(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0004250
(43) 공개일자 2019년01월11일

(51) 국제특허분류(Int. Cl.)
G06Q 20/32 (2012.01) *G06Q 20/38* (2012.01)
G06Q 20/40 (2012.01) *G06Q 40/02* (2012.01)
H04L 9/32 (2006.01) *H04W 88/02* (2009.01)
(52) CPC특허분류
G06Q 20/3227 (2013.01)
G06Q 20/3221 (2013.01)
(21) 출원번호 10-2018-0172421(분할)
(22) 출원일자 2018년12월28일
심사청구일자 2018년12월28일
(62) 원출원 특허 10-2017-0142862
원출원일자 2017년10월30일
심사청구일자 2017년10월30일

(71) 출원인
주식회사 비즈모델라인
서울특별시 마포구 와우산로 77, 6층 (서교동, 대창빌딩)
(72) 발명자
김재형
서울특별시 강남구 압구정로 313, 42동 302호 (압구정동, 한양아파트)
권봉기
경기도 안양시 동안구 관양동 그라테아오피스텔 1214호

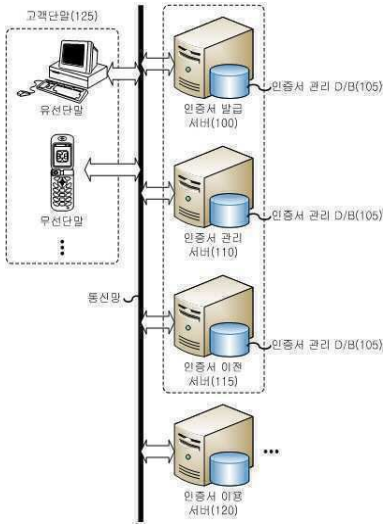
전체 청구항 수 : 총 2 항

(54) 발명의 명칭 **지정 단말을 이용한 비대면 거래 제공 방법**

(57) 요 약

본 발명의 지정 단말을 이용한 비대면 거래 제공 방법에 따르면, 사용자의 단말과 통신 가능한 서버에 의해 실행되는 방법에 있어서, 사용자의 인증서를 발급하거나 복사하는데 사용된 사용자의 단말로부터 상기 단말을 물리적으로 구성하는 M(M>1)개의 물리적 구성장치 중 기 설정된 m(1≤m≤M)개의 구성장치를 고유 식별하는 m개의 장치고유 정보를 등록받아 저장하고, 사용자의 단말을 이용한 비대면 거래 시, 상기 사용자의 단말로부터 상기 단말을 구성하는 m개의 구성장치를 고유 식별하는 m개의 장치고유 정보를 수신하고, 상기 저장된 m개의 장치고유 정보와 상기 수신된 m개의 장치고유 정보를 비교 인증하여 상기 사용자 단말에 대한 장치고유 정보 기반 유효성을 인증한 결과를 확인하며, 상기 장치고유 정보 기반 유효성 인증 시, 상기 인증된 m개의 장치고유 정보에 대응하는 구성장치를 구비한 단말을 이용한 비대면 거래를 처리하는 절차를 수행한다.

대 표 도 - 도1



(52) CPC특허분류
G06Q 20/3229 (2013.01)
G06Q 20/38215 (2013.01)
G06Q 20/4016 (2013.01)
G06Q 40/02 (2013.01)
H04L 9/32 (2013.01)
H04W 88/02 (2013.01)

명 세 서

청구범위

청구항 1

사용자의 단말과 통신 가능한 서버에 의해 실행되는 방법에 있어서,

사용자의 인증서를 발급하거나 복사하는데 사용된 사용자의 단말로부터 상기 단말을 물리적으로 구성하는 M(M>1)개의 물리적 구성장치 중 기 설정된 m(1≤m≤M)개의 구성장치를 고유 식별하는 m개의 장치고유 정보를 등록받아 저장하는 제1 단계;

사용자의 단말을 이용한 비대면 거래 시, 상기 사용자의 단말로부터 상기 단말을 구성하는 m개의 구성장치를 고유 식별하는 m개의 장치고유 정보를 수신하고, 상기 저장된 m개의 장치고유 정보와 상기 수신된 m개의 장치고유 정보를 비교 인증하여 상기 사용자 단말에 대한 장치고유 정보 기반 유효성을 인증한 결과를 확인하는 제2 단계; 및

상기 장치고유 정보 기반 유효성 인증 시, 상기 인증된 m개의 장치고유 정보에 대응하는 구성장치를 구비한 단말을 이용한 비대면 거래를 처리하는 절차를 수행하는 제3 단계;를 포함하는 지정 단말을 이용한 비대면 거래 제공 방법.

청구항 2

제 1항에 있어서,

상기 장치고유 정보 기반 유효성 인증이 확인되지 않는 경우, 상기 비대면 거래를 위한 다른 유효성 검증 결과와 무관하게 오류를 발생시키는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 지정 단말을 이용한 비대면 거래 제공 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은, 사용자의 단말과 통신 가능한 서버에 의해 실행되는 방법에 있어서, 사용자의 인증서를 발급하거나 복사하는데 사용된 사용자의 단말로부터 상기 단말을 물리적으로 구성하는 M(M>1)개의 물리적 구성장치 중 기 설정된 m(1≤m≤M)개의 구성장치를 고유 식별하는 m개의 장치고유 정보를 등록받아 저장하고, 사용자의 단말을 이용한 비대면 거래 시, 상기 사용자의 단말로부터 상기 단말을 구성하는 m개의 구성장치를 고유 식별하는 m개의 장치고유 정보를 수신하고, 상기 저장된 m개의 장치고유 정보와 상기 수신된 m개의 장치고유 정보를 비교 인증하여 상기 사용자 단말에 대한 장치고유 정보 기반 유효성을 인증한 결과를 확인하며, 상기 장치고유 정보 기반 유효성 인증 시, 상기 인증된 m개의 장치고유 정보에 대응하는 구성장치를 구비한 단말을 이용한 비대면 거래를 처리하는 절차를 수행하는 지정 단말을 이용한 비대면 거래 제공 방법에 관한 것이다.

배 경 기 술

[0003] 정보통신 기술의 지속적인 발전으로 종래 대면 인증을 통해 이루어지던 금융거래는 최근 유선 통신망 내지 유선 통신망을 기반으로 비대면 인증을 이용한 비대면 금융거래 방식으로 이전되었으며, 현재 상기 비대면 금융거래 중 인터넷 뱅킹을 통한 금융거래 금액만 하루 18조원에 이르고 있다.

[0005] 상기와 같은 비대면 금융거래를 위한 비대면 인증 방식 중 가장 대표적으로 사용되고 있는 인증 방식은, 공인인증서를 통해 비대면 거래를 인증하는 방식이다.

[0007] 상기 공인인증서 기반 비대면 인증은, 우선 공인인증기관에서 고객이 지정한 매체(예컨대, 컴퓨터 하드디스크, 플로피디스크, USB(Universal Serial Bus) 메모리, IC(Integrated Circuit)카드 등)로 공인인증서를 발급하고, 상기 매체를 운영하는 단말과 상기 단말이 접속한 통신망을 이용한 금융거래시, 상기 공인인증서에 구비된 암호화 키(예컨대, 공개키와 개인키, 또는 대칭키)를 이용하여 상기 단말과 서버 간 트랜잭션 데이터(Transaction Data)를 암호화/복호화 내지 전자서명 첨부/검증을 통해 상기 비대면 금융거래를 인증하는 것을 포함하여 이루어진다.

[0009] 한편, 상기 공인인증서는 오직 하나의 원본 인증서만을 유효하게 생각하며, 상기 원본 인증서에 대한 유효성은 DRM(Digital Rights Management)을 통해 확보된다. 즉, 원본 인증서에 대한 사본은 DRM을 통해 인정하지 않으며, 상기 인증서를 최초 발급된 매체에서 다른 매체로 이전시, 상기 DRM 인증 절차에 따른 인증서 이전 절차에 따라 이전하여 사용하게 된다.

[0011] 그런데, 상기와 같은 인증서의 이전은 사본 인증서를 인정하지 않는 것일 뿐, 해커에 의해 원본 인증서의 이전(예컨대, 상기 공인인증서가 발급되어 있는 매체에서 해커가 지정한 매체로의 이전)을 막을 수 있는 방법이 없는 문제점을 포함하고 있으며, 만약 상기 공인인증서가 고객의 매체로부터 해커가 지정한 매체로 이전되고, 상기 공인인증서에 대한 PIN 번호가 노출되는 경우, 해커는 상기 공인인증서와 PIN 번호를 기반으로 상기 고객의 계좌에 예치된 금액을 임의의 계좌(예컨대, 해커가 사용하는 계좌)로 이체할 수 있는 심각한 문제점을 포함하고 있으며, 최근 실제로 이와 같은 방식의 해킹 사례가 발생한 바 있다.

발명의 내용

해결하려는 과제

[0013] 본 발명의 목적은, 사용자의 단말과 통신 가능한 서버에 의해 실행되는 방법에 있어서, 사용자의 인증서를 발급하거나 복사하는데 사용된 사용자의 단말로부터 상기 단말을 물리적으로 구성하는 M(M>1)개의 물리적 구성장치 중 기 설정된 m(1≤m≤M)개의 구성장치를 고유 식별하는 m개의 장치고유 정보를 등록받아 저장하는 제1 단계와 사용자의 단말을 이용한 비대면 거래 시, 상기 사용자의 단말로부터 상기 단말을 구성하는 m개의 구성장치를 고유 식별하는 m개의 장치고유 정보를 수신하고, 상기 저장된 m개의 장치고유 정보와 상기 수신된 m개의 장치고유 정보를 비교 인증하여 상기 사용자 단말에 대한 장치고유 정보 기반 유효성을 인증한 결과를 확인하는 제2 단계 및 상기 장치고유 정보 기반 유효성 인증 시, 상기 인증된 m개의 장치고유 정보에 대응하는 구성장치를 구비한 단말을 이용한 비대면 거래를 처리하는 절차를 수행하는 제3 단계를 포함하는 지정 단말을 이용한 비대면 거래 제공 방법을 제공함에 있다.

과제의 해결 수단

[0015] 본 발명에 따른 지정 단말을 이용한 비대면 거래 제공 방법은, 사용자의 단말과 통신 가능한 서버에 의해 실행되는 방법에 있어서, 사용자의 인증서를 발급하거나 복사하는데 사용된 사용자의 단말로부터 상기 단말을 물리적으로 구성하는 M(M>1)개의 물리적 구성장치 중 기 설정된 m(1≤m≤M)개의 구성장치를 고유 식별하는 m개의 장치고유 정보를 등록받아 저장하는 제1 단계와 사용자의 단말을 이용한 비대면 거래 시, 상기 사용자의 단말로부터 상기 단말을 구성하는 m개의 구성장치를 고유 식별하는 m개의 장치고유 정보를 수신하고, 상기 저장된 m개의 장치고유 정보와 상기 수신된 m개의 장치고유 정보를 비교 인증하여 상기 사용자 단말에 대한 장치고유 정보 기반 유효성을 인증한 결과를 확인하는 제2 단계 및 상기 장치고유 정보 기반 유효성 인증 시, 상기 인증된 m개의 장치고유 정보에 대응하는 구성장치를 구비한 단말을 이용한 비대면 거래를 처리하는 절차를 수행하는 제3 단계를 포함하는 것을 특징으로 한다.

[0017] 본 발명에 따른 지정 단말을 이용한 비대면 거래 제공 방법에 있어서, 상기 장치고유 정보 기반 유효성 인증이

확인되지 않는 경우, 상기 비대면 거래를 위한 다른 유효성 검증 결과와 무관하게 오류를 발생시키는 단계를 더 포함하여 이루어지는 것을 특징으로 한다.

[0019] 본 발명에 따른 지정 단말을 이용한 비대면 거래 제공 방법은, 사용자의 단말과 통신 가능한 서버에 의해 실행되는 방법에 있어서, 사용자의 인증서를 발급하거나 복사하는데 사용된 사용자의 단말로부터 상기 단말을 구성하는 M(M>1)개의 물리적인 구성장치 중 기 설정된 하나 이상의 구성장치를 고유 식별하는 장치고유 정보를 등록받아 저장하는 제1 단계와 사용자의 단말을 이용한 비대면 거래 시, 상기 사용자의 단말로부터 상기 단말을 구성하는 M개의 물리적인 구성장치 중 상기 설정된 구성장치를 고유 식별하는 장치고유 정보를 수신하고, 상기 저장된 장치고유 정보와 상기 수신된 장치고유 정보를 비교 인증하여 상기 사용자 단말에 대한 장치고유 정보 기반 유효성을 인증한 결과를 확인하는 제2 단계 및 상기 장치고유 정보 기반 유효성 인증 시, 상기 인증된 장치고유 정보에 대응하는 구성장치를 구비한 단말을 이용한 비대면 거래를 처리하는 절차를 수행하는 제3 단계를 포함하는 것을 특징으로 한다.

[0021] 본 발명에 따른 지정 단말을 이용한 비대면 거래 제공 방법에 있어서, 상기 장치고유 정보 기반 유효성 인증이 확인되지 않는 경우, 상기 비대면 거래를 위한 다른 유효성 검증 결과와 무관하게 오류를 발생시키는 단계를 더 포함하여 이루어지는 것을 특징으로 한다.

[0023] 본 발명에 따른 지정 단말을 이용한 비대면 거래 제공 방법에 있어서, 상기 장치고유 정보는, 상기 단말을 구성하는 적어도 하나의 구성부품에 할당된 장치고유 정보, 상기 단말에 이탈착되는 IC(Integrated Circuit)칩에 기록된 장치고유 정보, 상기 단말의 통신모듈에 고유 할당된 장치고유 정보 중 적어도 하나의 장치고유 정보를 포함하여 이루어지는 것을 특징으로 한다.

[0026] 본 발명에 따른 지정 단말을 이용한 비대면 거래 제공 방법은, 사용자의 단말과 통신 가능한 서버에 의해 실행되는 방법에 있어서, 사용자의 단말에 탑재되거나 또는 상기 단말의 접촉식 리더를 통해 연결되거나 또는 상기 단말의 비접촉식 리더를 통해 연결되는 매체에 사용자의 인증서가 기록된 경우, 상기 단말의 내부를 구성하는 M(M>1)개의 구성장치 중 기 설정된 하나 이상의 구성장치를 고유 식별하는 장치고유 정보를 등록받아 저장하는 제1 단계와 사용자의 단말을 이용한 비대면 거래 시, 상기 단말로부터 상기 단말의 내부를 구성하는 M개의 구성장치 중 기 설정된 하나 이상의 구성장치에 대한 장치고유 정보를 수신하고 상기 저장된 장치고유 정보를 통해 비교 인증하여 상기 비대면 거래에 이용되는 단말에 구비된 구성장치에 대한 장치고유 정보 기반 유효성을 인증한 결과를 확인하는 제2 단계 및 상기 장치고유 정보 기반 유효성 인증 시, 상기 단말을 이용한 비대면 거래를 처리하는 절차를 수행하는 제3 단계를 포함하는 것을 특징으로 한다.

[0029] 본 발명에 따른 지정 단말을 이용한 비대면 거래 제공 방법에 있어서, 상기 장치고유 정보 기반 유효성 인증이 확인되지 않는 경우, 상기 비대면 거래를 위한 다른 유효성 검증 결과와 무관하게 오류를 발생시키는 단계를 더 포함하여 이루어지는 것을 특징으로 한다.

[0031] 본 발명에 따른 지정 단말을 이용한 비대면 거래 제공 방법에 있어서, 상기 사용자의 비대면 거래에 이용될 사용자의 인증서를 상기 사용자가 이용하는 단말에 탑재되거나 또는 상기 단말의 접촉식 리더를 통해 연결되거나 또는 상기 단말의 비접촉식 리더를 통해 연결되는 매체에 기록되도록 처리하는 단계를 더 포함하여 이루어지는 것을 특징으로 한다.

[0033] 본 발명에 따른 지정 단말을 이용한 비대면 거래 제공 방법에 있어서, 상기 장치고유 정보는, 상기 단말을 구성

하는 적어도 하나의 구성부품에 할당된 장치고유 정보, 상기 단말에 이탈착되는 IC(Integrated Circuit)칩에 기록된 장치고유 정보, 상기 단말의 통신모듈에 고유 할당된 장치고유 정보 중 적어도 하나의 장치고유 정보를 포함하여 이루어지는 것을 특징으로 한다.

[0036] 본 발명에 따른 부정거래 방지 방법은, 사용자의 단말과 통신 가능한 서버에 의해 실행되는 방법에 있어서, 사용자의 비대면 금융거래 또는 비대면 인증 또는 온라인 결제에 이용될 단말에 구비된 프로그램과 연동하여 상기 단말을 통해 비대면 금융거래 또는 비대면 인증 또는 온라인 결제를 처리하기 위한 유효성을 진단하는 절차를 수행하는 제1 단계와 상기 유효성 진단 성공 시, 상기 유효성을 진단하는 절차 중에 상기 단말을 통해 확인된 상기 단말의 고유 정보를 저장하는 제2 단계와 사용자의 단말을 이용한 비대면 금융거래 또는 비대면 인증 또는 온라인 결제 시, 상기 고유 정보를 이용하여 상기 비대면 금융거래 또는 비대면 인증 또는 온라인 결제에 이용되는 단말의 유효성을 인증한 결과를 확인하는 제3 단계 및 상기 고유 정보를 통해 상기 단말의 유효성이 인증된 경우에 상기 인증된 단말을 통해 비대면 금융거래 또는 비대면 인증 또는 온라인 결제를 처리하는 절차를 수행하는 제4 단계를 포함하는 것을 특징으로 한다.

[0038] 본 발명에 따른 부정거래 방지 방법에 있어서, 상기 사용자의 비대면 금융거래 또는 비대면 인증 또는 온라인 결제에 이용될 사용자의 인증서를 상기 사용자가 이용하는 단말에 탑재 또는 이탈착 또는 리더를 통해 비접촉식으로 연동하는 매체에 기록되도록 처리하는 단계를 더 포함하여 이루어지는 것을 특징으로 한다.

[0040] 본 발명에 따른 부정거래 방지 방법에 있어서, 상기 매체는, 상기 매체는, 상기 단말에 내장된 메모리, 상기 단말에 이탈착되는 IC(Integrated Circuit)칩, 상기 단말에 탑재된 하드웨어 보안 모듈(Hardware Security Module; HSM) 중 상기 사용자의 인증서를 기록한 적어도 하나의 매체를 포함하여 이루어지는 것을 특징으로 한다.

[0042] 본 발명에 따른 부정거래 방지 방법에 있어서, 상기 사용자의 비대면 금융거래 또는 비대면 인증 또는 온라인 결제 시, 상기 사용자가 이용하는 단말로부터 상기 비대면 금융거래 또는 비대면 인증 또는 온라인 결제에 이용되는 단말을 인증하기 위한 고유 정보를 수신하는 단계 및 상기 저장된 고유 정보를 통해 상기 수신된 고유 정보의 유효성을 인증하는 인증 절차가 수행되도록 처리하는 단계를 더 포함하여 이루어지는 것을 특징으로 한다.

[0044] 본 발명에 따른 부정거래 방지 방법에 있어서, 상기 비대면 금융거래는, 상기 사용자의 단말에 탑재 또는 이탈착 또는 리더를 통해 비접촉식으로 연동하는 매체에 기록된 사용자의 인증서를 이용하는 금융거래를 포함하여 이루어지는 것을 특징으로 한다.

[0046] 본 발명에 따른 부정거래 방지 방법에 있어서, 상기 비대면 인증은, 상기 사용자의 단말에 탑재 또는 이탈착 또는 리더를 통해 비접촉식으로 연동하는 매체에 기록된 사용자의 인증서를 이용하는 인증을 포함하여 이루어지는 것을 특징으로 한다.

[0048] 본 발명에 따른 부정거래 방지 방법에 있어서, 상기 온라인 결제는, 상기 온라인 결제는, 상기 사용자의 단말에 탑재 또는 이탈착 또는 리더를 통해 비접촉식으로 연동하는 매체에 기록된 사용자의 인증서를 이용하는 결제를 포함하여 이루어지는 것을 특징으로 한다.

[0050] 본 발명에 따른 부정거래 방지 방법에 있어서, 상기 고유 정보는, 상기 단말에 내장된 메모리에 기록된 고유 정보, 상기 단말을 구성하는 적어도 하나의 구성부품에 할당된 고유 정보, 상기 단말에 이탈착되는 IC(Integrated Circuit)칩에 기록된 고유 정보, 상기 단말의 통신모듈에 고유 할당된 고유 정보 중 적어도 하나의 고유 정보를

포함하여 이루어지는 것을 특징으로 한다.

[0052] 본 발명에 따른 인증서 운영 방법은, 사용자의 단말과 통신 가능한 서버에 의해 실행되는 인증서 운영 방법에 있어서, 사용자가 이용하는 단말에 탑재 또는 이탈착되는 매체에 사용자의 인증서가 기록되는 경우, 상기 인증서가 기록된 매체를 탑재 또는 이탈착하는 단말의 유효성을 인증하기 위한 고유 정보를 확인하여 저장하는 제1 단계와 상기 사용자의 인증서 이용 요청 확인 시, 상기 고유 정보를 이용하여 상기 매체에 기록된 상기 사용자의 인증서를 이용할 단말의 유효성을 인증한 결과를 확인하는 제2 단계 및 상기 고유 정보를 통해 상기 단말의 유효성이 인증된 경우에 상기 인증된 단말에 탑재 또는 이탈착되는 매체에 기록된 인증서를 이용하여 가공된 데이터가 이용되도록 처리하는 제3 단계를 포함하는 것을 특징으로 한다.

[0054] 본 발명에 따른 인증서 운영 방법에 있어서, 상기 사용자의 인증서 이용 요청 확인 시, 상기 단말로부터 상기 인증서를 이용할 단말의 고유 정보를 수신하는 단계 및 상기 저장된 고유 정보를 통해 상기 수신된 고유 정보의 유효성을 인증하는 인증 절차가 수행되도록 처리하는 단계;를 더 포함하여 이루어지는 것을 특징으로 한다.

[0056] 본 발명에 따른 인증서 운영 방법에 있어서, 상기 사용자의 인증서 이용 요청 확인 시, 상기 사용자의 인증서 이용을 인증하기 위해 i(i≥1)개의 인증정보를 결정하는 단계와 사용자의 단말로 상기 i개의 인증정보를 입력 요청하는 단계 및 상기 사용자의 단말을 통해 입력된 i개의 인증정보를 확인하여 유효성을 인증하는 단계를 더 포함하며, 상기 제3 단계는, 상기 i개의 인증정보가 인증된 경우에 상기 인증서를 통해 가공된 데이터가 이용되도록 처리하는 것을 특징으로 한다.

[0058] 본 발명에 따른 인증서 운영 방법에 있어서, 상기 단말에 탑재 또는 이탈착되는 매체에 기록된 인증서를 다른 매체로 전달하는 경우, 상기 인증서 전달을 인증하기 j(j≥1)개의 인증정보를 결정하는 제4 단계와 상기 사용자의 단말로 상기 j개의 인증정보를 입력 요청하는 제5 단계 및 상기 사용자의 단말을 통해 입력된 j개의 인증정보를 확인하여 유효성을 인증하는 제6 단계를 더 포함하며, 상기 j개의 인증정보를 인증한 결과로서 상기 단말의 매체에 구비된 인증서가 상기 다른 매체로 전달되도록 처리하는 제7 단계;를 포함하여 이루어지는 것을 특징으로 한다.

[0060] 본 발명에 따른 인증서 운영 방법에 있어서, 상기 매체는, 상기 단말에 탑재된 메모리 매체, 상기 단말에 이탈착되는 IC(Integrated Circuit)칩 매체, 상기 단말에 탑재된 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체 중 상기 사용자의 인증서를 기록한 적어도 하나의 매체를 포함하여 이루어지는 것을 특징으로 한다.

[0062] 본 발명에 따른 인증서 운영 방법에 있어서, 상기 고유 정보는, 상기 단말에 탑재된 메모리에 기록된 고유 정보, 상기 단말을 구성하는 적어도 하나의 구성장치에 할당된 고유 정보, 상기 단말에 이탈착되는 IC(Integrated Circuit)칩에 기록된 고유 정보, 상기 단말의 통신모듈에 고유 할당된 고유 정보 중 적어도 하나의 고유 정보를 포함하여 이루어지는 것을 특징으로 한다.

[0064] 본 발명에 따른 인증서 운영 방법은, 사용자의 단말과 통신 가능한 서버에 의해 실행되는 인증서 운영 방법에 있어서, 사용자의 단말로 상기 사용자의 인증서를 제공하여 상기 단말을 통해 이용되는 매체에 상기 인증서가 기록되는 경우, 상기 단말 또는 매체를 인증하기 위한 고유 정보를 확인하여 저장하는 제1 단계와 상기 사용자의 단말을 통해 상기 매체에 기록된 인증서가 이용되는 경우, 상기 인증서가 이용되는 단말 또는 매체를 식별하는 고유 정보 중 지정된 고유 정보를 인증한 결과를 확인하는 제2 단계 및 상기 지정된 고유 정보가 인증된 경우에 상기 매체에 기록된 인증서를 통해 가공된 데이터가 이용되도록 처리하는 제3 단계를 포함하는 것을 특징으로 한다.

[0066] 한편, 본 발명에 따른 인증서 운영 방법은, 상기 단말을 통해 상기 매체에 기록된 인증서가 이용되는 경우, 상기 단말로부터 상기 지정된 고유 정보를 수신하는 단계 및 상기 저장된 고유 정보를 통해 상기 수신된 고유 정보의 유효성을 인증하는 절차가 수행되도록 처리하는 단계를 더 포함하여 이루어지는 것을 특징으로 한다.

[0068] 본 발명에 따르면, 상기 인증서 운영 방법은, 상기 단말을 통해 상기 매체에 기록된 인증서가 이용되는 경우, 상기 저장된 고유 정보 중 지정된 고유 정보를 확인하는 단계 및 상기 단말로 상기 확인된 고유 정보를 제공하는 단계를 더 포함하며, 상기 확인된 고유 정보는, 상기 인증서를 이용하는 단말을 통해 인증되는 것을 특징으로 한다.

[0070] 본 발명에 따르면, 상기 인증서 운영 방법은, 상기 단말을 통해 상기 매체에 기록된 인증서가 이용되는 경우, 동적 결정된 i(i≥1)개의 인증정보가 상기 단말을 통해 입력되도록 처리하는 단계 및 상기 단말을 통해 입력된 i개의 인증정보를 확인하여 유효성을 인증하는 단계를 더 포함하며, 상기 제3 단계는, 상기 i개의 인증정보가 인증된 경우에 상기 인증서를 통해 가공된 데이터가 이용되도록 처리하는 것을 특징으로 한다.

발명의 효과

[0072] 본 발명에 따르면, 원본 인증서를 고객이 지정한 매체(1)로 최초 발급시, 상기 매체(1)가 탑재 또는 이탈착되는 단말에 구비 또는 이탈착되는 구성장치 중 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보를 상기 인증서 정보와 연계하여 저장한 후, 상기 원본 인증서를 통한 비대면 금융거래시, 상기 장치고유 정보를 인증하여 원본 인증서의 불법 이전 및 점유에 의해 발생하는 비대면 금융거래의 보안 문제를 해소하는 이점이 있다.

[0074] 본 발명에 따르면, 원본 인증서를 고객이 지정한 매체(1)에 발급한 후, 상기 원본 인증서를 매체(2)로 이전시, 상기 탑재 또는 이탈착되는 단말에 구비 또는 이탈착되는 구성장치 중 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보를 통해 상기 원본 인증서 이전에 대한 유효성을 확인하고, 상기 원본 인증서가 이전된 매체(2)가 탑재 또는 이탈착되는 단말에 구비 또는 이탈착되는 구성장치 중 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보를 상기 인증서 정보와 연계하여 저장함으로써, 상기 원본 인증서가 불법적으로 이전 및 점유되는 문제점을 해소하는 이점이 있다.

도면의 간단한 설명

[0076] 도 1은 본 발명의 실시 방법에 따라 인증서의 불법 이전 및 점유 방지하는 시스템 구성을 고시한 도면이다.

도 2는 본 발명의 실시 방법에 따라 고객단말에 탑재 또는 이탈착되는 매체(1)로 인증서를 발급하는 인증서 발급 시스템 구성을 도시한 도면이다.

도 3은 본 발명의 일 실시 방법에 따라 고객단말로 인증서를 발급하는 과정을 도시한 도면이다.

도 4는 본 발명의 다른 일 실시 방법에 따라 고객단말로 인증서를 발급하는 과정을 도시한 도면이다.

도 5는 본 발명의 실시 방법에 따라 고객단말로 발급된 인증서 검증 과정을 도시한 도면이다.

도 6은 본 발명의 실시 방법에 따라 고객단말에 탑재 또는 이탈착되는 매체(1)로 인증서를 관리하는 인증서 관리 시스템 구성을 도시한 도면이다.

도 7은 본 발명의 실시 방법에 따라 인증서를 관리하는 과정을 도시한 도면이다.

도 8은 본 발명의 실시 방법에 따라 고객단말에 탑재 또는 이탈착되는 매체(2)로 인증서를 이전하는 인증서 이전 시스템 구성을 도시한 도면이다.

도 9a와 도 9b는 본 발명의 실시 방법에 따라 인증서를 이전 요청하는 과정을 도시한 도면이다.

도 10은 본 발명의 일 실시 방법에 따라 인증서를 이전하는 과정을 도시한 도면이다.

도 11은 본 발명의 다른 일 실시 방법에 따라 인증서를 이전하는 과정을 도시한 도면이다.

도 12는 본 발명의 실시 방법에 따라 이전된 인증서 검증 과정을 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0077] 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. 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.

