상의 조합을 통해 상기 사용자가 이용 가능한 단말을 상기 저장된 인증서가 이용될 단말로 지정하는 지정대상 식별정보를 획득하는 단계를 더 포함할 수 있다.

[0017] 본 발명에 따르면, 상기 제3 단계는, 상기 인증서를 발급받은 사용자가 상기 저장된 인증서를 요청하는지에 대한 사용자 본인 인증 절차와, 상기 N개의 단말을 등록한 사용자가 상기 저장된 인증서를 요청하는지에 대한 사용자 본인 인증 절차 중, 적어도 하나의 본인 인증 절차를 수행하는 단계를 더 포함할 수 있다.

[0018] 본 발명에 따르면, 상기 제3 단계는, 상기 사용자를 고유 인증하는 사용자 식별정보가 상기 지정대상 식별정보와 매핑되어 저장된 경우, 상기 사용자의 단말로부터 수신되는 사용자 식별정보와 상기 저장된 사용자 식별정보를 비교하여 상기 사용자를 인증하는 단계를 더 포함할 수 있다.

[0019] 본 발명에 따르면, 상기 제3 단계는, 상기 사용자의 단말로부터 상기 저장된 지정대상 식별정보에 포함된 하나 이상의 지정 정보와 매칭되는 지정대상 식별정보를 수신하는 단계와, 상기 수신된 지정대상 식별정보와 상기 저장된 지정대상 식별정보를 비교하여 상기 사용자의 단말을 상기 지정된 제n 단말로 인증하는 단계를 더 포함할 수 있다.

[0020] 본 발명에 따르면, 상기 제3 단계는, 지정대상 식별정보로 이용 가능한 M(M≥1)개의 지정 정보 중에서 상기 사용자의 단말을 지정 식별하는데 이용되는 m(1≤m≤M)개의 지정 정보를 포함하는 지정대상 식별정보의 구성을 확인하는 단계와, 상기 사용자의 단말로부터 상기 m개의 지정 정보를 포함하는 지정대상 식별정보를 수신하는 단계와, 상기 수신된 지정대상 식별정보와 상기 저장된 지정대상 식별정보를 비교하여 상기 사용자의 단말을 상기 지정된 제n 단말로 인증하는 단계를 더 포함할 수 있다.

[0021] 본 발명에 따르면, 상기 지정대상 식별정보는, 지정된 단말에 고정 유지된 둘 이상의 지정 정보를 포함하며, 상기 지정된 단말에 고정 유지된 둘 이상의 정보 중 일부는 인증되고 나머지 일부는 인증되지 않는 경우에 상기 지정대상 식별정보에 대한 폐기 절차 또는 재등록 절차를 수행하는 단계를 더 포함할 수 있다.

[0022] 본 발명에 따르면, 상기 제4 단계는, 상기 저장된 사용자의 인증서를 상기 제n 단말로 제공할 수 있다.

[0023] 본 발명에 따르면, 상기 제4 단계는, 상기 사용자에게 발급된 인증서의 일부 구성을 상기 제n 단말로 제공하는

것을 특징으로 하며, 상기 제n 단말은, 상기 제공되는 인증서의 일부 구성을 제외한 나머지 구성이 구비되어 있거나, 상기 사용자 소유의 휴대 매체에 구비된 상기 인증서의 나머지 구성을 이용 가능할 수 있다. 한편 상기 인증서의 일부 구성은, N개의 지정된 단말에 대하여 동일하거나, 또는 N개의 지정된 단말 별로 서로 다른 것을 특징으로 하며, 상기 인증서의 나머지 구성은, N개의 지정된 단말에 대하여 동일하거나, 또는 N개의 지정된 단말 별로 서로 다를 수 있다.

[0024] 본 발명에 따르면, 상기 제4 단계는, 상기 저장된 사용자의 인증서를 통해 상기 제n 단말의 인증서 처리를 대행할 수 있다.

발명의 효과

[0025] 본 발명에 따르면, 비대면 거래를 위해 사용자가 이용하는 단말이 통신망에 연결되어 있기만 한다면 언제 어디서나 해당 단말을 통해 네트워크 상의 지정된 저장매체에 저장된 사용자의 인증서를 이용하여 상기 비대면 거래를 위한 인증서 처리가 가능해지는 이점이 있다.

도면의 간단한 설명

[0026] 도 1은 본 발명에 따른 클라우드 방식 인증서 운영 시스템 구성을 도시한 도면이다.

도 2는 본 발명의 실시 방법에 따라 사용자의 단말에 구비되는 애플리케이션의 기능 구성을 도시한 도면이다.

도 3은 본 발명에 따른 클라우드 방식 인증서 운영에서 인증서를 등록하는 과정을 도시한 도면이다.

도 4는 본 발명에 따른 클라우드 방식 인증서 운영에서 인증서를 이용 가능한 단말을 지정 등록하는 과정을 도시한 도면이다.

도 5는 본 발명에 따른 클라우드 방식 인증서 운영에서 인증서를 이용 가능한 사용자를 등록하는 과정을 도시한 도면이다.

도 6은 본 발명에 따른 클라우드 방식 인증서 운영에서 저장매체에 등록된 인증서를 확인/추출하는 과정을 도시한 도면이다.

도 7 또는 도 8은 본 발명의 실시 방법에 따라 클라우드 방식으로 인증서를 이용하는 과정을 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0027] 이하 첨부된 도면과 설명을 참조하여 본 발명의 바람직한 실시예에 대한 동작 원리를 상세히 설명한다. 다만, 하기에 도시되는 도면과 후술되는 설명은 본 발명의 특징을 효과적으로 설명하기 위한 여러 가지 방법 중에서 바람직한 실시 방법에 대한 것이며, 본 발명이 하기의 도면과 설명만으로 한정되는 것은 아니다. 예를들어, 서버 측에 구비된 구성부가 단말 측에 구현되거나, 반대로 단말 측에 구비된 구성부가 서버 측에 구현되는 형태로 실시되는 것이 가능하다.

[0028] 또한, 하기에서 본 발명을 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서, 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 발명에서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0029] 결과적으로, 본 발명의 기술적 사상은 청구범위에 의해 결정되며, 이하 실시예는 진보적인 본 발명의 기술적 사상을 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 효율적으로 설명하기 위한 일 수단일 뿐이다.

[0030] 도면1은 본 발명에 따른 클라우드 방식 인증서 운영 시스템 구성을 도시한 도면이다.

[0031] 보다 상세하게 본 도면1은 네트워크 상의 지정된 저장매체(115)에 사용자에게 발급된 인증서를 저장한 후에, 상기 사용자가 이용하는 단말(200)이 통신망을 통해 상기 저장매체(115)에 저장된 인증서를 이용할 수 있도록 처리하는 시스템 구성을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면1을 참조 및/또는 변형하여 상기 클라우드 방식 인증서 운영 시스템에 대한 다양한 실시 방법(예컨대, 일부 구성부가 생략되거나, 또는 세분화되거나, 또는 합쳐진 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면1에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다. 바람직하게, 본 발명의 도면을 통해 설명되는 실시 방법은 상기 저장매체(115)에 저장된 인증서를 이용 가능한 단말이 미리 지정되는 구성을 기본 구성으로 하여 본 발명의 특징을 설명하기로 한다. 그러나 본 발명의 기술적 특징이 이에 의해 한정되는 것은 결코 아니며, 상기 저장매체(115)에 인증서가 저장되는 시점과 상기 저장된 인증서가 이용되는 시점의 사용자 본인 인증 절차에 대한 보안성을 유지할 수 있다면, 상기 인증서를 이용 가능한 단말을 지정하는 구성이 생략될 수 있음을 밝혀두는 바이며, 본 발명은 이와 같이 본 발명의 일부 구성을 생략하거나 또는 변형하여 실시되는 모든 실시 방법을 포함함을 명백하게 밝혀두는 바이다.

[0032] 본 발명의 클라우드 방식 인증서 운영 시스템은, 인증서를 발급받은 사용자가 이용하는 하나 이상의 단말(200)과, 상기 사용자에게 발급된 인증서를 지정된 저장매체(115)에 저장하고, 상기 사용자가 이용하는 단말(200)이 통신망을 통해 상기 저장매체(115)에 저장된 인증서를 이용하도록 요청하는 경우에 상기 사용자의 요청에 따라 상기 사용자의 단말(200)을 통해 상기 저장매체(115)에 저장된 인증서가 이용될 수 있도록 처리하는 운영 서버(100)를 포함하여 구성된다. 상기 운영 서버(100)는 실시 방법에 따라 적어도 하나 또는 둘 이상의 서버 조합의 형태로 구현될 수 있으며, 상기 클라우드 방식의 인증서를 운영하는 사업자 측에 구축될 수 있음은 물론, 상기 인증서를 발급한 발급기관이나 상기 인증서의 등록기관(예컨대, 금융기관 등) 및 각종 제휴기관(예컨대, 금융결제원 등)을 포함하여 네트워크 상에 존재하는 서버라면 어떠한 형태로도 구축될 수 있다. 또한 본 발명이 실시되는 시점의 비즈니스 여건과 관련 법률에 따라 상기 운영 서버(100)의 일부 구성은 사업자 측에 구축되고 나머지 일부 구성은 상기 발급기관이나 등록기관 또는 제휴기관 등에 구출되는 것이 가능함을 밝혀두는 바이다. 아울러 본 발명의 도면과 설명은 하나의 운영 서버(100)에서 본 발명의 클라우드 방식 인증서를 운영하는 것으로 도시하여 설명하지만, 상기 운영 서버(100)가 둘 이상의 서버 형태로 구현될 경우에 상기 둘 이상의 서버 중 서버(2)에서 특정 프로세스를 실제로 처리하지만 이를 위해 단말 또는 서버(1)에서 상기 서버(2)의 특정 프로세스를 유발하거나 이와 연관된 프로세스가 수행되는 경우에 상기 단말 또는 서버(1)에서도 상기 특정 프로세스가 “~되도록 처리”한다는 용어를 사용할 수 있음을 밝혀두는 바이다.

[0033] 상기 사용자가 이용하는 단말(200)은 상기 사용자가 소유한 단말은 물론 상기 사용자가 인증서 등록 또는 이용을 위해 이용할 수 있는 모든 단말의 총칭으로서, 바람직하게, 사용자가 이용하는 개인컴퓨터와 노트북 등을 포함하는 유선단말(200), 사용자의 휴대폰, 스마트폰, 태블릿PC 등을 포함하는 무선단말(200)을 포함할 수 있다. 그러나 상기 사용자의 단말(200)이 상술된 유선단말(200)과 무선단말(200)로 한정되는 것은 아니며, 통신망에 연결되는 결제단말(200)(예컨대, POS, CAT 등), 금융단말(200)(예컨대, CD, ATM), 통화단말(200)(예컨대, 유선전화, 무선전화, VoIP폰), 가전단말(200) 등 모든 종류의 단말을 포함할 수 있음을 명백하게 밝혀두는 바이다.

[0034] 본 발명의 실시 방법에 따르면, 상기 사용자의 단말(200)은 상기 인증서 등록 또는 이용을 위해 하나 이상의 프로그램이 탑재될 수 있다. 상기 프로그램은 상기 사용자의 단말(200)의 운영체제에서 동작하는 애플리케이션의 형태로 구현되어 상기 사용자의 단말(200)에 탑재되거나, 또는 상기 사용자의 단말(200)에 구비된 응용프로그램(예컨대, 브라우져, 뱅킹프로그램, 결제프로그램 등)에 플러그인 처리되는 플러그인프로그램(예컨대, 액티브엑스 등)의 형태로 상기 사용자의 단말(200)에 탑재될 수 있다. 한편 상기 사용자의 단말(200)이 브라우져를 통해 상기 운영 서버(100)에 접속하는 경우에 상기 운영 서버(100)는 상기 사용자의 단말(200)로 제공하는 페이지에 상기 인증서 등록 또는 이용을 위한 프로그램코드(예컨대, 자바스크립트 등)를 삽입하여 상기 사용자의 단말(200)로 제공할 수 있으며, 이 경우에 상기 사용자의 단말(200)에는 별도의 프로그램이 탑재되지 않더라도

[0035] 상기 운영 서버(100)는 통신망을 이용하여 하나 이상의 사용자의 단말(200)을 대상으로 본 발명에 따른 클라우드 방식 인증서를 운영하는 적어도 하나의 서버 또는 둘 이상의 서버 조합의 총칭으로서, 상기 사용자에게 발급된 인증서를 지정된 저장매체(115)에 저장하는 절차와, 상기 저장된 인증서를 이용 가능한 N(N≥1)개의 단말(200)을 지정 식별하는 지정대상 식별정보를 저장하는 절차와, 상기 사용자가 이용하는 단말(200)이 상기 지정대상 식별정보에 의해 지정 식별되는 N개의 지정된 단말(200) 중 제n(1≤n≤N) 단말(200)인지 인증하는 절차와, 상기 사용자의 단말(200)이 상기 지정된 제n 단말(200)로 인증된 경우에 상기 저장매체(115)에 저장된 사용자의 인증서가 상기 제n 단말(200)을 통해 이용되도록 처리하는 절차를 수행한다. 만약 상기 운영 서버(100)가 둘 이상의 서버 조합으로 이루어지는 경우에 상기 절차는 각 서버에서 상호 연동하여 수행될 수 있음을 명백하게 밝혀두는 바이다. 아울러 상기 사용자의 단말(200)과 운영 서버(100)는 통신망을 통한 인증서 이용이 가능한 수준의 보안 프로토콜(예컨대, 암/복호화 방식, 키 교환 알고리즘 등)이 설정되며, 이에 대한 상세한 설명은 편의상 생략하기로 한다.

[0036] 도면1을 참조하면, 상기 운영 서버(100)는, 지정된 저장매체(115)에 저장될 인증서를 발급받은 사용자에 대한 본인 인증 절차를 수행하는 본인 인증 절차부(120)와, 상기 저장매체(115)에 저장될 사용자의 인증서를 획득하는 인증서 획득부(105)와, 상기 획득된 사용자의 인증서를 지정된 저장매체(115)에 저장하는 인증서 저장부(110)를 구비한다.

[0037] 운영 서버(100)에 접속한 사용자의 단말(200)로부터 상기 사용자에게 발급된 인증서를 지정된 저장매체(115)에 등록하도록 요청되는 경우, 상기 본인 인증 절차부(120)는 상기 사용자에 대한 하나 이상의 본인 인증 절차를 수행한다. 바람직하게, 상기 사용자에 대한 본인 인증은, 상기 사용자가 상기 운영 서버(100)의 회원으로 가입된 경우에 상기 사용자의 단말(200)로부터 상기 사용자에 대한 ID/PW를 제공받아 인증하는 ID/PW 인증, 상기 사용자의 단말(200)로부터 상기 사용자의 성명과 주민등록번호를 포함하는 개인정보를 제공받고 이를 실명인증 서버(도시생략)로 제공하여 상기 사용자의 실명을 인증받는 인터넷 실명 인증, 상기 사용자의 단말(200)로부터 상기 사용자가 가입한 가입통신망(예컨대, 이동통신망, 전화망, VoIP망 등)의 통신수단정보(예컨대, 통신사정보, 전화번호, 장치식별정보 등)를 제공받고 상기 사용자의 개인정보와 통신수단정보를 상기 가입통신망의 통신사서버(도시생략)로 제공하여 상기 사용자에 대한 가입자 명의를 인증받는 통신 가입자 인증, 상기 사용자의 단말(200)로부터 카드사에서 상기 사용자에게 발급한 카드에 대한 카드식별정보(예컨대, 카드사 정보와 카드번호 등)를 제공받고 상기 사용자의 개인정보와 카드식별정보를 상기 카드를 발급한 카드사서버(도시생략)로 제공하여 상기 카드의 명의자를 인증받는 카드 명의자 인증, 상기 사용자의 단말(200)로부터 은행에 개설된 사용자의 계좌에 대응하는 계좌식별정보(예컨대, 은행 정보와 계좌번호 등)를 제공받고 상기 사용자의 개인정보와 계좌식별정보를 상기 계좌가 개설된 은행서버(도시생략)로 제공하여 상기 계좌의 명의자를 인증받는 계좌 명의자 인증, 인증번호를 생성하여 사용자의 무선단말로 발송한 후에 상기 사용자의 단말(200)로 입력(여기서, 상기 인증번호가 입력되는 사용자의 단말(200)은 상기 인증번호를 수신한 무선단말은 물론 상기 무선단말 이외에 사용자가 이용하는 단말(200)을 포함)되어 수신되는 인증번호를 비교 인증하는 무선단말 점유 인증, 상기 사용자의 단말(200)에 상기 사용자에게 발급된 인증서가 존재하는 경우에 상기 사용자의 단말(200)에 구비된 인증서(예컨대, 사용자에게 기 발급된 공인인증서 등)를 이용한 인증서 인증, 중에서 상기 운영 서버(100)에 의해 지정한 적어도 하나 또는 둘 이상의 본인 인증을 포함할 수 있다. 그러나 본 발명의 본인 인증 절차가 상술된 방식으로만 한정되는 것은 결코 아니며, 통신망을 통해 사용자의 본인 여부를 인증할 수 있는 방식이면 어떤 방식이 적용되어도 무방하며, 본 발명의 본인 인증은 상술된 방식 이외에도 사용자의 본인 여부를 인증할 수 있는 모든 방식의 본인 인증(예컨대, ARS를 이용한 본인 인증, 신분증을 이용한 대면 방식의 본인 인증, 화상(안면) 인식을 통한 본인 인증, 생체 정보를 이용한 본인 인증 등)을 포함함을 명백하게 밝혀두는 바이다.