[0079] 또한, 이하 실시되는 본 발명의 바람직한 실시예는 본 발명을 이루는 기술적 구성요소를 효율적으로 설명하기 위해 각각의 시스템 기능구성에 기 구비되어 있거나, 또는 본 발명이 속하는 기술분야에서 통상적으로 구비되는 시스템 기능구성은 가능한 생략하고, 본 발명을 위해 추가적으로 구비되어야 하는 기능구성을 위주로 설명한다. 만약 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 하기에 도시하지 않고 생략된 기능구성 중에서 종래에 기 사용되고 있는 구성요소의 기능을 용이하게 이해할 수 있을 것이며, 또한 상기와 같이 생략된 구성요소와 본 발명을 위해 추가된 구성요소 사이의 관계도 명백하게 이해할 수 있을 것이다.

[0081] 또한, 이하 실시예는 본 발명의 핵심적인 기술적 특징을 효율적으로 설명하기 위해 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 명백하게 이해할 수 있도록 용어를 적절하게 변형, 또는 통합, 또는 분리하여 사용할 것이나, 이에 의해 본 발명이 한정되는 것은 결코 아니다. 즉, 본 발명을 구성하는 각각의 수단은 이하 실시예에 도시되는 시스템 상에 구비되는 서버(또는 단말) 이거나, 또는 적어도 하나 이상의 서버(또는 단말)에 구비된 소정의 기능 구성부이거나, 또는 적어도 하나 이상의 서버(또는 단말)에 구비된 적어도 두개 이상의 기능 구성부의 연합일 수 있다. 또한, 이하 실시예에 도시되는 서버(또는 단말)은 편의상 본 발명의 진보적인 기술적 특징을 이루기 위한 적어도 두개 이상의 기능 구성부를 포함하여 이루어지는 것으로 도시하지만, 상기 서버(또는 단말) 내에 도시되는 기능 구성부는 상술된 수단과 매칭되어 각 기능 구성부의 역할과 기능 및 해당 서버(또는 단말) 운용자(또는 운용기관)에 따라 서로 다른 두개 이상의 서버(또는 단말)에 구비될 수 있으며, 이에 의해 본 발명이 한정되지 아니한다.

[0083] 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.

[0085] 도면1은 본 발명의 실시 방법에 따라 인증서의 불법 이전 및 점유 방지하는 시스템 구성을 고시한 도면이다.

[0087] 보다 상세하게 본 도면1은 인증서가 발급된 매체(1)를 탑재 또는 이탈착하는 고객단말(125)에서 통신망을 통해 인증서 기반 비대면 인증을 기반으로 각종 서비스를 제공하는 인증서 이용 서버(120)(예컨대, 인터넷 뱅킹 서버, 무선 뱅킹 서버, 인터넷 쇼핑 서버 등)에 접속하여 인증서버(도시생략)와 연계하여 인증서 유효성 인증 기반 서비스를 제공받는 경우, 상기 고객단말(125)에 탑재 또는 이탈착하는 매체(1)로 발급된 인증서가 불법적으로 다른 매체(2)로 이전되어 점유되는 것을 방지하도록 인증서의 발급, 관리, 이전을 처리하는 시스템 구성에 대한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면1을 참조 및/또는 변형하여 상기 인증서의 불법 이전 및 점유 방지하는 시스템에 대한 다양한 실시 방법을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면1에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0089] 도면1을 참조하면, 상기 인증서의 불법 이전 및 점유 방지하는 시스템은, 상기 인증서가 발급되는 매체(1)를 탑재 또는 이탈착하고, 상기 매체(1)에 발급된 인증서를 통해 상기 인증서 이용 서버(120)에 접속하여 인증서 유효성 인증 기반 서비스를 제공받는 고객단말(125)과, 상기 고객단말(125)과 통신망을 통해 연결되어 상기 고객단말(125)로부터 요청된 인증서 이용 요청을 처리하는 인증서 이용 서버(120)와, 상기 고객단말(125)과 통신망을 통해 연결되어 상기 고객단말(125)로 상기 인증서를 발급시, 상기 인증서가 불법적으로 다른 매체로 이전되어 점유되는 것을 방지하기 위해 상기 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치 중 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 상기 매체(1)로 발급된 인증서 정보와 연계하여 인증서 관리 D/B(105)에 저장하는 인증서 발급 서버(100)와, 상기 고객단말(125)과 통신망을 통해 연결되며, 상기 고객단말(125)에서 인증서 이용 서버(120)를 통해 상기 인증서 이용시, 상기 인증서가 불법적으로 다른 매체로 이전되어 점유되는 것을 방지하기 위해 상기 인증서를 고객단말(125)에 구비된 장치고유 정보(2)를 수신하고, 상기 인증서 관리 D/B(105)와 연계하여 상기 매체(1)가 탑재 또는 이탈착되는 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치 중 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하고, 상기 장치고유 정보(1)과 장치고유 정보(2)를 비교하여 상기 인증서가 발급된 매체(1)에 대한 장치고유 정보 기반 유효성을 확인하는 인증서 관리 서버(110)와, 상기 인증서 이전시, 상기 인증서가 불법적으로 다른 매체로 이전되어 점유되는 것을 방지하기 위해 상기 인증서를 통해 매체(1)가 탑재 또는 이탈착되는 고객단말(125)에 구비된 장치고유 정보(2)에 대한 유효성을 검증하고, 상기 매체(2)가 탑재 또는 이탈착되는 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치 중 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 상기 매체(2)로 이전되는 인증서 정보와 연계하여 인증서 관리 D/B(105)에 저장하는 인증서 이전 서버(115)를 포함하여 이루어지는 것을 특징으로 한다.

[0091] 여기서, 상기 인증서 발급 서버(100)와 인증서 관리 서버(110) 및 인증서 이전 서버(115)는 하나의 서버로 실시되거나, 또는 기능 구성 별로 복수개의 서버군으로 실시되거나, 또는 상기 인증서를 발급하는 인증기관에 구비된 인증서버, 또는 상기 인증서 이용 서버(120)에 구비된 내부 구성요소 형태로 실시되는 것이 모두 가능하며, 본 발명은 상술된 모든 실시 방법을 포함하여 이루어지는 것을 특징으로 한다.

[0093] 도면2는 본 발명의 실시 방법에 따라 고객단말(125)에 탑재 또는 이탈착되는 매체(1)로 인증서를 발급하는 인증서 발급 시스템 구성을 도시한 도면이다.

[0095] 보다 상세하게 본 도면2는 상기 인증서가 불법적으로 이전되어 점유되는 것을 방지하기 위해 통신망을 통해 고객단말(125)에 탑재 또는 이탈착되는 매체(1)로 인증서 발급시, 상기 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치 중 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 상기 매체(1)로 발급된 인증서 정보와 연계하여 저장함으로써, 상기 통신망을 통해 상기 인증서를 이용하거나, 또는 상기 인증서를 다른 매체(2)로 이전하는 과정에서 상기 장치고유 정보(1)에 대한 유효성 확인을 통해 매체(1)로 발급된 인증서가 불법적으로 이전되어 점유되는 것을 방지하는 시스템 구성에 대한 것으로서, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 본 도면2를 참조 및/또는 변형하여 상기 고객단말(125)로 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(1)로 인증서를 발급하는 시스템 구성에 대한 다양한 실시 방법을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 실시 방법을 모두 포함하며, 본 도면2에 도시된 실시 방법에 의해 한정되지 아니한다.

[0097] 이하, 본 도면2에서 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(1)로 상기 인증서를 발급하는 시스템 상의 구성요소를 편의상 "인증서 발급 서버(100)"라고 한다.

[0099] 본 발명의 실시 방법을 따르는 도면2를 참조하면, 상기 인증서 발급 시스템은, 상기 매체(1)를 탑재 또는 이탈착하여 연동하고, 통신망을 통해 상기 인증서 발급 서버(100)에 접속하여 상기 인증서를 발급받는 고객단말(125)과, 상기 고객단말(125)과 통신망을 통해 연결되어 상기 고객단말(125)로 상기 인증서를 발급시, 상기 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치 중 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 상기 매체(1)로 발급된 인증서 정보와 연계하여 인증서 관리 D/B(105)에 저장하는 인증서 발급

서버(100)를 포함하여 이루어지는 것을 특징으로 하며, 상기 고객단말(125)로 발급된 인증서 이용시, 상기 인증서 관리 D/B(105)와 연계하여 상기 장치고유 정보(1)를 기반으로 상기 인증서가 발급된 매체(1)가 탑재 또는 이탈착되는 고객단말(125)의 유효성을 인증하여 상기 인증서가 불법적으로 이전되어 점유되는 것을 방지하는 인증서 관리 서버(110)를 더 포함하여 이루어지는 것을 특징으로 한다.

[0101] 여기서, 상기 인증서 발급 서버(100)는 본 도면2에 도시된 바와 같이 상기 인증서 발급 시스템 측에 구비되어 상기 인증서가 불법적으로 이전되어 점유되는 것을 방지하기 위해 통신망을 통해 고객단말(125)에 탑재 또는 이탈착되는 매체(1)로 인증서 발급시, 상기 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치 중 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 상기 매체(1)로 발급된 인증서 정보와 연계하여 저장하는 기능 구성의 총칭으로서, 상기 인증서 발급 서버(100)는 하나 이상의 서버(또는 장치) 형태로 실시되거나, 또는 상기 인증서 발급 서버(100) 내에 구비되는 기능 구성요소 형태로 실시되는 것이 가능하며, 이에 의해 본 발명이 한정되지 아니함을 명백하게 밝혀두는 바이다.

[0103] 상기 고객단말(125)은 TCP/IP(Transmission Control Protocol/Internet Protocol) 기반의 유선 통신망(예컨대, ADSL(Asymmetric Digital Subscriber Line)/VDSL(Very high-data rate Digital Subscriber Line) 또는 케이블 통신망)를 통해 상기 인증서 발급 서버(100)와 통신 연결되는 데스크탑 컴퓨터 또는 노트북을 포함하는 유선단말을 적어도 하나 이상 포함하여 이루어지거나, 또는 CDMA(Code Division Multiple Access) 기반의 이동 통신망에 연결되는 이동 통신단말, 또는 IEEE 802.16x 기반의 초고속 무선 인터넷에 연결되는 휴대 인터넷 단말을 적어도 하나 이상 포함하는 무선단말을 적어도 하나 이상 포함하여 이루어지는 것을 특징으로 하며, 상기 고객단말(125)은 상기 인증서 발급 서버(100)에서 발급하는 적어도 하나 이상의 인증서 발급 인터페이스를 출력하고, 상기 인증서 발급 인터페이스를 통해 상기 인증서를 발급하기 위한 인증서 발급 요청 정보를 입력(또는 선택)하여 상기 인증서 발급 서버(100)로 전송하기 위한 기능 구성(예컨대, 브라우져 프로그램과 통신 기능)이 구비되어 있는 것이 바람직하다.

[0105] 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 적어도 하나 이상의 유선단말 또는 무선단말에 대응하는 상기 고객단말(125)의 특징을 용이하게 유추할 수 있을 것이므로, 이에 대한 상세한 설명은 편의상 생략한다.

[0107] 본 발명의 실시 방법에 따라 상기 고객단말(125)이 유선단말인 경우, 상기 통신망은 상기 TCP/IP 기반의 유선 통신망을 포함하여 이루어지며, 상기 고객단말(125)이 무선단말인 경우, 상기 통신망은 상기 CDMA 기반의 이동 통신망, 또는 IEEE 802.16x 기반의 초고속 무선 인터넷을 적어도 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0109] 본 발명에 따르면, 상기 인증서 발급 서버(100)는 상기 고객단말(125)과 통신망에 대응하는 웹 인터페이스를 제공하기 위해 상기 통신망을 통해 상기 고객단말(125)과 통신채널을 연결 및 관리하는 인터페이스부(200)를 구비하여 이루어지는 것을 특징으로 하며, 이에 의해 상기 인증서 발급 서버(100)는 상기 고객단말(125)과 유선 통신망 또는 무선 통신망을 통해 통신 연결되는 웹서버의 기능을 구비한다.

[0111] 본 발명의 일 실시 방법에 따라 상기 고객단말(125)이 TCP/IP 기반의 유선 통신망을 통해 통신채널이 연결되는 유선단말인 경우, 상기 인터페이스부(200)는 상기 고객단말(125)과 HTTP(Hyper-Text Transfer Protocol) 프로토콜을 기반으로 통신채널을 연결하고, 상기 통신채널을 통해 상기 고객단말(125)로 HTML(Hyper-Text Markup Language) 호환 문서 형태의 인증서 발급 인터페이스를 전송하여 출력하고, 상기 고객단말(125)로부터 상기 인증서 발급 인터페이스를 통해 입력(또는 선택)된 인증서 발급 요청 정보를 수신 처리하는 기능을 수행하는 것이 바람직하다.

[0113] 본 발명의 다른 일 실시 방법에 따라 상기 고객단말(125)이 CDMA 기반의 무선 통신망을 통해 통신채널이 연결되는 무선단말인 경우, 상기 인터페이스부(200)는 상기 고객단말(125)과 WAP(Wireless Application Protocol) 또는 ME(Mobile Explorer) 프로토콜을 기반으로 통신채널, 또는 풀-브라우징 기반 무선 인터넷 통신채널을 연결하고, 상기 통신채널을 통해 상기 고객단말(125)로 WML(Wireless Markup Language) 또는 HTML 호환 문서 형태의 인증서 발급 인터페이스를 전송하여 출력하고, 상기 고객단말(125)로부터 상기 인증서 발급 인터페이스에 대응하는 인증서 발급 요청 정보를 수신 처리하는 기능을 수행하는 것이 바람직하다.

[0115] 본 발명의 또다른 일 실시 방법에 따라 상기 고객단말(125)이 IEEE 802.16x 기반의 무선 통신망을 통해 통신채널이 연결되는 무선단말인 경우, 상기 인터페이스부(200)는 상기 고객단말(125)과 상기 IEEE 802.16 규격에 대응하는 무선 프로토콜을 기반으로 통신채널을 연결하고, 상기 통신채널을 통해 상기 고객단말(125)로 인증서 발급 인터페이스를 전송하여 출력하고, 상기 고객단말(125)로부터 상기 인증서 발급 인터페이스에 대응하는 소정의 인증서 발급 요청 정보를 수신 처리하는 기능을 수행하는 것이 바람직하다.

[0117] 본 발명에 따르면, 상기 인증서 발급 서버(100)는 고객단말(125)이 상기 인터페이스부(200)를 통해 상기 인증서 발급 서버(100)에 접속(또는 인증서 발급 요청)시, 상기 인터페이스부(200)와 연동하여 상기 고객단말(125)에서 인증서 발급 요청 정보를 입력(또는 선택)하여 전송하도록 하는 인증서 발급 인터페이스를 생성(또는 추출)하여 제공하는 인터페이스 제공부(205)를 구비하여 이루어지는 것을 특징으로 한다.

[0119] 상기 인터페이스 제공부(205)는 상기 고객단말(125)이 상기 인터페이스부(200)를 통해 상기 인증서 발급 서버(100)에 접속(또는 인증서 발급 요청) 시, 상기 고객단말(125)에 구비된 기능구성(예컨대, 고객단말(125)에 구비된 브라우져 프로그램)에 대응하여 인증서 발급 요청 정보를 입력(또는 선택)하여 상기 통신망을 통해 상기 인증서 발급 서버(100)로 전송할 수 있는 인증서 발급 인터페이스를 생성하거나, 또는 데이터베이스(도시생략)로부터 추출하고, 상기 인터페이스부(200)와 연동하여 상기 생성(또는 추출)된 인증서 발급 인터페이스를 상기 통신망을 통해 상기 고객단말(125)로 제공하는 것을 특징으로 한다.

[0121] 이후, 상기 고객단말(125)은 상기 인증서 발급 인터페이스를 기반으로 인증서 발급 요청 정보를 입력(또는 선택)하며, 상기 입력(또는 선택)된 인증서 발급 요청 정보를 상기 통신망을 통해 상기 인증서 발급 서버(100)로 전송한다.

[0123] 여기서, 상기 인증서 발급 요청 정보는 상기 고객단말(125)에 탑재 또는 이탈착하는 매체(1)로 상기 인증서를 발급하도록 요청하는 고객정보와, 상기 고객단말(125)에 탑재 또는 이탈착되어 상기 인증서가 기록될 매체(1) 정보와, 상기 고객단말(125)에 대한 운영체제(또는 플랫폼) 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0125] 상기 인증서 발급 요청 정보에 포함된 상기 고객정보는, 상기 인증서를 발급받는 상기 고객의 회원ID정보와 비밀번호 정보를 포함하는 고객 회원정보, 또는 상기 고객의 성명, 주민등록번호, 주소, 연락처 등을 적어도 하나 이상 포함하는 고객 개인정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0127] 상기 인증서 발급 요청 정보에 포함된 상기 매체(1) 정보는, 상기 고객단말(125)에 탑재 또는 이탈착되는 매체 중 상기 인증서가 발급되어 저장되는 매체를 확인(또는 식별)하는 정보를 포함하여 이루어지는 것이 바람직하다.

[0129] 본 발명의 실시 방법에 따르면, 상기 매체(1) 정보는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체를 포함하여 이루어지는 것이 바람직

하다.

[0131] 또는, 상기 매체(1) 정보는 상기 고객단말(125)에 이탈착되는(예컨대, 플로피디스크 드라이브에 삽입되는) 플로피디스크 매체를 포함하여 이루어지는 것이 바람직하다.

[0133] 또는, 상기 매체(1) 정보는 상기 고객단말(125)에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체를 포함하여 이루어지는 것이 바람직하다.

[0135] 또는, 상기 매체(1) 정보는 상기 고객단말(125)에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체를 포함하여 이루어지는 것이 바람직하다.

[0137] 또는, 상기 매체(1) 정보는 상기 고객단말(125)에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체를 포함하여 이루어지는 것이 바람직하다.

[0139] 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 상술된 매체(1) 이외에 상기 고객단말(125)에 탑재 또는 이탈착되는 다양한 형태의 매체를 유추할 수 있을 것이며, 본 발명은 상기 유추되는 모든 매체(1)를 포함하여 이루어지는 것을 특징으로 한다.

[0141] 상기 인증서 발급 요청 정보에 포함된 상기 운영체제(또는 플랫폼) 정보는, 상기 인증서가 발급된 매체(1)이 탑재 또는 이탈착되는 고객단말(125)의 운영체제(또는 플랫폼)을 식별 내지 확인하는 정보로서, 상기 인증서에 대응하는 프로그램 코드가 실행되는 운영체제(또는 플랫폼)을 확인하는 것이 바람직하다.

[0143] 본 발명에 따르면, 상기 인증서 발급 서버(100)는 상기 인터페이스부(200)와 연계하여 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 수신하는 정보 수신부(225)(또는 정보 수신수단)를 구비하여 이루어지는 것을 특징으로 한다.

[0145] 본 발명의 일 실시 방법에 따르면, 상기 인터페이스 제공부(205)는 상기 고객단말(125)로 제공되는 인증서 발급 인터페이스에 상기 고객단말(125)에 구비 또는 이탈착되는 M(M>1)개의 구성장치 정보를 확인하여 통신망을 통해 상기 인증서 발급 서버(100)로 전송하는 기능, 상기 인증서 발급 서버(100)로부터 상기 M(M>1)개의 구성장치 정보 중 인증서 검증 대상에 m(1<=m<=M)개의 구성장치 정보를 수신하는 기능, 상기 수신된 m개의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 상기 통신망을 통해 상기 인증서 발급 서버(100)로 전송하는 기능을 포함하는 스크립트(또는 단말 프로그램)을 포함하여 제공하는 것이 바람직하며, 이에 대응하여 상기 인증서 발급 서버(100)는, 상기 인터페이스부(200)와 연계하여 상기 고객단말(125)에 구비 또는 이탈착되는 M(M>1)개의 구성장치 정보를 수신하는 장치정보 수신부(210)(또는 장치정보 수신수단)와, 상기 M(M>1)개의 구성장치 정보 중 인증서 검증 대상에 m(1<=m<=M)개의 구성장치 정보를 확인하는 장치정보 확인부(215)(또는 장치정보 확인수단)와, 상기 인터페이스부(200)와 연계하여 상기 고객단말(125)로 상기 확인된 m개의 구성장치 정보를 전송하는 장치정보 전송부(220)(또는 장치정보 전송수단)를 더 구비하여 이루어지는 것을 특징으로 하며, 상기 정보 수신부(225)는 상기 인터페이스부(200)와 연계하여 상기 고객단말(125)에 구비 또는 이탈착되는 M(M>1)개의 구성장치 중 상기 설정된 m(1<=m<=M)개의 구성장치에 대응하는 장치고유 정보(1)를 수신하는 것을 특징으로 한다.

[0147] 본 발명의 다른 일 실시 방법에 따르면, 상기 인터페이스 제공부(205)는 상기 고객단말(125)로 제공되는 인증서

발급 인터페이스에 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 통신망을 통해 전송하는 스크립트(또는 단말 프로그램)를 포함하여 제공하는 것이 바람직하며, 이에 대응하여 상기 정보 수신부(225)는 상기 인터페이스부(200)와 연계하여 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 수신하는 것을 특징으로 한다.

[0149] 본 발명의 실시 방법에 따르면, 상기 장치고유 정보(1)는 상기 인증서가 발급된 매체의 고유정보 또는 상기 매체가 탑재 또는 이탈착되는 단말의 고유 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0151] 예컨대, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0153] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형) 통신장치에 구비된 MAC(Media Access Control) 주소 정보를 포함하여 이루어지는 것이 바람직하다.

[0155] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0157] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체에 구비된 IC칩 일련번호, IC칩 고유정보, IC칩 식별정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0159] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체에 구비되는 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0161] 본 발명에 따르면, 상기 인증서 발급 서버(100)는 상기 고객단말(125)로 발급할 인증서에 대응하는 적어도 하나 이상의 인증서 프로그램 소스(또는 인증서 프로그램 파일)와 인증서 데이터(예컨대, 인증서 프로파일 정보)를 저장하는 인증서 D/B(250)와, 상기 고객단말(125)로부터 상기 인증서 발급 요청 정보가 수신되는 경우, 인증서 D/B(250)로부터 상기 인증서 발급 요청 정보에 대응하는 인증서를 추출 또는 동적으로 생성하는 인증서 추출/생성부(230)(또는 인증서 추출/생성수단)와, 여 상기 인터페이스부(200)를 통해 상기 고객단말(125)로 발급하는 인증서 발급부(235)(또는 인증서 발급수단)를 구비하여 이루어지는 것을 특징으로 한다.

[0164] *본 발명의 일 실시 방법에 따르면, 상기 인증서 D/B(250)는 상기 고객단말(125)에 구비된 운영체제(또는 단말 플랫폼)에서 동작할 수 있는 인증서 프로그램 파일과 인증서 데이터를 저장하는 것을 특징으로 하며, 상기 고객단말(125)로부터 상기 인증서 발급 요청 정보가 수신되는 경우, 상기 인증서 추출/생성부(230)는 상기 인증서 D/B(250)로부터 상기 인증서 발급 요청 정보와 매칭되는 인증서 프로그램 파일과 인증서 데이터를 포함하는 인증서를 추출하는 것을 특징으로 한다.

[0166] 본 발명의 다른 일 실시 방법에 따르면, 상기 인증서 D/B(250)는 상기 고객단말(125)에 구비된 운영체제(또는 단말 플랫폼)에서 동작할 수 있는 인증서 프로그램 소스와 인증서 데이터를 저장하는 것을 특징으로 하며, 상기 고객단말(125)로부터 상기 인증서 발급 요청 정보가 수신되는 경우, 상기 인증서 추출/생성부(230)는 상기 인증서 D/B(250)로부터 상기 인증서 발급 요청 정보와 매칭되는 인증서 프로그램 소스와 인증서 데이터를 추출하고, 상기 추출된 인증서 프로그램 소스를 컴파일(Compile)하여 상기 고객단말(125)로 발급할 인증서를 동적 생성하는 것을 특징으로 한다.

[0168] 이후, 상기 인증서 발급부(235)는 상기 인터페이스부(200)를 통해 상기 추출(또는 동적 생성)된 인증서를 상기 통신망을 통해 상기 고객단말(125)로 전송하여 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(1)로 발급하는데, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 상기 인증서를 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(1)에 발급하는 방법을 기 숙지하고 있을 것이므로, 이에 대한 상세한 설명은 편의상 생략한다.

[0170] 본 발명의 실시 방법에 따르면, 상기 인증서 발급부(235)에 의해 상기 고객단말(125)로 제공된 상기 인증서에 포함된 인증서 프로그램은, 통신망을 통한 인증서 기반 비대면 인증기능을 포함하고, 상기 비대면 인증시, 상기 매체(1)이 탑재 또는 이탈착된 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보(2)를 확인하고, 상기 확인된 하나 이상의 장치고유 정보(2)를 송수신 데이터(예컨대, 비대면 인증에 따라 고객단말(125)에서 통신망을 통해 전송하는 데이터, 또는 통신망을 통해 고객단말(125)로 수신하는 데이터)(에 포함하여 전송하는 기능을 구비하여 이루어지는 것일 특징으로 한다.

[0172] 상기와 같이 고객단말(125)에 구비된 매체(1)로 상기 인증서가 발급되면, 상기 고객단말(125)은 상기 인증서를 최초 실행하여 상기 인증서에 대한 유효성을 인증하는 상기 인증서 진단 모드를 개시하는데, 이를 위해 상기 인증서 발급 서버(100)는 상기 고객단말(125)에서 구비된 상기 인증서와 상호 연동하여 상기 인증서에 대한 유효성을 진단하는 진단부(240)(또는 인증서 진단수단)를 구비하여 이루어지는 것을 특징으로 한다.

[0174] 본 발명의 실시 방법에 따르면, 상기 인증서 진단 모드는, 상기 인증서를 통해 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보(2)를 전송하도록 하고, 상기 인증서를 통해 수신된 하나 이상의 장치고유 정보(2)와 상기 정보 수신부(225)를 통해 수신된 하나 이상의 장치고유 정보(1)을 비교하여 상기 인증서로부터 전송된 장치고유 정보(2)가 유효한지 확인하는 것을 포함하여 이루어지는 것이 바람직하다.

[0176] 본 발명의 실시 방법에 따르면, 상기 장치고유 정보(2)는 상기 인증서가 발급된 매체의 고유정보 또는 상기 매체가 탑재 또는 이탈착되는 단말의 고유 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0178] 예컨대, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0180] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형) 통신장치에 구비된 MAC(Media Access Control) 주소 정보를 포함하여 이루어지는 것이 바람직하다.

[0182] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정

보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0184] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체에 구비된 IC칩 일련번호, IC칩 고유정보, IC칩 식별정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0186] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체에 구비되는 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0188] 본 발명에 따르면, 상기 인증서 발급 서버(100)는 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(1)로 발급된 인증서에 대응하는 인증서 정보와, 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보(1)를 연계 처리하여 인증서 관리 D/B(105)에 저장하는 정보 저장부(255)를 구비하여 이루어지는 것을 특징으로 한다.

[0190] 본 발명의 실시 방법에 따르면, 상기 정보 저장부(255)는 상기 진단부(240)의 진단결과 상기 인증서의 유효성이 확인되면, 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(1)로 발급된 상기 인증서 정보와, 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 상기 정보 수신부(225)를 통해 수신된 하나 이상의 하나 이상의 장치고유 정보(1)를 연계 처리하여 인증서 관리 D/B(105)에 저장하는 것이 바람직하며, 이후 상기 인증서 관리 D/B(105)에 저장된 상기 인증서 정보와 하나 이상의 장치고유 정보(1)는 상기 인증서가 불법적으로 이전되어 점유하는 것을 방지하는데 이용되는 것을 특징으로 한다.

[0192] 본 발명에 따르면, 상기 인증서 발급 서버(100)는 고객단말(125)에 탑재 또는 이탈착하는 매체(1)로 상기 인증서 발급시, 상기 인증서 이전에 대한 유효성을 확인하기 위해, 상기 고객단말(125)로 I(I>1)개의 인증정보 입력 질의 정보를 포함하고, 상기 I개의 인증정보 입력 질의 정보 중 i(1<=i<=I)개의 인증정보 입력 질의 정보에 각기 대응하는 i개의 사용자 인증정보(1)를 입력하여 전송하도록 하는 사용자 인증정보 등록 인터페이스를 생성(또는 추출)하여 제공하는 인터페이스 제공부(205)를 구비하여 이루어지는 것을 특징으로 한다.

[0194] 상기 인터페이스 제공부(205)는 고객단말(125)에 탑재 또는 이탈착하는 매체(1)로 상기 인증서 발급시, 상기 인증서 이전에 대한 유효성을 확인하기 위해, 상기 고객단말(125)에 구비된 기능구성(예컨대, 고객단말(125)에 구비된 브라우져 프로그램)에 대응하여 상기 고객단말(125)로 I(I>1)개의 인증정보 입력 질의 정보를 포함하고, 상기 I개의 인증정보 입력 질의 정보 중 i(1<=i<=I)개의 인증정보 입력 질의 정보에 각기 대응하는 i개의 사용자 인증정보(1)를 입력하여 상기 인증서 발급 서버(100)로 전송할 수 있는 사용자 인증정보 등록 인터페이스를 생성하거나, 또는 데이터베이스(도시생략)로부터 추출하고, 상기 인터페이스부(200)와 연동하여 상기 생성(또는 추출)된 사용자 인증정보 등록 인터페이스를 상기 통신망을 통해 상기 고객단말(125)로 제공하는 것을 특징으로 한다.

[0196] 이후, 상기 고객단말(125)은 상기 사용자 인증정보 등록 인터페이스를 기반으로 i개의 사용자 인증정보(1)를 입력(또는 선택)하며, 상기 입력(또는 선택)된 i개의 사용자 인증정보(1)를 상기 통신망을 통해 상기 인증서 발급 서버(100)로 전송한다.

[0198] 본 발명에 따르면, 상기 고객단말(125)에서 상기 I개의 인증정보 입력 질의 정보 중 i(1<=i<=I)개의 인증정보 입력 질의 정보에 각기 대응하는 i개의 사용자 인증정보(1)를 입력하여 전송하면, 상기 인증서 발급 서버(100)

는 상기 인터페이스부(200)와 연계하여 i개의 사용자 인증정보(1)를 수신하는 인증정보 수신부(245)(또는 인증정보 수신수단)와, 상기 수신된 i개의 사용자 인증정보(1)와 사용자 인증정보(1)에 각기 대응하는 i개의 입력 질의 정보(또는 상기 i개의 인증정보 입력 질의 정보에 각기 대응하는 질의 식별코드) 및 상기 하나 이상의 장치고유 정보(1)를 연계하여 인증서 관리 D/B(105)에 저장하는 인증정보 저장부(260)(또는 인증정보 저장수단)을 구비하여 이루어지는 것을 특징으로 한다.

[0200] 상기 고객단말(125)에서 상기 I개의 인증정보 입력 질의 정보 중 i(1<=i<=I)개의 인증정보 입력 질의 정보에 각기 대응하는 i개의 사용자 인증정보(1)를 입력하여 전송하면, 상기 인증정보 수신부(245)는 상기 인터페이스부(200)와 연계하여 i개의 사용자 인증정보(1)를 수신하는 것을 특징으로 한다.

[0202] 본 발명의 실시 방법에 따르면, 상기 사용자 인증정보(1)가 상기 매체(1)로 발급된 인증서를 통해 가공(예컨대, 암호화 내지 전자서명 첨부)되고, 상기 인증서 정보가 첨부되어 수신되는 경우, 상기 인증정보 수신부(245)는 상기 고객단말(125)로부터 상기 장치고유 정보(2)를 더 포함하여 수신하는 것이 바람지하며, 이 경우 상기 정보 수신부(225)는 상기 수신된 장치고유 정보(2)를 통한 장치고유 정보 유효성 인증을 더 수행하는 것이 바람직하다.

[0204] 인증정보 수신부(245)를 통해 상기 고객단말(125)로부터 상기 i개의 사용자 인증정보(1)가 수신되면, 상기 인증정보 저장부(260)는 상기 수신된 i개의 사용자 인증정보(1)와 사용자 인증정보(1)에 각기 대응하는 i개의 입력 질의 정보(또는 상기 i개의 인증정보 입력 질의 정보에 각기 대응하는 질의 식별코드)를 확인하고, 상기 수신된 i개의 사용자 인증정보(1)와 상기 확인된 i개의 입력 질의 정보(또는 상기 i개의 인증정보 입력 질의 정보에 각기 대응하는 질의 식별코드) 및 상기 하나 이상의 장치고유 정보(1)를 연계하여 인증서 관리 D/B(105)에 저장하는 것을 특징으로 한다.

[0206] 본 발명의 다른 실시 방법에 따르면, 상기 인증정보 수신부(245)는 상기 수신된 i개의 사용자 인증정보(1)와 상기 확인된 i개의 입력 질의 정보(또는 상기 i개의 인증정보 입력 질의 정보에 각기 대응하는 질의 식별코드) 및 상기 인증서 정보를 연계하여 인증서 관리 D/B(105)에 저장하는 것이 가능하며, 이에 의해 본 발명이 한정되지 아니한다.

[0208] 도면3은 본 발명의 일 실시 방법에 따라 고객단말(125)로 인증서를 발급하는 과정을 도시한 도면이다.

[0210] 보다 상세하게 본 도면3은 상기 도면2에 도시된 인증서 발급 시스템을 통해 상기 고객단말(125)에서 인증서 발급 요청시, 상기 인증서 발급 서버(100)에서 상기 발급되는 인증서가 불법적으로 이전되어 점유되는 것을 방지하기 위해 상기 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치 중 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인한 후, 상기 발급 요청된 인증서를 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(1)로 발급하는 과정에 대한 것으로서, 구체적으로 상기 고객단말(125)에 구비 또는 이탈착되는 M(M>1)개의 구성장치 정보를 선 확인 후 상기 인증서 발급 서버(100)에서 상기 M(M>1)개의 구성장치 중 인증서 검증 대상에 m(1<=m<=M)개의 구성장치를 확인한 후, 상기 고객단말(125)로부터 상기 확인된 m개의 장치고유 정보(1)를 수신한 후, 상기 발급 요청된 인증서를 상기 고객단말(125)에 탑재 또는 이탈착하는 매체(1)로 발급하는 실시 방법을 도시한 도면이다.

[0212] 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 본 도면3을 참조 및/또는 변형하여 상기 고객단말(125)로 인증서를 발급하는 과정에 대한 다양한 실시 방법을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 실시 방법을 모두 포함하며, 본 도면3에 도시된 실시 방법에 의해 한정되지 아니한다.

[0214] 이하, 본 도면3에서 상기 도면2에 도시된 고객단말(125)을 편의상 "단말"이라고 하고, 상기 도면2에 도시된 인증서 발급 서버(100)를 편의상 "서버"라고 한다.

[0216] 도면3을 참조하면, 상기 단말은 통신망을 통해 상기 서버에 접속하고, 상기 서버로 상기 인증서를 발급하도록 요청하며(300), 이에 대응하여 상기 서버는 상기 인증서를 상기 단말로 발급하기 위한 인증서 발급 인터페이스를 추출(또는 생성)하여 상기 단말로 제공한다(305).

[0218] 본 발명의 일 실시 방법에 따르면, 상기 인증서 발급 인터페이스는, 상기 단말에 구비 또는 이탈착되는 M(M>1)개의 구성장치 정보를 확인하여 통신망을 통해 상기 인증서 발급 서버(100)로 전송하는 기능, 상기 인증서 발급 서버(100)로부터 상기 M(M>1)개의 구성장치 정보 중 인증서 검증 대상에 m(1<=m<=M)개의 구성장치 정보를 수신하는 기능, 상기 수신된 m개의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 상기 통신망을 통해 상기 인증서 발급 서버(100)로 전송하는 기능을 포함하는 스크립트(또는 단말 프로그램)을 포함하여 이루어지는 것이 바람직하다.

[0220] 이후, 상기 단말은 상기 인증서 발급 인터페이스를 통해 인증서 발급 요청 정보를 입력(또는 선택)하고(310), 상기 입력(또는 선택)된 인증서 발급 요청 정보를 상기 통신망을 통해 상기 서버로 전송한다(315).

[0222] 여기서, 상기 인증서 발급 요청 정보는 상기 단말에 탑재 또는 이탈착하는 매체(1)로 상기 인증서를 발급하도록 요청하는 고객정보와, 상기 단말에 탑재 또는 이탈착되어 상기 인증서가 기록될 매체(1) 정보와, 상기 단말에 대한 운영체제(또는 플랫폼) 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0224] 상기 인증서 발급 요청 정보에 포함된 상기 고객정보는, 상기 인증서를 발급받는 상기 고객의 회원ID정보와 비밀번호 정보를 포함하는 고객 회원정보, 또는 상기 고객의 성명, 주민등록번호, 주소, 연락처 등을 적어도 하나 이상 포함하는 고객 개인정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0227] *상기 인증서 발급 요청 정보에 포함된 상기 매체(1) 정보는, 상기 단말에 탑재 또는 이탈착되는 매체 중 상기 인증서가 발급되어 저장되는 매체를 확인(또는 식별)하는 정보를 포함하여 이루어지는 것이 바람직하다.

[0229] 본 발명의 실시 방법에 따르면, 상기 매체(1) 정보는 상기 단말에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체를 포함하여 이루어지는 것이 바람직하다.

[0231] 또는, 상기 매체(1) 정보는 상기 단말에 이탈착되는(예컨대, 플로피디스크 드라이브에 삽입되는) 플로피디스크 매체를 포함하여 이루어지는 것이 바람직하다.

[0233] 또는, 상기 매체(1) 정보는 상기 단말에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체를 포함하여 이루어지는 것이 바람직하다.

[0235] 또는, 상기 매체(1) 정보는 상기 단말에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체를 포함하여 이루어지는 것이 바람직하다.

[0237] *또는, 상기 매체(1) 정보는 상기 단말에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체를 포함하여 이루어지는 것이 바람직하다.

[0239] 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 상술된 매체(1) 이외에 상기 단말에 탑재 또는 이탈착되는 다양한 형태의 매체를 유추할 수 있을 것이며, 본 발명은 상기 유추되는 모든 매체(1)를 포함하여 이루어지는 것을 특징으로 한다.

[0241] 상기 인증서 발급 요청 정보에 포함된 상기 운영체제(또는 플랫폼) 정보는, 상기 인증서가 발급된 매체(1)이 탑재 또는 이탈착되는 단말의 운영체제(또는 플랫폼)을 식별 내지 확인하는 정보로서, 상기 인증서에 대응하는 프로그램 코드가 실행되는 운영체제(또는 플랫폼)을 확인하는 것이 바람직하다.

[0243] 이후, 상기 서버는 통신망을 통해 상기 단말로 제공된 스크립트(또는 단말 프로그램)으로 상기 단말에 구비 또는 이탈착되는 M(M>1)개의 구성장치 정보를 확인하여 전송하도록 요청하고(320), 이에 대응하여 상기 단말은 상기 단말에 구비 또는 이탈착되는 M(M>1)개의 구성장치 정보를 확인하여 통신망을 통해 상기 서버로 전송한다(325).

[0245] 이후, 상기 서버는 상기 수신된 M(M>1)개의 구성장치 정보 중 인증서 검증 대상에 m(1<=m<=M)개의 구성장치 정보를 확인한다(330).

[0247] 만약 상기 인증서 검증 대상에 m개의 구성장치 정보가 확인되면(335), 상기 서버는 통신망을 통해 상기 단말로 상기 확인된 m개의 구성장치 정보를 전송하고(340), 이에 대응하여 상기 단말은 상기 m개의 구성장치에 대응하는 m개의 장치고유 정보(1)를 확인하여 통신망을 통해 상기 서버로 전송한다(345).

[0249] 본 발명의 실시 방법에 따르면, 상기 장치고유 정보(1)는 상기 인증서가 발급된 매체의 고유정보 또는 상기 매체가 탑재 또는 이탈착되는 단말의 고유 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0252] *예컨대, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0254] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형) 통신장치에 구비된 MAC(Media Access Control) 주소 정보를 포함하여 이루어지는 것이 바람직하다.

[0256] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0258] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는

(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체에 구비된 IC칩 일련번호, IC칩 고유정보, IC칩 식별정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0260] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체에 구비되는 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0262] 만약 상기 단말로부터 m개의 장치고유 정보(1)가 수신되면(350), 상기 서버는 상기 인증서 D/B(250)로부터 상기 인증서 발급 요청 정보와 매칭되는 인증서를 추출(또는 동적 생성)한고(355).

[0264] 본 발명의 일 실시 방법에 따르면, 상기 인증서 D/B(250)는 상기 단말에 구비된 운영체제(또는 단말 플랫폼)에서 동작할 수 있는 인증서 프로그램 파일과 인증서 데이터를 저장하는 것을 특징으로 하며, 상기 단말로부터 상기 인증서 발급 요청 정보가 수신되는 경우, 상기 서버는 상기 인증서 D/B(250)로부터 상기 인증서 발급 요청 정보와 매칭되는 인증서 프로그램 파일과 인증서 데이터를 포함하는 인증서를 추출하는 것이 바람직하다.

[0266] 본 발명의 다른 일 실시 방법에 따르면, 상기 인증서 D/B(250)는 상기 단말에 구비된 운영체제(또는 단말 플랫폼)에서 동작할 수 있는 인증서 프로그램 소스와 인증서 데이터를 저장하는 것을 특징으로 하며, 상기 단말로부터 상기 인증서 발급 요청 정보가 수신되는 경우, 상기 서버는 상기 인증서 D/B(250)로부터 상기 인증서 발급 요청 정보와 매칭되는 인증서 프로그램 소스와 인증서 데이터를 추출하고, 상기 추출된 인증서 프로그램 소스를 컴파일(Compile)하여 상기 단말로 발급할 인증서를 동적 생성하는 것이 바람직하다.

[0268] 또한, 상기 서버는 상기 추출(또는 동적 생성)된 상기 인증서를 상기 통신망을 통해 상기 단말로 제공하여 상기 단말에 탑재 또는 이탈착되는 매체(1)에 발급한다(360).

[0270] 도면4는 본 발명의 다른 일 실시 방법에 따라 고객단말(125)로 인증서를 발급하는 과정을 도시한 도면이다.

[0272] 보다 상세하게 본 도면4는 상기 도면2에 도시된 인증서 발급 시스템을 통해 상기 고객단말(125)에서 인증서 발급 요청시, 상기 인증서 발급 서버(100)에서 상기 발급되는 인증서가 불법적으로 이전되어 점유되는 것을 방지하기 위해 상기 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치 중 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인한 후, 상기 발급 요청된 인증서를 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(1)로 발급하는 과정에 대한 것으로서, 구체적으로 상기 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치 정보 중 기 설정된 하나 이상의 장치고유 정보(1)를 수신한 후, 상기 발급 요청된 인증서를 상기 고객단말(125)에 탑재 또는 이탈착하는 매체(1)로 발급하는 실시 방법을 도시한 도면이다.

[0274] 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 본 도면4를 참조 및/또는 변형하여 상기 고객단말(125)로 인증서를 발급하는 과정에 대한 다양한 실시 방법을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 실시 방법을 모두 포함하며, 본 도면4에 도시된 실시 방법에 의해 한정되지 아니한다.

[0276] 이하, 본 도면4에서 상기 도면2에 도시된 고객단말(125)을 편의상 "단말"이라고 하고, 상기 도면2에 도시된 인증서 발급 서버(100)를 편의상 "서버"라고 한다.

[0278] 도면4를 참조하면, 상기 단말은 통신망을 통해 상기 서버에 접속하고, 상기 서버로 상기 인증서를 발급하도록 요청하며(400), 이에 대응하여 상기 서버는 상기 인증서를 상기 단말로 발급하기 위한 인증서 발급 인터페이스를 추출(또는 생성)하여 상기 단말로 제공한다(405).

[0280] 본 발명의 실시 방법에 따르면, 상기 인증서 발급 인터페이스는, 상기 단말에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 통신망을 통해 전송하는 스크립트(또는 단말 프로그램)를 포함하여 이루어지는 것이 바람직하다.

[0282] 이후, 상기 단말은 상기 인증서 발급 인터페이스를 통해 인증서 발급 요청 정보를 입력(또는 선택)하고(410), 상기 입력(또는 선택)된 인증서 발급 요청 정보를 상기 통신망을 통해 상기 서버로 전송한다(415).

[0284] 여기서, 상기 인증서 발급 요청 정보는 상기 단말에 탑재 또는 이탈착하는 매체(1)로 상기 인증서를 발급하도록 요청하는 고객정보와, 상기 단말에 탑재 또는 이탈착되어 상기 인증서가 기록될 매체(1) 정보와, 상기 단말에 대한 운영체제(또는 플랫폼) 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0286] 상기 인증서 발급 요청 정보에 포함된 상기 고객정보는, 상기 인증서를 발급받는 상기 고객의 회원ID정보와 비밀번호 정보를 포함하는 고객 회원정보, 또는 상기 고객의 성명, 주민등록번호, 주소, 연락처 등을 적어도 하나 이상 포함하는 고객 개인정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0289] *상기 인증서 발급 요청 정보에 포함된 상기 매체(1) 정보는, 상기 단말에 탑재 또는 이탈착되는 매체 중 상기 인증서가 발급되어 저장되는 매체를 확인(또는 식별)하는 정보를 포함하여 이루어지는 것이 바람직하다.

[0291] 본 발명의 실시 방법에 따르면, 상기 매체(1) 정보는 상기 단말에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체를 포함하여 이루어지는 것이 바람직하다.

[0293] 또는, 상기 매체(1) 정보는 상기 단말에 이탈착되는(예컨대, 플로피디스크 드라이브에 삽입되는) 플로피디스크 매체를 포함하여 이루어지는 것이 바람직하다.

[0295] 또는, 상기 매체(1) 정보는 상기 단말에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체를 포함하여 이루어지는 것이 바람직하다.

[0297] 또는, 상기 매체(1) 정보는 상기 단말에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체를 포함하여 이루어지는 것이 바람직하다.

[0299] 또는, 상기 매체(1) 정보는 상기 단말에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체를 포함하여 이루어지는 것이 바람직하다.

[0301] 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 상술된 매체(1) 이외에 상기 단말에 탑재 또는 이탈

착되는 다양한 형태의 매체를 유추할 수 있을 것이며, 본 발명은 상기 유추되는 모든 매체(1)를 포함하여 이루어지는 것을 특징으로 한다.

[0303] 상기 인증서 발급 요청 정보에 포함된 상기 운영체제(또는 플랫폼) 정보는, 상기 인증서가 발급된 매체(1)이 탑재 또는 이탈착되는 단말의 운영체제(또는 플랫폼)을 식별 내지 확인하는 정보로서, 상기 인증서에 대응하는 프로그램 코드가 실행되는 운영체제(또는 플랫폼)을 확인하는 것이 바람직하다.

[0305] 이후, 상기 서버는 통신망을 통해 상기 단말로 제공된 스크립트(또는 단말 프로그램)으로 상기 단말에 구비 또는 이탈착되는 복수개의 구성장치 정보 중 기 설정된 하나 이상의 구성장치에 대한 하나 이상의 장치고유 정보(1)를 확인하여 전송하도록 요청하고(420), 이에 대응하여 상기 단말은 상기 설정된 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보(1)를 확인하여 통신망을 통해 상기 서버로 전송한다(425).

[0307] 본 발명의 실시 방법에 따르면, 상기 장치고유 정보(1)는 상기 인증서가 발급된 매체의 고유정보 또는 상기 매체가 탑재 또는 이탈착되는 단말의 고유 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0309] 예컨대, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0311] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형) 통신장치에 구비된 MAC(Media Access Control) 주소 정보를 포함하여 이루어지는 것이 바람직하다.

[0313] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0315] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체에 구비된 IC칩 일련번호, IC칩 고유정보, IC칩 식별정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0317] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체에 구비되는 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0319] 만약 상기 단말로부터 m개의 장치고유 정보(1)가 수신되면(430), 상기 서버는 상기 인증서 D/B(250)로부터 상기 인증서 발급 요청 정보와 매칭되는 인증서를 추출(또는 동적 생성)한고(435).

[0321] 본 발명의 일 실시 방법에 따르면, 상기 인증서 D/B(250)는 상기 단말에 구비된 운영체제(또는 단말 플랫폼)에서 동작할 수 있는 인증서 프로그램 파일과 인증서 데이터를 저장하는 것을 특징으로 하며, 상기 단말로부터 상기 인증서 발급 요청 정보가 수신되는 경우, 상기 서버는 상기 인증서 D/B(250)로부터 상기 인증서 발급 요청 정보와 매칭되는 인증서 프로그램 파일과 인증서 데이터를 포함하는 인증서를 추출하는 것이 바람직하다.

[0323] 본 발명의 다른 일 실시 방법에 따르면, 상기 인증서 D/B(250)는 상기 단말에 구비된 운영체제(또는 단말 플랫폼)에서 동작할 수 있는 인증서 프로그램 소스와 인증서 데이터를 저장하는 것을 특징으로 하며, 상기 단말로부터 상기 인증서 발급 요청 정보가 수신되는 경우, 상기 서버는 상기 인증서 D/B(250)로부터 상기 인증서 발급 요청 정보와 매칭되는 인증서 프로그램 소스와 인증서 데이터를 추출하고, 상기 추출된 인증서 프로그램 소스를 컴파일(Compile)하여 상기 단말로 발급할 인증서를 동적 생성하는 것이 바람직하다.

[0325] 또한, 상기 서버는 상기 추출(또는 동적 생성)된 상기 인증서를 상기 통신망을 통해 상기 단말로 제공하여 상기 단말에 탑재 또는 이탈착되는 매체(1)에 발급한다(440).

[0327] 도면5는 본 발명의 실시 방법에 따라 고객단말(125)로 발급된 인증서 검증 과정을 도시한 도면이다.

[0329] 보다 상세하게 본 도면5는 상기 도면3 또는 도면4에 도시된 인증서 발급 과정을 통해 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(1)로 인증서 발급시, 상기 매체(1)로 발급된 인증서가 상기 인증서의 불법 이전 및 점유 방지를 위한 기능이 정상적으로 동작하는지 검증하는 과정에 대한 것으로서, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 본 도면5를 참조 및/또는 변형하여 상기 고객단말(125)로 발급된 인증서 검증 과정에 대한 다양한 실시 방법을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 실시 방법을 모두 포함하며, 본 도면5에 도시된 실시 방법에 의해 한정되지 아니한다.

[0331] 이하, 본 도면5에서 상기 도면2에 도시된 고객단말(125)을 편의상 "단말"이라고 하고, 상기 도면2에 도시된 인증서 발급 서버(100)를 편의상 "서버"라고 한다.

[0333] 도면5를 참조하면, 상기 도면3 또는 도면4에 도시된 인증서 발급 과정을 통해 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(1)로 인증서 발급시, 상기 서버는 상기 단말에 탑재 또는 이탈착되는 매체(1)로 상기 인증서가 발급되는지 확인한다(500).

[0335] 만약 상기 단말에 탑재 또는 이탈착되는 매체(1)로 상기 인증서가 발급되면(505), 상기 단말은 상기 인증서를 실행하여 상기 인증서에 대한 진단 모드를 개시하고(510), 이에 대응하여 상기 단말은 상기 인증서를 통해 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보(2)를 전송하도록 하고(515), 이에 대응하여 상기 서버는 상기 수신된 하나 이상의 장치고유 정보(2)를 판독하여 상기 인증서에 대한 유효성을 확인한다(520)

[0337] 본 발명의 실시 방법에 따르면, 상기 인증서에 대한 유효성을 확인은, 상기 인증서를 통해 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보(2)를 전송하도록 하고, 상기 인증서를 통해 수신된 하나 이상의 장치고유 정보(2)와 상기 수신된 하나 이상의 장치고유 정보(1)을 비교하여 상기 인증서로부터 전송된 장치고유 정보(2)가 유효한지 확인하는 것을 포함하여 이루어지는 것이 바람직하다.

[0339] 만약 상기 인증서에 대한 유효성이 확인되지 않으면(525), 상기 서버는 인증서 진단 오류 정보를 생성하여 상기 통신망을 통해 상기 단말로 전송한다(530).

[0342] *반면 상기 인증서에 대한 유효성이 확인되면(525), 상기 서버는 상기 단말에 탑재된 인증서에 대응하는 인증서 정보와, 상기 수신된 하나 이상의 하나 이상의 장치고유 정보(1)를 연계 처리하여 인증서 관리 D/B(105)에 저장하며(535), 이후 상기 인증서 관리 D/B(105)에 저장된 상기 인증서 정보와 하나 이상의 장치고유 정보(1)는 상기 인증서가 불법적으로 이전되어 점유하는 것을 방지하는데 이용된다.

[0344] 또한, 상기 서버는 상기 인증서 이전에 대한 유효성 검증을 위해, 상기 단말로 I(I>1)개의 인증정보 입력 질의 정보를 포함하고, 상기 I개의 인증정보 입력 질의 정보 중 i(1<=i<=I)개의 인증정보 입력 질의 정보에 각기 대응하는 i개의 사용자 인증정보(1)를 입력하여 전송하도록 하는 사용자 인증정보 등록 인터페이스를 생성(또는 추출)하여 제공하며(540), 이에 대응하여 상기 단말은 상기 사용자 인증정보 등록 인터페이스를 통해 개의 인증정보 입력 질의 정보 중 i(1<=i<=I)개의 인증정보 입력 질의 정보에 각기 대응하는 i개의 사용자 인증정보(1)가 입력되는지 확인한다(545).

[0346] 만약 상기 i개의 사용자 인증정보(1)가 입력되면(550), 상기 단말은 상기 서버로 상기 입력된 i개의 사용자 인증정보(1)를 전송한다(555).

[0348] 본 발명의 실시 방법에 따르면, 상기 사용자 인증정보(1)가 상기 매체(1)로 발급된 인증서를 통해 가공(예컨대, 암호화 내지 전자서명 첨부)되고, 상기 인증서 정보가 첨부되어 수신되는 경우, 상기 단말은 상기 사용자 인증정보(1)에 상기 장치고유 정보(2)를 더 포함하여 수신하는 것이 바람지하며, 이 경우 상기 서버는 상기 수신된 장치고유 정보(2)를 통한 장치고유 정보 유효성 인증을 더 수행하는 것이 바람직하다.

[0350] 이후, 상기 서버는 상기 수신된 i개의 사용자 인증정보(1)와 사용자 인증정보(1)에 각기 대응하는 i개의 입력 질의 정보(또는 상기 i개의 인증정보 입력 질의 정보에 각기 대응하는 질의 식별코드)를 확인하고, 상기 수신된 i개의 사용자 인증정보(1)와 상기 확인된 i개의 입력 질의 정보(또는 상기 i개의 인증정보 입력 질의 정보에 각기 대응하는 질의 식별코드) 및 상기 하나 이상의 장치고유 정보(1)를 연계하여 인증서 관리 D/B(105)에 저장한다(560).

[0352] 본 발명의 다른 실시 방법에 따르면, 상기 서버는 상기 수신된 i개의 사용자 인증정보(1)와 상기 확인된 i개의 입력 질의 정보(또는 상기 i개의 인증정보 입력 질의 정보에 각기 대응하는 질의 식별코드) 및 상기 인증서 정보를 연계하여 인증서 관리 D/B(105)에 저장하는 것이 가능하며, 이에 의해 본 발명이 한정되지 아니한다.

[0354] 도면6은 본 발명의 실시 방법에 따라 고객단말(125)에 탑재 또는 이탈착되는 매체(1)로 인증서를 관리하는 인증서 관리 시스템 구성을 도시한 도면이다.

[0356] 보다 상세하게 본 도면6은 통신망을 통해 고객단말(125)에 탑재 또는 이탈착되는 매체(1)로 발급된 인증서 이용시, 상기 인증서가 불법적으로 이전되어 점유되는 것을 방지하기 위해 상기 도면2에 도시된 인증서 발급 시스템을 통해 상기 인증서 관리 D/B(105)에 구비된 인증서 정보와 하나 이상의 장치고유 정보(1)를 통해 상기 인증서가 발급되어 있는 매체(1)에 대한 장치고유 정보 기반 유효성 확인을 수행하는 인증서 관리 시스템 구성에 대한 것으로서, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 본 도면6을 참조 및/또는 변형하여 상기 고객단말(125)로 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(1)로 인증서를 관리하는 시스템 구성에 대한 다양한 실시 방법을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 실시 방법을 모두 포함하며, 본 도면6에 도시된 실시 방법에 의해 한정되지 아니한다.

[0358] 예컨대, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면6에 도시된 인증서 관리 시스템이 적용되는 다양한 형태의 인증서 이용 시스템(예컨대, 비대면 금융거래 시스템, 비대면 인증 시스템, 온라인 결제

시스템 등)을 유추할 수 있을 것이며, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지는 것을 특징으로 한다.

[0360] 이하, 본 도면6에서 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(1)에 발급된 인증서를 관리하는 시스템 상의 구성요소를 편의상 "인증서 관리 서버(110)"라고 한다.

[0362] 본 발명의 실시 방법을 따르는 도면6을 참조하면, 상기 인증서 관리 시스템은, 상기 도면2에 도시된 인증서 발급 시스템을 통해 상기 인증서가 발급된 매체(1)를 탑재 또는 이탈착하여 연동하고, 통신망을 통해 상기 인증서 관리 서버(110)에 접속하여 매체(1)에 발급된 인증서를 통한 인증서 이용을 요청(예컨대, 비대면 금융거래 요청, 비대면 인증 요청, 온라인 결제 요청)하는 고객단말(125)과, 상기 고객단말(125)과 통신망을 통해 연결되어 상기 고객단말(125)로부터 요청된 인증서 이용 요청을 처리하는 인증서 이용 서버(120)와, 상기 고객단말(125)과 통신망을 통해 연결되며, 상기 고객단말(125)에서 인증서 이용 서버(120)를 통해 상기 인증서 이용시, 상기 인증서를 통해 매체(1)가 탑재 또는 이탈착되는 고객단말(125)에 구비된 장치고유 정보(2)를 수신하고, 상기 도면2에 도시된 인증서 발급 시스템 상의 인증서 관리 D/B(105)와 연계하여 상기 매체(1)가 탑재 또는 이탈착되는 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치 중 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하고, 상기 장치고유 정보(1)과 장치고유 정보(2)를 비교하여 상기 인증서가 발급된 매체(1)에 대한 장치고유 정보 기반 유효성을 확인하는 인증서 관리 서버(110)를 포함하여 이루어지는 것을 특징으로 한다.

[0364] 여기서, 상기 인증서 관리 서버(110)는 본 도면6에 도시된 바와 같이 상기 인증서 관리 시스템 측에 구비되어 상기 인증서가 불법적으로 이전되어 점유되는 것을 방지하는 기능 구성의 총칭으로서, 상기 인증서 관리 서버(110)는 하나 이상의 서버(또는 장치) 형태로 실시되거나, 또는 상기 인증서 이용 서버(120) 내에 구비되는 기능 구성요소 형태로 실시되는 것이 가능하며, 이에 의해 본 발명이 한정되지 아니함을 명백하게 밝혀두는 바이다.