[0038] 본 발명의 실시 방법에 따르면, 상기 본인 인증 절차부(120)는 인증서를 발급받은 사용자에 대한 본인 인증을 처리하기 위한 i(i≥1)개의 본인 인증 방식이 설정되어 있으며, 상기 본인 인증 절차부(120)는 지정된 순서에 따라 상기 설정된 i개의 본인 인증 절차를 수행하여 인증서를 발급받은 사용자에 대한 본인 인증을 처리한다.

[0039] 상기 인증서 획득부(105)는 지정된 저장매체(115)에 저장될 사용자의 인증서를 획득한다. 상기 사용자의 인증서

는 인증서 발급기관에서 상기 사용자에게 발급한 인증서의 원본이거나, 또는 상기 인증서 발급기관에서 상기 사용자에게 발급한 인증서의 사본이거나, 또는 상기 인증서 발급기관에서 상기 사용자에게 발급된 후 이를 복사한 인증서의 복사본 중 적어도 하나를 포함할 수 있다.

[0040] 본 발명의 제1 인증서 획득 방식에 따르면, 상기 인증서 획득부(105)는 상기 사용자에게 상기 인증서를 발급한 인증서 발급기관에 구비된 인증서 서버로부터 상기 사용자에게 발급된 인증서를 획득할 수 있다. 바람직하게, 사용자는 상기 인증서 발급기관으로 인증서 발급을 신청하며, 상기 인증서 발급기관으로부터 상기 인증서 발급 승인(또는 발급)됨에 따라 상기 사용자의 단말(200)로부터 상기 사용자에게 발급되는 인증서에 대한 인증서 발급정보(예컨대, 인증서 발급기관에서 인증서를 발급받을 사용자에게 전달한 각종 정보)가 수신되면, 상기 인증서 획득부(105)는 상기 인증서 발급정보를 근거로 상기 인증서 서버로부터 상기 사용자에게 발급되는 인증서를 획득할 수 있다.

[0041] 본 발명의 제2 인증서 획득 방식에 따르면, 상기 인증서 획득부(105)는 상기 사용자에게 발급된 인증서의 사본을 저장 또는 관리하는 관리기관에 구비된 기관 서버로부터 상기 사용자에게 발급된 인증서를 획득할 수 있다. 바람직하게, 상기 사용자에게 발급된 인증서의 사본은 상기 인증서의 발급 신청을 처리하는 등록기관이나 상기 사용자의 인증서를 통한 각종 인증을 처리하는 금융기관 등을 포함하는 관리기관의 기관 서버에 저장될 수 있으며, 상기 인증서 획득부(105)는 상기 사용자의 인증서 사본을 관리하는 기관 서버로부터 상기 사용자에게 발급된 인증서를 획득할 수 있다.

[0042] 본 발명의 제3 인증서 획득 방식에 따르면, 상기 인증서 획득부(105)는 사용자의 단말(200)로부터 상기 사용자에 발급된 인증서를 복사하거나 또는 이전시키는 형태로 상기 사용자의 인증서를 획득할 수 있다. 바람직하게, 상기 사용자의 단말(200)에 구비된 메모리(예컨대, 컴퓨터에 구비된 하드디스크, 무선단말(200)에 구비된 비휘발성 메모리 등)나 또는 상기 사용자의 단말(200)과 연동 가능한 사용자의 각종 휴대 매체(예컨대, USB메모리, IC카드, HSM, 플로피디스크 등)에 상기 사용자에게 발급된 인증서가 보관될 수 있으며, 상기 인증서 획득부(105)는 상기 사용자의 단말(200)로부터 상기 단말(200)의 메모리나 각종 휴대 매체에 보관된 인증서를 지정된 인증서 복사/이동 절차에 따라 획득할 수 있다.

[0043] 한편 상기 획득된 사용자의 인증서가 상기 인증서 서버로부터 획득된 것이 아니라면, 상기 인증서 획득부(105)는 상기 획득된 사용자의 인증서가 상기 인증서 서버를 통해 상기 인증서 발급기관에서 상기 사용자에게 발급된 인증서와 동일한 인증서인지 검증할 수 있다. 바람직하게, 상기 인증서 획득부(105)는 상기 획득된 인증서를 상기 인증서 서버로 제공하여 상기 인증서의 유효성을 검증 받거나, 또는 상기 인증서에 대응하는 인증서 파일을 해시한 해시 값을 상기 인증서 서버로 제공하여 상기 인증서의 유효성을 검증 받거나, 또는 상기 인증서 서버로부터 사용자에 발급된 인증서 원본에 대한 해시 값을 수신한 후 상기 획득된 인증서의 해시 값과 비교하여 상기 인증서의 유효성을 검증할 수 있다. 상기 사용자의 인증서가 검증된다고 함은, 상기 획득된 인증서는 상기 사용자에게 발급된 인증서의 원본과 동일한 인증서로서 해당 인증서의 위/변조나 손상이 전혀 없음을 의미한다.

[0044] 상기 사용자의 인증서가 획득되면, 상기 인증서 저장부(110)는 상기 획득된 사용자의 인증서를 지정된 저장매체(115)에 저장한다. 상기 인증서가 저장되는 저장매체(115)는, 네트워크 상에서 사용자의 인증서를 보관할 만큼의 보안성이 확보된 저장용 매체의 총칭으로서, 실시 방법에 따라 상기 인증서의 발급기관이 운영하는 저장매체(115), 상기 인증서의 등록기관이 운영하는 저장매체(115), 상기 운영 서버(100)에 구비된 저장매체(115), 상기 운영 서버(100)에서 접근 가능한 네트워크 상의 저장매체(115) 중 적어도 하나일 수 있다. 본 도면1은 편의상 상기 저장매체(115)가 상기 운영 서버(100)에 구비된 것으로 도시하여 설명하기로 한다.

[0045] 본 발명의 실시 방법에 따르면, 상기 저장매체(115)에 저장되는 사용자의 인증서는, 상기 사용자에게 발급된 인증서의 전체 구성을 포함하거나, 또는 상기 사용자에게 발급된 인증서의 일부 구성을 저장하는 것이 모두 가능하다. 바람직하게, 상기 인증서의 일부 구성이라 함은, 상기 사용자의 인증서에 대응하는 인증서 파일을 구성하

는 T(T≥1)개의 구성 항목 중에서 t(1≤t<T)개의 구성 항목을 포함하여 이루어질 수 있다. 또는 상기 인증서의 일부 구성은, 상기 인증서 파일을 구성하는 T개의 구성 항목 중 t개의 구성 항목의 일부 구성 값을 포함하여 이루어질 수 있다. 예를들어, 상기 인증서 파일을 구성하는 T개의 구성 항목 중 특정 구성 항목의 구성 값이 "123456789"일 경우에, 상기 인증서의 일부 구성은 상기 "123456789"라는 구성 값 중에서 "12345" 또는 "13579"와 같은 일부 구성 값을 포함할 수 있다.

[0046] 한편 상기 저장매체(115)에 저장된 인증서에 일부 구성이 포함되는 경우, 상기 저장된 인증서의 일부 구성을 제외한 나머지 구성은, 상기 인증서를 이용하는 N개의 지정된 단말(200)에 저장되거나, 또는 상기 N개의 지정된 단말(200)을 통해 인증될 인증서를 저장하는 사용자 소유의 휴대 매체(예컨대, USB메모리, IC카드, HSM, 플로피 디스크 등)에 저장될 수 있다.

[0047] 본 발명의 실시 방법에 따르면, 상기 저장매체(115)에 저장되는 사용자의 인증서는, 상기 저장되는 인증서가 누구에게 발급된 인증서인지를 고유 식별하는 사용자 식별정보와 매핑되어 저장될 수 있다.

[0048] 도면1을 참조하면, 상기 운영 서버(100)는, 상기 인증서를 발급받은 사용자가 상기 인증서가 이용될 단말(200)을 지정 등록하는지에 대한 사용자 본인 인증 절차를 수행하는 본인 인증 절차부(120)와, 상기 저장된 인증서를 이용 가능한 단말(200)을 지정 식별하는 지정대상 식별정보를 획득하는 식별정보 획득부(125)와, 상기 식별정보 획득부(125)에 의해 획득되는 N(N≥1)개의 지정된 단말(200)에 대한 N개의 지정대상 식별정보를 저장하는 식별정보 저장부(130)를 구비한다. 만약 본 발명의 실시 방법에 따라 상기 인증서를 이용 가능한 단말(200)을 지정 식별하여 등록하지 않는다면 상기 식별정보 획득부(125)와 식별정보 저장부(130)는 생략 가능하다.

[0049] 상기 사용자의 인증서가 지정된 저장매체(115)에 저장되기 전, 중, 후의 어느 시점에, 상기 저장매체(115)에 저장되는 인증서를 이용 가능한 단말(200)을 지정 등록하는 절차가 수행되며, 이를 위해 상기 본인 인증 절차부(120)는 상기 인증서를 이용 가능한 단말(200) 지정 등록을 상기 운영 서버(100)에 접속한 사용자의 단말(200)과 연동하여 상기 인증서를 발급받은 사용자가 상기 인증서가 이용될 단말(200)을 지정 등록하는지에 대한 하나 이상의 사용자 본인 인증 절차를 수행한다. 바람직하게, 상기 사용자에 대한 본인 인증은, ID/PW 인증, 인터넷 실명 인증, 통신 가입자 인증, 카드 명의자 인증, 계좌 명의자 인증, 무선단말 점유 인증, 인증서 인증 중에서 상기 운영 서버(100)에 의해 지정한 적어도 하나 또는 둘 이상의 본인 인증을 포함할 수 있으며, 상술된 방식 이외에도 다양한 형태의 본인 인증이 수행될 수 있음은 전술한 바와 같다.

[0050] 본 발명의 실시 방법에 따르면, 상기 본인 인증 절차부(120)는 상기 인증서를 발급받은 사용자가 상기 인증서가 이용될 단말(200)을 지정 등록하는지에 대한 사용자 본인 인증을 처리하기 위한 j(j≥1)개의 본인 인증 방식이 설정되어 있으며, 상기 본인 인증 절차부(120)는 지정된 순서에 따라 상기 설정된 j개의 본인 인증 절차를 수행하여 상기 인증서를 발급받은 사용자가 상기 인증서가 이용될 단말(200)을 지정 등록하는지에 대한 사용자 본인 인증을 처리한다. 상기 사용자에게 발급된 인증서의 등록 절차와 단말 지정 등록 절차가 연결되어 일괄적으로 처리되는 경우에 상기 사용자에 대한 본인 인증 절차는 1회만 수행되는 것이 가능하다. 그러나 본 발명의 단말 지정 등록 절차는 지정된 한도 내에서 반복 수행되는 것이 가능하며, 이 경우에 상기 단말 지정 등록 절차를 위한 사용자 본인 인증이 수행될 수 있다.

[0051] 상기 식별정보 획득부(125)는 상기 인증서 저장부(110)에 의해 지정된 저장매체(115)에 저장된 인증서를 이용 가능한 단말(200)을 지정 식별하는 지정대상 식별정보를 획득한다. 바람직하게, 상기 지정대상 식별정보는, 상기 지정 등록되는 단말(200)의 읽기/쓰기 메모리에 저장된 정보, 지정 등록되는 단말(200)에 구비된 IC칩에 저장된 정보, 지정 등록되는 단말(200)의 읽기전용 메모리에 기록된 정보, 지정 등록되는 단말(200)의 하드웨어적 구성품에 할당된 정보, 지정 등록되는 단말(200)의 통신식별 정보, 지정 등록되는 단말(200)에서 생성된 정보, 지정 등록되는 단말(200)에서 입력된 정보, 지정 등록되는 단말(200)에 구비된 프로그램을 식별하는 정보, 지정

된 코드생성모듈을 통해 동적 생성된 정보 중 적어도 하나 또는 둘 이상의 조합으로 이루어질 수 있다.

[0052] 상기 지정 등록되는 단말(200)의 읽기/쓰기 메모리에 저장된 정보는, 상기 지정 등록되는 단말(200)의 하드디스크, 비휘발성 읽기/쓰기 메모리 등에 저장되어 상기 지정 등록되는 단말(200)을 고유하게 식별하는 정보의 총칭으로서, 바람직하게 상기 메모리에 저장된 각종 키 값, 상기 인증서 이용과 관련(또는 지정된)된 프로그램의 식별 값, 상기 프로그램에 의해 생성되어 저장된 값, 상기 프로그램을 통해 통신망으로부터 수신되어 저장된 값, 상기 프로그램의 고유 값(예컨대, 프로그램의 일련번호, 프로그램에 할당된 토큰 등), 운영체제 고유 값(예컨대, 운영체제의 일련번호 등), 운영체제에 의해 저장된 값, 상기 메모리에 저장된 사용자의 인증서, 상기 저장매체(115)에 저장되는 사용자 인증서의 나머지 일부 구성, 카드정보, 계좌정보, 금융정보 중 적어도 하나의 지정 정보를 포함할 수 있다.

[0053] 상기 지정 등록되는 단말(200)에 구비된 IC칩에 저장된 정보는, 상기 지정 등록되는 단말(200)에 탑재 또는 이탈착되는 IC칩(예컨대, USIM, 금융IC칩, SE(Security Element) 등)에 저장되어 상기 IC칩을 통해 상기 지정 등록되는 단말(200)을 고유하게 식별하는 정보의 총칭으로서, 바람직하게 상기 IC칩의 고유코드, 칩 일련번호, 상기 IC칩에 구비된 애플릿 식별코드, 상기 IC칩에 저장된 키 값, 상기 IC칩에 저장된 사용자의 인증서, 상기 저장매체(115)에 저장되는 사용자 인증서의 나머지 일부 구성, 카드정보, 계좌정보, 금융정보 중 적어도 하나의 지정 정보를 포함할 수 있다.

[0054] 상기 지정 등록되는 단말(200)의 읽기전용 메모리에 기록된 정보는, 상기 지정 등록되는 단말(200)에 구비된 ROM 또는 상기 단말(200)을 구성하는 하드웨어적 구성품의 ROM에 저장되는 정보의 총칭으로서, 바람직하게 상기 메모리에 저장된 각종 키 값, 고유코드, 식별코드, 일련번호 중 적어도 하나의 지정 정보를 포함할 수 있다.

[0055] 상기 지정 등록되는 단말(200)의 하드웨어적 구성품에 할당된 정보는, 상기 지정 등록되는 단말(200)을 구성하는 하드웨어적 구성품의 제조사에 의해 상기 하드웨어적 구성품에 할당되는 정보의 총칭으로서, 바람직하게 상기 지정되는 단말(200)을 구성하는 CPU에 할당된 고유코드, 메인보드에 할당된 고유코드, 메모리에 할당된 고유코드, 하드디스크에 할당된 고유코드, 비휘발성 메모리에 할당된 고유코드, 통신모듈에 구비된 고유코드(예컨대, MAC 주소 등), 입력모듈에 할당된 고유코드, 출력모듈(예컨대, 디스플레이)에 할당된 고유코드 중 적어도 하나의 지정 정보를 포함할 수 있다.

[0056] 상기 지정 등록되는 단말(200)의 통신식별 정보는, 상기 지정 등록되는 단말(200)의 통신망 접속을 위해 상기 단말(200)에 할당되는 정보의 총칭으로서, 바람직하게 상기 단말(200)이 접속하는 통신망의 종류/프로토콜에 따라 IP주소, MAC주소, 전화번호 등을 적어도 하나 포함함은 물론, 상기 단말(200)이 접속하는 통신망에 등록되는 네트워크ID, 시스템ID, 가입자 식별 값 중 적어도 하나의 지정 정보를 포함할 수 있다.

[0057] 상기 지정 등록되는 단말(200)에서 생성된 정보는, 상기 지정 등록되는 단말(200)에 구비된 프로그램에 의해 동적 생성되는 정보의 총칭으로서, 바람직하게 상기 지정 등록되는 단말(200)에서 동적 생성되는 일회용코드, 각종 키 값을 적어도 하나 포함함은 물론, 상기 동적 생성되는 일회용코드나 각종 키 값을 가공(예컨대, 문자, 이미지, 1/2차원 바코드, 사운드, 멀티미디어 등의 형태로 가공)하거나 또는 상기 동적 생성되는 일회용코드나 각종 키 값을 이용하여 다른 정보를 가공(예컨대, 암호화 등)한 정보 중 적어도 하나의 지정 정보를 포함할 수 있다.

[0058] 상기 지정 등록되는 단말(200)에서 입력된 정보는, 상기 지정 등록되는 단말(200)에 구비된 입력모듈을 통해 키 입력되는 정보의 총칭으로서, 바람직하게 상기 입력되는 정보는 사용자의 기억을 토대로 키 입력되는 정보(예컨대, 비밀번호, PIN 등), 다른 단말기나 매체에 표시된 상태에서 키 입력되는 정보 중 적어도 하나의 지정 정보를 포함할 수 있다.

[0059] 상기 지정 등록되는 단말(200)에 구비된 프로그램을 식별하는 정보는, 상기 인증서 이용과 관련하여 상기 지정 등록되는 단말(200)에 구비된 프로그램을 식별하거나 또는 상기 지정 등록되는 단말(200)에 필수적으로 구비되는 프로그램을 식별하는 정보의 총칭으로서, 바람직하게 상기 프로그램의 식별 값, 상기 프로그램에 의해 생성된 값, 상기 프로그램을 통해 통신망으로부터 수신된 값, 상기 프로그램의 고유 값(예컨대, 프로그램의 일련번호, 프로그램에 할당된 토큰 등) 중 적어도 하나의 지정 정보를 포함할 수 있다.

[0060] 상기 지정된 코드생성모듈을 통해 동적 생성된 정보는, 상기 지정 등록되는 단말(200)에 구비된 코드생성모듈이나 또는 상기 지정 등록되는 단말(200)과 관련된 외부 장치나 서버에 구비된 코드생성모듈에 의해 동적 생성되는 정보의 총칭으로서, 바람직하게 상기 지정된 코드생성모듈을 통해 동적 생성되는 일회용코드, 각종 키 값을 적어도 하나의 지정 정보를 포함함 물론, 상기 동적 생성되는 일회용코드나 각종 키 값을 가공(예컨대, 문자, 이미지, 1/2차원 바코드, 사운드, 멀티미디어 등의 형태로 가공)한 지정 정보, 또는 상기 동적 생성되는 일회용코드나 각종 키 값을 이용하여 다른 정보를 가공(예컨대, 암호화 등)한 지정 정보 중 적어도 하나의 지정 정보를 포함할 수 있다. 한편 상기 지정된 코드생성모듈이 상기 지정 등록되는 단말(200)의 외부에 존재하는 경우에 상기 코드생성모듈에 의해 동적 생성된 지정 정보는 통신망을 통해 상기 지정 등록되는 단말(200)로 수신되거나, NFC를 통해 상기 지정 등록되는 단말(200)로 수신되거나, 상기 지정 등록되는 단말(200)에 구비된 카메라를 통해 상기 지정 등록되는 단말(200)로 인식(예컨대, 1/2차원 바코드 인식)될 수 있다.

[0061] 그러나 본 발명의 지정대상 식별정보를 구성하는 지정 정보들이 상술된 지정 정보로 한정되는 것은 결코 아니며, 상기 지정 등록되는 단말(200)을 지정 식별할 수 있는 지정 정보라면 어떠한 정보라도 상기 지정대상 식별정보에 포함될 수 있으며, 본 발명의 지정대상 식별정보는 상기 지정 등록되는 단말(200)을 지정 식별할 수 있는 모든 지정 정보를 포함함을 명백하게 밝혀두는 바이다.

[0062] 본 발명의 실시 방법에 따르면, 상기 식별정보 획득부(125)는 상기 인증서가 이용될 단말(200)로 등록 가능한 각 단말(200)의 종류, 통신망 및 플랫폼 중 적어도 하나를 기준으로 각 단말(200)의 지정대상 식별정보로 이용 가능한 M(M≥1)개의 지정 정보를 지정하는 지정대상 식별정보 조건이 설정되어 있을 수 있으며, 이 경우에 상기 등록되는 단말(200)의 지정대상 식별정보 조건에 부합하는 M개의 지정 정보 중에서 m(1≤m≤M)개의 지정 정보를 포함하는 지정대상 식별정보를 획득할 수 있다.

[0063] 본 발명의 제1 단말 지정 등록 방식에 따르면, 단말 지정 등록을 위해 접속한 사용자의 단말(200)을 상기 인증서를 이용 가능한 단말(200)로 지정 등록할 수 있다. 이 경우 상기 식별정보 획득부(125)는 상기 단말 지정 등록을 위해 접속한 사용자의 단말(200)로부터 지정된 하나 이상의 지정 정보를 포함하는 지정대상 식별정보를 수신하거나, 상기 사용자의 단말(200)을 관리하는 관리서버로부터 상기 사용자의 단말(200)에 지정된 하나 이상의 지정 정보를 포함하는 지정대상 식별정보를 수신하는 것 중, 적어도 하나 또는 둘 이상의 조합을 통해 상기 사용자의 단말(200)을 상기 저장된 인증서가 이용될 단말(200)로 지정할 수 있는 m개의 지정 정보를 포함하는 지정대상 식별정보를 획득할 수 있다.

[0064] 본 발명의 제2 단말 지정 등록 방식에 따르면, 단말 지정 등록을 위해 접속한 사용자의 단말(200) 이외에 상기 사용자가 이용 가능한 다른 단말(200)을 상기 인증서를 이용 가능한 단말(200)로 지정 등록할 수 있다. 이 경우 상기 식별정보 획득부(125)는 상기 사용자의 단말(200)로부터 상기 인증서를 이용 가능한 단말(200)로 등록되는 대상 단말(200)에 지정된 하나 이상의 지정 정보를 포함하는 지정대상 식별정보를 수신하거나, 상기 사용자의 단말(200)로부터 제공되는 상기 대상 단말(200)에 대한 단말정보를 근거로 상기 대상 단말(200)로부터 지정된 하나 이상의 지정 정보를 포함하는 지정대상 식별정보를 수신하거나, 상기 대상 단말(200)을 관리하는 관리서버로부터 상기 대상 단말(200)에 지정된 하나 이상의 지정대상 식별정보를 수신하는 것 중, 적어도 하나 또는 둘 이상의 조합을 통해 상기 사용자가 이용 가능한 다른 단말(200)을 상기 저장된 인증서가 이용될 단말(200)로 지정할 수 있는 m개의 지정 정보를 포함하는 지정대상 식별정보를 획득할 수 있다.

[0065] 한편 상기 식별정보 획득부(125)는 상기 획득된 지정대상 식별정보가 상기 지정 등록되는 단말(200)을 고유하게 지정 식별할 수 있는 지정 정보를 포함하여 구성되어 있는지 검증한다. 바람직하게, 상기 식별정보 획득부(125)는 상기 지정대상 식별정보를 포함하는 m개의 지정 정보 중에서 상기 지정 등록되는 단말(200)에 고정 유지되는 하나 이상의 정보에 대하여 기 저장된 다른 지정대상 식별정보에 포함된 각 지정 정보 항목 별로 중복 검사를 실시함으로써, 상기 획득된 지정대상 식별정보가 상기 지정 등록되는 단말(200)을 고유하게 지정 식별할 수 있는지 유효성을 검증할 수 있다. 예를들어, 상기 획득된 지정대상 식별정보에 상기 지정 등록되는 단말(200)의 MAC 주소가 포함된 경우, 상기 MAC 주소는 기 저장된 다른 지정대상 식별정보에 포함된 MAC 주소와 중복되어서는 안된다.

[0066] 상기 저장된 인증서를 이용 가능한 단말(200)을 지정 식별하는 지정대상 식별정보가 획득되면, 상기 식별정보 저장부(130)는 상기 식별정보 획득부(125)에 의해 획득된 지정대상 식별정보를 저장한다. 바람직하게, 상기 식별정보 획득부(125)는 N개의 단말(200)을 지정 식별하는 N개의 지정대상 식별정보를 획득할 수 있으며, 상기 식별정보 저장부(130)는 상기 식별정보 획득부(125)에 의해 획득되는 N개의 지정된 단말(200)에 대한 N개의 지정대상 식별정보를 저장한다.

[0067] 본 발명의 실시 방법에 따르면, 상기 N개의 지정대상 식별정보는, 상기 사용자의 인증서가 저장된 저장매체(115)에 상기 인증서와 직접 매핑되어 저장되거나, 또는 상기 인증서가 저장된 저장매체(115) 이외의 다른 데이터베이스에 저장될 수 있다. 만약 상기 N개의 지정대상 식별정보가 상기 인증서가 저장된 저장매체(115) 이외의 다른 데이터베이스에 저장되더라도, 상기 N개의 지정대상 식별정보는 지정된 식별자를 통해 상기 저장매체(115)에 저장된 인증서와 간접적으로 매핑되는 것이 바람직하다.

[0068] 한편 상기 식별정보 획득부(125)는 상기 지정대상 식별정보가 획득되는 시점의 전, 중, 후의 어느 시점에 상기 인증서를 발급받은 사용자를 고유 인증하는 사용자 식별정보를 획득할 수 있다. 상기 사용자 식별정보는 상기 저장매체(115)에 저장된 인증서를 발급받은 사용자 및/또는 상기 저장된 인증서가 이용될 단말(200)을 지정 등록한 사용자를 고유하게 식별함과 동시에 상기 사용자를 인증하는 정보의 총칭으로서, 상기 본인 인증 절차부(120)에 의해 수행되는 사용자 본인 인증 절차의 결과로서 상기 본인 인증에 사용된 정보를 포함하거나, 또는 상기 사용자 본인 인증 절차와 연동되거나 또는 별도로 처리되는 사용자 식별정보 등록 과정을 통해 상기 사용자의 단말(200)로부터 수신되는 사용자 정보(예컨대, ID/PW 등)를 포함할 수 있다. 또는 상기 지정대상 식별정보를 구성하는 지정 정보 중에 하나 이상의 지정 정보가 상기 사용자 식별정보로 이용될 수도 있다.

[0069] 한편 상기 식별정보 획득부(125)는 상기 획득된 사용자 식별정보가 상기 저장매체(115)에 저장된 인증서를 발급받은 사용자와 동일인을 식별하거나, 또는 상기 단말(200)을 지정 등록하는 사용자와 동일인을 식별하는지 검증한다. 바람직하게, 상기 식별정보 획득부(125)는 상기 사용자 식별정보에 대응하는 사용자 명의를 확인하고, 상기 확인된 사용자 명의가 상기 저장매체(115)에 저장된 인증서의 발급자 명의와 동일인이거나, 또는 상기 단말(200)을 지정 등록한 사용자의 명의와 동일인을 식별하는지 검증할 수 있다. 만약 상기 사용자 식별정보가 상기 사용자에 대한 본인 인증 절차의 결과로서 획득된 것이라면, 상기 사용자 식별정보에 대한 유효성 검증은 생략 가능하다.

[0070] 상기 식별정보 획득부(125)에 의해 상기 사용자를 고유 인증하는 사용자 식별정보가 획득되면, 상기 식별정보 저장부(130)는 상기 식별정보 획득부(125)에 의해 획득된 N개의 지정대상 식별정보와 상기 사용자 식별정보를 매핑하여 저장한다.

[0071] 본 발명의 실시 방법에 따르면, 상기 N개의 지정대상 식별정보와 사용자 식별정보는, 상기 사용자의 인증서가 저장된 저장매체(115)에 상기 인증서와 함께 직접 매핑되어 저장되거나, 또는 상기 인증서가 저장된 저장매체

(115) 이외의 다른 데이터베이스에 매핑되어 저장될 수 있다. 만약 상기 N개의 지정대상 식별정보와 사용자 식별정보가 상기 인증서가 저장된 저장매체(115) 이외의 다른 데이터베이스에 저장되더라도, 상기 N개의 지정대상 식별정보 또는 사용자 식별정보는 지정된 식별자를 통해 상기 저장매체(115)에 저장된 인증서와 간접적으로 매핑되는 것이 바람직하다.

[0072] 한편 본 발명의 다른 실시 방법에 따라 상기 단말 지정 등록이 생략되는 경우, 상기 식별정보 획득부(125)는 상기 사용자를 고유 인증하는 사용자 식별정보를 획득할 수 있으며, 이 경우에 상기 사용자 식별정보는 상기와 같이 사용자의 인증서와 직/간접적으로 매핑되어 저장될 수 있다.

[0073] 상기와 같이 사용자에게 발급된 인증서가 지정된 저장매체(115)에 저장되고, 상기 인증서가 이용될 N개의 지정된 단말(200)에 대한 지정대상 식별정보와 상기 사용자를 고유 인증하는 사용자 식별정보 중 하나 이상의 식별정보가 상기 인증서와 직/간접적으로 매핑되어 저장됨으로써, 상기 저장매체(115)에 저장된 인증서를 클라우드 방식으로 이용할 수 있는 준비가 완료된다.

[0074] 도면1을 참조하면, 상기 운영 서버(100)는, 사용자의 단말(200)로부터 상기 저장매체(115)에 저장된 인증서를 상기 사용자의 단말(200)에서 이용되도록 요청하는 요청 정보를 수신하는 요청 정보 수신부(135)를 구비하며, 상기 인증서 이용을 요청하는 사용자에 대한 본인 인증 절차를 수행하는 본인 인증 절차부(120)를 더 구비하거나, 또는 상기 사용자를 고유 인증하는 사용자 식별정보가 상기 지정대상 식별정보와 매핑되어 저장된 경우, 상기 사용자 식별정보를 통해 상기 인증서 이용을 요청하는 사용자를 인증하는 사용자 인증부(140)를 더 구비할 수 있다.

[0075] 사용자는 자신이 이용하는 단말(200)을 통해 상기 운영 서버(100)에 접속하여 상기 저장매체(115)에 저장된 인증서를 상기 사용자의 단말(200)에서 이용되도록 요청하게 되는데, 상기 요청 정보 수신부(135)는 상기 사용자의 단말(200)로부터 상기 저장매체(115)에 저장된 인증서를 상기 사용자의 단말(200)에서 이용되도록 요청하는 요청 정보를 수신한다. 여기서, 상기 요청 정보는, 상기 저장매체(115)에 저장된 인증서를 요청하는데 필요한 하나 이상의 구성 정보(예컨대, 사용자 식별정보, 인증서 이용 방식, 용도, 대상, 관련서버 등에 대한 정보)를 포함할 수 있으며, 실시 방법에 따라서는 상기 지정대상 식별정보를 통해 지정 식별되는 사용자의 단말(200)이 상기 운영 서버(100)에 접속하는 것 자체가 상기 인증서를 이용하도록 요청하는 요청 정보로 해석될 수 있다.

[0076] 만약 상기 식별정보 저장부(130)에 의해 상기 사용자를 고유 인증하는 사용자 식별정보가 저장된 경우, 상기 사용자 인증부(140)는 상기 요청 정보 수신부(135)에 포함된 사용자 식별정보(또는 별도의 통신 연결을 통해 사용자의 단말(200)로부터 수신되는 사용자 식별정보)와 상기 저장된 사용자 식별정보를 비교 인증(또는 검증 연산 후 예측된 결과 인증)하여 상기 저장된 인증서의 이용을 요청하는 사용자를 인증한다.

[0077] 한편 상기 식별정보 저장부(130)에 의해 상기 사용자를 고유 인증하는 사용자 식별정보가 저장되지 않거나, 또는 상기 저장된 인증서를 이용 가능한 단말(200)에 대한 지정대상 식별정보가 저장되지 않은 경우, 상기 본인 인증 절차부(120)는 상기 인증서를 발급받은 사용자가 상기 저장된 인증서를 요청하는지에 대한 사용자 본인 인증 절차와 상기 N개의 단말(200)을 등록한 사용자가 상기 저장된 인증서를 요청하는지에 대한 사용자 본인 인증 절차 중 적어도 하나의 본인 인증 절차를 수행한다. 바람직하게, 상기 사용자에 대한 본인 인증은, ID/PW 인증, 인터넷 실명 인증, 통신 가입자 인증, 카드 명의자 인증, 계좌 명의자 인증, 무선단말 점유 인증, 인증서 인증 중에서 상기 운영 서버(100)에 의해 지정한 적어도 하나 또는 둘 이상의 본인 인증을 포함할 수 있으며, 상술된 방식 이외에도 다양한 형태의 본인 인증이 수행될 수 있음은 전술한 바와 같다.

[0078] 본 발명의 실시 방법에 따르면, 상기 본인 인증 절차부(120)는 상기 인증서를 발급받은 사용자가 상기 저장된 인증서를 요청하는지, 또는 상기 N개의 단말(200)을 등록한 사용자가 상기 저장된 인증서를 요청하는지에 대한

사용자 본인 인증을 처리하기 위한 k(k≥1)개의 본인 인증 방식이 설정되어 있으며, 상기 본인 인증 절차부(120)는 지정된 순서에 따라 상기 설정된 k개의 본인 인증 절차를 수행할 수 있다.

[0079] 도면1을 참조하면, 상기 운영 서버(100)는, 상기 인증서 이용을 요청한 사용자의 단말(200)이 상기 지정대상 식별정보에 의해 지정 식별되는 N개의 지정된 단말(200) 중 제n(1≤n≤N) 단말(200)인지 인증하는 지정대상 인증부(145)와, 상기 사용자의 단말(200)이 상기 지정된 제n 단말(200)로 인증된 경우에 상기 저장매체(115)에 저장된 사용자의 인증서가 상기 제n 단말(200)을 통해 이용되도록 처리하는 인증서 처리부(150)를 구비한다.

[0080] 상기 지정대상 인증부(145)는 상기 인증서 이용을 요청한 사용자의 단말(200)로부터 해당 단말(200)에 지정된 하나 이상의 지정 정보를 포함하는 지정대상 식별정보를 수신하고, 상기 수신된 지정대상 식별정보를 상기 식별정보 저장부(130)에 의해 저장된 N개의 지정된 단말(200)에 대한 N개의 지정대상 식별정보와 비교함으로써, 상기 인증서 이용을 요청한 사용자의 단말(200)이 상기 지정대상 식별정보에 의해 지정 식별되는 N개의 지정된 단말(200) 중 어느 하나에 대응하는 제n 단말(200)인지 인증한다. 바람직하게, 상기 사용자의 단말(200)로부터 수신되는 지정대상 식별정보는 상기 사용자의 단말(200)에 저장된 지정 정보, 상기 사용자의 단말(200)에 의해 생성된 지정 정보, 상기 사용자의 단말(200)에서 입력된 지정 정보 중 하나 이상의 지정 정보를 포함하여 이루어진다.

[0081] 본 발명의 실시 방법에 따르면, 상기 지정대상 인증부(145)는 지정대상 식별정보로 이용 가능한 M개의 지정 정보 중에서 상기 사용자의 단말(200)을 지정 식별하는데 이용되는 m개의 지정 정보를 포함하는 지정대상 식별정보의 구성을 확인하고, 상기 사용자의 단말(200)로부터 상기 m개의 지정 정보를 포함하는 지정대상 식별정보를 수신한 후, 상기 수신된 지정대상 식별정보를 상기 식별정보 저장부(130)에 의해 저장된 N개의 지정된 단말(200)에 대한 N개의 지정대상 식별정보와 비교함으로써, 상기 인증서 이용을 요청한 사용자의 단말(200)이 상기 지정대상 식별정보에 의해 지정 식별되는 N개의 지정된 단말(200) 중 어느 하나에 대응하는 제n 단말(200)인지 인증할 수 있다.