[0366] 상기 고객단말(125)은 TCP/IP(Transmission Control Protocol/Internet Protocol) 기반의 유선 통신망(예컨대, ADSL(Asymmetric Digital Subscriber Line)/VDSL(Very high-data rate Digital Subscriber Line) 또는 케이블 통신망)를 통해 상기 인증서 관리 서버(110)와 통신 연결되는 데스크탑 컴퓨터 또는 노트북을 포함하는 유선단말을 적어도 하나 이상 포함하여 이루어지거나, 또는 CDMA(Code Division Multiple Access) 기반의 이동 통신망에 연결되는 이동 통신단말, 또는 IEEE 802.16x 기반의 초고속 무선 인터넷에 연결되는 휴대 인터넷 단말을 적어도 하나 이상 포함하는 무선단말을 적어도 하나 이상 포함하여 이루어지는 것을 특징으로 하며, 상기 고객단말(125)은 상기 인증서 이용 서버(120)에서 제공하는 하나 이상의 인증서 이용 인터페이스를 출력하고, 상기 인증서 이용 인터페이스를 통해 상기 인증서를 이용하기 위한 인증서 이용 요청 정보(예컨대, 비대면 금융거래 요청 정보, 비대면 인증 요청 정보, 온라인 결제 요청 정보)를 입력(또는 선택)하여 상기 인증서 이용 서버(120)(또는 인증서 관리 서버(110))로 전송하기 위한 기능 구성(예컨대, 브라우져 프로그램과 통신 기능)이 구비되어 있는 것이 바람직하다.

[0368] 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 적어도 하나 이상의 유선단말 또는 무선단말에 대응하는 상기 고객단말(125)의 특징을 용이하게 유추할 수 있을 것이므로, 이에 대한 상세한 설명은 편의상 생략한다.

[0370] 본 발명의 실시 방법에 따라 상기 고객단말(125)이 유선단말인 경우, 상기 통신망은 상기 TCP/IP 기반의 유선 통신망을 포함하여 이루어지며, 상기 고객단말(125)이 무선단말인 경우, 상기 통신망은 상기 CDMA 기반의 이동 통신망, 또는 IEEE 802.16x 기반의 초고속 무선 인터넷을 적어도 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0372] 본 발명에 따르면, 상기 인증서 관리 서버(110)는 상기 고객단말(125)과 통신망에 대응하는 웹 인터페이스를 제공하여 상기 고객단말(125)로부터 인증서 이용 요청 정보를 수신하기 위한 통신채널을 연결 및 관리하거나, 또는 상기 인증서 이용 서버(120)로부터 상기 고객단말(125)로부터 수신된 인증서 이용 요청 정보를 중계 수신하기 위한 통신채널을 연결 및 관리하는 인터페이스부(600)를 구비하여 이루어지는 것을 특징으로 한다.

[0374] 본 발명의 일 실시 방법에 따라 상기 고객단말(125)이 TCP/IP 기반의 유선 통신망을 통해 통신채널이 연결되는 유선단말이고, 상기 유선단말에 대응하는 고객단말(125)로부터 상기 인증서 이용 요청 정보를 수신하는 경우, 상기 인터페이스부(600)는 상기 고객단말(125)과 HTTP(Hyper-Text Transfer Protocol) 프로토콜을 기반으로 통신채널을 연결하고, 상기 통신채널을 통해 상기 고객단말(125)로 HTML(Hyper-Text Markup Language) 호환 문서 형태의 인증서 이용 인터페이스를 전송하여 출력하고, 상기 고객단말(125)로부터 상기 인증서 이용 인터페이스를 통해 입력(또는 선택)된 인증서 이용 요청 정보를 수신 처리하는 기능을 수행하는 것이 바람직하다.

[0376] 본 발명의 다른 일 실시 방법에 따라 상기 고객단말(125)이 CDMA 기반의 무선 통신망을 통해 통신채널이 연결되는 무선단말이고, 상기 무선단말에 대응하는 고객단말(125)로부터 상기 인증서 이용 요청 정보를 수신하는 경우, 상기 인터페이스부(600)는 상기 고객단말(125)과 WAP(Wireless Application Protocol) 또는 ME(Mobile Explorer) 프로토콜을 기반으로 통신채널, 또는 풀-브라우징 기반 무선 인터넷 통신채널을 연결하고, 상기 통신채널을 통해 상기 고객단말(125)로 WML(Wireless Markup Language) 또는 HTML 호환 문서 형태의 인증서 이용 인터페이스를 전송하여 출력하고, 상기 고객단말(125)로부터 상기 인증서 이용 인터페이스에 대응하는 인증서 이용 요청 정보를 수신 처리하는 기능을 수행하는 것이 바람직하다.

[0378] 본 발명의 또다른 일 실시 방법에 따라 상기 고객단말(125)이 IEEE 802.16x 기반의 무선 통신망을 통해 통신채널이 연결되는 무선단말이고, 상기 무선단말에 대응하는 고객단말(125)로부터 상기 인증서 이용 요청 정보를 수신하는 경우, 상기 인터페이스부(600)는 상기 고객단말(125)과 상기 IEEE 802.16 규격에 대응하는 무선 프로토콜을 기반으로 통신채널을 연결하고, 상기 통신채널을 통해 상기 고객단말(125)로 인증서 이용 인터페이스를 전송하여 출력하고, 상기 고객단말(125)로부터 상기 인증서 이용 인터페이스에 대응하는 소정의 인증서 이용 요청 정보를 수신 처리하는 기능을 수행하는 것이 바람직하다.

[0380] 본 발명의 다른 실시 방법에 따라 상기 인증서 이용 서버(120)로부터 상기 인증서 이용 요청 정보를 수신하는 경우, 상기 인터페이스부(600)는 상기 인증서 이용 서버(120)로부터 상기 인증서 이용 요청 정보를 수신하기 위한 통신채널을 연결 및 관리하는 것을 특징으로 한다.

[0382] 본 발명에 따르면, 상기 인증서 관리 서버(110)는, 고객단말(125)로부터 상기 인증서 이용 요청 정보를 수신하는 경우, 고객단말(125)이 상기 인터페이스부(600)를 통해 상기 인증서 관리 서버(110)에 접속(또는 인증서 이용 요청)시, 상기 인터페이스부(600)와 연동하여 상기 고객단말(125)에서 인증서 이용 요청 정보를 입력(또는 선택)하여 전송하도록 하는 인증서 이용 인터페이스를 생성(또는 추출)하여 제공하는 인터페이스 제공부(605)를 구비하여 이루어지는 것을 특징으로 한다.

[0384] 상기 인터페이스 제공부(605)는 상기 고객단말(125)이 상기 인터페이스부(600)를 통해 상기 인증서 관리 서버(110)에 접속(또는 인증서 이용 요청) 시, 상기 고객단말(125)에 구비된 기능구성(예컨대, 고객단말(125)에 구비된 브라우져 프로그램)에 대응하여 인증서 이용 요청 정보를 입력(또는 선택)하여 상기 통신망을 통해 상기 인증서 관리 서버(110)로 전송할 수 있는 인증서 이용 인터페이스를 생성하거나, 또는 데이터베이스(도시생략)로부터 추출하고, 상기 인터페이스부(600)와 연동하여 상기 생성(또는 추출)된 인증서 이용 인터페이스를 상기 통신망을 통해 상기 고객단말(125)로 제공하는 것을 특징으로 한다.

[0386] 이후, 상기 고객단말(125)은 상기 인증서 이용 인터페이스를 기반으로 인증서 이용 요청 정보를 입력(또는 선택)하며, 상기 입력(또는 선택)된 인증서 이용 요청 정보를 상기 통신망을 통해 상기 인증서 관리 서버(110)로 전송한다.

[0388] 본 발명의 다른 실시 방법에 따르면, 상기 인증서 이용 서버(120)는 상기 고객단말(125)에서 통신망을 통해 접속하여 인증서 이용 요청시, 상기 고객단말(125)에 구비된 기능구성(예컨대, 고객단말(125)에 구비된 브라우져 프로그램)에 대응하여 인증서 이용 요청 정보를 입력(또는 선택)하여 상기 통신망을 통해 상기 인증서 관리 서버(110)로 전송할 수 있는 인증서 이용 인터페이스를 생성하거나, 또는 데이터베이스(도시생략)로부터 추출하고, 상기 생성(또는 추출)된 인증서 이용 인터페이스를 상기 통신망을 통해 상기 고객단말(125)로 제공하는 것을 특징으로 하며, 이에 대응하여 상기 고객단말(125)은 상기 인증서 이용 인터페이스를 기반으로 인증서 이용 요청 정보를 입력(또는 선택)하며, 상기 입력(또는 선택)된 인증서 이용 요청 정보를 상기 통신망을 통해 상기 인증서 이용 서버(120)(또는 인증서 관리 서버(110))로 전송한다.

[0390] 만약 상기 인증서 이용 서버(120)로 상기 인증서 이용 요청 정보가 수신된 경우, 상기 인증서 이용 서버(120)는 상기 인증서 관리 서버(110)로 상기 수신된 인증서 이용 요청 정보를 중계 제공하는 것이 바람직하다.

[0392] 여기서, 상기 인증서 이용 요청 정보는 비대면 금융거래를 위한 비대면 금융거래 요청 정보(예컨대, 비대면 계좌조회 거래 요청 정보, 비대면 계좌이체 거래 요청 정보, 비대면 적립금 적립 요청 정보, 비대면 공과금 납부 요청 정보 등), 비대면 인증을 처리하기 위한 비대면 인증 요청 정보(예컨대, 각종 비밀번호, 인증서 정보, 보안카드 정보, OTP 정보 등), 온라인 결제를 처리하기 위한 온라인 결제 요청 정보(예컨대, 온라인 신용카드 결제 요청 정보, 온라인 체크카드 결제 요청 정보, 온라인 선불카드 결제 요청 정보, 온라인 직불카드 결제 요청 정보 등)를 하나 이상 포함하여 이루어지는 것이 바람직하며, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 상기 인증서 이용 요청 정보에 대한 다양한 정보 구성을 유추할 수 있을 것이며, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지는 것을 특징으로 한다.

[0394] 본 발명에 따르면, 상기 인증서 이용 요청 정보는, 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(1)에 발급된 인증서를 통해 가공(예컨대, 암호화 내지 전자서명 첨부)되고, 상기 인증서 정보가 첨부되는 것을 특징으로 하며, 상기 인증서의 불법 이전 및 점유 방지를 위해 상기 인증서를 통해 상기 고객단말(125)에 구비 또는 이탈착되는 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보(2)을 포함하는 것이 바람직하다.

[0396] 본 발명의 실시 방법에 따르면, 상기 장치고유 정보(2)는 상기 인증서가 발급된 매체의 고유정보 또는 상기 매체가 탑재 또는 이탈착되는 단말의 고유 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0398] 예컨대, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0400] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형) 통신장치에 구비된 MAC(Media Access Control) 주소 정보를 포함하여 이루어지는 것이 바람직하다.

[0402] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정

보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0404] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체에 구비된 IC칩 일련번호, IC칩 고유정보, IC칩 식별정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0406] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체에 구비되는 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0408] 본 발명에 따르면, 상기 인증서 관리 서버(110)는 상기 인터페이스부(600)와 연계하여 상기 인증서 이용 요청 정보를 수신하는 정보 수신부(610)(또는 정보 수신수단)와, 상기 인증서를 발급한 인증기관에 구비된 인증서버(도시생략)와 연계하여(또는 상기 인증서 정보에 포함된 인증서 사본을 판독하여) 상기 인증서 이용 요청 정보에 첨부된 인증서 정보를 기반으로 상기 인증서 이용 요청 정보에 대한 인증서 기반 유효성을 검증하는 인증서 검증부(615)(또는 인증서 검증수단)와, 상기 인증서 이용 요청 정보에 대한 인증서 기반 유효성 검증시, 상기 인증서 이용 요청 정보에 포함된 인증서 정보와 하나 이상의 장치고유 정보(2)를 추출하는 정보 추출부(620)(또는 정보 추출수단)와, 상기 추출된 인증서 정보를 기반으로 상기 인증서 관리 D/B(105)에 저장된 하나 이상의 장치고유 정보(1)를 확인하는 정보 확인부(625)(또는 정보 확인수단)와, 상기 확인된 장치고유 정보(1)와 상기 추출된 장치고유 정보(2)를 비교하여 상기 인증서 이용 요청 정보에 대한 장치고유 정보 기반 유효성을 확인하는 유효성 확인부(630)(또는 유효성 확인수단)와, 상기 인증서 기반 유효성이 검증되고 장치고유 정보 기반 유효성이 확인된 인증서 이용 요청 정보를 상기 인증서 이용 서버(120)로 제공하여 상기 인증서 이용 요청 정보에 대응하는 인증서 기반 서비스가 제공되도록 처리하는 정보 처리부(635)(또는 정보 처리수단)을 구비하여 이루어지는 것을 특징으로 한다.

[0410] 본 발명의 일 실시 방법에 따르면, 상기 고객단말(125)은 상기 인증서 이용 요청 정보를 상기 인증서에 구비된 하나 이상의 암호화 키(예컨대, 개인키, 공개키, 대칭키/비밀키)를 통해 암호화 내지 전자서명을 첨부하고, 상기 장치고유 정보(2)를 상기 인증서에 구비된 하나 이상의 암호화 키로 암호화한 후, 상기 인증서 정보를 첨부하여 전송하는 것이 바람직하며, 당업자의 의도에 따라 상기 인증서 정보는 생략(예컨대, 인증기관에 구비된 인증서버(도시생략)을 통해 인증서 정보를 확인할 수 있는 경우 생략)될 수 있으며, 이에 의해 본 발명이 한정되지 아니한다.

[0412] 또는, 상기 고객단말(125)은 상기 인증서 이용 요청 정보와 장치고유 정보(2)를 상기 인증서에 구비된 하나 이상의 암호화 키(예컨대, 개인키, 공개키, 대칭키/비밀키)를 통해 암호화 내지 전자서명을 첨부하고, 상기 인증서 정보를 첨부하여 전송하는 것이 바람직하며, 당업자의 의도에 따라 상기 인증서 정보는 생략(예컨대, 인증기관에 구비된 인증서버(도시생략)을 통해 인증서 정보를 확인할 수 있는 경우 생략)될 수 있으며, 이에 의해 본 발명이 한정되지 아니한다.

[0414] 또는, 상기 고객단말(125)은 상기 인증서 이용 요청 정보와 장치고유 정보(2) 및 인증서 정보를 상기 인증서에 구비된 하나 이상의 암호화 키(예컨대, 개인키, 공개키, 대칭키/비밀키)를 통해 암호화 내지 전자서명을 첨부하여 전송하는 것이 바람직하며, 당업자의 의도에 따라 상기 인증서 정보는 생략(예컨대, 인증기관에 구비된 인증서버(도시생략)을 통해 인증서 정보를 확인할 수 있는 경우 생략)될 수 있으며, 이에 의해 본 발명이 한정되지 아니한다.

[0416] 본 발명의 다른 일 실시 방법에 따르면, 상기 고객단말(125)은 상기 장치고유 정보(2)를 암호화 키로 사용하여

상기 인증서 이용 요청 정보를 제1 암호화하고, 상기 인증서에 구비된 하나 이상의 암호화 키(예컨대, 개인키, 공개키, 대칭키/비밀키)를 통해 제2 암호화 내지 전자서명을 첨부하고, 상기 인증서 정보를 첨부(생략가능)하여 전송하는 것이 바람직하다.

[0418] 또는, 상기 고객단말(125)은 상기 장치고유 정보(2)를 암호화 키로 사용하여 상기 인증서 이용 요청 정보와 인증서 정보를 제1 암호화하고, 상기 인증서에 구비된 하나 이상의 암호화 키(예컨대, 개인키, 공개키, 대칭키/비밀키)를 통해 제2 암호화 내지 전자서명을 첨부하여 전송하는 것이 바람직하다.

[0420] 본 발명의 또다른 일 실시 방법에 따르면, 상기 고객단말(125)은 상기 인증서 이용 요청 정보를 상기 인증서에 구비된 하나 이상의 암호화 키(예컨대, 개인키, 공개키, 대칭키/비밀키)를 통해 제1 암호화 내지 전자서명을 첨부하고, 상기 인증서 정보를 첨부(생략가능)한 후, 상기 장치고유 정보(2)를 암호화 키로 사용하여 제2 암호화하여 전송하는 것이 바람직하다.

[0422] 또는, 상기 고객단말(125)은 상기 인증서 이용 요청 정보와 인증서 정보를 상기 인증서에 구비된 하나 이상의 암호화 키(예컨대, 개인키, 공개키, 대칭키/비밀키)를 통해 제1 암호화 내지 전자서명을 첨부하고, 상기 장치고유 정보(2)를 암호화 키로 사용하여 제2 암호화하여 전송하는 것이 바람직하다.

[0424] 본 발명의 다른 실시 방법에 따르면, 상기 인증서에 구비된 하나 이상의 암호화 키(예컨대, 개인키, 공개키, 대칭키/비밀키)를 통한 암호화 내지 전자서명 첨부를 생략하고, 상기 장치고유 정보(2)를 암호화 키로 사용하여 암호화하는 것이 가능하며, 이에 의해 본 발명이 한정되지 아니한다.

[0426] 본 발명의 실시 방법에 따라 상기 장치고유 정보(2)를 암호화 키로 사용함에 있어서, 상기 장치고유 정보(2)가 암호화 키 구조를 포함하는 경우, 상기 고객단말(125)은 상기 장치고유 정보(2)를 그대로 암호화 키로 사용하는 것이 바람직하며, 상기 장치고유 정보(2)가 암호화 키 구조를 포함하지 않는 경우, 상기 고객단말(125)은 상기 장치고유 정보(2)를 암호화 키 구조로 변환하는 해시함수를 통해 해시하여 상기 장치고유 정보(2)에 대응하는 암호화 키를 생성하여 암호화 키로 사용하는 것이 바람직하다.

[0428] 본 발명의 일 실시 방법에 따르면, 상기 고객단말(125)은 상기 장치고유 정보(2)를 포함(또는 이용)하여 상기 방식 중 어느 하나의 방식으로 가공(예컨대, 암호화 내지 전자서명 첨부, 또는 제1 암호화 후 제2 암호화 내지 전자서명 첨부, 또는 제1 암호화 내지 전자서명 첨부 후 제2 암호화)된 인증서 이용 요청 정보를 상기 인증서 관리 서버로 전송하며, 이에 대응하여 상기 정보 수신부(610)는 상기 인터페이스부(600)와 연계하여 상기 고객단말(125)로부터 인증서 이용 요청 정보를 수신하는 것을 특징으로 한다.

[0430] 본 발명의 다른 일 실시 방법에 따르면, 상기 고객단말(125)은 상기 장치고유 정보(2)를 포함(또는 이용)하여 상기 방식 중 어느 하나의 방식으로 가공(예컨대, 암호화 내지 전자서명 첨부, 또는 제1 암호화 후 제2 암호화 내지 전자서명 첨부, 또는 제1 암호화 내지 전자서명 첨부 후 제2 암호화)된 인증서 이용 요청 정보를 상기 인증서 이용 서버로 전송하면, 이에 대응하여 상기 정보 수신부(610)는 상기 인터페이스부(600)와 연계하여 상기 인증서 이용 서버(120)로부터 상기 인증서 이용 요청 정보를 중계 수신하는 것을 특징으로 한다.

[0432] 상기 정보 수신부(610)를 통해 상기 매체(1)에 발급된 인증서를 통해 가공(예컨대, 암호화 내지 전자서명 첨부)되고, 상기 인증서 정보가 첨부되며, 상기 고객단말(125)에 구비 또는 이탈착되는 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보(2)를 포함하는 상기 인증서 이용 요청 정보가 수신되면, 상기 인증서 검증부(615)는 상기 인증서 이용 요청 정보에 첨부된 상기 인증서 정보를 통해 상기 인증서를 발급한 인증기관을 확인하고, 상기 인증기관에 구비된 인증서버(도시생략)와 연계하여(또는 상기 인증서 정보에 포함된 인증서 사본

을 판독하여) 상기 인증서 이용 요청 정보를 복호화 내지 전자서명 검증을 처리함으로써, 상기 인증서 이용 요청 정보에 대한 인증서 기반 유효성을 검증하는 것을 특징으로 한다.

[0434] 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 상기 인증서 검증부(615)가 상기 인증서를 발급한 인증기관에 구비된 인증서버(도시생략)와 연계하여(또는 상기 인증서 정보에 포함된 인증서 사본을 판독하여) 상기 인증서 이용 요청 정보에 첨부된 인증서 정보를 기반으로 상기 인증서 이용 요청 정보에 대한 인증서 기반 유효성을 검증하는 기술적 특징을 기 숙지하고 있을 것이므로, 이에 대한 상세한 설명은 편의상 생략하기로 한다.

[0436] 상기 인증서 검증부(615)에 의해 상기 인증서 기반 유효성이 검증되면, 상기 정보 추출부(620)는 인증서 기반 유효성이 검증되어 복호화된 인증서 이용 요청 정보로부터 상기 인증서 정보와 하나 이상의 장치고유 정보(2)를 추출하는 것을 특징으로 한다.

[0438] 상기 정보 추출부(620)를 통해 상기 인증서 정보와 하나 이상의 장치고유 정보(2)가 추출되면, 상기 정보 확인부(625)는 상기 추출된 인증서 정보를 기반으로 상기 도면2에 도시된 인증서 발급 시스템을 통해 상기 매체(1)로 발급된 인증서 정보와 장치고유 정보(1)를 연계하여 저장하는 인증서 관리 D/B(105)와 연계하여 상기 인증서 정보와 연계된 하나 이상의 장치고유 정보(1)를 확인하는 것을 특징으로 한다.

[0440] 본 발명의 실시 방법에 따르면, 상기 장치고유 정보(1)는 상기 인증서가 발급된 매체의 고유정보 또는 상기 매체가 탑재 또는 이탈착되는 단말의 고유 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0442] 예컨대, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0444] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형) 통신장치에 구비된 MAC(Media Access Control) 주소 정보를 포함하여 이루어지는 것이 바람직하다.

[0446] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0448] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체에 구비된 IC칩 일련번호, IC칩 고유정보, IC칩 식별정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0450] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체에 구비되는 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0452] 상기 인증서 정보와 연계된 하나 이상의 장치고유 정보(1)가 확인되면, 상기 유효성 확인부(630)는 상기 확인된

장치고유 정보(1)와 상기 추출된 장치고유 정보(2)를 비교하여 상기 인증서 이용 요청 정보에 대한 장치고유 정보 기반 유효성을 확인하는 것을 특징으로 한다.

[0454] 본 발명의 실시 방법에 따르면, 상기 확인된 장치고유 정보(1)와 상기 추출된 장치고유 정보(2)가 매칭되면, 상기 유효성 확인부(630)는 상기 인증서 이용 요청 정보에 대한 장치고유 정보 기반 유효성이 확인된 것으로 확인하는 것이 바람직하다.

[0456] 본 발명의 실시 방법에 따라 상기 인증서 이용 요청 정보(또는 상기 인증서 이용 요청 정보와 인증서 정보)가 상기 장치고유 정보(2)를 암호화 키로 사용하여 암호화된 경우, 상기 암호화된 인증서 이용 요청 정보(또는 상기 인증서 이용 요청 정보와 인증서 정보)를 상기 확인된 장치고유 정보(1)를 복호화 키로 사용하여 복호화하고, 상기 장치고유 정보(1)를 복호화 키로 사용한 복호화 처리가 정상적으로 수행되면, 상기 유효성 확인부(630)는 상기 인증서 이용 요청 정보에 대한 장치고유 정보 기반 유효성이 확인된 것으로 확인하는 것이 바람직하다.

[0458] 본 발명의 실시 방법에 따라 상기 장치고유 정보(1)를 복호화 키로 사용함에 있어서, 상기 장치고유 정보(1)가 암호화 키 구조를 포함하는 경우, 상기 유효성 확인부(630)는 상기 장치고유 정보(2)를 그대로 복호화 키로 사용하는 것이 바람직하며, 상기 장치고유 정보(1)가 복호화 키 구조를 포함하지 않는 경우, 상기 유효성 확인부(630)는 상기 고객단말(125)에서 상기 장치고유 정보(2)를 해시한 해시함수(또는 해시 알고리즘)과 동일한 해시함수(또는 해시 알고리즘)를 통해 상기 장치고유 정보(1)를 해시하여 상기 장치고유 정보(1)에 대응하는 복호화 키를 생성하여 복호화 키로 사용하는 것이 바람직하다.

[0460] 본 발명의 실시 방법에 따르면, 상기 확인된 장치고유 정보(1)와 상기 추출된 장치고유 정보(2)가 매칭되지 않는 경우(예컨대, 상기 장치고유 정보 기반 유효성이 확인되지 않는 경우), 상기 유효성 확인부(630)는 상기 인증서 검증부(615)를 통한 상기 인증서 기반 유효성 검증 결과와 무관하게 상기 인증서 이용 요청 정보에 대한 오류가 발생한 것으로 처리하는 것이 바람직하다.

[0462] 상기 인증서 검증부(615)에 의해 상기 인증서 기반 유효성이 검증되고, 상기 유효성 확인부(630)에 의해 상기 장치고유 정보 기반 유효성이 확인되면, 상기 정보 처리부(635)는 상기 인증서 이용 요청 정보를 상기 인증서 이용 서버(120)로 제공하여 상기 인증서 이용 요청 정보에 대응하는 인증서 기반 서비스가 제공되도록 처리하는 것을 특징으로 한다.

[0464] 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 상기 인증서 이용 서버(120)가 상기 인증서 이용 요청 정보를 기반으로 비대면 금융거래, 비대면 인증, 온라인 결제를 하나 이상 처리하는 기술적 특징을 기 숙지하고 있을 것이므로, 이에 대한 상세한 설명은 편의상 생략하기로 한다.

[0466] 도면7은 본 발명의 실시 방법에 따라 인증서를 관리하는 과정을 도시한 도면이다.

[0468] 보다 상세하게 본 도면7은 상기 도면6에 도시된 인증서 관리 시스템을 통해 상기 고객단말(125)에서 인증서 이용 요청시, 상기 인증서 관리 서버(110)에서 상기 인증서가 불법적으로 이전되어 점유되는 것을 방지하기 위해 상기 인증서 이용 요청 정보에 대한 인증서 기반 유효성 검증과 상기 매체(1)이 탑재 또는 이탈착되는 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치에 대한 장치고유 정보 기반 유효성 인증을 수행하는 과정에 대한 것으로서, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 본 도면7을 참조 및/또는 변형하여 상기 인증서를 관리하는 과정에 대한 다양한 실시 방법을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 실시 방법을 모두 포함하며, 본 도면7에 도시된 실시 방법에 의해 한정되지 아니한다.

[0470] 예컨대, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면7에 도시된 인증서 관리 과정이 적용되는 다양한 형태의 인증서 이용 과정(예컨대, 비대면 금융거래 시스템, 비대면 인증 시스템, 온라인 결제 시스템 등)을 유추할 수 있을 것이며, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지는 것을 특징으로 한다.

[0472] 또한, 본 도면7은 편의상 상기 고객단말(125)에서 상기 인증서 이용 요청 정보를 상기 인증서 관리 서버(110)로 직접 전송하는 것으로 도시하여 설명하지만, 이에 의해 본 발명이 한정되지 아니함을 명백하게 밝혀두는 바이다.

[0474] 이하, 본 도면7에서 상기 도면6에 도시된 고객단말(125)을 편의상 "단말"이라고 하고, 상기 도면6에 도시된 인증서 관리 서버(110)를 편의상 "서버"라고 한다.

[0476] 도면7을 참조하면, 상기 단말은 통신망을 통해 상기 서버에 접속하고, 상기 서버로 상기 인증서를 이용하여 하나 이상의 비대면 금융거래, 비대면 인증, 온라인 결제를 하나 이상 포함하는 인증서 이용을 요청하며(700), 이에 대응하여 상기 서버는 상기 고객단말(125)로 상기 인증서를 이용하기 위한 인증서 이용 인터페이스를 추출(또는 생성)하여 상기 단말로 제공한다(705).

[0478] 이후, 상기 단말은 상기 인증서 이용 인터페이스를 통해 인증서 이용 요청 정보를 입력(또는 선택)하고(710), 상기 입력(또는 선택)된 인증서 이용 요청 정보를 상기 매체(1)로 발급된 인증서를 통해 가공(예컨대, 암호화 내지 전자서명 첨부)하고, 상기 인증서 정보를 첨부하여 상기 통신망을 통해 상기 서버로 전송한다(715).

[0480] 여기서, 상기 인증서 이용 요청 정보는 비대면 금융거래를 위한 비대면 금융거래 요청 정보(예컨대, 비대면 계좌조회 거래 요청 정보, 비대면 계좌이체 거래 요청 정보, 비대면 적립금 적립 요청 정보, 비대면 공과금 납부 요청 정보 등), 비대면 인증을 처리하기 위한 비대면 인증 요청 정보(예컨대, 각종 비밀번호, 인증서 정보, 보안카드 정보, OTP 정보 등), 온라인 결제를 처리하기 위한 온라인 결제 요청 정보(예컨대, 온라인 신용카드 결제 요청 정보, 온라인 체크카드 결제 요청 정보, 온라인 선불카드 결제 요청 정보, 온라인 직불카드 결제 요청 정보 등)를 하나 이상 포함하여 이루어지는 것이 바람직하며, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 상기 인증서 이용 요청 정보에 대한 다양한 정보 구성을 유추할 수 있을 것이며, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지는 것을 특징으로 한다.

[0482] 본 발명에 따르면, 상기 인증서 이용 요청 정보는, 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(1)에 발급된 인증서를 통해 가공(예컨대, 암호화 내지 전자서명 첨부)되고, 상기 인증서 정보가 첨부되는 것을 특징으로 하며, 상기 인증서의 불법 이전 및 점유 방지를 위해 상기 인증서를 통해 상기 고객단말(125)에 구비 또는 이탈착되는 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보(2)을 포함하는 것이 바람직하다.