[0082] 본 발명의 실시 방법에 따르면, 상기 지정대상 식별정보는 지정된 단말(200)에 고정 유지된 둘 이상의 지정 정보를 포함할 수 있는데, 이 경우 상기 지정대상 인증부(145)는 상기 지정된 단말(200)에 고정 유지된 둘 이상의 정보 중 일부는 인증되고 나머지 일부는 인증되지 않는지 판별하며, 만약 상기 지정된 단말(200)에 고정 유지된 둘 이상의 정보 중 일부는 인증되고 나머지 일부는 인증되지 않는다면 상기 지정대상 식별정보에 대한 폐기 절차 또는 재등록 절차를 수행할 수 있다. 즉, 상기 지정된 단말(200)에 고정 유지된 둘 이상의 정보 중 일부는 인증되고 나머지 일부는 인증되지 않는다면, 이는 상기 지정된 단말(200)에 구비된 프로그램이나 운영체제를 비롯하여 하드웨어 구성품 등, 상기 단말(200)을 지정 식별하는 지정 정보가 변경되었음을 의미하며, 따라서 상기 지정대상 인증부(145)는 상기 지정대상 식별정보에 대한 폐기 절차 또는 재등록 절차를 수행할 수 있다. 한편 상기 지정대상 식별정보는 지정된 단말(200)에서 입력되거나 또는 생성되는 적어도 하나의 지정 정보를 포함할 수 있는데, 이 경우 상기 지정대상 인증부(145)는 상기 입력 또는 생성되는 정보가 인증되지 않는 경우에 상기 지정 단말 식별에 대한 오류를 발생시킨다. 또는 상기 지정대상 식별정보는 지정된 단말(200)에 고정 유지된 지정 정보를 포함할 수 있는데, 이 경우 상기 지정대상 인증부(145)는 상기 지정된 단말(200)에 고정 유지된 지정 정보가 모두 인증되지 않는 경우에 상기 지정 단말 식별에 대한 오류를 발생시킬 수 있다.

[0083] 만약 상기 인증서 이용을 요청한 사용자의 단말(200)이 상기 인증서를 이용 가능한 제n 단말(200)로 인증되면, 상기 인증서 처리부(150)는 상기 저장매체(115)에 저장된 사용자의 인증서가 상기 제n 단말(200)을 통해 이용되도록 처리한다. 본 발명에서 지정된 제n 단말(200)을 통해 저장된 인증서가 이용되도록 처리한다는 것은, 상기 저장매체(115)에 저장된 사용자의 인증서를 상기 지정된 제n 단말(200)로 제공하여 상기 제n 단말(200)에서 상기 인증서를 사용할 수 있도록 하는 것과, 상기 제n 단말(200)에서 인증서를 이용하여 처리해야 할 동작(또는 작업)을 상기 운영 서버(100)(또는 인증서 처리부(150)가 구비된 서버)가 상기 제n 단말(200)을 대신하여 처리하는 것 중, 적어도 하나 또는 둘의 조합을 의미한다.

[0084] 본 발명의 제1 인증서 이용 방식에 따르면, 상기 인증서 처리부(150)는 상기 저장된 사용자의 인증서를 상기 지정된 제n 단말(200)로 제공하며, 상기 제n 단말(200)은 상기 사용자의 인증서를 수신하여 상기 제n 단말(200)의 인증서로 이용하여 금융거래, 지불결제를 포함하는 각종 인증서 이용 대상에 상기 수신된 인증서를 이용(예컨대, 사용자 인증, 암/복호화, 전자서명 등)한다.

[0085] 상기 제1 인증서 이용 방식에서 상기 인증서 처리부(150)는 상기 저장된 사용자 인증서의 전체 구성을 상기 지정된 제n 단말(200)로 제공하거나, 또는 상기 저장된 사용자 인증서의 일부 구성을 상기 제n 단말(200)로 제공하는 것(단, 인증서의 일부 구성을 제n 단말(200)로 제공하는 경우에도 저장매체(115)에는 인증서의 전체 구성이 저장되는 것이 가능)이 가능하다.

[0086] 만약 인증서 처리부(150)가 상기 저장된 사용자 인증서의 일부 구성을 상기 지정된 제n 단말(200)로 제공하는 경우, 상기 제n 단말(200)은 상기 제공되는 인증서의 일부 구성을 제외한 나머지 구성이 구비되어 있거나, 상기 사용자 소유의 휴대 매체에 구비된 상기 인증서의 나머지 구성을 이용 가능한 상태인 것이 바람직하며, 상기 수신되는 인증서의 일부 구성과 상기 구비된 나머지 구성을 조합하여 상기 인증서의 전체 구성을 만든 후에 상기 인증서의 전체 구성을 이용하여 각종 인증서 처리에 이용할 수 있다. 한편 상기 인증서 처리부(150)가 상기 저장된 사용자 인증서의 일부 구성을 지정된 단말(200)로 제공하는 경우, 상기 제공되는 인증서의 일부 구성은 N개의 지정된 단말(200)에 대하여 동일하거나, 또는 N개의 지정된 단말(200) 별로 서로 다른 것이 가능하며, 이때 상기 지정된 단말(200) 측에 구비된 상기 인증서의 나머지 구성은 상기 수신되는 일부 구성에 대응하여 N개의 지정된 단말(200)에 대하여 동일하거나, 또는 N개의 지정된 단말(200) 별로 서로 다른 것이 가능하다.

[0087] 본 발명의 실시 방법에 따르면, 상기 지정된 제n 단말(200)로 제공되는 인증서는 지정된 사용 제한이 설정되는 것이 바람직하다. 바람직하게, 상기 제n 단말(200)로 제공되는 인증서는 상기 제n 단말(200)에 임시 저장될 수 있다. 즉, 상기 제n 단말(200)로 제공되는 인증서는 상기 제n 단말(200)의 휘발성 메모리에 저장됨으로써 상기 제n 단말(200)의 전원 공급이 차단되는 경우에 자동으로 소멸될 수 있다. 또는 상기 제n 단말(200)로 제공되는 인증서는 일회용 또는 지정된 횟수 이내의 사용 횟수 제한이 설정될 수 있다. 즉, 상기 제n 단말(200)로 제공되는 인증서는 상기 제n 단말(200)에 저장되는 형태와 무관하게 지정된 횟수만큼만 사용 가능하며, 이후에는 자동으로 소멸(예컨대, 상기 인증서 파일 내에 자동 소멸 코드가 포함됨)되거나, 또는 인증서 기능이 자동으로 중지될 수 있다. 또는 제n 단말(200)로 제공되는 인증서는 만료 일시 제한이 설정될 수 있다. 즉, 상기 제n 단말(200)로 제공되는 인증서는 수 분에서 수 시간, 또는 하루 내지 일주일 등과 같이 제한된 만료 일시에서만 사용 가능하며, 이후에는 자동으로 소멸되거나, 또는 인증서 기능이 자동으로 중지될 수 있다.

[0088] 한편 상기 제1 인증서 이용 방식에서 상기 인증서 처리부(150)는 상기 인증서를 상기 제n 단말(200)에서 이용 가능한 구조로 가공하여 상기 제n 단말(200)로 제공할 수 있다. 즉, 상기 저장매체(115)에 저장된 사용자의 인증서는 해당 인증서의 발급 시점과 동일한 구성 정보를 지닌 원본이라고 할지라도, 상기 구성 정보를 포함하는 인증서 파일의 파일 구조는 상기 제n 단말(200)에서 이용 가능한 파일 구조로 가공되거나, 또는 상기 제n 단말(200)에 구비된 프로그램을 통해 이용 가능한 형태로 가공될 수 있다. 또한 상기 제n 단말(200)로 제공되는 인증서에 지정된 사용 제한이 설정되는 경우, 상기 사용 제한에 따라 상기 인증서의 구성 정보 중 일부(예컨대, 인증서 만료 일시 등)가 변경되거나, 또는 상기 사용 제한을 설정하는 데이터 셋트나 실행 코드(예컨대, 자동소멸 스크립트 코드 등)가 상기 인증서에 첨부될 수 있다.

[0089] 본 발명의 실시 방법에 따르면, 상기 제1 인증서 이용 방식에서 상기 인증서 처리부(150)는 상기 인증서를 저장하는 저장매체(115)를 상기 제n 단말(200)에서 이용 가능한 가상의 저장영역으로 마운트(Mount)시키는 동작을 수행할 수 있으며, 이 경우에 상기 제n 단말(200)은 상기 저장매체(115)에 저장된 인증서를 상기 제n 단말(200)에 구비된 인증서처럼 이용할 수 있다.

[0090] 본 발명의 제2 인증서 이용 방식에 따르면, 상기 인증서 처리부(150)는 상기 저장된 사용자의 인증서를 통해 상기 제n 단말(200)의 인증서 처리를 대행할 수 있다. 여기서, 상기 대행되는 인증서 처리는, 상기 제n 단말(200)에서 상기 인증서를 이용할 수 있는 모든 인증서 처리(예컨대, 인증서 기반 사용자 인증, 암/복호화, 전자서명 등)를 대행할 수 있다.

[0091] 상기 제2 인증서 이용 방식에서 상기 인증서 처리부(150)는 상기 지정된 제n 단말(200)로부터 인증서 처리할 데이터를 수신하고, 상기 저장된 인증서를 이용하여 수신된 데이터에 대한 인증서 처리 절차(예컨대, 인증서 기반 사용자 인증 절차, 암/복호화 절차, 전자서명 절차 등)를 수행한 후, 상기 인증서 처리된 데이터를 지정된 대상 장치(예컨대, 제n 단말(200) 또는 상기 제n 단말(200)로부터 인증서 처리된 데이터를 수신할 인증 서버(도시생략))로 전달한다. 본 발명의 실시 방법에 따르면, 상기 인증서 처리부(150)는 상기 제n 단말(200)로부터 상기 인증서 처리된 데이터를 전달할 대상 장치를 식별하는 대상 장치 식별정보를 수신하며, 상기 수신된 대상 장치 식별정보로 상기 인증서 처리된 데이터를 전달할 수 있다. 만약 상기 대상 장치가 고정된다면 상기 대상 장치 식별정보를 수신하지 않아도 무방하다.

[0092] 본 발명의 실시 방법에 따르면, 상기 제2 인증서 이용 방식에서 상기 인증서 처리부(150)는 상기 인증서를 저장하는 저장매체(115)와 인증서 처리부(150)를 상기 제n 단말(200)과 연동 이용 가능한 가상의 외부 디바이스로 마운트 시키는 동작을 수행할 수 있으며, 이 경우에 상기 제n 단말(200)은 상기 제n 단말(200)에 의해 수행될 인증서 처리를 상기 마운트 처리된 가상의 디바이스를 통해 처리하는 것처럼 이용할 수 있다.

[0093] 도면2는 본 발명의 실시 방법에 따라 사용자의 단말(200)에 구비되는 애플리케이션(215)의 기능 구성을 도시한 도면이다.

[0094] 보다 상세하게 본 도면2는 상기 사용자의 단말(200)이 무선단말(200)인 경우에 본 발명에 따른 인증서 등록과 이용을 위한 애플리케이션의 형태로 상기 사용자의 무선단말(200)에 구비되는 프로그램의 기능 구성을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면2를 참조 및/또는 변형하여 사용자가 이용하는 각종 단말(200)에 구비되는 애플리케이션(215)의 기능에 대한 다양한 실시 방법을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면2에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0095] 도면2를 참조하면, 상기 무선단말(200)은, 제어부(201)와 메모리부(213)와 화면 출력부(202)와 키 입력부(203)와 사운드 출력부(204)와 사운드 입력부(205)와 카메라부(206)와 무선망 통신모듈(209)과 근거리 무선 통신모듈(208)과 NFC모듈(210)과 위치 측위모듈(211)과 USIM 리더부(212) 및 USIM를 구비하며, 전원 공급을 위한 배터리(207)를 구비한다.

[0096] 상기 제어부(201)는 상기 무선단말(200)의 동작을 제어하는 구성의 총칭으로서, 적어도 하나의 프로세서와 실행 메모리를 포함하여 구성되며, 상기 무선단말(200)에 구비된 각 구성부와 버스(BUS)를 통해 연결된다. 본 발명에 따르면, 상기 제어부(201)는 상기 프로세서를 통해 상기 무선단말(200)에 구비되는 적어도 하나의 프로그램코드를 상기 실행 메모리에 로딩하여 연산하고, 그 결과를 상기 버스를 통해 적어도 하나의 구성부로 전달하여 상기 무선단말(200)의 동작을 제어한다. 이하, 편의상 본 발명에 따른 인증서 등록과 이용을 위한 애플리케이션(215)의 구성을 본 제어부(201) 내에 도시하여 설명하기로 한다.

[0097] 상기 메모리부(213)는 상기 무선단말(200)에 구비되는 저장 자원에 대응되는 비휘발성 메모리의 총칭으로서, 상기 제어부(201)를 통해 실행되는 적어도 하나의 프로그램코드와, 상기 프로그램코드가 이용하는 적어도 하나의

데이터셋트를 저장하여 유지한다. 상기 메모리부(213)는 기본적으로 상기 무선단말(200)의 운영체제에 대응하는 시스템프로그램코드와 시스템데이터셋트, 상기 무선단말(200)의 무선 통신 연결을 처리하는 통신프로그램코드와 통신데이터셋트 및 적어도 하나의 응용프로그램코드와 응용데이터셋트를 저장하며, 본 발명의 애플리케이션(215)에 대응하는 프로그램코드와 데이터셋트도 상기 메모리부(213)에 저장된다.

[0098] 상기 화면 출력부(202)는 상기 무선단말(200)에 구비되는 출력 자원에 대응되는 화면출력장치(예컨대, LCD(Liquid Crystal Display) 장치)와 이를 구동하는 화면출력모듈로 구성되며, 상기 제어부(201)와 버스로 연결되어 상기 제어부(201)의 각종 연산 결과 중 화면 출력에 대응하는 연산 결과를 상기 화면출력 장치로 출력한다.

[0099] 상기 키 입력부(203)는 상기 무선단말(200)에 구비되는 입력 자원에 대응되는 키입력장치(또는 상기 화면 출력부(202)와 연동하는 터치스크린장치)와 이를 구동하는 키입력모듈로 구성되며, 상기 제어부(201)와 버스로 연결되어 상기 제어부(201)의 각종 연산을 명령하는 명령을 입력하거나, 또는 상기 제어부(201)의 연산에 필요한 데이터를 입력한다.

[0100] 상기 사운드 출력부(204)는 상기 무선단말(200)에 구비되는 출력 자원에 대응되는 스피커와 상기 스피커를 구동하는 사운드모듈로 구성되며, 상기 제어부(201)와 버스로 연결되어 상기 제어부(201)의 각종 연산 결과 중 사운드 출력에 대응하는 연산 결과를 상기 스피커를 통해 출력한다. 상기 사운드 모듈은 기 스피커를 통해 출력할 사운드 데이터를 디코딩(Decoding)하여 사운드 신호로 변환한다.

[0101] 상기 사운드 입력부(205)는 상기 무선단말(200)에 구비되는 입력 자원에 대응되는 마이크로폰과 상기 마이크로폰을 구동하는 사운드모듈로 구성되며, 상기 마이크로폰을 통해 입력되는 사운드 데이터를 상기 제어부(201)로 전달한다. 상기 사운드 모듈은 상기 마이크로폰을 통해 입력되는 사운드 신호를 엔코딩(Encoding)하여 부호화한다.

[0102] 상기 카메라부(206)는 상기 무선단말(200)에 구비되는 카메라 자원의 총칭으로서, 광학부와 CCD(Charge Coupled Device)와 이를 구동하는 카메라모듈로 구성되며, 상기 광학부를 통해 상기 CCD에 입력된 비트맵 데이터를 획득한다. 상기 비트맵 데이터는 정지 영상의 이미지 데이터와 동영상 데이터를 모두 포함할 수 있다.

[0103] 상기 무선망 통신모듈(209)과 근거리 무선 통신모듈(208)은 상기 무선단말(200)에 구비되는 통신 자원으로서, 상기 무선망 통신모듈(209)은 기지국을 통해 무선 통신망에 접속하고, 상기 근거리 무선 통신모듈(208)은 근거리에 위치한 근거리통신장치 또는 무선AP에 접속한다.

[0104] 상기 무선망 통신모듈(209)은 상기 무선단말(200)을 무선 통신에 접속시키는 통신 구성의 총칭으로서, 특정 주파수 대역의 무선 주파수 신호를 송수신하는 안테나, RF모듈, 기저대역모듈, 신호처리모듈을 적어도 하나 포함하여 구성되며, 상기 제어부(201)와 버스로 연결되어 상기 제어부(201)의 각종 연산 결과 중 무선 통신에 대응하는 연산 결과를 무선 통신을 통해 전송하거나, 또는 무선 통신을 통해 데이터를 수신하여 상기 제어부(201)로 전달함과 동시에, 상기 무선 통신의 접속, 등록, 통신, 핸드오프의 절차를 유지한다. 본 발명에 따르면, 상기 무선망 통신모듈(209)은 상기 무선단말(200)을 교환기를 경유하는 전화 통화채널과 데이터채널을 포함하는 전화 통화망에 연결할 수 있으며, 경우에 따라 상기 교환기를 경유하지 않고 패킷 통신 기반의 무선망 데이터 통신을 제공하는 데이터망에 연결할 수 있다.

[0105] 본 발명의 실시 방법에 따르면, 상기 무선망 통신모듈(209)은 CDMA/WCDMA 규격에 따라 이동 통신망에 접속, 위치등록, 호처리, 통화연결, 데이터통신, 핸드오프를 적어도 하나 수행하는 이동 통신 구성을 포함한다. 한편 당

업자의 의도에 따라 상기 무선망 통신모듈(209)은 IEEE 802.16 관련 규격에 따라 휴대인터넷에 접속, 위치등록, 데이터통신, 핸드오프를 적어도 하나 수행하는 휴대 인터넷 통신 구성을 더 포함할 수 있으며, 상기 무선망 통신모듈(209)이 제공하는 무선 통신 구성에 의해 본 발명이 한정되지 아니함을 명백히 밝혀두는 바이다.