[0484] 본 발명의 실시 방법에 따르면, 상기 장치고유 정보(2)는 상기 인증서가 발급된 매체의 고유정보 또는 상기 매체가 탑재 또는 이탈착되는 단말의 고유 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0486] 예컨대, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0488] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형) 통신장치에 구비된 MAC(Media Access Control) 주소 정보를 포함하여 이루어지는 것이 바람직하다.

[0490] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0492] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체에 구비된 IC칩 일련번호, IC칩 고유정보, IC칩 식별정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0494] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체에 구비되는 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0496] 본 발명의 일 실시 방법에 따르면, 상기 단말은 상기 인증서 이용 요청 정보를 상기 인증서에 구비된 하나 이상의 암호화 키(예컨대, 개인키, 공개키, 대칭키/비밀키)를 통해 암호화 내지 전자서명을 첨부하고, 상기 장치고유 정보(2)를 상기 인증서에 구비된 하나 이상의 암호화 키로 암호화한 후, 상기 인증서 정보를 첨부하여 전송하는 것이 바람직하며, 당업자의 의도에 따라 상기 인증서 정보는 생략(예컨대, 인증기관에 구비된 인증서버(도시생략)을 통해 인증서 정보를 확인할 수 있는 경우 생략)될 수 있으며, 이에 의해 본 발명이 한정되지 아니한다.

[0498] 또는, 상기 단말은 상기 인증서 이용 요청 정보와 장치고유 정보(2)를 상기 인증서에 구비된 하나 이상의 암호화 키(예컨대, 개인키, 공개키, 대칭키/비밀키)를 통해 암호화 내지 전자서명을 첨부하고, 상기 인증서 정보를 첨부하여 전송하는 것이 바람직하며, 당업자의 의도에 따라 상기 인증서 정보는 생략(예컨대, 인증기관에 구비된 인증서버(도시생략)을 통해 인증서 정보를 확인할 수 있는 경우 생략)될 수 있으며, 이에 의해 본 발명이 한정되지 아니한다.

[0500] 또는, 상기 단말은 상기 인증서 이용 요청 정보와 장치고유 정보(2) 및 인증서 정보를 상기 인증서에 구비된 하나 이상의 암호화 키(예컨대, 개인키, 공개키, 대칭키/비밀키)를 통해 암호화 내지 전자서명을 첨부하여 전송하는 것이 바람직하며, 당업자의 의도에 따라 상기 인증서 정보는 생략(예컨대, 인증기관에 구비된 인증서버(도시생략)을 통해 인증서 정보를 확인할 수 있는 경우 생략)될 수 있으며, 이에 의해 본 발명이 한정되지 아니한다.

[0502] 본 발명의 다른 일 실시 방법에 따르면, 상기 단말은 상기 장치고유 정보(2)를 암호화 키로 사용하여 상기 인증서 이용 요청 정보를 제1 암호화하고, 상기 인증서에 구비된 하나 이상의 암호화 키(예컨대, 개인키, 공개키, 대칭키/비밀키)를 통해 제2 암호화 내지 전자서명을 첨부하고, 상기 인증서 정보를 첨부(생략가능)하여 전송하는 것이 바람직하다.

[0504] 또는, 상기 단말은 상기 장치고유 정보(2)를 암호화 키로 사용하여 상기 인증서 이용 요청 정보와 인증서 정보를 제1 암호화하고, 상기 인증서에 구비된 하나 이상의 암호화 키(예컨대, 개인키, 공개키, 대칭키/비밀키)를 통해 제2 암호화 내지 전자서명을 첨부하여 전송하는 것이 바람직하다.

[0506] 본 발명의 또다른 일 실시 방법에 따르면, 상기 단말은 상기 인증서 이용 요청 정보를 상기 인증서에 구비된 하나 이상의 암호화 키(예컨대, 개인키, 공개키, 대칭키/비밀키)를 통해 제1 암호화 내지 전자서명을 첨부하고, 상기 인증서 정보를 첨부(생략가능)한 후, 상기 장치고유 정보(2)를 암호화 키로 사용하여 제2 암호화하여 전송하는 것이 바람직하다.

[0508] 또는, 상기 단말은 상기 인증서 이용 요청 정보와 인증서 정보를 상기 인증서에 구비된 하나 이상의 암호화 키(예컨대, 개인키, 공개키, 대칭키/비밀키)를 통해 제1 암호화 내지 전자서명을 첨부하고, 상기 장치고유 정보(2)를 암호화 키로 사용하여 제2 암호화하여 전송하는 것이 바람직하다.

[0510] 본 발명의 다른 실시 방법에 따르면, 상기 인증서에 구비된 하나 이상의 암호화 키(예컨대, 개인키, 공개키, 대칭키/비밀키)를 통한 암호화 내지 전자서명 첨부를 생략하고, 상기 장치고유 정보(2)를 암호화 키로 사용하여 암호화하는 것이 가능하며, 이에 의해 본 발명이 한정되지 아니한다.

[0512] 본 발명의 실시 방법에 따라 상기 장치고유 정보(2)를 암호화 키로 사용함에 있어서, 상기 장치고유 정보(2)가 암호화 키 구조를 포함하는 경우, 상기 단말은 상기 장치고유 정보(2)를 그대로 암호화 키로 사용하는 것이 바람직하며, 상기 장치고유 정보(2)가 암호화 키 구조를 포함하지 않는 경우, 상기 단말은 상기 장치고유 정보(2)를 암호화 키 구조로 변환하는 해시함수를 통해 해시하여 상기 장치고유 정보(2)에 대응하는 암호화 키를 생성하여 암호화 키로 사용하는 것이 바람직하다.

[0514] 이후, 상기 서버는 통신망을 통해 상기 인증서 이용 요청 정보를 수신하고, 상기 인증서 이용 요청 정보에 첨부된 상기 인증서 정보를 통해 상기 인증서를 발급한 인증기관을 확인하고, 상기 인증기관에 구비된 인증서버와 연계하여(또는 상기 인증서 정보에 포함된 인증서 사본을 판독하여) 상기 인증서 이용 요청 정보를 복호화 내지 전자서명 검증을 처리함으로써, 상기 인증서 이용 요청 정보에 대한 인증서 기반 유효성을 검증한다(720).

[0516] 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 상기 서버가 상기 인증서를 발급한 인증기관에 구비된 인증서버와 연계하여(또는 상기 인증서 정보에 포함된 인증서 사본을 판독하여) 상기 인증서 이용 요청 정보에 첨부된 인증서 정보를 기반으로 상기 인증서 이용 요청 정보에 대한 인증서 기반 유효성을 검증하는 기술적 특징을 기 숙지하고 있을 것이므로, 이에 대한 상세한 설명은 편의상 생략하기로 한다.

[0518] 만약 상기 인증서 기반 유효성이 검증되지 않으면(725), 상기 서버는 인증서 기반 유효성 오류 정보를 생성하여 상기 단말로 전송하고(730), 상기 인증서 이용 과정을 종료한다.

[0520] 반면 상기 인증서 기반 유효성이 검증되면(725), 상기 서버는 인증서 기반 유효성이 검증되어 복호화된 인증서 이용 요청 정보로부터 상기 인증서 정보와 하나 이상의 장치고유 정보(2)를 추출하고(735), 상기 추출된 인증서 정보를 기반으로 상기 도면2에 도시된 인증서 발급 시스템을 통해 상기 매체(1)로 발급된 인증서 정보와 장치고유 정보(1)를 연계하여 저장하는 인증서 관리 D/B(105)와 연계하여 상기 인증서 정보와 연계된 하나 이상의 장치고유 정보(1)를 확인한다(740).

[0522] 본 발명의 실시 방법에 따르면, 상기 장치고유 정보(1)는 상기 인증서가 발급된 매체의 고유정보 또는 상기 매체가 탑재 또는 이탈착되는 단말의 고유 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0524] 예컨대, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별

코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0526] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형) 통신장치에 구비된 MAC(Media Access Control) 주소 정보를 포함하여 이루어지는 것이 바람직하다.

[0528] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0530] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체에 구비된 IC칩 일련번호, IC칩 고유정보, IC칩 식별정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0532] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체에 구비되는 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0534] 만약 상기 인증서 정보와 연계된 하나 이상의 장치고유 정보(1)가 확인되면(745), 상기 서버는 상기 확인된 장치고유 정보(1)와 상기 추출된 장치고유 정보(2)를 비교하여 상기 인증서 이용 요청 정보에 대한 장치고유 정보 기반 유효성을 확인한다(750).

[0536] 본 발명의 실시 방법에 따르면, 상기 확인된 장치고유 정보(1)와 상기 추출된 장치고유 정보(2)가 매칭되면, 상기 서버는 상기 인증서 이용 요청 정보에 대한 장치고유 정보 기반 유효성이 확인된 것으로 확인하는 것이 바람직하다.

[0538] 또는, 상기 확인된 장치고유 정보(1)와 상기 추출된 장치고유 정보(2)가 매칭되지 않는 경우(예컨대, 상기 장치고유 정보 기반 유효성이 확인되지 않는 경우), 상기 서버는 상기 인증서 기반 유효성 검증 결과와 무관하게 상기 인증서 이용 요청 정보에 대한 오류가 발생한 것으로 처리하는 것이 바람직하다.

[0540] 본 발명의 실시 방법에 따라 상기 인증서 이용 요청 정보(또는 상기 인증서 이용 요청 정보와 인증서 정보)가 상기 장치고유 정보(2)를 암호화 키로 사용하여 암호화된 경우, 상기 암호화된 인증서 이용 요청 정보(또는 상기 인증서 이용 요청 정보와 인증서 정보)를 상기 확인된 장치고유 정보(1)를 복호화 키로 사용하여 복호화하고, 상기 장치고유 정보(1)를 복호화 키로 사용한 복호화 처리가 정상적으로 수행되면, 상기 서버는 상기 인증서 이용 요청 정보에 대한 장치고유 정보 기반 유효성이 확인된 것으로 확인하는 것이 바람직하다.

[0542] 본 발명의 실시 방법에 따라 상기 장치고유 정보(1)를 복호화 키로 사용함에 있어서, 상기 장치고유 정보(1)가 암호화 키 구조를 포함하는 경우, 상기 서버는 상기 장치고유 정보(2)를 그대로 복호화 키로 사용하는 것이 바람직하며, 상기 장치고유 정보(1)가 복호화 키 구조를 포함하지 않는 경우, 상기 서버는 상기 고객단말(125)에서 상기 장치고유 정보(2)를 해시한 해시함수(또는 해시 알고리즘)과 동일한 해시함수(또는 해시 알고리즘)를 통해 상기 장치고유 정보(1)를 해시하여 상기 장치고유 정보(1)에 대응하는 복호화 키를 생성하여 복호화 키로 사용하는 것이 바람직하다.

[0544] 또는, 상기 인증서 이용 요청 정보(또는 상기 인증서 이용 요청 정보와 인증서 정보)가 상기 확인된 장치고유 정보(1)를 복호화 키로 사용하여 복호화되지 않는 경우, 상기 서버는 상기 인증서 기반 유효성 검증 결과와 무관하게 상기 인증서 이용 요청 정보에 대한 오류가 발생한 것으로 처리하는 것이 바람직하다.

[0546] 만약 상기 장치고유 정보 기반 유효성이 확인되지 않으면(755), 상기 서버는 장치고유 정보 기반 유효성 오류 정보를 생성하여 상기 단말로 전송하고(760), 상기 인증서 이용 과정을 종료한다.

[0548] 만약 상기 장치고유 정보 기반 유효성이 확인되면(755), 상기 서버는 상기 인증서 기반 유효성 검증 결과와 장치고유 정보 기반 유효성 확인 결과를 기반으로 상기 인증서 이용 요청 정보를 상기 인증서 이용 서버(120)로 제공하여 상기 인증서 이용 서버(120)에서 상기 인증서 이용 요청 정보를 기반으로 비대면 금융거래, 비대면 인증, 온라인 결제를 하나 이상 제공하도록 처리한다(765).

[0550] 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 상기 인증서 이용 서버(120)가 상기 인증서 이용 요청 정보를 기반으로 비대면 금융거래, 비대면 인증, 온라인 결제를 하나 이상 처리하는 기술적 특징을 기 숙지하고 있을 것이므로, 이에 대한 상세한 설명은 편의상 생략하기로 한다.

[0552] 도면8은 본 발명의 실시 방법에 따라 고객단말(125)에 탑재 또는 이탈착되는 매체(2)로 인증서를 이전하는 인증서 이전 시스템 구성을 도시한 도면이다.

[0554] 보다 상세하게 본 도면8은 상기 인증서가 불법적으로 이전되어 점유되는 것을 방지하기 위해 통신망을 통해 고객단말(125)에 탑재 또는 이탈착되는 매체(2)로 인증서 이전시, 상기 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치 중 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 상기 매체(2)로 발급된 인증서 정보와 연계하여 저장함으로써, 상기 통신망을 통해 상기 인증서를 이용하거나, 또는 상기 인증서를 다른 매체(2)로 이전하는 과정에서 상기 장치고유 정보(1)에 대한 유효성 확인을 통해 매체(2)로 발급된 인증서가 불법적으로 이전되어 점유되는 것을 방지하는 시스템 구성에 대한 것으로서, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 본 도면8을 참조 및/또는 변형하여 상기 고객단말(125)로 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(2)로 인증서를 이전하는 시스템 구성에 대한 다양한 실시 방법을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 실시 방법을 모두 포함하며, 본 도면8에 도시된 실시 방법에 의해 한정되지 아니한다.

[0556] 예컨대, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면8에 도시된 인증서 이전 시스템과 상기 도면2에 도시된 인증서 발급 시스템을 참조 및/또는 변형하여 상기 인증서가 불법적으로 이전되어 점유되는 것을 방지하도록 인증서를 재이전하는 인증서 재발급 시스템 구성을 유추할 수 있을 것이며, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지는 것을 특징으로 한다.

[0558] 이하, 본 도면8에서 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(2)로 상기 인증서를 이전하는 시스템 상의 구성요소를 편의상 "인증서 이전 서버(115)"라고 한다.

[0560] 여기서, 상기 고객단말(125)은 상기 도면2에 도시된 인증서 발급 시스템을 통해 상기 인증서가 발급된 매체(1)을 탑재 또는 이탈착하는 고객단말(125)과 동일한 단말이거나, 또는 상기 다른 단말이어도 무관하며, 이에 의해 본 발명이 한정되지 아니함을 명백하게 밝혀두는 바이다.

[0562] 만약 상기 고객단말(125)이 상기 도면2에 도시된 인증서 발급 시스템을 통해 상기 인증서가 발급된 매체(1)을 탑재 또는 이탈착하는 고객단말(125)과 동일한 단말인 경우, 상기 인증서 이전을 위해 확인되는 장치고유 정보

(1)는 상기 도면2에 도시된 인증서 발급 시스템 상의 인증서 관리 D/B(105)에 저장된 장치고유 정보(1)과 동일하거나, 또는 달라도 무관하며, 반면 상기 도면2에 도시된 인증서 발급 시스템을 통해 상기 인증서가 발급된 매체(1)을 탑재 또는 이탈착하는 고객단말(125)과 다른 단말인 경우, 상기 인증서 이전을 위해 확인되는 장치고유 정보(1)는 상기 도면2에 도시된 인증서 발급 시스템 상의 인증서 관리 D/B(105)에 저장된 장치고유 정보(1)와 다른 장치고유 정보를 포함하는 것이 바람직하며, 이에 의해 본 발명이 한정되지 아니함을 명백하게 밝혀두는 바이다.

[0564] 다만, 상기 인증서가 이전되는 매체(2)는 상기 도면2에 도시된 인증서 발급 시스템을 통해 상기 인증서가 발급된 매체(1)와 다른 매체를 포함하여 이루어지는 것을 특징으로 한다.

[0566] 이하, 본 도면8은 편의상 상기 고객단말(125)에 상기 도면2에 도시된 인증서 발급 시스템을 통해 상기 인증서가 발급된 매체(1)가 탑재 또는 이탈착되고, 상기 고객단말(125)에 상기 인증서가 이전되는 매체(2) 역시 탑재 또는 이탈착되어 있는 실시 방법을 통해 본 발명의 기술적 특징을 상세히 설명하기로 한다. 그러나, 본 발명의 기술적 특징이 본 도면8에 도시된 실시 방법으로 한정되는 것은 결코 아니며, 상기 매체(1)와 매체(2)는 서로 다른 단말에 구비되는 것이 가능하며, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면8을 참조 및/또는 변형하여 상기 매체(1)와 매체(2)는 서로 다른 단말에 구비된 경우, 인증서가 불법적으로 이전되어 점유되는 것을 방지하도록 상기 인증서를 상기 매체(1)에서 상기 매체(2)로 이전하는 다양한 실시 방법을 유추할 수 있을 것이며, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지는 것을 특징으로 한다.

[0568] 본 발명의 실시 방법을 따르는 도면8을 참조하면, 상기 인증서 이전 시스템은, 상기 도면2에 도시된 인증서 발급 시스템을 통해 상기 인증서가 발급된 매체(1)와, 상기 인증서가 이전되는 매체(2)를 탑재 또는 이탈착하여 연동하고, 통신망을 통해 상기 인증서 이전 서버(115)에 접속하여 상기 인증서를 매체(1)에서 매체(2)로 이전하는 고객단말(125)과, 상기 고객단말(125)과 통신망을 통해 연결되어 상기 인증서 이전시, 상기 인증서를 통해 매체(1)가 탑재 또는 이탈착되는 고객단말(125)에 구비된 장치고유 정보(2)에 대한 유효성을 검증하고, 상기 매체(2)가 탑재 또는 이탈착되는 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치 중 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 상기 매체(2)로 이전되는 인증서 정보와 연계하여 인증서 관리 D/B(105)에 저장하는 인증서 이전 서버(115)를 포함하여 이루어지는 것을 특징으로 하며, 상기 매체(2)가 탑재 또는 이탈착되는 고객단말(125)로 이전된 인증서 이용시, 상기 인증서 관리 D/B(105)와 연계하여 상기 장치고유 정보(1)를 기반으로 상기 인증서가 이전되는 매체(2)가 탑재 또는 이탈착되는 고객단말(125)의 유효성을 인증하여 상기 인증서가 불법적으로 이전되어 점유되는 것을 방지하는 인증서 관리 서버(110)를 더 포함하여 이루어지는 것을 특징으로 한다.

[0570] 여기서, 상기 인증서 이전 서버(115)는 본 도면8에 도시된 바와 같이 상기 인증서 이전 시스템 측에 구비되어 상기 인증서가 불법적으로 이전되어 점유되는 것을 방지하기 위해 통신망을 통해 고객단말(125)에 탑재 또는 이탈착되는 매체(2)로 인증서 이전시, 상기 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치 중 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 상기 매체(2)로 이전되는 인증서 정보와 연계하여 저장하는 기능 구성의 총칭으로서, 상기 인증서 이전 서버(115)는 하나 이상의 서버(또는 장치) 형태로 실시되거나, 또는 상기 인증서 이전 서버(115) 내에 구비되는 기능 구성요소 형태로 실시되는 것이 가능하며, 이에 의해 본 발명이 한정되지 아니함을 명백하게 밝혀두는 바이다.

[0572] 상기 고객단말(125)은 TCP/IP(Transmission Control Protocol/Internet Protocol) 기반의 유선 통신망(예컨대, ADSL(Asymmetric Digital Subscriber Line)/VDSL(Very high-data rate Digital Subscriber Line) 또는 케이블 통신망)를 통해 상기 인증서 이전 서버(115)와 통신 연결되는 데스크탑 컴퓨터 또는 노트북을 포함하는 유선단말을 적어도 하나 이상 포함하여 이루어지거나, 또는 CDMA(Code Division Multiple Access) 기반의 이동 통신망에 연결되는 이동 통신단말, 또는 IEEE 802.16x 기반의 초고속 무선 인터넷에 연결되는 휴대 인터넷 단말을 적어도 하나 이상 포함하는 무선단말을 적어도 하나 이상 포함하여 이루어지는 것을 특징으로 하며, 상기 고객단말(125)은 상기 인증서 이전 서버(115)에서 이전하는 적어도 하나 이상의 인증서 이전 인터페이스를

출력하고, 상기 인증서 이전 인터페이스를 통해 상기 인증서를 이전하기 위한 인증서 이전 요청 정보를 입력(또는 선택)하여 상기 인증서 이전 서버(115)로 전송하기 위한 기능 구성(예컨대, 브라우져 프로그램과 통신 기능)이 구비되어 있는 것이 바람직하다.

[0574] 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 적어도 하나 이상의 유선단말 또는 무선단말에 대응하는 상기 고객단말(125)의 특징을 용이하게 유추할 수 있을 것이므로, 이에 대한 상세한 설명은 편의상 생략한다.

[0576] 본 발명의 실시 방법에 따라 상기 고객단말(125)이 유선단말인 경우, 상기 통신망은 상기 TCP/IP 기반의 유선 통신망을 포함하여 이루어지며, 상기 고객단말(125)이 무선단말인 경우, 상기 통신망은 상기 CDMA 기반의 이동 통신망, 또는 IEEE 802.16x 기반의 초고속 무선 인터넷을 적어도 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0578] 본 발명에 따르면, 상기 인증서 이전 서버(115)는 상기 고객단말(125)과 통신망에 대응하는 웹 인터페이스를 제공하기 위해 상기 통신망을 통해 상기 고객단말(125)과 통신채널을 연결 및 관리하는 인터페이스부(800)를 구비하여 이루어지는 것을 특징으로 하며, 이에 의해 상기 인증서 이전 서버(115)는 상기 고객단말(125)과 유선 통신망 또는 무선 통신망을 통해 통신 연결되는 웹서버의 기능을 구비한다.

[0580] 본 발명의 일 실시 방법에 따라 상기 고객단말(125)이 TCP/IP 기반의 유선 통신망을 통해 통신채널이 연결되는 유선단말인 경우, 상기 인터페이스부(800)는 상기 고객단말(125)과 HTTP(Hyper-Text Transfer Protocol) 프로토콜을 기반으로 통신채널을 연결하고, 상기 통신채널을 통해 상기 고객단말(125)로 HTML(Hyper-Text Markup Language) 호환 문서 형태의 인증서 이전 인터페이스를 전송하여 출력하고, 상기 고객단말(125)로부터 상기 인증서 이전 인터페이스를 통해 입력(또는 선택)된 인증서 이전 요청 정보를 수신 처리하는 기능을 수행하는 것이 바람직하다.

[0582] 본 발명의 다른 일 실시 방법에 따라 상기 고객단말(125)이 CDMA 기반의 무선 통신망을 통해 통신채널이 연결되는 무선단말인 경우, 상기 인터페이스부(800)는 상기 고객단말(125)과 WAP(Wireless Application Protocol) 또는 ME(Mobile Explorer) 프로토콜을 기반으로 통신채널, 또는 풀-브라우징 기반 무선 인터넷 통신채널을 연결하고, 상기 통신채널을 통해 상기 고객단말(125)로 WML(Wireless Markup Language) 또는 HTML 호환 문서 형태의 인증서 이전 인터페이스를 전송하여 출력하고, 상기 고객단말(125)로부터 상기 인증서 이전 인터페이스에 대응하는 인증서 이전 요청 정보를 수신 처리하는 기능을 수행하는 것이 바람직하다.

[0584] 본 발명의 또다른 일 실시 방법에 따라 상기 고객단말(125)이 IEEE 802.16x 기반의 무선 통신망을 통해 통신채널이 연결되는 무선단말인 경우, 상기 인터페이스부(800)는 상기 고객단말(125)과 상기 IEEE 802.16 규격에 대응하는 무선 프로토콜을 기반으로 통신채널을 연결하고, 상기 통신채널을 통해 상기 고객단말(125)로 인증서 이전 인터페이스를 전송하여 출력하고, 상기 고객단말(125)로부터 상기 인증서 이전 인터페이스에 대응하는 소정의 인증서 이전 요청 정보를 수신 처리하는 기능을 수행하는 것이 바람직하다.

[0586] 본 발명에 따르면, 상기 인증서 이전 서버(115)는 고객단말(125)이 상기 인터페이스부(800)를 통해 상기 인증서 이전 서버(115)에 접속(또는 인증서 이전 요청)시, 상기 인터페이스부(800)와 연동하여 상기 고객단말(125)에서 인증서 이전 요청 정보를 입력(또는 선택)하여 전송하도록 하는 인증서 이전 인터페이스를 생성(또는 추출)하여 제공하는 인터페이스 제공부(805)를 구비하여 이루어지는 것을 특징으로 한다.

[0588] 상기 인터페이스 제공부(805)는 상기 고객단말(125)이 상기 인터페이스부(800)를 통해 상기 인증서 이전 서버

(115)에 접속(또는 인증서 이전 요청) 시, 상기 고객단말(125)에 구비된 기능구성(예컨대, 고객단말(125)에 구비된 브라우져 프로그램)에 대응하여 인증서 이전 요청 정보를 입력(또는 선택)하여 상기 통신망을 통해 상기 인증서 이전 서버(115)로 전송할 수 있는 인증서 이전 인터페이스를 생성하거나, 또는 데이터베이스(도시생략)로부터 추출하고, 상기 인터페이스부(800)와 연동하여 상기 생성(또는 추출)된 인증서 이전 인터페이스를 상기 통신망을 통해 상기 고객단말(125)로 제공하는 것을 특징으로 한다.

[0590] 이후, 상기 고객단말(125)은 상기 인증서 이전 인터페이스를 기반으로 인증서 이전 요청 정보를 입력(또는 선택)하며, 상기 입력(또는 선택)된 인증서 이전 요청 정보를 상기 통신망을 통해 상기 인증서 이전 서버(115)로 전송한다.

[0592] 여기서, 상기 인증서 이전 요청 정보는 상기 고객단말(125)에 탑재 또는 이탈착하는 매체(2)로 상기 인증서를 이전하도록 요청하는 고객정보와, 상기 고객단말(125)에 탑재 또는 이탈착되어 상기 인증서가 이전될 매체(2) 정보와, 상기 매체(2)가 탑재 또는 이탈착되는 고객단말(125)에 대한 운영체제(또는 플랫폼) 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0594] 상기 인증서 이전 요청 정보에 포함된 상기 고객정보는, 상기 인증서를 이전받는 상기 고객의 회원ID정보와 비밀번호 정보를 포함하는 고객 회원정보, 또는 상기 고객의 성명, 주민등록번호, 주소, 연락처 등을 적어도 하나 이상 포함하는 고객 개인정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0596] 상기 인증서 이전 요청 정보에 포함된 상기 매체(2) 정보는, 상기 고객단말(125)에 탑재 또는 이탈착되는 매체 중 상기 인증서가 이전되어 저장되는 매체를 확인(또는 식별)하는 정보를 포함하여 이루어지는 것이 바람직하다.

[0598] 본 발명의 실시 방법에 따르면, 상기 매체(2) 정보는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체를 포함하여 이루어지는 것이 바람직하다.

[0600] 또는, 상기 매체(2) 정보는 상기 고객단말(125)에 이탈착되는(예컨대, 플로피디스크 드라이브에 삽입되는) 플로피디스크 매체를 포함하여 이루어지는 것이 바람직하다.

[0602] 또는, 상기 매체(2) 정보는 상기 고객단말(125)에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체를 포함하여 이루어지는 것이 바람직하다.

[0604] 또는, 상기 매체(2) 정보는 상기 고객단말(125)에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체를 포함하여 이루어지는 것이 바람직하다.

[0606] 또는, 상기 매체(2) 정보는 상기 고객단말(125)에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체를 포함하여 이루어지는 것이 바람직하다.

[0608] 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 상술된 매체(2) 이외에 상기 고객단말(125)에 탑재

또는 이탈착되는 다양한 형태의 매체를 유추할 수 있을 것이며, 본 발명은 상기 유추되는 모든 매체(2)를 포함하여 이루어지는 것을 특징으로 한다.

[0610] 상기 인증서 이전 요청 정보에 포함된 상기 운영체제(또는 플랫폼) 정보는, 상기 인증서가 이전되는 매체(2)이 탑재 또는 이탈착되는 고객단말(125)의 운영체제(또는 플랫폼)을 식별 내지 확인하는 정보로서, 상기 인증서에 대응하는 프로그램 코드가 실행되는 운영체제(또는 플랫폼)을 확인하는 것이 바람직하다.

[0612] 본 발명의 실시 방법에 따르면, 상기 인증서 이전 요청 정보는 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(1)에 발급된 인증서를 통해 가공(예컨대, 암호화 내지 전자서명 첨부)되고, 상기 인증서 정보가 첨부되어 전송되는 것이 바람직하며, 상기 인증서의 불법 이전 및 점유 방지를 위해 상기 인증서를 통해 상기 고객단말(125)에 구비 또는 이탈착되는 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보(2)을 포함하여 전송되는 것을 특징으로 한다.

[0614] 본 발명에 따르면, 상기 인증서 이전 서버(115)는 상기 인터페이스부(800)와 연계하여 상기 인증서 이전 요청 정보를 수신하는 정보 수신부(810)(또는 정보 수신수단)와, 상기 인증서를 발급한 인증기관에 구비된 인증서버(도시생략)와 연계하여(또는 상기 인증서 정보에 포함된 인증서 사본을 판독하여) 상기 인증서 이전 요청 정보에 첨부된 인증서 정보를 기반으로 상기 인증서 이전 요청 정보에 대한 인증서 기반 유효성을 검증하는 인증서 검증부(815)(또는 인증서 검증수단)와, 상기 인증서 이전 요청 정보에 대한 인증서 기반 유효성 검증시, 상기 인증서 이전 요청 정보에 포함된 인증서 정보와 하나 이상의 장치고유 정보(2)를 추출하는 정보 추출부(820)(또는 정보 추출수단)와, 상기 추출된 인증서 정보를 기반으로 상기 인증서 관리 D/B(105)에 저장된 하나 이상의 장치고유 정보(1)를 확인하는 정보 확인부(825)(또는 정보 확인수단)와, 상기 확인된 장치고유 정보(1)와 상기 추출된 장치고유 정보(2)를 비교하여 상기 인증서 이전 요청 정보에 대한 장치고유 정보 기반 유효성을 확인하는 유효성 확인부(830)(또는 유효성 확인수단)을 구비하여 이루어지는 것을 특징으로 한다.

[0616] 상기 고객단말(125)에서 상기 인증서 이전 요청 정보가 상기 매체(1)에 발급된 인증서를 통해 가공(예컨대, 암호화 내지 전자서명 첨부)되고, 상기 인증서 정보가 첨부되어 전송되면, 상기 정보 수신부(810)는 상기 인터페이스부(800)와 연계하여 상기 인증서 이전 요청 정보를 수신하는 것을 특징으로 한다.

[0619] *상기 정보 수신부(810)를 통해 상기 매체(1)에 발급된 인증서를 통해 가공(예컨대, 암호화 내지 전자서명 첨부)되고, 상기 인증서 정보가 첨부된 인증서 이전 요청 정보가 수신되면, 상기 인증서 검증부(815)는 상기 인증서 이전 요청 정보에 첨부된 상기 인증서 정보를 통해 상기 인증서를 발급한 인증기관을 확인하고, 상기 인증기관에 구비된 인증서버(도시생략)와 연계하여(또는 상기 인증서 정보에 포함된 인증서 사본을 판독하여) 상기 인증서 이전 요청 정보를 복호화 내지 전자서명 검증을 처리함으로써, 상기 인증서 이전 요청 정보에 대한 인증서 기반 유효성을 검증하는 것을 특징으로 한다.

[0621] 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 상기 인증서 검증부(815)가 상기 인증서를 발급한 인증기관에 구비된 인증서버(도시생략)와 연계하여(또는 상기 인증서 정보에 포함된 인증서 사본을 판독하여) 상기 인증서 이전 요청 정보에 첨부된 인증서 정보를 기반으로 상기 인증서 이전 요청 정보에 대한 인증서 기반 유효성을 검증하는 기술적 특징을 기 숙지하고 있을 것이므로, 이에 대한 상세한 설명은 편의상 생략하기로 한다.

[0623] 상기 인증서 검증부(815)에 의해 상기 인증서 기반 유효성이 검증되면, 상기 정보 추출부(820)는 인증서 기반 유효성이 검증되어 복호화된 인증서 이전 요청 정보로부터 상기 인증서 정보와 하나 이상의 장치고유 정보(2)를

추출하는 것을 특징으로 한다.

[0625] 상기 정보 추출부(820)를 통해 상기 인증서 정보와 하나 이상의 장치고유 정보(2)가 추출되면, 상기 정보 확인부(825)는 상기 추출된 인증서 정보를 기반으로 상기 도면2에 도시된 인증서 발급 시스템을 통해 상기 매체(1)로 발급된 인증서 정보와 장치고유 정보(1)를 연계하여 저장하는 인증서 관리 D/B(105)와 연계하여 상기 인증서 정보와 연계된 하나 이상의 장치고유 정보(1)를 확인하는 것을 특징으로 한다.

[0627] 상기 인증서 정보와 연계된 하나 이상의 장치고유 정보(1)가 확인되면, 상기 유효성 확인부(830)는 상기 확인된 장치고유 정보(1)와 상기 추출된 장치고유 정보(2)를 비교하여 상기 인증서 이전 요청 정보에 대한 장치고유 정보 기반 유효성을 확인하는 것을 특징으로 한다.

[0629] 본 발명에 따르면, 상기 인증서 이전 서버(115)는, 상기 인증서 이전 요청 정보에 대한 인증서 기반 유효성과 장치고유 정보 기반 유효성이 확인되면, 상기 고객단말(125)로 이전할 인증서에 대응하는 적어도 하나 이상의 인증서 프로그램 소스(또는 인증서 프로그램 파일)와 인증서 데이터(예컨대, 인증서 프로파일 정보)를 저장하는 인증서 D/B(880)와, 상기 고객단말(125)로부터 상기 인증서 이전 요청 정보가 수신되는 경우, 인증서 D/B(880)로부터 상기 인증서 이전 요청 정보에 대응하는 인증서를 추출 또는 동적으로 생성하는 인증서 추출/생성부(855)(또는 인증서 추출/생성수단)와, 여 상기 인터페이스부(800)를 통해 상기 고객단말(125)로 이전하는 인증서 이전부(또는 인증서 이전수단)를 구비하여 이루어지는 것을 특징으로 한다.

[0631] 본 발명의 일 실시 방법에 따르면, 상기 인증서 D/B(880)는 상기 고객단말(125)에 구비된 운영체제(또는 단말 플랫폼)에서 동작할 수 있는 인증서 프로그램 파일과 인증서 데이터를 저장하는 것을 특징으로 하며, 상기 고객단말(125)로부터 상기 인증서 이전 요청 정보가 수신되는 경우, 상기 인증서 추출/생성부(855)는 상기 인증서 D/B(880)로부터 상기 인증서 이전 요청 정보와 매칭되는 인증서 프로그램 파일과 인증서 데이터를 포함하는 인증서를 추출하는 것을 특징으로 한다.

[0633] 본 발명의 다른 일 실시 방법에 따르면, 상기 인증서 D/B(880)는 상기 고객단말(125)에 구비된 운영체제(또는 단말 플랫폼)에서 동작할 수 있는 인증서 프로그램 소스와 인증서 데이터를 저장하는 것을 특징으로 하며, 상기 고객단말(125)로부터 상기 인증서 이전 요청 정보가 수신되는 경우, 상기 인증서 추출/생성부(855)는 상기 인증서 D/B(880)로부터 상기 인증서 이전 요청 정보와 매칭되는 인증서 프로그램 소스와 인증서 데이터를 추출하고, 상기 추출된 인증서 프로그램 소스를 컴파일(Compile)하여 상기 고객단말(125)로 이전할 인증서를 동적 생성하는 것을 특징으로 한다.

[0635] 이후, 상기 인증서 이전부는 상기 인터페이스부(800)를 통해 상기 매체(1)에 발급되어 있는 인증서를 무효화 처리하여 폐기하고, 상기 추출(또는 동적 생성)된 인증서를 상기 통신망을 통해 상기 고객단말(125)로 전송하여 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(2)에 기록하여 상기 인증서를 상기 매체(1)에서 매체(2)로 이전하는데, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 상기 인증서를 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(2)에 이전하는 방법을 기 숙지하고 있을 것이므로, 이에 대한 상세한 설명은 편의상 생략한다.

[0637] 본 발명의 실시 방법에 따르면, 상기 인증서 이전부에 의해 상기 고객단말(125)로 제공된 상기 인증서에 포함된 인증서 프로그램은, 통신망을 통한 인증서 기반 비대면 인증기능을 포함하고, 상기 비대면 인증시, 상기 매체(2)이 탑재 또는 이탈착된 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보(2)를 확인하고, 상기 확인된 하나 이상의 장치고유 정보(2)를 송수신 데이터(예컨대, 비대면 인증에 따라 고객단말(125)에서 통신망을 통해 전송하는 데이터, 또는 통신망을 통해 고객단말(125)로 수신하는 데이터)(에 포함하여 전송하는 기능을 구비하여 이루어지는 것일 특징으로

한다.

[0639] 본 발명의 일 실시 방법에 따르면, 상기 인증서 이전부는 상기 매체(2)가 탑재 또는 이탈착되는 고객단말(125)로 제공하는 인증서에 상기 고객단말(125)에 구비 또는 이탈착되는 M(M>1)개의 구성장치 정보를 확인하여 통신망을 통해 상기 인증서 이전 서버(115)로 전송하는 기능, 상기 인증서 이전 서버(115)로부터 상기 M(M>1)개의 구성장치 정보 중 인증서 검증 대상에 m(1<=m<=M)개의 구성장치 정보를 수신하는 기능, 상기 수신된 m개의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 상기 통신망을 통해 상기 인증서 이전 서버(115)로 전송하는 기능을 포함하는 스크립트(또는 단말 프로그램)을 포함하여 제공하는 것이 바람직하다.

[0641] 본 발명의 다른 일 실시 방법에 따르면, 상기 인증서 이전부는 상기 매체(2)가 탑재 또는 이탈착되는 고객단말(125)로 제공하는 인증서에 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 통신망을 통해 전송하는 스크립트(또는 단말 프로그램)를 포함하여 제공하는 것이 바람직하다.

[0643] 본 발명의 또다른 일 실시 방법에 따르면, 상기 인증서 이전부는 상기 매체(2)가 탑재 또는 이탈착되는 고객단말(125)로 상기 인증서를 제공하기 전, 또는 상기 고객단말(125)로 상기 인증서를 제공한 후 유효성 진단 전에 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 통신망을 통해 전송하는 스크립트(또는 단말 프로그램)를 상기 고객단말(125)로 제공하는 것이 바람직하다.

[0645] 본 발명에 따르면, 상기 인증서 이전 서버(115)는 상기 인터페이스부(800)와 연계하여 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 수신하는 정보 수신부(850)(또는 정보 수신수단)를 구비하여 이루어지는 것을 특징으로 한다.

[0647] 본 발명의 일 실시 방법에 따라 상기 고객단말(125)로 상기 고객단말(125)에 구비 또는 이탈착되는 M(M>1)개의 구성장치 정보를 확인하여 통신망을 통해 상기 인증서 이전 서버(115)로 전송하는 기능, 상기 인증서 이전 서버(115)로부터 상기 M(M>1)개의 구성장치 정보 중 인증서 검증 대상에 m(1<=m<=M)개의 구성장치 정보를 수신하는 기능, 상기 수신된 m개의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 상기 통신망을 통해 상기 인증서 이전 서버(115)로 전송하는 기능을 포함하는 스크립트(또는 단말 프로그램)가 제공된 경우, 상기 인증서 이전 서버(115)는, 상기 인터페이스부(800)와 연계하여 상기 고객단말(125)에 구비 또는 이탈착되는 M(M>1)개의 구성장치 정보를 수신하는 장치정보 수신부(835)(또는 장치정보 수신수단)와, 상기 M(M>1)개의 구성장치 정보 중 인증서 검증 대상에 m(1<=m<=M)개의 구성장치 정보를 확인하는 장치정보 확인부(840)(또는 장치정보 확인수단)와, 상기 인터페이스부(800)와 연계하여 상기 고객단말(125)로 상기 확인된 m개의 구성장치 정보를 전송하는 장치정보 전송부(845)(또는 장치정보 전송수단)를 더 구비하여 이루어지는 것을 특징으로 하며, 상기 정보 수신부(850)는 상기 인터페이스부(800)와 연계하여 상기 고객단말(125)에 구비 또는 이탈착되는 M(M>1)개의 구성장치 중 상기 설정된 m(1<=m<=M)개의 구성장치에 대응하는 장치고유 정보(1)를 수신하는 것을 특징으로 한다.

[0649] 본 발명의 다른 일 실시 방법에 따라 상기 고객단말(125)로 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하여 통신망을 통해 전송하는 스크립트(또는 단말 프로그램)가 제공된 경우, 상기 정보 수신부(850)는 상기 인터페이스부(800)와 연계하여 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 수신하는 것을 특징으로 한다.

[0651] 본 발명의 실시 방법에 따르면, 상기 장치고유 정보(1)는 상기 인증서가 발급된 매체의 고유정보 또는 상기 매체가 탑재 또는 이탈착되는 단말의 고유 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0653] 예컨대, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0655] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형) 통신장치에 구비된 MAC(Media Access Control) 주소 정보를 포함하여 이루어지는 것이 바람직하다.

[0657] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0659] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체에 구비된 IC칩 일련번호, IC칩 고유정보, IC칩 식별정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0661] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체에 구비되는 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0663] 상기와 같이 고객단말(125)에 구비된 매체(2)로 상기 인증서가 이전되면, 상기 고객단말(125)은 상기 인증서를 최초 실행하여 상기 인증서에 대한 유효성을 인증하는 상기 인증서 진단 모드를 개시하는데, 이를 위해 상기 인증서 이전 서버(115)는 상기 고객단말(125)에서 구비된 상기 인증서와 상호 연동하여 상기 인증서에 대한 유효성을 진단하는 진단부(865)(또는 인증서 진단수단)를 구비하여 이루어지는 것을 특징으로 한다.

[0665] 본 발명의 실시 방법에 따르면, 상기 인증서 진단 모드는, 상기 인증서를 통해 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보(2)를 전송하도록 하고, 상기 인증서를 통해 수신된 하나 이상의 장치고유 정보(2)와 상기 정보 수신부(850)를 통해 수신된 하나 이상의 장치고유 정보(1)을 비교하여 상기 인증서로부터 전송된 장치고유 정보(2)가 유효한지 확인하는 것을 포함하여 이루어지는 것이 바람직하다.

[0667] 본 발명의 실시 방법에 따르면, 상기 장치고유 정보(2)는 상기 인증서가 발급된 매체의 고유정보 또는 상기 매체가 탑재 또는 이탈착되는 단말의 고유 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0669] 예컨대, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0671] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형) 통신장치에 구비된 MAC(Media Access Control) 주소 정보를 포함하여 이루어지는 것이 바람직하다.

[0673] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0675] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체에 구비된 IC칩 일련번호, IC칩 고유정보, IC칩 식별정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0677] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체에 구비되는 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0679] 본 발명에 따르면, 상기 인증서 이전 서버(115)는 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(2)로 이전된 인증서에 대응하는 인증서 정보와, 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보(1)를 연계 처리하여 인증서 관리 D/B(105)에 저장하는 정보 저장부(885)를 구비하여 이루어지는 것을 특징으로 한다.

[0681] 본 발명의 실시 방법에 따르면, 상기 정보 저장부(885)는 상기 진단부(865)의 진단결과 상기 인증서의 유효성이 확인되면, 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(2)로 이전된 상기 인증서 정보와, 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 상기 정보 수신부(850)를 통해 수신된 하나 이상의 하나 이상의 장치고유 정보(1)를 연계 처리하여 인증서 관리 D/B(105)에 저장하는 것이 바람직하며, 이후 상기 인증서 관리 D/B(105)에 저장된 상기 인증서 정보와 하나 이상의 장치고유 정보(1)는 상기 인증서가 불법적으로 이전되어 점유하는 것을 방지하는데 이용되는 것을 특징으로 한다.

[0683] 본 발명의 실시 방법을 따르는 도면8을 참조하면, 상기 인증서 발급 서버(100)는 고객단말(125)에 탑재 또는 이탈착하는 매체(1)에 발급된 인증서를 매체(2)로 이전시, 상기 인증서 이전에 대한 유효성을 확인하기 위해, 상기 인증서 관리 D/B(105)와 연계하여 i개의 인증정보 입력 질의 정보 중 인증서 이전 검증 대상에 포함될 j(1<=j<=i)개의 인증정보 입력 질의 정보를 확인하는 인증정보 확인부(890)(또는 인증정보 확인수단)와, 상기 확인된 j개의 인증정보 입력 질의 정보에 대응하는 j개의 사용자 인증정보(2)를 입력하는 사용자 인증정보 입력 인터페이스를 상기 고객단말(125)로 전송하는 인터페이스 제공부(805)(또는 인터페이스 제공수단)와, 상기 고객단말(125)에서 사용자 인증정보 입력 인터페이스를 통해 상기 j개의 인증정보 입력 질의 정보에 각기 대응하는 j개의 사용자 인증정보(2)를 입력하여 전송하면, 상기 j개의 사용자 인증정보(2)를 수신하는 인증정보 수신부(870)(또는 인증정보 수신수단)와, 상기 저장매체와 연계하여 상기 j개의 인증정보 입력 질의 정보와 매칭되는 j개의 사용자 인증정보(1)를 확인 및 추출하는 인증정보 추출부(895)(또는 인증정보 추출수단)와, 상기 확인 및 추출된 된 사용자 인증정보(1)와 수신된 사용자 인증정보(2)를 비교하여 상기 인증서 이전에 대한 유효성을 인증하는 인증정보 인증부(875)(또는 인증정보 인증수단)을 더 구비하여 이루어지는 것을 특징으로 한다.

[0685] 고객단말(125)에 탑재 또는 이탈착하는 매체(1)에 발급된 인증서를 매체(2)로 이전시, 상기 인증서 이전에 대한 유효성을 확인하기 위해, 상기 인증정보 확인부(890)는 상기 인증서 관리 D/B(105)와 연계하여 i개의 인증정보 입력 질의 정보 중 인증서 이전 검증 대상에 포함될 j(1<=j<=i)개의 인증정보 입력 질의 정보를 확인하는 것을 특징으로 하며, 상기 인터페이스 제공부(805)는 상기 확인된 j개의 인증정보 입력 질의 정보에 대응하는 j개의 사용자 인증정보(2)를 입력하는 사용자 인증정보 입력 인터페이스를 상기 고객단말(125)로 전송하는 것을 특징으로 한다.

[0687] 이후, 상기 고객단말(125)에서 사용자 인증정보 입력 인터페이스를 통해 상기 j개의 인증정보 입력 질의 정보에 각기 대응하는 j개의 사용자 인증정보(2)를 입력하여 전송하면, 상기 인증정보 수신부(870)는 상기 고객단말(125)로부터 상기 j개의 사용자 인증정보(2)를 수신하는 것을 특징으로 한다.

[0689] 본 발명의 실시 방법에 따르면, 상기 사용자 인증정보(2)가 상기 매체(1)로 발급된 인증서를 통해 가공(예컨대, 암호화 내지 전자서명 첨부)되고, 상기 인증서 정보가 첨부되어 수신되는 경우, 상기 인증정보 수신부(870)는 상기 고객단말(125)로부터 상기 장치고유 정보(2)를 더 포함하여 수신하는 것이 바람지하며, 이 경우 상기 정보 수신부(810)는 상기 수신된 장치고유 정보(2)를 통한 장치고유 정보 유효성 인증을 더 수행하는 것이 바람직하다.

[0691] 상기 인증정보 추출부(895)는 상기 저장매체와 연계하여 상기 고객단말(125)로 제공된 j개의 인증정보 입력 질의 정보와 매칭되는 j개의 사용자 인증정보(1)를 확인 및 추출하는 것을 특징으로 한다.

[0693] 상기 인증정보 수신부(870)를 통해 j개의 사용자 인증정보(2)가 수신되고, 상기 인증정보 추출부(895)를 통해 j개의 사용자 인증정보(1)가 추출 및 확인되면, 상기 인증정보 인증부(875)는 상기 확인 및 추출된 된 사용자 인증정보(1)와 수신된 사용자 인증정보(2)를 비교하여 상기 인증서 이전에 대한 유효성을 인증하는 것을 특징으로 한다.

[0695] 도면9a와 도면9b는 본 발명의 실시 방법에 따라 인증서를 이전 요청하는 과정을 도시한 도면이다.

[0697] 보다 상세하게 본 도면9a와 도면9b는 상기 도면8에 도시된 인증서 이전 시스템을 통해 상기 고객단말(125)에서 인증서 이전 요청시, 상기 인증서 이전 서버(115)에서 상기 인증서가 불법적으로 이전되어 점유되는 것을 방지하기 위해 상기 인증서 이전 요청 정보에 대한 인증서 기반 유효성 검증과 상기 매체(1)이 탑재 또는 이탈착되는 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치에 대한 장치고유 정보 기반 유효성 인증을 수행하고(도면9a), 상기 도면2에 도시된 인증서 발급 시스템을 통해 등록된 인증서 이전을 위한 사용자 인증정보 인증을 수행하는(돋9b) 과정에 대한 것으로서, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 본 도면9a와 도면9b를 참조 및/또는 변형하여 상기 인증서를 이전 요청하는 과정에 대한 다양한 실시 방법을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 실시 방법을 모두 포함하며, 본 도면9a와 도면9b에 도시된 실시 방법에 의해 한정되지 아니한다.

[0699] 이하, 본 도면9a와 도면9b에서 상기 도면8에 도시된 고객단말(125)을 편의상 "단말"이라고 하고, 상기 도면8에 도시된 인증서 이전 서버(115)를 편의상 "서버"라고 한다.

[0701] 도면9a와 도면9b를 참조하면, 상기 단말은 통신망을 통해 상기 서버에 접속하고, 상기 서버로 상기 인증서를 이전하도록 요청하며(900), 이에 대응하여 상기 서버는 상기 인증서를 상기 고객단말(125)로 이전하기 위한 인증서 이전 인터페이스를 추출(또는 생성)하여 상기 단말로 제공한다(905).

[0703] 이후, 상기 단말은 상기 인증서 이전 인터페이스를 통해 인증서 이전 요청 정보를 입력(또는 선택)하고(910), 상기 입력(또는 선택)된 인증서 이전 요청 정보를 상기 매체(1)로 발급된 인증서를 통해 가공(예컨대, 암호화 내지 전자서명 첨부)하고, 상기 인증서 정보를 첨부하여 상기 통신망을 통해 상기 서버로 전송한다(915).

[0705] 여기서, 상기 인증서 이전 요청 정보는 상기 단말에 탑재 또는 이탈착하는 매체(2)로 상기 인증서를 이전하도록 요청하는 고객정보와, 상기 단말에 탑재 또는 이탈착되어 상기 인증서가 이전될 매체(2) 정보와, 상기 매체(2)

가 탑재 또는 이탈착되는 단말에 대한 운영체제(또는 플랫폼) 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0707] 상기 인증서 이전 요청 정보에 포함된 상기 고객정보는, 상기 인증서를 이전받는 상기 고객의 회원ID정보와 비밀번호 정보를 포함하는 고객 회원정보, 또는 상기 고객의 성명, 주민등록번호, 주소, 연락처 등을 적어도 하나 이상 포함하는 고객 개인정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0709] 상기 인증서 이전 요청 정보에 포함된 상기 매체(2) 정보는, 상기 단말에 탑재 또는 이탈착되는 매체 중 상기 인증서가 이전되어 저장되는 매체를 확인(또는 식별)하는 정보를 포함하여 이루어지는 것이 바람직하다.

[0711] 본 발명의 실시 방법에 따르면, 상기 매체(2) 정보는 상기 단말에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체를 포함하여 이루어지는 것이 바람직하다.

[0713] 또는, 상기 매체(2) 정보는 상기 단말에 이탈착되는(예컨대, 플로피디스크 드라이브에 삽입되는) 플로피디스크 매체를 포함하여 이루어지는 것이 바람직하다.

[0715] 또는, 상기 매체(2) 정보는 상기 단말에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체를 포함하여 이루어지는 것이 바람직하다.

[0717] 또는, 상기 매체(2) 정보는 상기 단말에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체를 포함하여 이루어지는 것이 바람직하다.

[0719] 또는, 상기 매체(2) 정보는 상기 단말에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체를 포함하여 이루어지는 것이 바람직하다.

[0721] 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 상술된 매체(2) 이외에 상기 단말에 탑재 또는 이탈착되는 다양한 형태의 매체를 유추할 수 있을 것이며, 본 발명은 상기 유추되는 모든 매체(2)를 포함하여 이루어지는 것을 특징으로 한다.

[0723] 상기 인증서 이전 요청 정보에 포함된 상기 운영체제(또는 플랫폼) 정보는, 상기 인증서가 이전되는 매체(2)이 탑재 또는 이탈착되는 단말의 운영체제(또는 플랫폼)을 식별 내지 확인하는 정보로서, 상기 인증서에 대응하는 프로그램 코드가 실행되는 운영체제(또는 플랫폼)을 확인하는 것이 바람직하다.

[0725] 이후, 상기 서버는 통신망을 통해 상기 인증서 이전 요청 정보를 수신하고, 상기 인증서 이전 요청 정보에 첨부된 상기 인증서 정보를 통해 상기 인증서를 발급한 인증기관을 확인하고, 상기 인증기관에 구비된 인증서버와 연계하여(또는 상기 인증서 정보에 포함된 인증서 사본을 판독하여) 상기 인증서 이전 요청 정보를 복호화 내지 전자서명 검증을 처리함으로써, 상기 인증서 이전 요청 정보에 대한 인증서 기반 유효성을 검증한다(920).

[0727] 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 상기 서버가 상기 인증서를 발급한 인증기관에 구비된 인증서버와 연계하여(또는 상기 인증서 정보에 포함된 인증서 사본을 판독하여) 상기 인증서 이전 요청 정보

에 첨부된 인증서 정보를 기반으로 상기 인증서 이전 요청 정보에 대한 인증서 기반 유효성을 검증하는 기술적 특징을 기 숙지하고 있을 것이므로, 이에 대한 상세한 설명은 편의상 생략하기로 한다.

[0729] 만약 상기 인증서 기반 유효성이 검증되지 않으면(925), 상기 서버는 인증서 기반 유효성 오류 정보를 생성하여 상기 단말로 전송하고(930), 상기 인증서 이전 과정을 종료한다.

[0731] 반면 상기 인증서 기반 유효성이 검증되면(925), 상기 서버는 인증서 기반 유효성이 검증되어 복호화된 인증서 이전 요청 정보로부터 상기 인증서 정보와 하나 이상의 장치고유 정보(2)를 추출하고(935), 상기 추출된 인증서 정보를 기반으로 상기 도면2에 도시된 인증서 발급 시스템을 통해 상기 매체(1)로 발급된 인증서 정보와 장치고유 정보(1)를 연계하여 저장하는 인증서 관리 D/B(105)와 연계하여 상기 인증서 정보와 연계된 하나 이상의 장치고유 정보(1)를 확인한다(940).

[0733] 만약 상기 인증서 정보와 연계된 하나 이상의 장치고유 정보(1)가 확인되면(945), 상기 서버는 상기 확인된 장치고유 정보(1)와 상기 추출된 장치고유 정보(2)를 비교하여 상기 인증서 이전 요청 정보에 대한 장치고유 정보 기반 유효성을 확인한다(950).

[0735] 만약 상기 장치고유 정보 기반 유효성이 확인되지 않으면(955), 상기 서버는 장치고유 정보 기반 유효성 오류 정보를 생성하여 상기 단말로 전송하고(960), 상기 인증서 이전 과정을 종료한다.

[0737] 반면 상기 장치고유 정보 기반 유효성이 확인되면(955), 상기 서버는 상기 인증서 기반 유효성 검증 결과와 장치고유 정보 기반 유효성 확인 결과를 기반으로 상기 매체(1)에서 매체(2)로 상기 인증서를 이전하는 과정을 수행한다.

[0739] 또한, 고객단말(125)에 탑재 또는 이탈착하는 매체(1)에 발급된 인증서를 매체(2)로 이전시, 상기 인증서 이전에 대한 유효성을 확인하기 위해, 상기 인증서 관리 D/B(105)와 연계하여 i개의 인증정보 입력 질의 정보 중 인증서 이전 검증 대상에 포함될 j(1<=j<=i)개의 인증정보 입력 질의 정보를 확인하고(965), 상기 확인된 j개의 인증정보 입력 질의 정보에 대응하는 j개의 사용자 인증정보(2)를 입력하는 사용자 인증정보 입력 인터페이스를 상기 단말로 제공한다(970).

[0741] 이후, 상기 단말은 사용자 인증정보 입력 인터페이스를 통해 상기 j개의 인증정보 입력 질의 정보에 각기 대응하는 j개의 사용자 인증정보(2)가 입력되는지 확인하며(975), 만약 상기 사용자 인증정보 입력 인터페이스를 통해 상기 j개의 사용자 인증정보(2)가 입력되면(980), 상기 단말은 상기 서버로 상기 입력된 j개의 사용자 인증정보(2)를 전송한다(985).

[0743] 본 발명의 실시 방법에 따르면, 상기 사용자 인증정보(2)가 상기 매체(1)로 발급된 인증서를 통해 가공(예컨대, 암호화 내지 전자서명 첨부)되고, 상기 인증서 정보가 첨부되어 수신되는 경우, 상기 서버는 상기 고객단말(125)로부터 상기 장치고유 정보(2)를 더 포함하여 수신하는 것이 바람지하며, 이 경우 서버는 상기 수신된 장치고유 정보(2)를 통한 장치고유 정보 유효성 인증을 더 수행하는 것이 바람직하다.

[0745] 이후, 상기 서버는 상기 저장매체와 연계하여 상기 고객단말(125)로 제공된 j개의 인증정보 입력 질의 정보와 매칭되는 j개의 사용자 인증정보(1)를 확인 및 추출하고(990), 상기 확인 및 추출된 된 사용자 인증정보(1)와 수신된 사용자 인증정보(2)를 비교하여 상기 인증서 이전에 대한 유효성을 인증한다(992).

[0747] 만약 상기 인증서 이전 유효성이 확인되지 않으면(994), 상기 서버는 인증서 이전 유효성 오류 정보를 생성하여 상기 단말로 전송하고(996), 상기 인증서 이전 과정을 종료한다.

[0749] 반면 상기 인증서 이전 유효성이 확인되면(994), 상기 서버는 상기 매체(1)에서 매체(2)로 상기 인증서를 이전하는 과정을 수행한다.

[0751] 도면10은 본 발명의 일 실시 방법에 따라 인증서를 이전하는 과정을 도시한 도면이다.