[0106] 상기 근거리 무선 통신모듈(208)은 일정 거리 이내에서 무선 주파수 신호를 통신매체로 이용하여 통신세션을 연결하는 근거리 통신모듈로서, 바람직하게는 와이파이 통신, 블루투스 통신, 공중무선 통신 중 적어도 하나를 포함할 수 있다. 본 발명의 실시 방법에 따르면, 상기 근거리 무선 통신모듈(208)은 상기 무선망 통신모듈(209)과 통합될 수 있다. 본 발명에 따르면, 상기 근거리 무선 통신모듈(208)은 무선AP를 통해 상기 무선단말(200)을 패킷 통신 기반의 근거리 무선 데이터 통신을 제공하는 데이터망에 연결한다.

[0107] 상기 NFC모듈(210)은 무선단말(200)에 구비되는 NFC 자원의 총칭으로서, 13.56Mz 주파수 대역을 사용하는 NFC(Near Field Communication) 규격에 따라 10cm 내외의 근접 거리에서 단말 간 데이터를 전송하는 근접 통신모듈을 포함하여 구성된다. 상기 NFC 모듈은 상기 근거리 무선 통신모듈(208)과 일체형으로 구현되거나 또는 별도 통신모듈로 구현될 수 있다. 당업자의 의도에 따라 상기 NFC모듈(210)은 13.56Mz 주파수 대역 이외에 ISO 18000 시리즈 규격이 지원하는 다른 주파수 대역(예컨대, 900Mhz 대역 등)의 근접 통신을 제공할 수 있으며, 이에 의해 본 발명아 한정되지 아니한다. 한편 상기 NFC모듈(210)이 근접하여 통신하는 대상에 따라 상기 NFC모듈(210)은 상기 무선단말(200)에 구비되는 통신 자원에 포함될 수 있다.

[0108] 상기 위치 측위모듈(211)은 상기 무선단말(200)에 구비되는 위치측위 자원의 총칭으로서, 상기 무선단말(200)의 이동 위치를 측위하는 GPS 측위모듈로 구성되며, 지구 궤도를 공전하는 적어도 3개 이상의 GPS 위성으로부터 송출되는 위성 신호를 수신하여 상기 무선단말(200)의 이동 위치 정보를 산정한다. 한편, 본 발명의 다른 실시 방법에 따르면, 상기 위치 측위모듈(211)은 적어도 두개 이상의 기지국(또는 접속 포인트)과 연계된 통신망 상의 측위장치와 연계하여 상기 무선단말(200)과 기지국(또는 접속 포인트) 간 주파수 도달 시간(또는 도달 각)을 이용하여 지상파 측위 방식으로 상기 무선단말(200)의 위치를 측위하는 지상파 측위모듈을 포함할 수 있다.

[0109] 상기 USIM 리더부(212)는 ISO/IEC 7816 규격을 기반으로 상기 무선단말(200)에 탑재 또는 이탈착되는 범용가입자식별모듈(Universal Subscriber Identity Module)과 적어도 하나의 데이터셋트를 교환하는 구성의 총칭으로서, 상기 데이터셋트는 APDU(Application Protocol Data Unit)를 통해 반이중 통신 방식으로 교환된다.

[0110] 상기 USIM은 상기 ISO/IEC 7816 규격에 따른 IC칩이 구비된 SIM 타입의 카드로서, 상기 USIM 리더부(212)와 연결되는 적어도 하나의 접점을 포함하는 입출력 인터페이스와, 적어도 하나의 IC칩용 프로그램코드와 데이터셋트를 저장하는 IC칩 메모리와, 상기 입출력 인터페이스와 연결되어 상기 무선단말(200)로부터 전달되는 적어도 하나의 명령에 따라 상기 IC칩용 프로그램코드를 연산하거나 상기 데이터셋트를 추출(또는 가공)하여 상기 입출력 인터페이스로 전달하는 프로세서를 포함하여 이루어진다.

[0111] 상기 통신 자원이 접속 가능한 데이터망을 통해 프로그램제공서버(예컨대, 애플사의 앱스토어 등)로부터 본 발명의 애플리케이션(215)이 다운로드되어 상기 메모리부(213)에 저장된다. 상기 다운로드된 애플리케이션(215)은 운영 서버(100)와 연동하여 동작하며, 사용자에 의해 수동으로 구동되거나, 메시지 수신에 의해 사용자 확인 후 또는 자동으로 구동(또는 활성화)될 수 있다. 한편 상기 애플리케이션(215)을 사용자 확인 후 또는 자동으로 구동하기 위해 별도의 프로그램이 미리 구동 중일 수 있으며, 이에 의해 본 발명이 한정되지 아니한다.

[0112] 도면2를 참조하면, 상기 애플리케이션(215)은, 상기 통신 자원이 접속 가능한 데이터망을 통해 상기 운영 서버(100)에 접속하여 사용자를 회원으로 가입시키나 또는 사용자의 회원 자격을 인증받는 회원가입/인증부(220)와, 상기 통신 자원이 접속 가능한 적어도 하나의 통신망을 개입시켜 상기 애플리케이션(215)

의 유효성을 인증받는 애플리케이션 인증부(225)를 구비하며, 상기 운영 서버(100)에는 상기 회원 가입/인증부(220)와 애플리케이션 인증부(225)의 동작에 대응하는 서버 측 동작을 수행하는 구성부(도시생략)가 구비된다.

[0113] 상기 애플리케이션(215)은 상기 통신 자원이 접속 가능한 데이터망을 통해 상기 운영 서버(100)에 접속하는 통신 연결 매크로 정보를 구비하며, 상기 회원 가입/인증부(220)는 상기 화면 출력부(202)를 통해 사용자를 회원으로 가입시키는 사용자 정보(예컨대, 성명, 주민등록번호 등)와 회원 계정을 입력하는 인터페이스를 출력하고, 상기 데이터망을 통해 상기 운영 서버(100)로 상기 인터페이스를 통해 입력된 사용자 정보와 회원 계정을 전송하여 상기 사용자를 회원으로 가입시킨다.

[0114] 한편 상기 사용자의 회원 가입은 상기 무선단말(200) 이외에 별도의 사용자의 단말(200)을 통해 가입될 수 있다. 따라서 상기 사용자가 이미 회원으로 가입되어 있거나, 또는 상기 사용자의 단말(200)을 통해 회원으로 가입된 경우, 상기 회원 가입/인증부(220)는 상기 사용자의 회원 계정을 입력하는 인터페이스를 출력하고, 상기 데이터망을 통해 상기 운영 서버(100)로 상기 인터페이스를 통해 입력된 회원 계정을 전송하여 상기 사용자가 회원인지 인증시킨다.

[0115] 상기 애플리케이션 인증부(225)는 상기 통신 자원이 접속 가능한 데이터망과 전화통화망 중 적어도 하나의 통신망을 개입시켜 상기 운영 서버(100)로 상기 애플리케이션(215)의 유효성을 인증시킨다. 본 발명의 실시 방법에 따르면, 상기 애플리케이션(215)의 유효성을 인증하는 과정은 상기 애플리케이션(215)과 운영 서버(100) 사이에 미리 합의된 암/복호화 통신 과정을 수행되며, 편의상 상기 암/복호화 과정에 대한 상세한 설명은 생략하기로 한다.

[0116] 본 발명의 제1 애플리케이션 인증 방식에 의하면, 상기 애플리케이션(215)은 상기 운영 서버(100)에 의해 운영되는 애플리케이션임을 식별할 수 있는 고유 키 값이 설정된 상태로 상기 프로그램제공서버를 통해 다운로드되며, 이 경우에 상기 애플리케이션 인증부(225)는 상기 고유 키 값을 상기 운영 서버(100)로 전송함으로써, 상기 애플리케이션(215)이 상기 운영 서버(100)에 의해 운영되는 애플리케이션임을 인증시킬 수 있다. 한편, 상기 애플리케이션 인증부(225)는 상기 운영 서버(100)로 상기 고유 키 값을 전송하는 과정에서 상기 무선단말(200)에 저장되거나 통신망에 할당된 적어도 하나의 고유정보를 상기 고유 키 값과 함께 전송함으로써, 상기 애플리케이션(215)이 상기 운영 서버(100)에 의해 운영되는 애플리케이션임과 동시에 상기 애플리케이션(215)이 상기 무선단말(200)에서 구동 중임을 동시에 인증시킬 수 있다.

[0117] 본 발명의 제2 애플리케이션 인증 방식에 의하면, 상기 애플리케이션(215)은 상기 프로그램제공서버를 통해 다운로드된 후에 기 지정된 절차에 따라 데이터망 상에서 상기 애플리케이션(215)을 고유하게 식별하는 앱 식별 값(예컨대, 애플사의 APNS에 의해 할당되는 디바이스 토큰 등)이 할당될 수 있으며, 이 경우에 상기 애플리케이션 인증부(225)는 상기 앱 식별 값을 상기 운영 서버(100)로 전송함으로써, 상기 애플리케이션(215)이 상기 운영 서버(100)에 의해 운영되는 애플리케이션임을 인증시킬 수 있다. 한편, 상기 애플리케이션 인증부(225)는 상기 운영 서버(100)로 상기 앱 식별 값을 전송하는 과정에서 상기 무선단말(200)에 저장되거나 통신망에 할당된 적어도 하나의 고유정보를 상기 앱 식별 값과 함께 전송함으로써, 상기 애플리케이션(215)이 상기 운영 서버(100)에 의해 운영되는 애플리케이션임과 동시에 상기 애플리케이션(215)이 상기 무선단말(200)에서 구동 중임을 동시에 인증시킬 수 있다.

[0118] 본 발명의 제3 애플리케이션 인증 방식에 의하면, 상기 애플리케이션(215)은 적어도 하나의 키 값과 키 교환 프로토콜 및 암/복호화 규칙이 설정되고 이를 이용하여 상기 애플리케이션(215)을 인증하는 인증 절차가 정의된 인증서가 탑재된 상태로 상기 프로그램제공서버를 통해 다운로드될 수 있으며, 이 경우에 상기 애플리케이션 인증부(225)는 상기 인증서에 정의된 인증 절차에 따라 상기 인증서에 설정된 적어도 하나의 키 값과 키 교환 프로토콜 및 암/복호화 규칙을 선택적으로 이용하여 상기 애플리케이션(215)이 상기 운영 서버(100)에 의해 운영되는 애플리케이션임을 인증시킬 수 있다. 한편, 상기 애플리케이션 인증부(225)는 상기 인증서를 이용하는 과

정에서 상기 무선단말(200)에 저장되거나 통신망에 할당된 적어도 하나의 고유정보를 상기 인증 절차에 더 이용함으로써, 상기 애플리케이션(215)이 상기 운영 서버(100)에 의해 운영되는 애플리케이션임과 동시에 상기 애플리케이션(215)이 상기 무선단말(200)에서 구동 중임을 동시에 인증시킬 수 있다.

[0119] 본 발명의 제4 애플리케이션 인증 방식에 의하면, 상기 무선단말(200)은 상기 전화통화망의 메시지 교환 프로토콜을 통해 상기 운영 서버(100)로부터 발송된 인증번호가 수신되면, 상기 수신된 인증번호를 상기 입력받아 상기 데이터망을 통해 상기 운영 서버(100)로 전송함으로써, 상기 애플리케이션(215)이 상기 운영 서버(100)에 의해 운영되는 애플리케이션임을 인증시킬 수 있다. 한편, 상기 애플리케이션 인증부(225)는 상기 운영 서버(100)로 상기 인증번호를 전송하는 과정에서 상기 무선단말(200)에 저장되거나 통신망에 할당된 적어도 하나의 고유정보를 상기 인증번호와 함께 전송함으로써, 상기 애플리케이션(215)이 상기 운영 서버(100)에 의해 운영되는 애플리케이션임과 동시에 상기 애플리케이션(215)이 상기 무선단말(200)에서 구동 중임을 동시에 인증시킬 수 있다.

[0120] 본 발명의 제5 애플리케이션 인증 방식에 의하면, 상기 애플리케이션 인증부(225)는 상기 제1 내지 제4 애플리케이션 인증 방식 중 하나 이상을 선택적으로 조합한 인증 방식을 통해 상기 운영 서버(100)로부터 상기 애플리케이션(215)의 유효성을 인증시키는 것이 가능하며, 이에 의해 본 발명이 한정되지 아니한다.

[0121] 도면2를 참조하면, 상기 애플리케이션(215)은, 상기 운영 서버(100)의 본인 인증 절차부(120)와 연동하여 상기 사용자에 대한 본인 인증을 처리하는 본인 인증 처리부(230)를 구비한다.

[0122] 상기 본인 인증 처리부(230)는 상기 운영 서버(100)의 본인 인증 절차부(120)가 사용자의 본인 인증을 위해 지정된 순서에 따라 수행하는 하나 이상의 본인 인증 절차에 대한 단말 측 동작을 수행하는 구성부의 총칭으로서, 바람직하게 ID/PW 인증, 인터넷 실명 인증, 통신 가입자 인증, 카드 명의자 인증, 계좌 명의자 인증, 무선단말 점유 인증, 인증서 인증 중 하나 이상의 본인 인증 절차를 수행할 수 있다.

[0123] 상기 본인 인증 처리부(230)는 인증서 등록, 단말 지정 등록 및 인증서 이용 과정 중 하나 이상의 과정에서 상기 사용자의 본인 여부를 인증하는 동작을 수행한다.

[0124] 도면2를 참조하면, 상기 애플리케이션(215)은, 상기 운영 서버(100)의 인증서 획득부(105)를 통해 사용자에게 발급된 인증서가 획득되어 상기 운영 서버(100)의 인증서 저장부(110)를 통해 지정된 저장매체(115)에 사용자의 인증서가 저장되도록 처리하는 인증서 등록부(235)를 구비한다.

[0125] 상기 인증서 등록부(235)는 상기 운영 서버(100)의 인증서 획득부(105)를 통해 지정된 저장매체(115)에 저장될 사용자의 인증서가 획득되도록 처리한다.

[0126] 본 발명의 제1 인증서 획득 방식에 따라 인증서 서버를 통해 상기 사용자의 인증서가 획득되는 경우, 상기 인증서 등록부(235)는 상기 운영 서버(100)의 인증서 획득부(105)가 상기 인증서 서버를 통해 상기 사용자의 인증서를 획득하는데 필요한 인증서 발급정보를 상기 운영 서버(100)로 전송함으로써, 상기 운영 서버(100)의 인증서 획득부(105)를 통해 상기 지정된 저장매체(115)에 저장될 사용자의 인증서가 획득되도록 처리할 수 있다.

[0127] 본 발명의 제2 인증서 획득 방식에 따라 지정된 기관 서버를 통해 사용자의 인증서가 획득되는 경우, 상기 인증서 등록부(235)는 상기 사용자를 고유 식별하는 식별정보와 상기 기관 서버를 운영하는 기관 정보를 상기 운영 서버(100)로 전송함으로써, 상기 운영 서버(100)의 인증서 획득부(105)를 통해 상기 지정된 저장매체(115)에 저

장될 사용자의 인증서가 획득되도록 처리할 수 있다.

[0128] 본 발명의 제3 인증서 획득 방식에 따라 사용자의 단말(200)에 구비되거나 또는 상기 사용자의 단말(200)에서 이용 중인 사용자의 인증서가 획득되는 경우, 상기 인증서 등록부(235)는 상기 무선단말(200)의 메모리부(213)(또는 USIM을 포함하는 IC칩)에 저장되거나 또는 상기 사용자의 휴대 매체에 저장된 인증서를 추출하고, 지정된 인증서 복사/이전 절차에 따라 상기 추출된 인증서를 상기 운영 서버(100)로 전달하는 동작을 수행함으로써, 상기 운영 서버(100)의 인증서 획득부(105)를 통해 상기 지정된 저장매체(115)에 저장될 사용자의 인증서가 획득되도록 처리할 수 있다.

[0129] 상기 제1 내지 제3 인증서 획득 방식 중에서 적어도 하나의 방식을 통해 획득된 인증서는 상기 지정된 저장매체(115)에 저장된다.

[0130] 한편 상기 인증서 등록부(235)는 상기 운영 서버(100)로부터 상기 저장매체(115)에 저장된 인증서의 나머지 일부 구성을 제공받아 상기 메모리부(213) 또는 IC칩에 저장할 수 있으며, 상기 인증서의 나머지 일부 구성은 상기 지정대상 식별정보로 이용되거나, 또는 상기 저장매체(115)에 저장된 인증서가 이용되는 시점에 상기 운영 서버(100)로부터 수신되는 인증서의 일부 구성과 조합되어 이용 가능한 인증서의 전체 구성을 구성하는데 이용된다.

[0131] 도면2를 참조하면, 상기 애플리케이션(215)은, 상기 운영 서버(100)의 식별정보 획득부(125)를 통해 상기 무선단말(200)(또는 무선단말(200) 이외에 사용자가 이용 가능한 다른 단말(200))에 대한 지정대상 식별정보가 획득되어 상기 운영 서버(100)의 식별정보 저장부(130)를 통해 저장되도록 처리하는 단말 지정 처리부(240)를 구비한다.

[0132] 상기 단말 지정 처리부(240)는 상기 메모리부(213)에 저장된 정보, 상기 USIM을 포함하는 IC칩에 저장된 정보, 상기 무선단말(200)의 읽기전용 메모리에 기록된 정보, 상기 무선단말(200)의 하드웨어적 구성부에 할당된 정보, 상기 무선단말(200)의 통신식별 정보, 상기 무선단말(200)에서 생성된 정보, 키 입력부(203)를 통해 입력된 정보, 상기 애플리케이션(215)을 식별하는 정보, 지정된 코드생성모듈을 통해 동적 생성된 정보 중 적어도 하나 또는 둘 이상이 조합된 m개의 지정 정보를 획득하고, 상기 획득된 m개의 지정 정보를 포함하는 지정대상 식별정보를 통신망을 통해 상기 운영 서버(100)로 제공함으로써, 상기 운영 서버(100)의 식별정보 획득부(125)를 통해 상기 지정대상 식별정보가 획득되도록 처리한다.