[0753] 보다 상세하게 본 도면10은 상기 도면8에 도시된 인증서 이전 시스템 상의 고객단말(125)에서 인증서 이전을 요청함에 의해 상기 도면9a와 도면9b에 도시된 인증서 이전 요청 과정을 통해 상기 인증서 이전 요청에 대한 인증서 기반 유효성이 검증되고, 상기 장치고유 정보 기반 유효성이 확인되면, 상기 도면8에 도시된 인증서 이전 서버(115)에서 상기 인증서를 매체(1)에서 매체(2)로 이전하고, 이후에 인증서가 불법적으로 이전되어 점유되는 것을 방지하기 위해 상기 매체(2)가 탑재 또는 이탈착되는 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치 중 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하는 과정에 대한 것으로서, 구체적으로 상기 고객단말(125)에 구비 또는 이탈착되는 M(M>1)개의 구성장치 정보를 선 확인 후 상기 인증서 이전 서버(115)에서 상기 M(M>1)개의 구성장치 중 인증서 검증 대상에 m(1<=m<=M)개의 구성장치를 확인한 후, 상기 고객단말(125)로부터 상기 확인된 m개의 장치고유 정보(1)를 수신한 후, 상기 이전된 인증서를 상기 고객단말(125)에 탑재 또는 이탈착하는 매체(2)로 이전하는 실시 방법을 도시한 도면이다.

[0755] 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 본 도면10을 참조 및/또는 변형하여 상기 인증서를 이전하는 과정에 대한 다양한 실시 방법을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 실시 방법을 모두 포함하며, 본 도면10에 도시된 실시 방법에 의해 한정되지 아니한다.

[0757] 이하, 본 도면10에서 상기 도면8에 도시된 고객단말(125)을 편의상 "단말"이라고 하고, 상기 도면8에 도시된 인증서 이전 서버(115)를 편의상 "서버"라고 한다.

[0759] 도면10을 참조하면, 상기 도면8에 도시된 인증서 이전 시스템 상의 단말에서 인증서 이전을 요청함에 의해 상기 도면9a와 도면9b에 도시된 인증서 이전 요청 과정을 통해 상기 인증서 이전 요청에 대한 인증서 기반 유효성이 검증되고, 상기 장치고유 정보 기반 유효성이 확인되면, 상기 서버는 통신망을 통해 상기 도면2에 도시된 인증서 발급 시스템을 통해 매체(1)에 발급된 인증서를 무효화 처리하여 폐기한다(1000).

[0761] 만약 상기 매체(1)에 발급된 인증서를 무효화 처리되어 폐기되면(1005), 상기 서버는 상기 인증서 D/B(880)로부터 상기 인증서 이전 요청 정보와 매칭되는 인증서를 추출(또는 동적 생성)한다(1010).

[0763] 본 발명의 일 실시 방법에 따르면, 상기 인증서 D/B(880)는 상기 단말에 구비된 운영체제(또는 단말 플랫폼)에서 동작할 수 있는 인증서 프로그램 파일과 인증서 데이터를 저장하는 것을 특징으로 하며, 상기 단말로부터 상기 인증서 이전 요청 정보가 수신되는 경우, 상기 서버는 상기 인증서 D/B(880)로부터 상기 인증서 이전 요청 정보와 매칭되는 인증서 프로그램 파일과 인증서 데이터를 포함하는 인증서를 추출하는 것이 바람직하다.

[0765] 본 발명의 다른 일 실시 방법에 따르면, 상기 인증서 D/B(880)는 상기 단말에 구비된 운영체제(또는 단말 플랫폼)에서 동작할 수 있는 인증서 프로그램 소스와 인증서 데이터를 저장하는 것을 특징으로 하며, 상기 단말로부터 상기 인증서 이전 요청 정보가 수신되는 경우, 상기 서버는 상기 인증서 D/B(880)로부터 상기 인증서 이전 요청 정보와 매칭되는 인증서 프로그램 소스와 인증서 데이터를 추출하고, 상기 추출된 인증서 프로그램 소스를

컴파일(Compile)하여 상기 매체(2)로 이전할 인증서를 동적 생성하는 것이 바람직하다.

[0767] 또한, 상기 서버는 상기 추출(또는 동적 생성)된 상기 인증서를 상기 통신망을 통해 상기 단말로 제공하여 상기 단말에 탑재 또는 이탈착되는 매체(2)에 저장하여 상기 인증서를 이전한다(1015).

[0769] 만약 상기 인증서가 상기 매체(2)로 이전되면(1020), 상기 단말은 상기 단말에 구비 또는 이탈착되는 M(M>1)개의 구성장치 정보를 확인하여 통신망을 통해 상기 서버로 전송한다(1025).

[0771] 이후, 상기 서버는 상기 수신된 M(M>1)개의 구성장치 정보 중 인증서 검증 대상에 m(1<=m<=M)개의 구성장치 정보를 확인한다(1030).

[0773] 만약 상기 인증서 검증 대상에 m개의 구성장치 정보가 확인되면(1035), 상기 서버는 통신망을 통해 상기 단말로 상기 확인된 m개의 구성장치 정보를 전송하고(1040), 이에 대응하여 상기 단말은 상기 m개의 구성장치에 대응하는 m개의 장치고유 정보(1)를 확인하여 통신망을 통해 상기 서버로 전송한다(1045).

[0775] 본 발명의 실시 방법에 따르면, 상기 장치고유 정보(1)는 상기 인증서가 발급된 매체의 고유정보 또는 상기 매체가 탑재 또는 이탈착되는 단말의 고유 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0777] 예컨대, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0779] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형) 통신장치에 구비된 MAC(Media Access Control) 주소 정보를 포함하여 이루어지는 것이 바람직하다.

[0781] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0783] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체에 구비된 IC칩 일련번호, IC칩 고유정보, IC칩 식별정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0785] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체에 구비되는 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0787] 도면11은 본 발명의 다른 일 실시 방법에 따라 인증서를 이전하는 과정을 도시한 도면이다.

[0789] 보다 상세하게 본 도면11은 상기 도면8에 도시된 인증서 이전 시스템 상의 고객단말(125)에서 인증서 이전을 요

청함에 의해 상기 도면9a와 도면9b에 도시된 인증서 이전 요청 과정을 통해 상기 인증서 이전 요청에 대한 인증서 기반 유효성이 검증되고, 상기 장치고유 정보 기반 유효성이 확인되면, 상기 도면8에 도시된 인증서 이전 서버(115)에서 상기 인증서를 매체(1)에서 매체(2)로 이전하고, 이후에 인증서가 불법적으로 이전되어 점유되는 것을 방지하기 위해 상기 매체(2)가 탑재 또는 이탈착되는 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치 중 하나 이상의 구성장치에 대응하는 장치고유 정보(1)를 확인하는 과정에 대한 것으로서, 구체적으로 상기 고객단말(125)에 구비 또는 이탈착되는 복수개의 구성장치 정보 중 기 설정된 하나 이상의 장치고유 정보(1)를 수신한 후, 상기 이전된 인증서를 상기 고객단말(125)에 탑재 또는 이탈착하는 매체(2)로 이전하는 실시 방법을 도시한 도면이다.

[0791] 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 본 도면11을 참조 및/또는 변형하여 상기 인증서를 이전하는 과정에 대한 다양한 실시 방법을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 실시 방법을 모두 포함하며, 본 도면11에 도시된 실시 방법에 의해 한정되지 아니한다.

[0793] 이하, 본 도면11에서 상기 도면8에 도시된 고객단말(125)을 편의상 "단말"이라고 하고, 상기 도면8에 도시된 인증서 이전 서버(115)를 편의상 "서버"라고 한다.

[0795] 도면11을 참조하면, 상기 도면8에 도시된 인증서 이전 시스템 상의 단말에서 인증서 이전을 요청함에 의해 상기 도면9a와 도면9b에 도시된 인증서 이전 요청 과정을 통해 상기 인증서 이전 요청에 대한 인증서 기반 유효성이 검증되고, 상기 장치고유 정보 기반 유효성이 확인되면, 상기 서버는 통신망을 통해 상기 도면2에 도시된 인증서 발급 시스템을 통해 매체(1)에 발급된 인증서를 무효화 처리하여 폐기한다(1100).

[0797] 만약 상기 매체(1)에 발급된 인증서를 무효화 처리되어 폐기되면(1105), 상기 서버는 상기 인증서 D/B(880)로부터 상기 인증서 이전 요청 정보와 매칭되는 인증서를 추출(또는 동적 생성)한다(1110).

[0799] 본 발명의 일 실시 방법에 따르면, 상기 인증서 D/B(880)는 상기 단말에 구비된 운영체제(또는 단말 플랫폼)에서 동작할 수 있는 인증서 프로그램 파일과 인증서 데이터를 저장하는 것을 특징으로 하며, 상기 단말로부터 상기 인증서 이전 요청 정보가 수신되는 경우, 상기 서버는 상기 인증서 D/B(880)로부터 상기 인증서 이전 요청 정보와 매칭되는 인증서 프로그램 파일과 인증서 데이터를 포함하는 인증서를 추출하는 것이 바람직하다.

[0801] 본 발명의 다른 일 실시 방법에 따르면, 상기 인증서 D/B(880)는 상기 단말에 구비된 운영체제(또는 단말 플랫폼)에서 동작할 수 있는 인증서 프로그램 소스와 인증서 데이터를 저장하는 것을 특징으로 하며, 상기 단말로부터 상기 인증서 이전 요청 정보가 수신되는 경우, 상기 서버는 상기 인증서 D/B(880)로부터 상기 인증서 이전 요청 정보와 매칭되는 인증서 프로그램 소스와 인증서 데이터를 추출하고, 상기 추출된 인증서 프로그램 소스를 컴파일(Compile)하여 상기 매체(2)로 이전할 인증서를 동적 생성하는 것이 바람직하다.

[0803] 또한, 상기 서버는 상기 추출(또는 동적 생성)된 상기 인증서를 상기 통신망을 통해 상기 단말로 제공하여 상기 단말에 탑재 또는 이탈착되는 매체(2)에 저장하여 상기 인증서를 이전한다(1115).

[0805] 만약 상기 인증서가 상기 매체(2)로 이전되면(1120), 상기 단말은 상기 설정된 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보(1)를 확인하여 통신망을 통해 상기 서버로 전송한다(1125).

[0807] 본 발명의 실시 방법에 따르면, 상기 장치고유 정보(1)는 상기 인증서가 발급된 매체의 고유정보 또는 상기 매체가 탑재 또는 이탈착되는 단말의 고유 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0809] 예컨대, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0811] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형) 통신장치에 구비된 MAC(Media Access Control) 주소 정보를 포함하여 이루어지는 것이 바람직하다.

[0813] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0815] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체에 구비된 IC칩 일련번호, IC칩 고유정보, IC칩 식별정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0817] 또는, 상기 장치고유 정보(1)는 상기 고객단말(125)에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체에 구비되는 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0819] 도면12는 본 발명의 실시 방법에 따라 이전된 인증서 검증 과정을 도시한 도면이다.

[0821] 보다 상세하게 본 도면12는 상기 도면10 또는 도면11에 도시된 인증서 이전 과정을 통해 상기 고객단말(125)에 탑재 또는 이탈착되는 매체(2)로 인증서가 이전되고, 상기 고객단말(125)로부터 하나 이상의 장치고유 정보(1)가 수신되면, 상기 매체(2)로 이전된 인증서가 상기 인증서의 불법 이전 및 점유 방지를 위한 기능이 정상적으로 동작하는지 검증하는 과정에 대한 것으로서, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 본 도면12를 참조 및/또는 변형하여 상기 이전된 인증서 검증 과정에 대한 다양한 실시 방법을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 실시 방법을 모두 포함하며, 본 도면12에 도시된 실시 방법에 의해 한정되지 아니한다.

[0823] 이하, 본 도면12에서 상기 도면8에 도시된 고객단말(125)을 편의상 "단말"이라고 하고, 상기 도면8에 도시된 인증서 이전 서버(115)를 편의상 "서버"라고 한다.

[0825] 도면12를 참조하면, 상기 도면10 또는 도면11에 도시된 인증서 이전 과정을 통해 상기 단말에 탑재 또는 이탈착되는 매체(2)로 인증서가 이전되고, 상기 단말로부터 하나 이상의 장치고유 정보(1)가 수신되면, 상기 서버는 상기 단말에 탑재 또는 이탈착되는 매체(2)로 상기 인증서의 이전 여부를 확인한다(1200).

[0827] 만약 상기 단말에 탑재 또는 이탈착되는 매체(2)로 상기 인증서가 이전되면(1205), 상기 단말은 상기 인증서를 실행하여 상기 인증서에 대한 진단 모드를 개시하고(1210), 이에 대응하여 상기 단말은 상기 인증서를 통해 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보(2)를 전송하도록 하고(1215), 이에 대응하여 상기 서버는 상기 수신된 하나 이상의 장

치고유 정보(2)를 판독하여 상기 인증서에 대한 유효성을 확인한다(1220)

[0829] 본 발명의 실시 방법에 따르면, 상기 인증서에 대한 유효성을 확인은, 상기 인증서를 통해 상기 고객단말(125)에 구비 또는 이탈착되는 복수의 구성장치 중 기 설정된 하나 이상의 구성장치에 대응하는 하나 이상의 장치고유 정보(2)를 전송하도록 하고, 상기 인증서를 통해 수신된 하나 이상의 장치고유 정보(2)와 상기 수신된 하나 이상의 장치고유 정보(1)을 비교하여 상기 인증서로부터 전송된 장치고유 정보(2)가 유효한지 확인하는 것을 포함하여 이루어지는 것이 바람직하다.

[0831] 본 발명의 실시 방법에 따르면, 상기 장치고유 정보(2)는 상기 인증서가 발급된 매체의 고유정보 또는 상기 매체가 탑재 또는 이탈착되는 단말의 고유 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0833] 예컨대, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형, 또는 네트워크를 통해 마운트되는) 하드디스크 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0835] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, 내장형) 또는 이탈착되는(예컨대, 외장형) 통신장치에 구비된 MAC(Media Access Control) 주소 정보를 포함하여 이루어지는 것이 바람직하다.

[0837] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, USB 단자를 통해 PCB 상에 탑재되는) 또는 이탈착되는(예컨대, USB 포트에 연결되는) USB 매체에 구비된 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0839] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, IC카드 슬롯을 이용하는) 또는 이탈착되는(예컨대, 접촉식 IC카드 리더, 또는 비접촉식 IC카드 리더를 통해 연결되는) IC카드 매체에 구비된 IC칩 일련번호, IC칩 고유정보, IC칩 식별정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0841] 또는, 상기 장치고유 정보(2)는 상기 고객단말(125)에 탑재(예컨대, 카드 슬롯을 삽입, 또는 PCB 상에 실장되는) 또는 이탈착되는(예컨대, 통신포트를 통해 연결되는 연결되는) 하드웨어 보안 모듈(Hardware Security Module; HSM) 매체에 구비되는 장치일련번호 정보, 고유번호 정보, 식별코드 정보를 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0843] 만약 상기 인증서에 대한 유효성이 확인되지 않으면(1225), 상기 서버는 인증서 진단 오류 정보를 생성하여 상기 통신망을 통해 상기 단말로 전송한다(1230).

[0845] 반면 상기 인증서에 대한 유효성이 확인되면(1225), 상기 서버는 상기 단말에 탑재된 인증서에 대응하는 인증서 정보와, 상기 수신된 하나 이상의 하나 이상의 장치고유 정보(1)를 연계 처리하여 인증서 관리 D/B(105)에 저장하며(1235), 이후 상기 인증서 관리 D/B(105)에 저장된 상기 인증서 정보와 하나 이상의 장치고유 정보(1)는 상기 인증서가 불법적으로 이전되어 점유하는 것을 방지하는데 이용된다.

부호의 설명

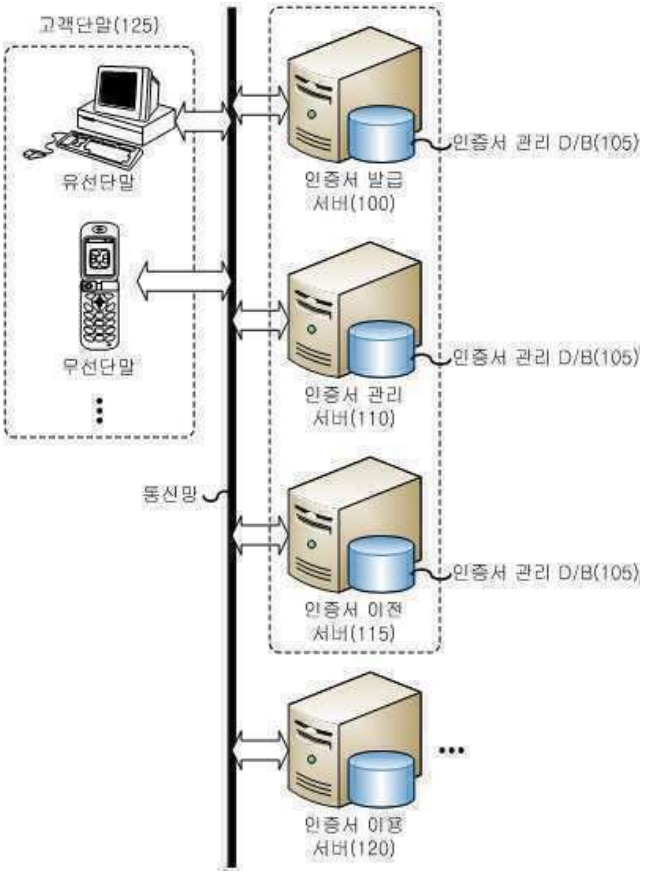
[0847] 100 : 인증서 발급 서버 105 : 인증서 관리 D/B

110 : 인증서 관리 서버 115 : 인즈엇 이전 서버

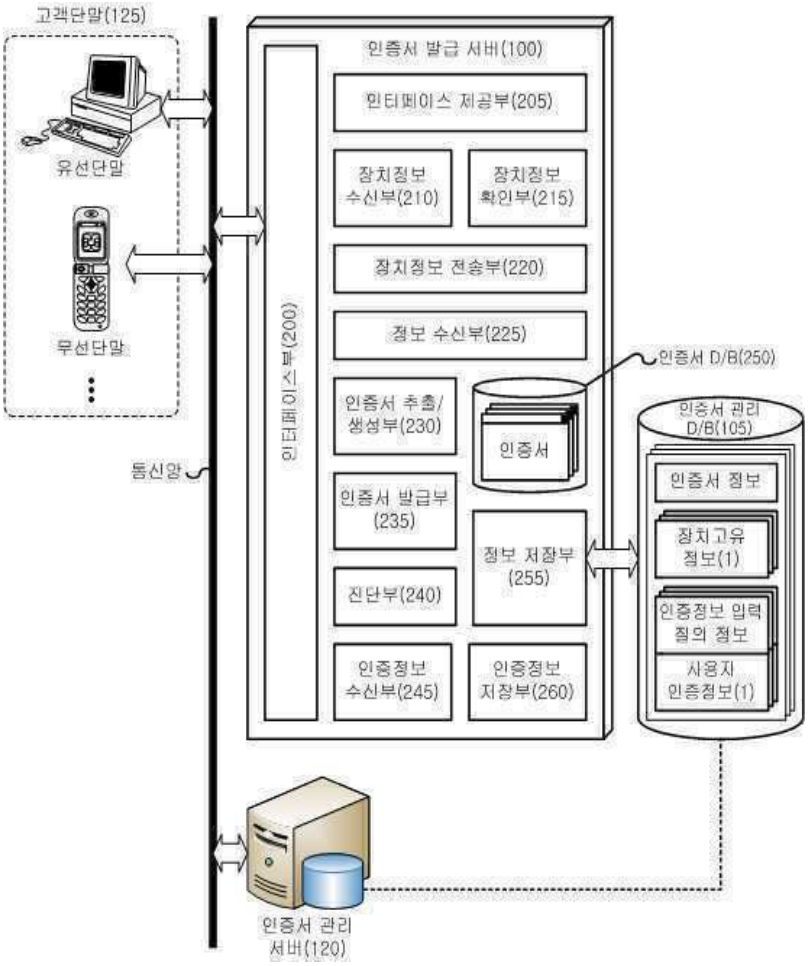
120 : 인증서 이용 서버 125 : 고객단말

도면

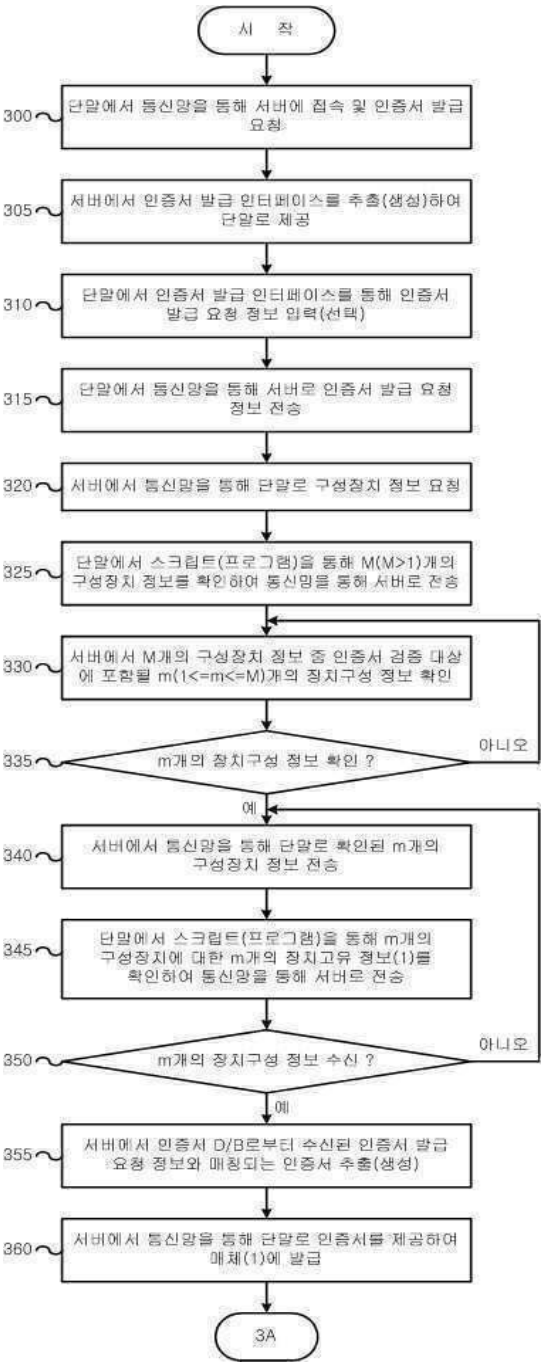
도면1



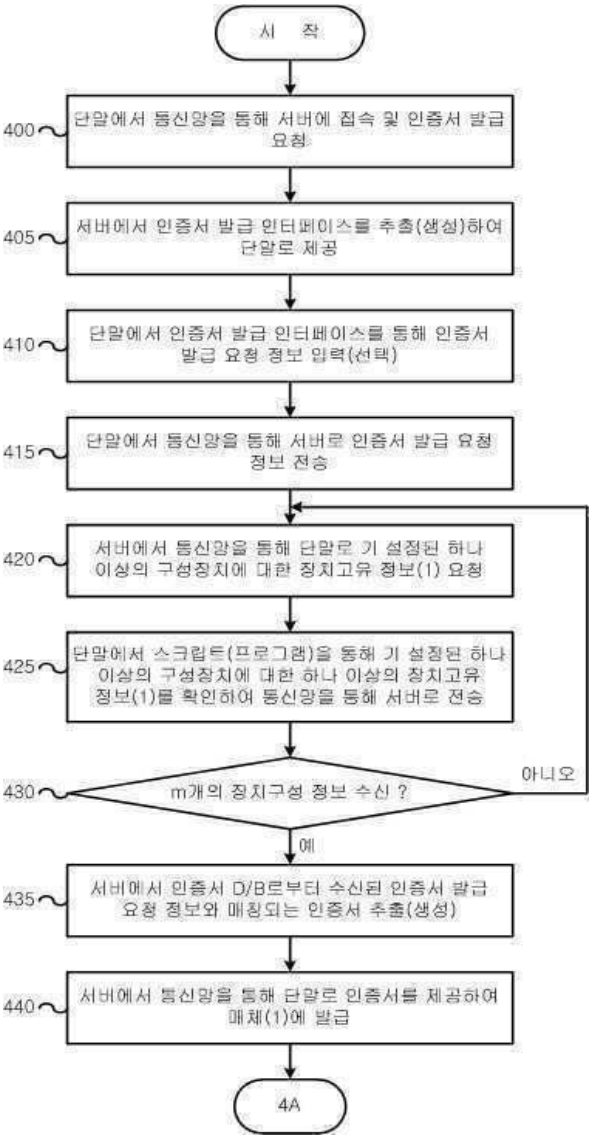
도면2


고객단말(125)
유선단말
무선단말
통신망
인증서 발급 서버(100)
인터페이스 제공부(205)
장치정보 수신부(210)
장치정보 확인부(215)
장치정보 전송부(220)
정보 수신부(225)
인증서 추출/생성부(230)
인증서 발급부(235)
진단부(240)
인증정보 수신부(245)
인증정보 저장부(260)
정보 저장부(255)
인터페이스부(200)
인증서
인증서 D/B(250)
인증서 관리 D/B(105)
인증서 정보
장치고유 정보(1)
인증정보 입력 질의 정보
사용자 인증정보(1)
인증서 관리 서버(120)

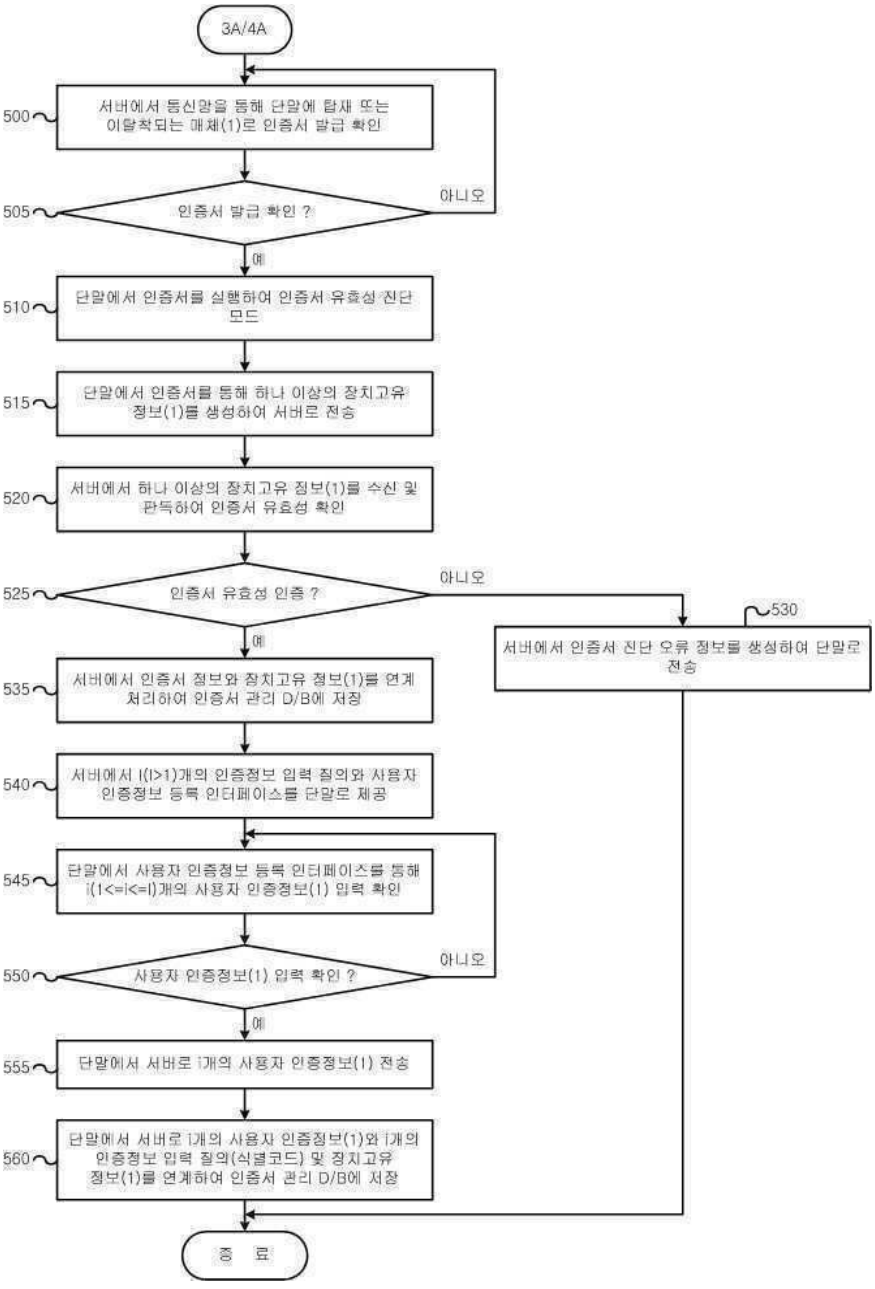
도면3


시 작
300
단말에서 통신망을 통해 서버에 접속 및 인증서 발급 요청
305
서버에서 인증서 발급 인터페이스를 추출(생성)하여 단말로 제공
310
단말에서 인증서 발급 인터페이스를 통해 인증서 발급 요청 정보 입력(선택)
315
단말에서 통신망을 통해 서버로 인증서 발급 요청 정보 전송
320
서버에서 통신망을 통해 단말로 구성장치 정보 요청
325
단말에서 스크립트(프로그램)을 통해 M(M>1)개의 구성장치 정보를 확인하여 통신망을 통해 서버로 전송
330
서버에서 M개의 구성장치 정보 중 인증서 검증 대상에 포함될 m(1<=m<=M)개의 장치구성 정보 확인
335
m개의 장치구성 정보 확인 ?
아니오
예
340
서버에서 통신망을 통해 단말로 확인된 m개의 구성장치 정보 전송
345
단말에서 스크립트(프로그램)을 통해 m개의 구성장치에 대한 m개의 장치고유 정보(1)를 확인하여 통신망을 통해 서버로 전송
350
m개의 장치구성 정보 수신 ?
아니오
예
355
서버에서 인증서 D/B로부터 수신된 인증서 발급 요청 정보와 매칭되는 인증서 추출(생성)
360
서버에서 통신망을 통해 단말로 인증서를 제공하여 매체(1)에 발급
3A