[0133] 본 발명의 실시 방법에 따르면, 상기 무선단말(200)에 대한 지정대상 식별정보는 상기 무선단말(200)에 저장된 지정 정보, 상기 무선단말(200)에서 생성된 지정 정보, 상기 무선단말(200)에서 입력된 지정 정보 중 하나 이상의 지정 정보를 포함하여 이루어지며, 상기 지정대상 식별정보를 구성하기 위해 상기 단말 지정 처리부(240)는 상기 무선단말(200)에 구비된 각종 자원(예컨대, 저장 자원, 출력 자원, 입력 자원, 카메라 자원, 통신 자원, NFC 자원, 위치측위 자원 등)의 사용권한을 득하고 이를 통해 상기 무선단말(200)의 지정대상 식별정보에 포함될 m개의 지정 정보를 획득한다. 예를들어, 상기 단말 지정 처리부(240)는 상기 무선단말(200)에 구비된 각종 자원으로부터 상기 지정대상 식별정보에 포함될 특정 지정 정보를 획득하거나, 또는 상기 각종 자원으로부터 획득되는 정보를 이용하여 특정 지정 정보를 생성할 수 있다.

[0134] 도면2를 참조하면, 상기 애플리케이션(215)은, 상기 운영 서버(100)의 지정대상 인증부(145)를 통해 상기 무선단말(200)이 상기 저장매체(115)에 저장된 인증서를 이용 가능한 N개의 지정된 단말(200) 중 제n 단말(200)로 인증시키는 지정 단말 인증부(245)와, 상기 운영 서버(100)의 인증서 처리부(150)와 연동하여 상기 지정된 저장매체(115)에 저장된 인증서를 이용한 인증서 처리가 수행되도록 처리하는 인증서 이용부(250)를 구비한다.

[0135] 상기 인증서 이용부(250)를 통해 사용자의 인증서를 이용한 인증서 처리가 수행되어야 하는 경우, 상기 지정 단말 인증부(245)는 상기 메모리부(213)에 저장된 정보, 상기 USIM을 포함하는 IC칩에 저장된 정보, 상기 무선단말(200)의 읽기전용 메모리에 기록된 정보, 상기 무선단말(200)의 하드웨어적 구성부에 할당된 정보, 상기 무선단말(200)의 통신식별 정보, 상기 무선단말(200)에서 생성된 정보, 키 입력부(203)를 통해 입력된 정보, 상기 애플리케이션(215)을 식별하는 정보, 지정된 코드생성모듈을 통해 동적 생성된 정보 중 적어도 하나 또는 둘 이상이 조합된 m개의 지정 정보를 획득하고, 상기 획득된 m개의 지정 정보를 포함하는 지정대상 식별정보를 통신망을 통해 상기 운영 서버(100)로 제공함으로써, 상기 운영 서버(100)의 지정대상 인증부(145)를 통해 상기 무선단말(200)이 상기 저장매체(115)에 저장된 인증서를 이용 가능한 N개의 지정된 단말(200) 중 제n 단말(200)로 인증되도록 처리한다.

[0136] 본 발명의 실시 방법에 따르면, 상기 무선단말(200)을 제n 단말(200)로 인증시키는 지정대상 식별정보는 상기 무선단말(200)에 저장된 지정 정보, 상기 무선단말(200)에서 생성된 지정 정보, 상기 무선단말(200)에서 입력된 지정 정보 중 하나 이상의 지정 정보를 포함하여 이루어지며, 상기 지정대상 식별정보를 구성하기 위해 상기 지정 단말 인증부(245)는 상기 무선단말(200)에 구비된 각종 자원(예컨대, 저장 자원, 출력 자원, 입력 자원, 카메라 자원, 통신 자원, NFC 자원, 위치측위 자원 등)의 사용권한을 득하고 이를 통해 상기 무선단말(200)의 지정대상 식별정보에 포함될 m개의 지정 정보를 획득한다. 예를들어, 상기 지정 단말 인증부(245)는 상기 무선단말(200)에 구비된 각종 자원으로부터 상기 지정대상 식별정보에 포함될 특정 지정 정보를 획득하거나, 또는 상기 각종 자원으로부터 획득되는 정보를 이용하여 특정 지정 정보를 생성할 수 있다.

[0137] 상기 지정 단말 인증부(245)를 통해 상기 무선단말(200)이 상기 저장매체(115)에 저장된 사용자의 인증서를 이용 가능한 제n 단말(200)로 인증되면, 상기 인증서 이용부(250)는 상기 운영 서버(100)의 인증서 처리부(150)를 통해 상기 저장매체(115)에 저장된 사용자의 인증서를 제공받거나, 또는 상기 운영 서버(100)의 인증서 처리부(150)로 인증서 처리가 데이터를 전송한다.

[0138] 본 발명의 제1 인증서 이용 방식에 따라 상기 운영 서버(100)의 인증서 처리부(150)를 통해 상기 저장매체(115)에 저장된 사용자의 인증서가 수신되는 경우, 상기 인증서 이용부(250)는 상기 수신된 사용자의 인증서를 지정된 저장 영역(예컨대, 휘발성 메모리 영역, 비휘발성 메모리 영역 등)에 저장하고, 상기 사용자의 인증서를 이용한 인증서 처리의 대상에 해당하는 데이터(예컨대, 금융거래 정보, 지불결제 정보 등)를 확인한 후, 상기 인증서에 구비된 각종 키(예컨대, 사용자의 공개키, 개인키 등)를 이용하여 상기 데이터에 대한 인증서 처리 절차를 수행한다. 상기 인증서 이용부(250)는 상기 인증서 처리된 데이터는 통신망을 통해 지정된 인증 서버로 전송된다.

[0139] 본 발명의 제2 인증서 이용 방식에 따라 상기 운영 서버(100)의 인증서 처리부(150)가 상기 인증서 처리 대상 데이터에 대한 인증서 처리를 대행하는 경우, 상기 인증서 이용부(250)는 상기 사용자의 인증서를 이용한 인증서 처리의 대상에 해당하는 데이터(예컨대, 금융거래 정보, 지불결제 정보 등)를 확인하여 통신망을 통해 상기 운영 서버(100)로 전송한다. 만약 상기 인증서 처리된 데이터가 상기 무선단말(200)로 수신되도록 지정된다면, 상기 인증서 이용부(250)는 상기 운영 서버(100)의 인증서 처리부(150)로부터 상기 저장매체(115)에 저장된 사용자의 인증서를 통해 인증서 처리된 데이터를 수신한 후에 상기 인증서 처리된 데이터를 통신망을 통해 지정된 인증 서버로 전송하다. 한편 상기 운영 서버(100)의 인증서 처리부(150)는 상기 인증서 처리된 데이터를 상기 지정된 인증 서버로 직접 전송할 수 있으며, 이에 의해 본 발명이 한정되지 아니한다.

[0140] 도면3은 본 발명에 따른 클라우드 방식 인증서 운영에서 인증서를 등록하는 과정을 도시한 도면이다.

[0141] 보다 상세하게 본 도면3은 사용자에 대한 본인 인증 후에 인증서 발급기관에서 상기 사용자에게 발급한 인증서

를 네트워크 상의 지정된 저장매체(115)에 등록하는 과정에 대한 일 실시 방법을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면3을 참조 및/또는 변형하여 상기 인증서 등록 과정에 대한 다양한 실시 방법(예컨대, 일부 단계가 생략되거나, 또는 순서가 변경된 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면3에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0142] 도면3을 참조하면, 사용자의 단말(200)은 통신망을 통해 운영 서버(100)에 접속하여 인증서 발급기관에서 상기 사용자에게 발급한 인증서를 네트워크 상의 지정된 저장매체(115)에 등록하도록 요청하며(300), 이에 대응하여 상기 운영 서버(100)는 상기 사용자의 단말(200)에서 이용 가능한 i개의 본인 인증 방식을 확인하고(305), 상기 사용자의 단말(200)과 연계하여 상기 i개의 본인 인증 절차를 지정된 순서에 따라 수행한다(310).

[0143] 만약 상기 사용자의 본인 인증이 처리되지 않는다면, 상기 운영 서버(100)는 상기 사용자의 단말(200)로 본인 인증 오류를 제공하여 출력시킨다(315). 한편 상기 사용자의 본인 인증이 처리되면, 상기 운영 서버(100)는 지정된 저장매체(115)에 저장될 사용자의 인증서를 획득한다(320). 상기 지정된 저장매체(115)에 저장될 사용자의 인증서는 상기 도면1에 설명된 제1 인증서 획득 방식에 따라 상기 사용자의 인증서를 발급한 인증서 발급기관에 구비된 인증서 서버로부터 획득되거나(320), 또는 제2 인증서 획득 방식에 따라 상기 사용자에게 발급된 인증서를 관리하는 관리기관의 기관 서버로부터 획득되거나(320), 또는 제3 인증서 획득 방식에 따라 상기 사용자의 단말(200)에서 이용 중인 인증서를 복사/이전하는 방식으로 획득될 수 있다(320).

[0144] 만약 상기 지정된 저장매체(115)에 저장될 사용자의 인증서가 획득되지 않는다면, 상기 운영 서버(100)는 상기 사용자의 단말(200)로 인증서 획득 오류를 제공하여 출력시킨다(325). 한편 상기 지정된 저장매체(115)에 저장될 사용자의 인증서가 획득되면, 상기 운영 서버(100)는 상기 획득된 사용자의 인증서에 대한 유효성을 검증한다(330).

[0145] 만약 상기 획득된 사용자의 인증서에 대한 유효성이 검증되면, 상기 운영 서버(100)는 상기 획득된 사용자의 인증서를 지정된 저장매체(115)에 저장한다(340).

[0146] 도면4는 본 발명에 따른 클라우드 방식 인증서 운영에서 인증서를 이용 가능한 단말(200)을 지정 등록하는 과정을 도시한 도면이다.

[0147] 보다 상세하게 본 도면4는 상기 도면3에 도시된 과정을 통해 저장매체(115)에 저장된 사용자의 인증서를 이용 가능한 N개의 단말(200)을 미리 지정하여 등록하는 과정에 대한 일 실시 방법을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면4를 참조 및/또는 변형하여 상기 단말 지정 등록 과정에 대한 다양한 실시 방법(예컨대, 일부 단계가 생략되거나, 또는 순서가 변경된 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면4에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다. 한편 본 도면4에 도시된 과정은 상기 도면3의 과정 전에 수행되는 것이 가능하다. 또한 상기 인증서를 이용 가능한 단말(200)을 미리 지정 등록하지 않는다면 본 도면4에 도시된 과정이 생략될 수도 있다.

[0148] 도면4를 참조하면, 사용자의 단말(200)은 자신(또는 사용자가 이용 가능한 다른 각종 단말(200))을 상기 도면3에 도시된 과정을 통해 저장매체(115)에 저장된 사용자의 인증서를 이용 가능한 단말(200)로 지정 등록하도록 요청하며(400), 이에 대응하여 상기 운영 서버(100)는 상기 사용자의 단말(200)에서 이용 가능한 j개의 본인 인증 방식을 확인하고(405), 상기 사용자의 단말(200)과 연계하여 상기 j개의 본인 인증 절차를 지정된 순서에 따라 수행한다(410). 한편 본 도면4가 상기 도면3의 과정과 함께 일괄 수행된다면, 상기 사용자 본인 인증은 상기 도면3에서 이미 수행되었으므로 생략 가능하다.

[0149] 만약 상기 사용자의 본인 인증이 처리되지 않는다면, 상기 운영 서버(100)는 상기 사용자의 단말(200)로 본인 인증 오류를 제공하여 출력시킨다(415). 한편 상기 사용자의 본인 인증이 처리되면, 상기 운영 서버(100)는 상기 사용자의 단말(200)에 의해 지정 등록될 단말(200)에 대한 지정대상 식별정보에 대응하는 m개의 지정 정보를 확인하고(420), 상기 사용자의 단말(200)로 상기 지정 등록될 단말(200)에 대한 m개의 지정 정보를 포함하는 지정대상 식별정보를 요청한다(425).

[0150] 상기 사용자의 단말(200)은 상기 지정 등록될 단말(200)에 대한 m개의 지정 정보를 포함하는 지정대상 식별정보를 추출하거나, 생성하거나, 입력받는 것 중 하나 이상을 통해 획득한 후(430), 상기 획득된 m개의 지정 정보를 포함하는 지정대상 식별정보를 상기 운영 서버(100)로 전송한다(435).

[0151] 상기 운영 서버(100)는 상기 m개의 지정 정보를 포함하는 지정 대상 식별정보를 수신하고(440), 상기 지정대상 식별정보에 포함된 m개의 지정 정보 중에서 적어도 하나에 대한 유효성 검증을 실시한다(445).

[0152] 만약 상기 수신된 지정대상 식별정보가 검증되지 않는다면, 상기 운영 서버(100)는 상기 사용자의 단말(200)로 지정대상 식별정보 오류를 제공하여 출력시킨다(450). 한편 상기 수신된 지정대상 식별정보가 검증된다면, 상기 운영 서버(100)는 상기 지정대상 식별정보를 상기 도면3에 도시된 과정을 통해 지정된 저장매체(115)에 저장된 사용자의 인증서와 직/간접적으로 매핑하여 저장한다(455).

[0153] 도면5는 본 발명에 따른 클라우드 방식 인증서 운영에서 인증서를 이용 가능한 사용자를 등록하는 과정을 도시한 도면이다.

[0154] 보다 상세하게 본 도면5는 상기 도면3에 도시된 과정을 통해 인증서를 등록한 사용자 또는 상기 도면4에 도시된 과정을 통해 단말(200)을 지정 등록한 사용자를 미리 식별하여 등록하는 과정에 대한 일 실시 방법을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면5를 참조 및/또는 변형하여 상기 사용자 등록 과정에 대한 다양한 실시 방법(예컨대, 일부 단계가 생략되거나, 또는 순서가 변경된 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면5에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다. 특히 본 도면5는 상기 저장매체(115)에 저장된 인증서를 이용하는 과정에서 사용자에 대한 인증을 간소화하거나 또는 자동화하기 위한 것으로, 만약 상기 인증서를 이용하는 과정에서 사용자의 본인 인증 절차가 이용된다면 본 도면5는 생략될 수 있다.

[0155] 도면5를 참조하면, 상기 도면3 또는 도면4에 도시된 과정 중에 상기 운영 서버(100)는 상기 사용자의 단말(200)로 상기 저장매체(115)에 저장된 인증서에 대응하는 사용자를 고유 인증하는 사용자 식별정보를 요청하고(500), 이에 대응하여 상기 사용자의 단말(200)은 상기 사용자를 고유 인증하는 사용자 식별정보를 결정하여 상기 운영 서버(100)로 전송하며(505), 상기 운영 서버(100)는 상기 사용자의 단말(200)로부터 상기 사용자를 고유 인증하는 사용자 식별정보를 획득한다(510). 한편 상기 사용자 식별정보는 상기 도면3 또는 도면4에 도시된 과정에서 수행된 사용자에 대한 본인 인증 절차의 결과로서 상기 사용자 본인 인증 과정에 사용된 정보 중에서 획득될 수 있다(510).

[0156] 상기 운영 서버(100)는 상기 획득된 사용자 식별정보에 대한 유효성을 검증하는데(515), 만약 상기 사용자 식별정보에 대한 유효성이 검증되지 않으면, 상기 운영 서버(100)는 상기 사용자의 단말(200)로 사용자 식별정보에 대한 오류를 제공하여 출력시킨다(520). 한편 상기 사용자 식별정보에 대한 유효성이 검증되면, 상기 운영 서버(100)는 상기 도면4에 도시된 과정을 통해 등록된 지정대상 식별정보와 상기 사용자의 식별정보를 상기 도면3에 도시된 과정을 통해 저장매체(115)에 저장된 사용자의 인증서와 직/간접적으로 매핑하여 저장한다(525).

[0157] 도면6은 본 발명에 따른 클라우드 방식 인증서 운영에서 저장매체(115)에 등록된 인증서를 확인/추출하는 과정을 도시한 도면이다.

[0158] 보다 상세하게 본 도면6은 클라우드 방식으로 인증서를 이용하기 위해 상기 도면3에 도시된 과정을 통해 저장매체(115)에 저장된 인증서를 확인하거나 추출하는 과정에 대한 일 실시 방법을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면6을 참조 및/또는 변형하여 상기 인증서 확인/추출 과정에 대한 다양한 실시 방법(예컨대, 일부 단계가 생략되거나, 또는 순서가 변경된 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면6에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다. 한편 본 도면6에 도시된 과정은 상기 도면3의 과정 전에 수행되는 것이 가능하다. 또한 상기 인증서를 이용 가능한 단말(200)을 미리 지정 등록하지 않는다면 본 도면6에 도시된 과정이 생략될 수도 있다.

[0159] 도면6을 참조하면, 사용자의 단말(200)은 운영 서버(100)로 상기 도면3에 도시된 과정을 통해 저장매체(115)에 저장된 인증서를 이용하도록 요청하며(600), 이에 대응하여 상기 운영 서버(100)는 상기 사용자의 단말(200)에서 이용 가능한 k개의 본인 인증 방식을 확인하고(605), 상기 사용자의 단말(200)과 연계하여 상기 k개의 본인 인증 절차를 지정된 순서에 따라 수행한다(610). 한편 상기 도면5에 도시된 과정을 통해 사용자 식별정보가 등록된 경우, 상기 운영 서버(100)는 상기 등록된 사용자 식별정보를 통해 상기 사용자를 인증할 수 있다(615).

[0160] 만약 상기 사용자의 본인 인증이 처리되지 않거나 또는 상기 사용자 식별정보를 통한 사용자 인증이 처리되지 않는다면, 상기 운영 서버(100)는 상기 사용자의 단말(200)로 상기 사용자에 대한 인증 오류를 제공하여 출력시킨다(620). 한편 상기 사용자의 본인 인증이 처리되거나 또는 상기 사용자 식별정보를 통한 사용자 인증이 처리되면, 상기 운영 서버(100)는 상기 인증서 이용을 요청한 사용자의 단말(200)을 지정 등록된 단말(200)로 인증하기 위한 m개의 지정 정보를 확인하고(625), 상기 사용자의 단말(200)로 상기 m개의 지정 정보를 포함하는 지정대상 식별정보를 요청한다(630).

[0161] 상기 사용자의 단말(200)은 상기 요청된 m개의 지정 정보를 포함하는 지정대상 식별정보를 추출하거나, 생성하거나, 입력받는 것 중 하나 이상을 통해 획득한 후(635), 상기 획득된 m개의 지정 정보를 포함하는 지정대상 식별정보를 상기 운영 서버(100)로 전송한다(640).

[0162] 상기 운영 서버(100)는 상기 m개의 지정 정보를 포함하는 지정 대상 식별정보를 획득하고(645), 상기 도면4에 도시된 과정을 통해 등록된 지정대상 식별정보와 상기 획득된 지정대상 식별정보를 비교하여 상기 사용자의 단말(200)을 상기 도면4에 도시된 과정을 통해 지정 등록된 제n 단말(200)로 인증한다(650).

[0163] 만약 상기 사용자의 단말(200)이 지정 등록된 제n 단말(200)로 인증되지 않으면, 상기 운영 서버(100)는 상기 사용자의 단말(200)에 대한 지정대상 오류를 제공하여 출력시키며(655), 필요에 따라 상기 사용자의 단말(200)에 대한 지정대상 식별정보를 폐기하거나, 또는 도면4에 도시된 과정을 응용하여 상기 사용자의 단말(200)을 지정대상으로 다시 등록하는 과정을 수행할 수 있다. 한편 상기 사용자의 단말(200)이 지정 등록된 제n 단말(200)로 인증되면, 상기 운영 서버(100)는 지정된 저장매체(115)로부터 상기 지정대상 식별정보와 직/간접적으로 매핑된 사용자의 인증서를 확인 또는 추출한다(660). 한편 본 발명의 실시 방법에 따라 상기 사용자의 단말(200)은 상기 저장매체(115)에 저장된 사용자의 인증서가 확인됨에 따라 상기 운영 서버(100)로부터 상기 저장매체(115)에 저장된 사용자의 인증서가 이용 가능한 상태임을 확인할 수 있다(665).

[0164] 도면7은 본 발명의 일 실시 방법에 따라 클라우드 방식으로 인증서를 이용하는 과정을 도시한 도면이다.

[0165] 보다 상세하게 본 도면7은 지정된 저장매체(115)에 저장된 사용자의 인증서를 사용자의 단말(200)로 제공하여 이용되도록 처리하는 과정에 대한 일 실시 방법을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면7을 참조 및/또는 변형하여 상기 인증서 이용 과정에 대한 다양한 실시 방법(예컨대, 일부 단계가 생략되거나, 또는 순서가 변경된 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면7에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다. 한편 본 도면7에 도시된 과정은 상기 도면3의 과정 전에 수행되는 것이 가능하다. 또한 상기 인증서를 이용 가능한 단말(200)을 미리 지정 등록하지 않는다면 본 도면7에 도시된 과정이 생략될 수도 있다.

[0166] 도면7을 참조하면, 상기 도면6에 도시된 과정을 통해 저장매체(115)에 저장된 사용자의 인증서가 추출되면, 상기 운영 서버(100)는 상기 저장매체(115)로부터 추출된 사용자의 인증서에 지정된 사용 제한을 설정한 후(700), 상기 사용자의 인증서를 상기 도면6에 도시된 과정을 통해 인증된 사용자의 제n 단말(200)로 제공하며(705), 이에 대응하여 상기 사용자의 제n 단말(200)은 통신망을 통해 상기 저장매체(115)로부터 추출된 사용자의 인증서를 수신하여 상기 인증서에 설정된 사용 제한에 따라 유지한다(710).

[0167] 이후, 상기 사용자의 제n 단말(200)은 인증서 처리 대상 데이터를 확인하고(715), 상기 유지된 사용자의 인증서를 통해 상기 데이터에 대한 인증서 처리 절차(예컨대, 사용자 인증, 암/복호화, 전자서명 등)를 수행한다(720).

[0168] 만약 상기 데이터에 대한 인증서 처리가 완료되면, 상기 사용자의 제n 단말(200)은 상기 인증서 처리된 데이터를 지정된 인증 서버로 전송하며(725), 이에 대응하여 상기 인증 서버는 상기 인증서 처리된 데이터를 수신하고(730), 상기 사용자에게 발급된 인증서를 통해 상기 인증서 처리된 데이터를 인증(예컨대, 사용자 인증, 암/복호화, 전자서명 검증 등)한다(735).

[0169] 만약 상기 인증서 처리된 데이터가 인증되면, 상기 인증 서버는 상기 인증된 데이터를 이용하여 상기 사용자의 단말(200)로부터 요청된 서비스가 제공되도록 처리하며(740), 상기 인증된 데이터를 이용한 서비스는 상기 인증 서버와 연동하는 별도의 서비스제공서버(예컨대, 은행 서버, 카드사 서버 등)를 통해 제공될 수 있다.

[0170] 도면8은 본 발명의 다른 일 실시 방법에 따라 클라우드 방식으로 인증서를 이용하는 과정을 도시한 도면이다.

[0171] 보다 상세하게 본 도면8은 지정된 저장매체(115)에 저장된 사용자의 인증서를 통해 사용자의 단말(200)에서 수행될 인증서 처리를 대행하는 과정에 대한 일 실시 방법을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면8을 참조 및/또는 변형하여 상기 인증서 이용 과정에 대한 다양한 실시 방법(예컨대, 일부 단계가 생략되거나, 또는 순서가 변경된 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면8에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다. 한편 본 도면8에 도시된 과정은 상기 도면3의 과정 전에 수행되는 것이 가능하다. 또한 상기 인증서를 이용 가능한 단말(200)을 미리 지정 등록하지 않는다면 본 도면8에 도시된 과정이 생략될 수도 있다.

[0172] 도면8을 참조하면, 상기 도면6에 도시된 과정을 통해 저장매체(115)에 저장된 사용자의 인증서를 이용 가능함이 확인되면, 상기 사용자의 제n 단말(200)은 인증서 처리 대상 데이터를 확인하고(800), 상기 운영 서버(100)로 상기 인증서 처리 대상 데이터를 전송하여 상기 저장매체(115)에 저장된 사용자의 인증서를 이용한 인증서 처리가 수행되도록 요청하며(805), 이에 대응하여 상기 운영 서버(100)는 상기 사용자의 제n 단말(200)로부터 상기 인증서 처리 대상 데이터를 수신하고(810), 상기 저장매체(115)에 저장된 사용자의 인증서를 통해 상기 수신된

데이터에 대한 인증서 처리 절차(예컨대, 사용자 인증, 암/복호화, 전자서명 등)를 대행하여 수행한다(815).

[0173] 만약 상기 데이터에 대한 인증서 처리가 완료되면, 상기 운영 서버(100)는 지정된 대상 장치로 상기 인증서 처리된 데이터를 전달한다(820). 바람직하게, 상기 인증서 처리된 데이터는 상기 사용자의 제n 단말(200)로 전달될 수 있으며, 이 경우에 상기 사용자의 단말(200)은 상기 사용자의 인증서를 통해 인증서 처리된 데이터를 수신하고(825), 상기 인증서 처리된 데이터를 지정된 인증 서버로 전송할 수 있다(830). 또는 인증서 처리된 데이터는 상기 인증 서버로 직접 전달될 수 있다.

[0174] 상기 인증 서버는 상기 사용자의 단말(200) 또는 운영 서버(100)로부터 상기 사용자의 인증서를 통해 인증서 처리된 데이터를 수신하고(835), 상기 사용자에게 발급된 인증서를 통해 상기 인증서 처리된 데이터를 인증(예컨대, 사용자 인증, 암/복호화, 전자서명 검증 등)한다(840).

[0175] 만약 상기 인증서 처리된 데이터가 인증되면, 상기 인증 서버는 상기 인증된 데이터를 이용하여 상기 사용자의 단말(200)로부터 요청된 서비스가 제공되도록 처리하며(845), 상기 인증된 데이터를 이용한 서비스는 상기 인증 서버와 연동하는 별도의 서비스제공서버(예컨대, 은행 서버, 카드사 서버 등)를 통해 제공될 수 있다.

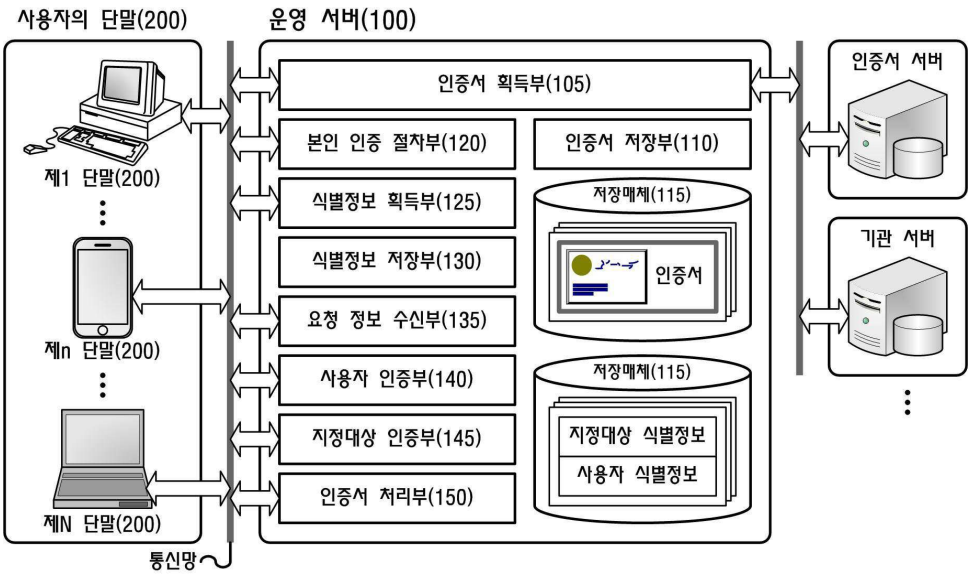
부호의 설명

[0176]

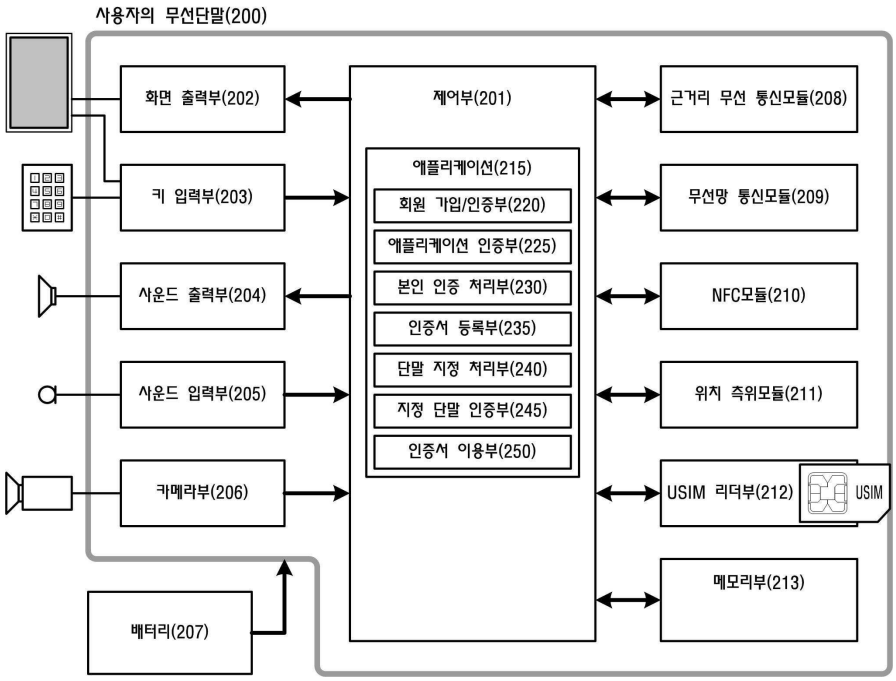
100 : 운영 서버	105 : 인증서 획득부
110 : 인증서 저장부	115 : 저장매체
120 : 본인 인증 절차부	125 : 식별정보 획득부
130 : 식별정보 저장부	135 : 요청 정보 수신부
140 : 사용자 인증부	145 : 지정대상 인증부
150 : 인증서 처리부	200 : 단말

도면

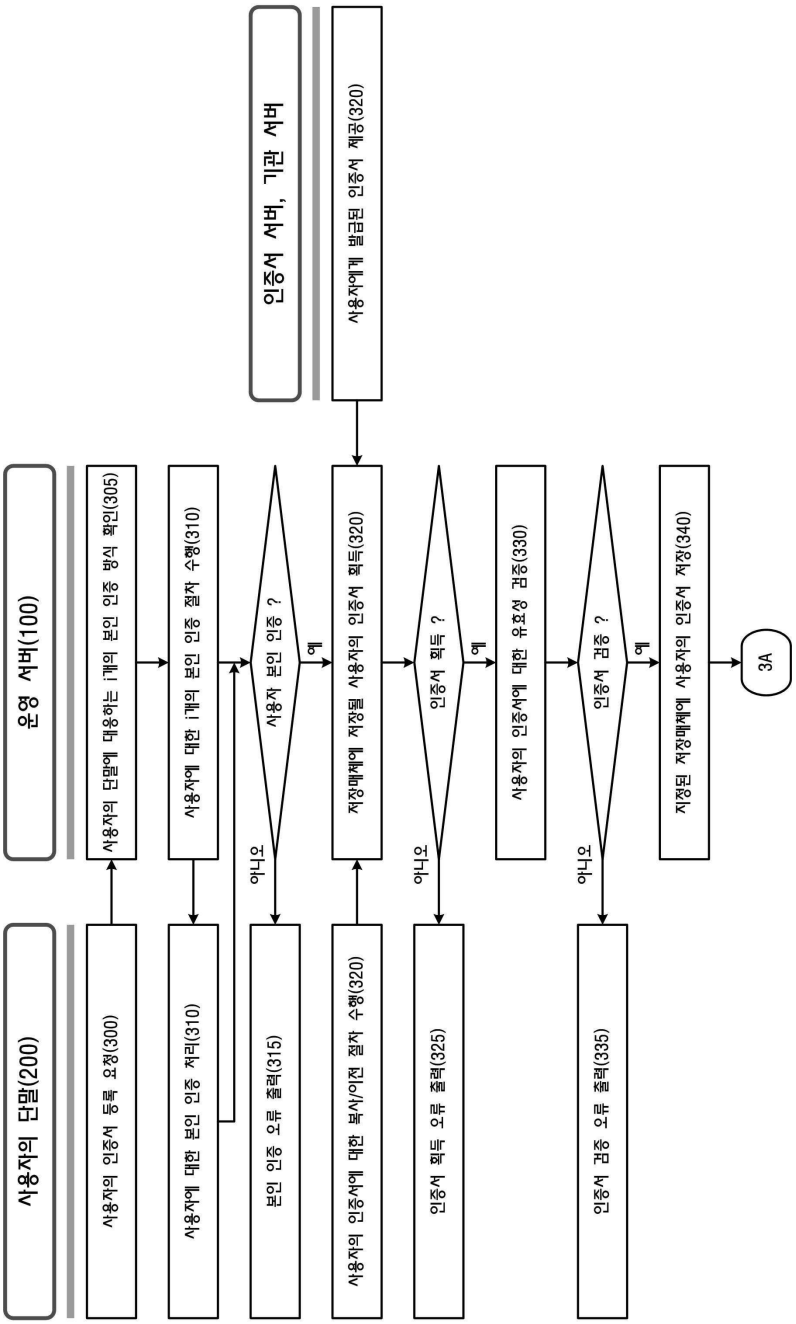
도면1



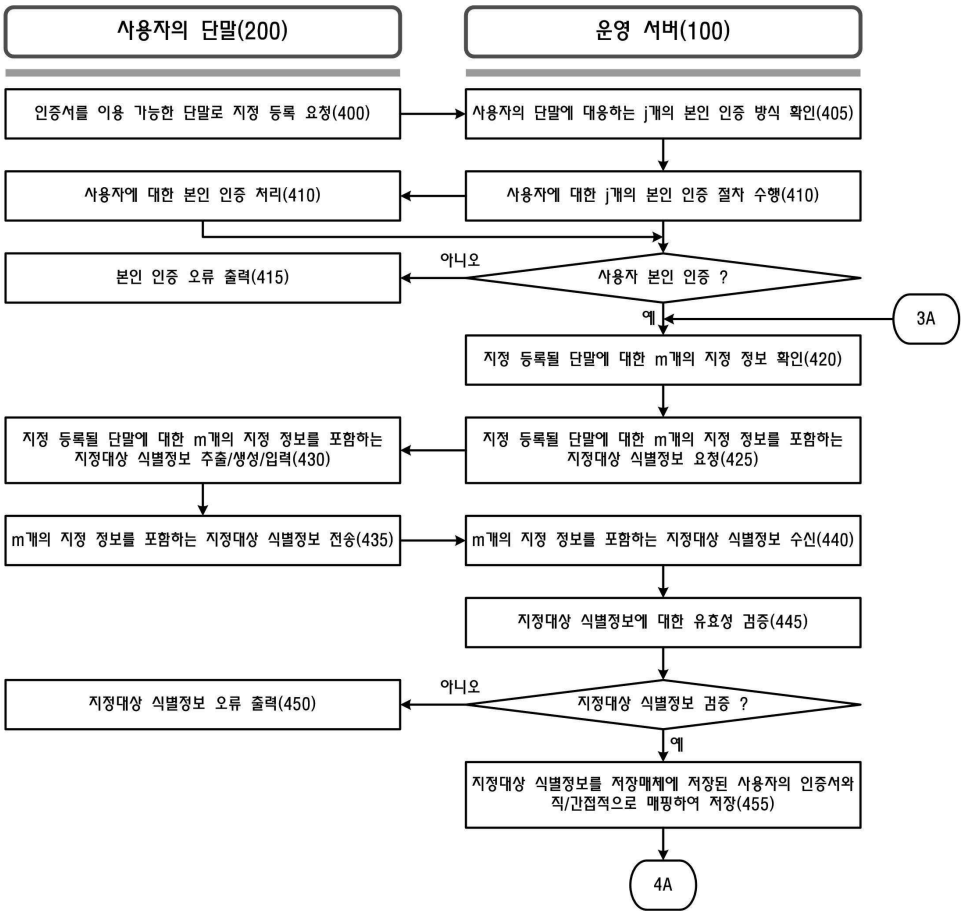
도면2


사용자의 무선단말(200)
화면 출력부(202)
키 입력부(203)
사운드 출력부(204)
사운드 입력부(205)
카메라부(206)
배터리(207)
제어부(201)
애플리케이션(215)
회원 가입/인증부(220)
애플리케이션 인증부(225)
본인 인증 처리부(230)
인증서 등록부(235)
단말 지정 처리부(240)
지정 단말 인증부(245)
인증서 이용부(250)
근거리 무선 통신모듈(208)
무선망 통신모듈(209)
NFC모듈(210)
위치 측위모듈(211)
USIM 리더부(212)
USIM
메모리부(213)