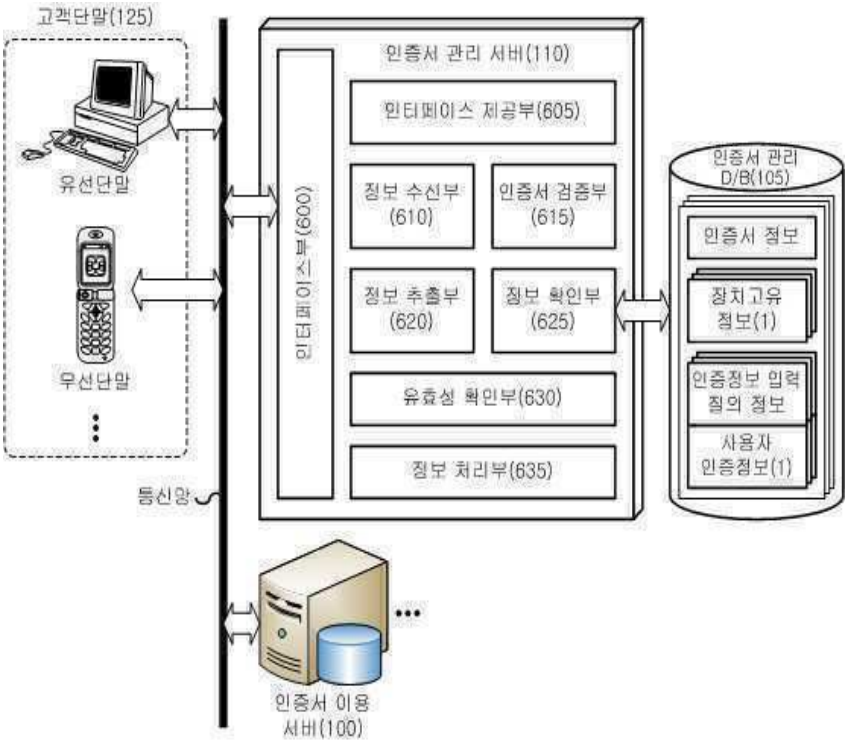
도면4


시 작
400
단말에서 통신망을 통해 서버에 접속 및 인증서 발급 요청
405
서버에서 인증서 발급 인터페이스를 추출(생성)하여 단말로 제공
410
단말에서 인증서 발급 인터페이스를 통해 인증서 발급 요청 정보 입력(선택)
415
단말에서 통신망을 통해 서버로 인증서 발급 요청 정보 전송
420
서버에서 통신망을 통해 단말로 기 설정된 하나 이상의 구성장치에 대한 장치고유 정보(1) 요청
425
단말에서 스크립트(프로그램)을 통해 기 설정된 하나 이상의 구성장치에 대한 하나 이상의 장치고유 정보(1)를 확인하여 통신망을 통해 서버로 전송
430
m개의 장치구성 정보 수신 ?
아니오
예
435
서버에서 인증서 D/B로부터 수신된 인증서 발급 요청 정보와 매칭되는 인증서 추출(생성)
440
서버에서 통신망을 통해 단말로 인증서를 제공하여 매체(1)에 발급
4A

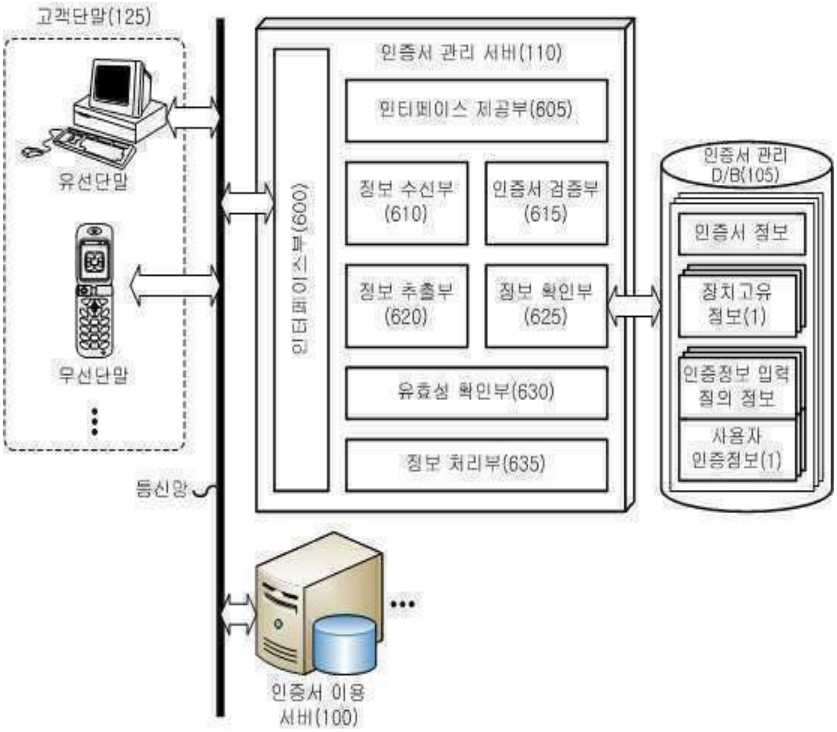
도면5


3A/4A
500
서버에서 동신망을 통해 단말에 탑재 또는 이탈착되는 매체(1)로 인증서 발급 확인
505
인증서 발급 확인 ?
아니오
예
510
단말에서 인증서를 실행하여 인증서 유효성 진단 모드
515
단말에서 인증서를 통해 하나 이상의 장치고유 정보(1)를 생성하여 서버로 전송
520
서버에서 하나 이상의 장치고유 정보(1)를 수신 및 판독하여 인증서 유효성 확인
525
인증서 유효성 인증 ?
아니오
예
530
서버에서 인증서 진단 오류 정보를 생성하여 단말로 전송
535
서버에서 인증서 정보와 장치고유 정보(1)를 연계 처리하여 인증서 관리 D/B에 저장
540
서버에서 I(I>1)개의 인증정보 입력 질의와 사용자 인증정보 등록 인터페이스를 단말로 제공
545
단말에서 사용자 인증정보 등록 인터페이스를 통해 i(1<=i<=I)개의 사용자 인증정보(1) 입력 확인
550
사용자 인증정보(1) 입력 확인 ?
아니오
예
555
단말에서 서버로 i개의 사용자 인증정보(1) 전송
560
단말에서 서버로 i개의 사용자 인증정보(1)와 i개의 인증정보 입력 질의(식별코드) 및 장치고유 정보(1)를 연계하여 인증서 관리 D/B에 저장
종 료

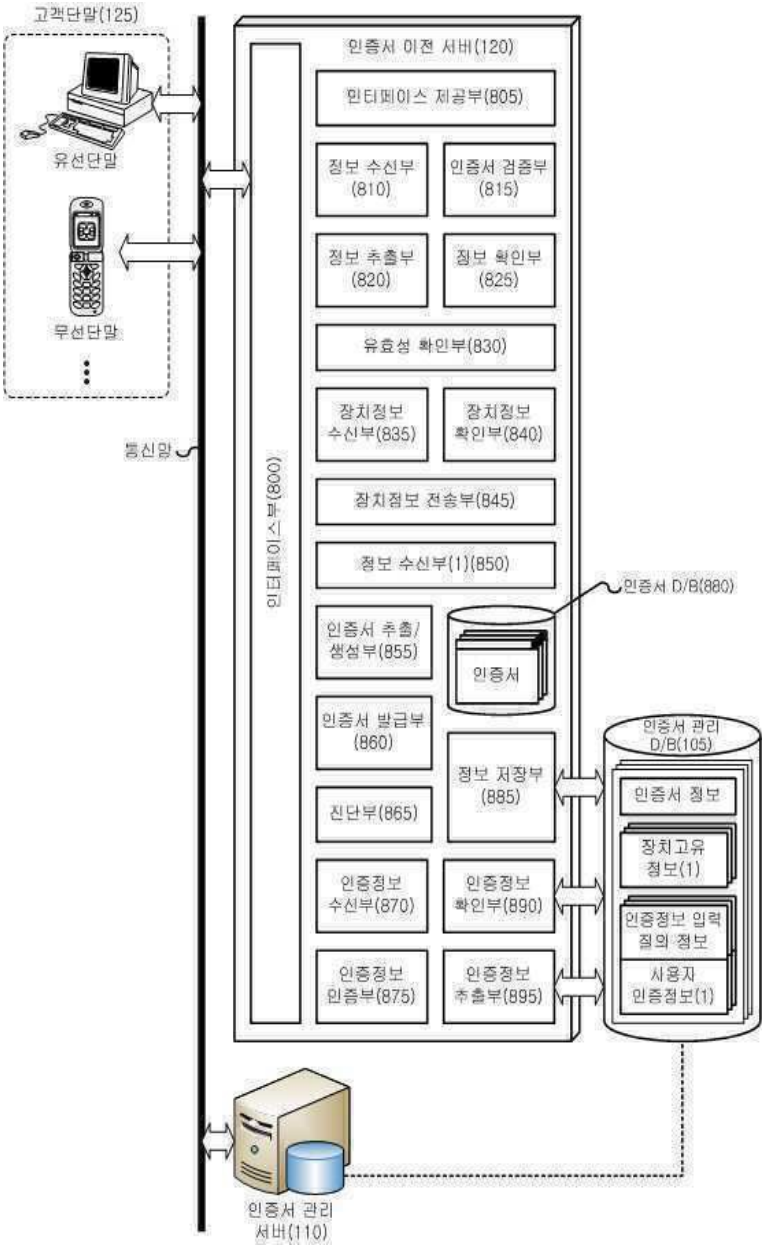
도면6


고객단말(125)
유선단말
무선단말
통신망
인증서 관리 서버(110)
인터페이스 제공부(605)
인터페이스부(600)
정보 수신부 (610)
인증서 검증부 (615)
정보 추출부 (620)
정보 확인부 (625)
유효성 확인부(630)
정보 처리부(635)
인증서 관리 D/B(105)
인증서 정보
장치고유 정보(1)
인증정보 입력 질의 정보
사용자 인증정보(1)
인증서 이용 서버(100)

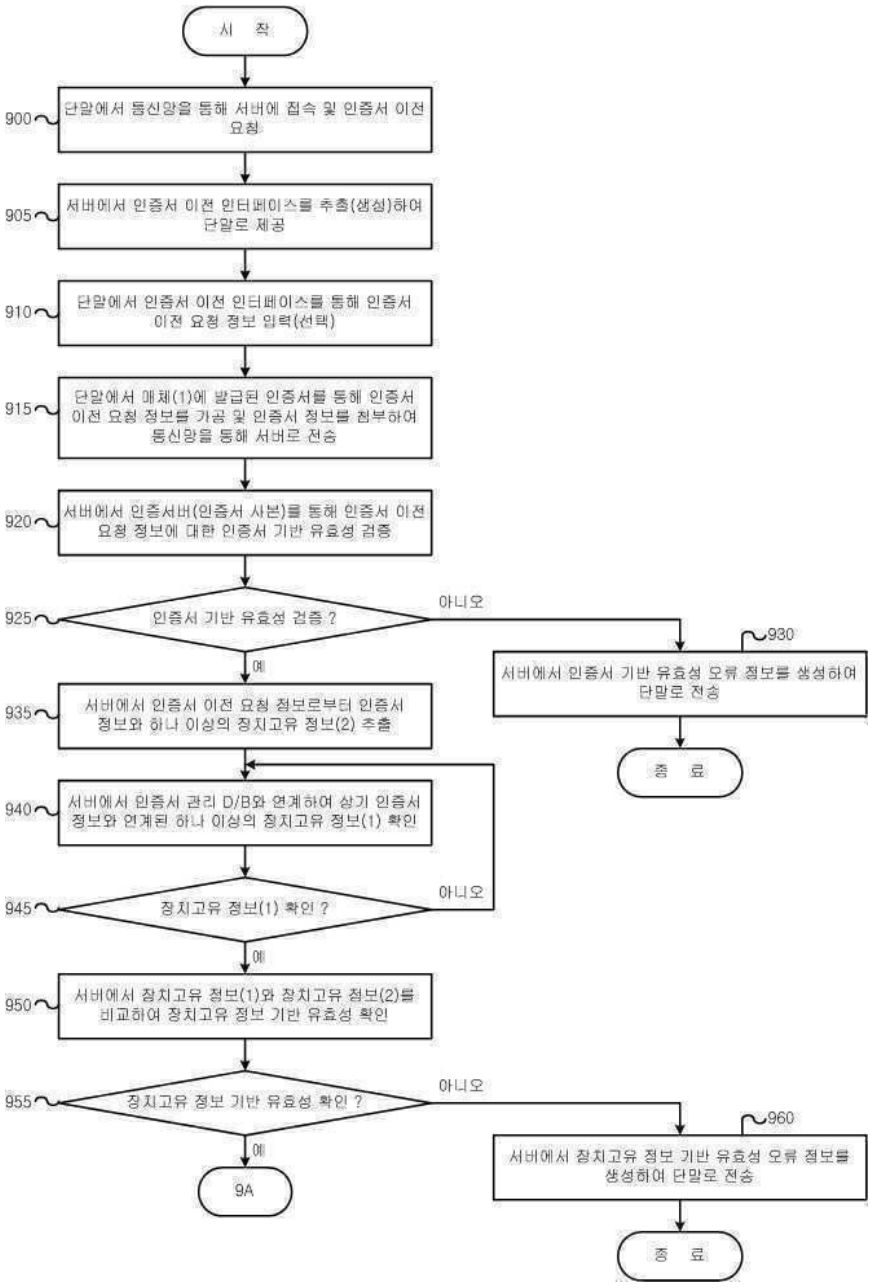
도면7


고객단말(125)
유선단말
무선단말
통신망
인증서 관리 서버(110)
인터페이스 제공부(605)
인터페이스부(600)
정보 수신부 (610)
인증서 검증부 (615)
정보 추출부 (620)
정보 확인부 (625)
유효성 확인부(630)
정보 처리부(635)
인증서 관리 D/B(105)
인증서 정보
장치고유 정보(1)
인증정보 입력 질의 정보
사용자 인증정보(1)
인증서 이용 서버(100)

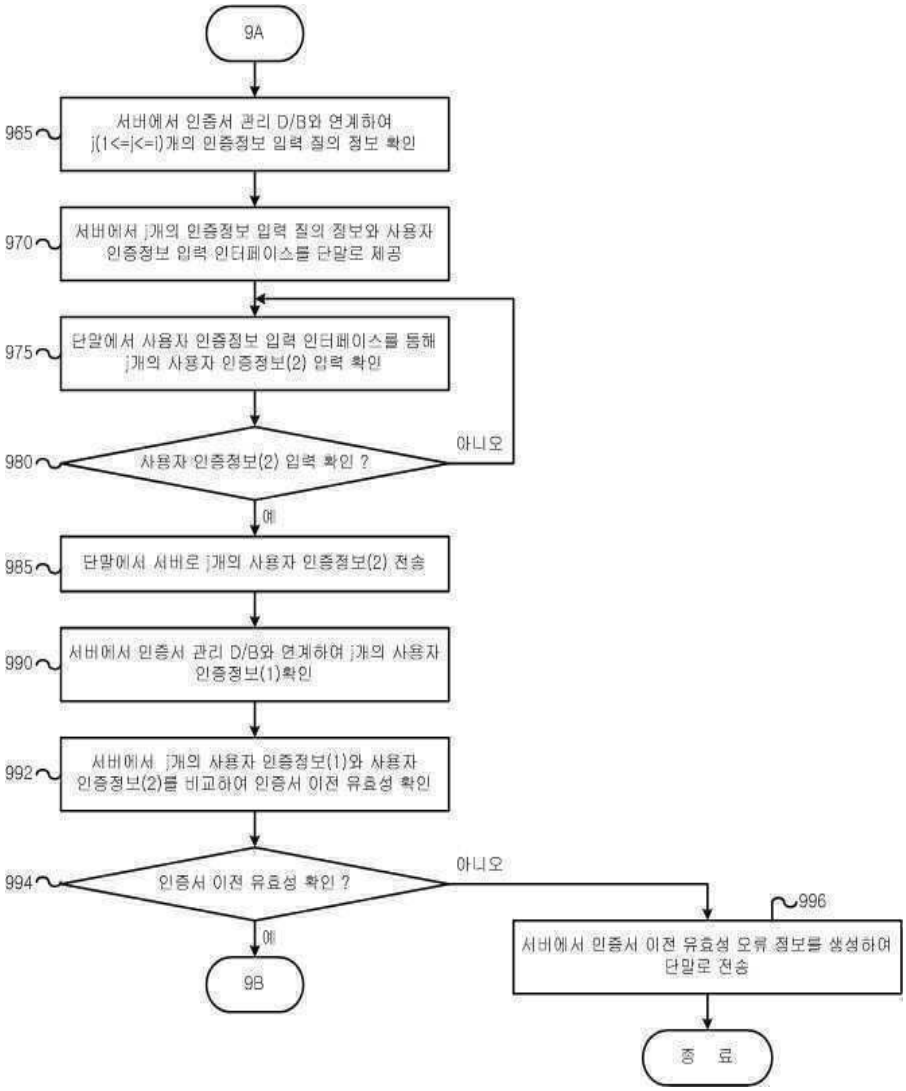
도면8


고객단말(125)
유선단말
무선단말
통신망
인증서 이전 서버(120)
인터페이스 제공부(805)
정보 수신부 (810)
인증서 검증부 (815)
정보 추출부 (820)
정보 확인부 (825)
유효성 확인부(830)
장치정보 수신부(835)
장치정보 확인부(840)
장치정보 전송부(845)
정보 수신부(1)(850)
인터페이스부(800)
인증서 D/B(880)
인증서 추출/ 생성부(855)
인증서
인증서 발급부 (860)
정보 저장부 (885)
진단부(865)
인증정보 수신부(870)
인증정보 확인부(890)
인증정보 인증부(875)
인증정보 추출부(895)
인증서 관리 D/B(105)
인증서 정보
장치고유 정보(1)
인증정보 입력 질의 정보
사용자 인증정보(1)
인증서 관리 서버(110)

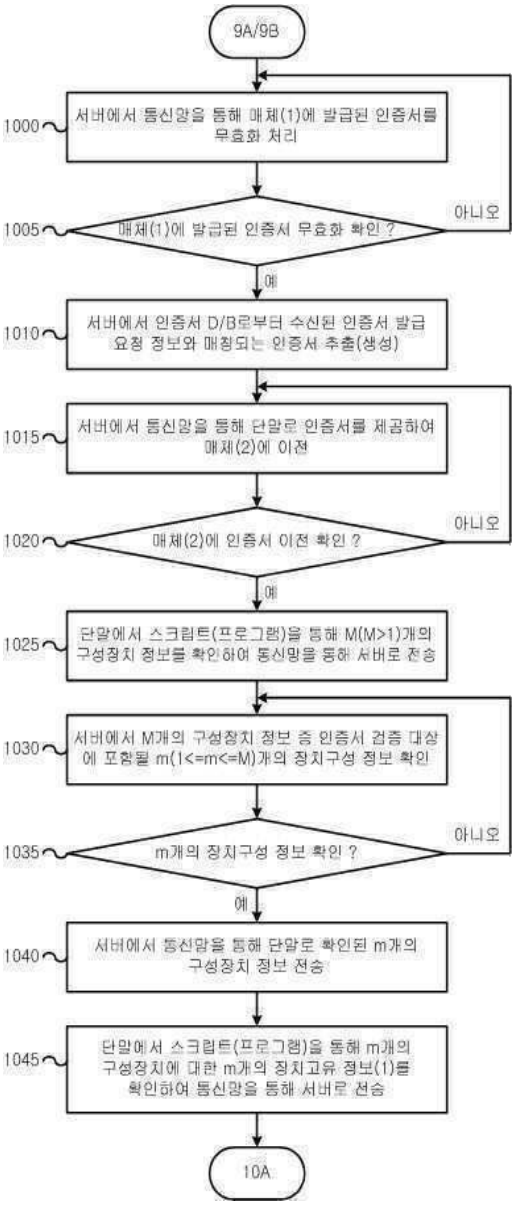
도면9a


시 작
900
단말에서 통신망을 통해 서버에 접속 및 인증서 이전 요청
905
서버에서 인증서 이전 인터페이스를 추출(생성)하여 단말로 제공
910
단말에서 인증서 이전 인터페이스를 통해 인증서 이전 요청 정보 입력(선택)
915
단말에서 매체(1)에 발급된 인증서를 통해 인증서 이전 요청 정보를 가공 및 인증서 정보를 첨부하여 통신망을 통해 서버로 전송
920
서버에서 인증서버(인증서 사본)를 통해 인증서 이전 요청 정보에 대한 인증서 기반 유효성 검증
925
인증서 기반 유효성 검증 ?
아니오
930
서버에서 인증서 기반 유효성 오류 정보를 생성하여 단말로 전송
종 료
예
935
서버에서 인증서 이전 요청 정보로부터 인증서 정보와 하나 이상의 장치고유 정보(2) 추출
940
서버에서 인증서 관리 D/B와 연계하여 상기 인증서 정보와 연계된 하나 이상의 장치고유 정보(1) 확인
945
장치고유 정보(1) 확인 ?
아니오
예
950
서버에서 장치고유 정보(1)와 장치고유 정보(2)를 비교하여 장치고유 정보 기반 유효성 확인
955
장치고유 정보 기반 유효성 확인 ?
아니오
960
서버에서 장치고유 정보 기반 유효성 오류 정보를 생성하여 단말로 전송
종 료
예
9A

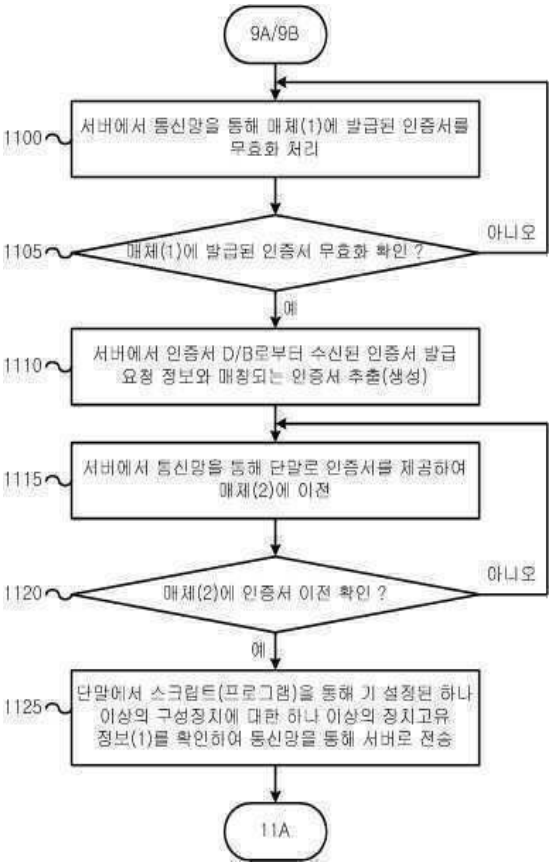
도면9b


9A
965
서버에서 인증서 관리 D/B와 연계하여 j(1<=j<=i)개의 인증정보 입력 질의 정보 확인
970
서버에서 j개의 인증정보 입력 질의 정보와 사용자 인증정보 입력 인터페이스를 단말로 제공
975
단말에서 사용자 인증정보 입력 인터페이스를 통해 j개의 사용자 인증정보(2) 입력 확인
980
사용자 인증정보(2) 입력 확인 ?
아니오
예
985
단말에서 서버로 j개의 사용자 인증정보(2) 전송
990
서버에서 인증서 관리 D/B와 연계하여 j개의 사용자 인증정보(1)확인
992
서버에서 j개의 사용자 인증정보(1)와 사용자 인증정보(2)를 비교하여 인증서 이전 유효성 확인
994
인증서 이전 유효성 확인 ?
아니오
예
9B
996
서버에서 인증서 이전 유효성 오류 정보를 생성하여 단말로 전송
종 료

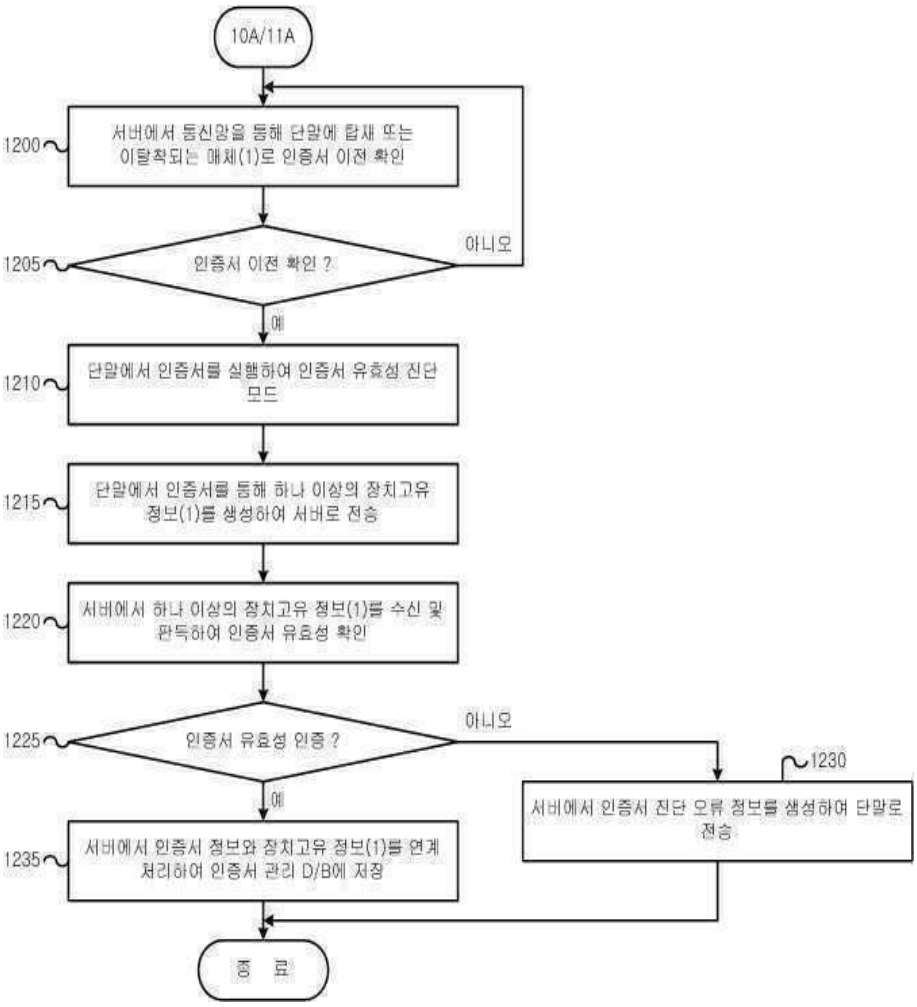
도면10


9A/9B
1000
서버에서 통신망을 통해 매체(1)에 발급된 인증서를 무효화 처리
1005
매체(1)에 발급된 인증서 무효화 확인 ?
아니오
예
1010
서버에서 인증서 D/B로부터 수신된 인증서 발급 요청 정보와 매칭되는 인증서 추출(생성)
1015
서버에서 통신망을 통해 단말로 인증서를 제공하여 매체(2)에 이전
1020
매체(2)에 인증서 이전 확인 ?
아니오
예
1025
단말에서 스크립트(프로그램)을 통해 M(M>1)개의 구성장치 정보를 확인하여 통신망을 통해 서버로 전송
1030
서버에서 M개의 구성장치 정보 중 인증서 검증 대상에 포함될 m(1<=m<=M)개의 장치구성 정보 확인
1035
m개의 장치구성 정보 확인 ?
아니오
예
1040
서버에서 통신망을 통해 단말로 확인된 m개의 구성장치 정보 전송
1045
단말에서 스크립트(프로그램)을 통해 m개의 구성장치에 대한 m개의 장치고유 정보(1)를 확인하여 통신망을 통해 서버로 전송
10A

도면11


9A/9B
1100
서버에서 통신망을 통해 매체(1)에 발급된 인증서를 무효화 처리
1105
매체(1)에 발급된 인증서 무효화 확인 ?
아니오
예
1110
서버에서 인증서 D/B로부터 수신된 인증서 발급 요청 정보와 매칭되는 인증서 추출(생성)
1115
서버에서 통신망을 통해 단말로 인증서를 제공하여 매체(2)에 이전
1120
매체(2)에 인증서 이전 확인 ?
아니오
예
1125
단말에서 스크립트(프로그램)을 통해 기 설정된 하나 이상의 구성장치에 대한 하나 이상의 장치고유 정보(1)를 확인하여 통신망을 통해 서버로 전송
11A

도면12


10A/11A
1200
서버에서 통신망을 통해 단말에 탑재 또는 이탈착되는 매체(1)로 인증서 이전 확인
1205
인증서 이전 확인 ?
아니오
예
1210
단말에서 인증서를 실행하여 인증서 유효성 진단 모드
1215
단말에서 인증서를 통해 하나 이상의 장치고유 정보(1)를 생성하여 서버로 전송
1220
서버에서 하나 이상의 장치고유 정보(1)를 수신 및 판독하여 인증서 유효성 확인
1225
인증서 유효성 인증 ?
아니오
예
1230
서버에서 인증서 진단 오류 정보를 생성하여 단말로 전송
1235
서버에서 인증서 정보와 장치고유 정보(1)를 연계 처리하여 인증서 관리 D/B에 저장
종 료