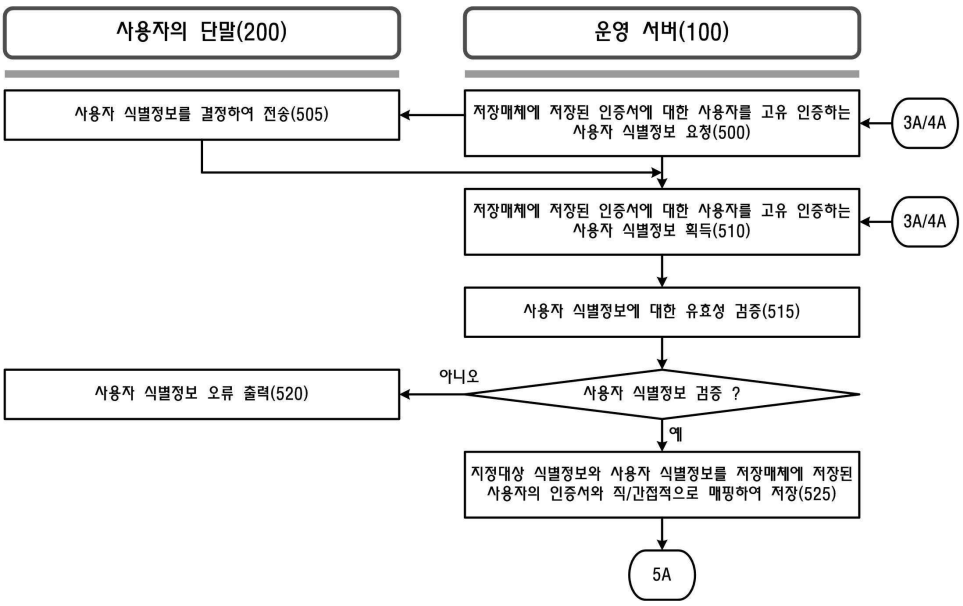
도면3


사용자의 단말(200)
운영 서버(100)
인증서 서버, 기관 서버
사용자의 인증서 등록 요청(300)
사용자의 단말에 대응하는 i개의 본인 인증 방식 확인(305)
사용자에 대한 본인 인증 처리(310)
사용자에 대한 i개의 본인 인증 절차 수행(310)
본인 인증 오류 출력(315)
아니오
사용자 본인 인증 ?
예
사용자의 인증서에 대한 복사/이전 절차 수행(320)
저장매체에 저장될 사용자의 인증서 획득(320)
사용자에게 발급된 인증서 제공(320)
인증서 획득 오류 출력(325)
아니오
인증서 획득 ?
예
사용자의 인증서에 대한 유효성 검증(330)
인증서 검증 오류 출력(335)
아니오
인증서 검증 ?
예
지정된 저장매체에 사용자의 인증서 저장(340)
3A

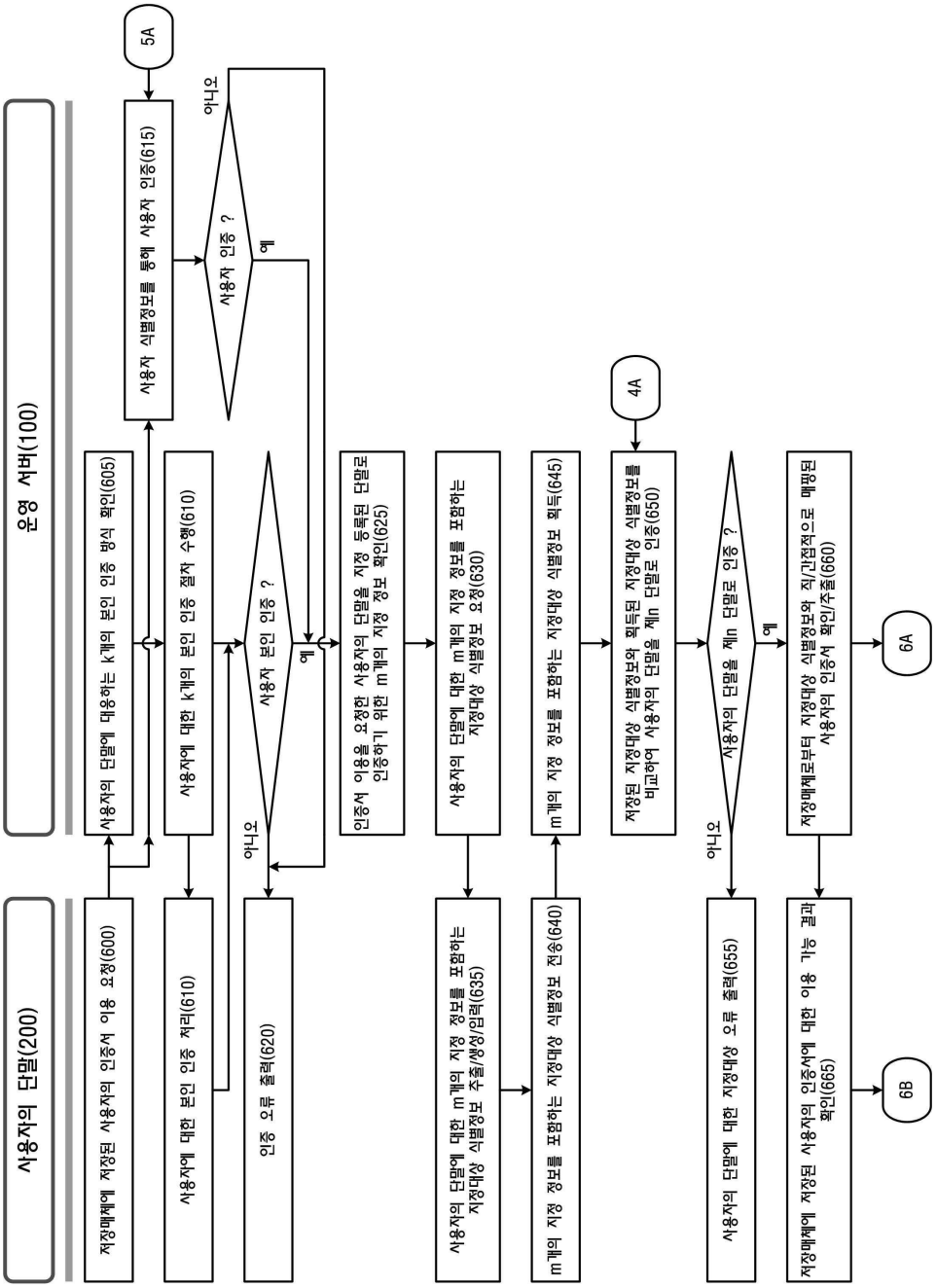
도면4


사용자의 단말(200)
운영 서버(100)
인증서를 이용 가능한 단말로 지정 등록 요청(400)
사용자의 단말에 대응하는 j개의 본인 인증 방식 확인(405)
사용자에 대한 본인 인증 처리(410)
사용자에 대한 j개의 본인 인증 절차 수행(410)
본인 인증 오류 출력(415)
아니오
사용자 본인 인증 ?
예
3A
지정 등록될 단말에 대한 m개의 지정 정보 확인(420)
지정 등록될 단말에 대한 m개의 지정 정보를 포함하는 지정대상 식별정보 추출/생성/입력(430)
지정 등록될 단말에 대한 m개의 지정 정보를 포함하는 지정대상 식별정보 요청(425)
m개의 지정 정보를 포함하는 지정대상 식별정보 전송(435)
m개의 지정 정보를 포함하는 지정대상 식별정보 수신(440)
지정대상 식별정보에 대한 유효성 검증(445)
지정대상 식별정보 오류 출력(450)
아니오
지정대상 식별정보 검증 ?
예
지정대상 식별정보를 저장매체에 저장된 사용자의 인증서와 직/간접적으로 매핑하여 저장(455)
4A

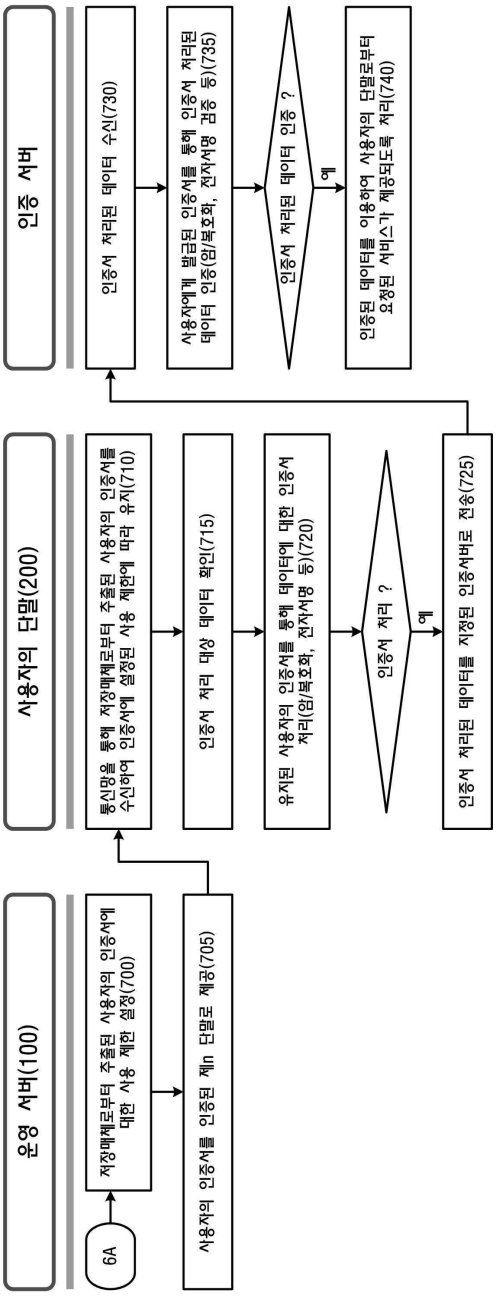
도면5


사용자의 단말(200)
운영 서버(100)
사용자 식별정보를 결정하여 전송(505)
저장매체에 저장된 인증서에 대한 사용자를 고유 인증하는 사용자 식별정보 요청(500)
3A/4A
저장매체에 저장된 인증서에 대한 사용자를 고유 인증하는 사용자 식별정보 획득(510)
3A/4A
사용자 식별정보에 대한 유효성 검증(515)
사용자 식별정보 오류 출력(520)
아니오
사용자 식별정보 검증 ?
예
지정대상 식별정보와 사용자 식별정보를 저장매체에 저장된 사용자의 인증서와 직/간접적으로 매핑하여 저장(525)
5A

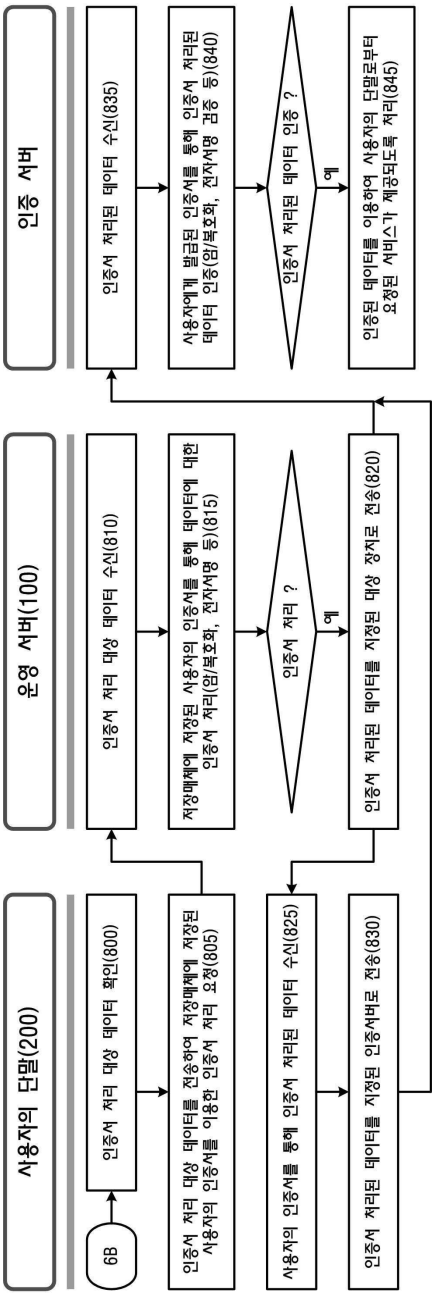
도면6


운영 서버(100)
사용자의 단말(200)
저장매체에 저장된 사용자의 인증서 이용 요청(600)
사용자의 단말에 대응하는 k개의 본인 인증 방식 확인(605)
사용자에 대한 본인 인증 처리(610)
사용자에 대한 k개의 본인 인증 절차 수행(610)
인증 오류 출력(620)
사용자 본인 인증 ?
아니오
예
5A
사용자 식별정보를 통해 사용자 인증(615)
사용자 인증 ?
아니오
예
인증서 이용을 요청한 사용자의 단말을 지정 등록된 단말로 인증하기 위한 m개의 지정 정보 확인(625)
사용자의 단말에 대한 m개의 지정 정보를 포함하는 지정대상 식별정보 요청(630)
사용자의 단말에 대한 m개의 지정 정보를 포함하는 지정대상 식별정보 전송(635)
m개의 지정 정보를 포함하는 지정대상 식별정보 수신(640)
m개의 지정 정보를 포함하는 지정대상 식별정보 획득(645)
4A
저장된 지정대상 식별정보와 획득된 지정대상 식별정보를 비교하여 사용자의 단말을 제n 단말로 인증(650)
사용자의 단말을 제n 단말로 인증 ?
아니오
예
사용자의 단말에 대한 지정대상 오류 출력(655)
저장매체로부터 지정대상 식별정보와 직/간접적으로 매핑된 사용자의 인증서 확인/추출(660)
6A
저장매체에 저장된 사용자의 인증서에 대한 이용 가능 결과 확인(665)
6B

도면7


운영 서버(100)
사용자의 단말(200)
인증 서버
6A
저장매체로부터 추출된 사용자의 인증서에 대한 사용 제한 설정(700)
사용자의 인증서를 인증된 제n 단말로 제공(705)
통신망을 통해 저장매체로부터 추출된 사용자의 인증서를 수신하여 인증서에 설정된 사용 제한에 따라 유지(710)
인증서 처리 대상 데이터 확인(715)
유지된 사용자의 인증서를 통해 데이터에 대한 인증서 처리(암/복호화, 전자서명 등)(720)
인증서 처리 ?
예
인증서 처리된 데이터를 지정된 인증서버로 전송(725)
인증서 처리된 데이터 수신(730)
사용자에게 발급된 인증서를 통해 인증서 처리된 데이터 인증(암/복호화, 전자서명 검증 등)(735)
인증서 처리된 데이터 인증 ?
예
인증된 데이터를 이용하여 사용자의 단말로부터 요청된 서비스가 제공되도록 처리(740)

도면8


사용자의 단말(200)
운영 서버(100)
인증 서버
6B
인증서 처리 대상 데이터 확인(800)
인증서 처리 대상 데이터 수신(810)
인증서 처리 대상 데이터 수신(835)
인증서 처리 대상 데이터를 전송하여 저장매체에 저장된 사용자의 인증서를 이용한 인증서 처리 요청(805)
저장매체에 저장된 사용자의 인증서를 통해 데이터에 대한 인증서 처리(암/복호화, 전자서명 등)(815)
사용자에게 발급된 인증서를 통해 인증서 처리된 데이터 인증(암/복호화, 전자서명 검증 등)(840)
인증서 처리 ?
예
인증서 처리 ?
예
사용자의 인증서를 통해 인증서 처리된 데이터 수신(825)
인증서 처리된 데이터를 지정된 인증서버로 전송(830)
인증서 처리된 데이터를 지정된 대상 장치로 전송(820)
인증된 데이터를 이용하여 사용자의 단말로부터 요청된 서비스가 제공되도록 처리(845)