(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2007-0117371
(43) 공개일자 2007년12월12일

(51) Int. Cl.
G06F 15/00 (2006.01) *G06F 9/06* (2006.01)
(21) 출원번호 10-2006-0051564
(22) 출원일자 2006년06월08일
심사청구일자 2006년06월08일

(71) 출원인
주식회사 프럼나우
서울시 마포구 마포동 35-1 현대빌딩 303호
(72) 발명자
이지훈
경기 남양주시 오남읍 오남리 롯데아파트 104동 208호
(74) 대리인
문춘오, 오위환

전체 청구항 수 : 총 8 항

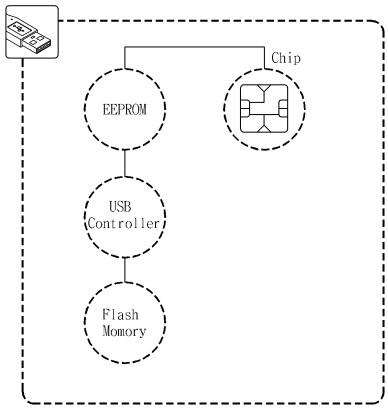
(54) 객체 지향 ＯＴＰ 난수 생성 장치

(57) 요 약

본 발명은 전자금융거래의 보안 장치에 관한 것으로서, 특히 전자금융거래의 보안수단으로 이용되는 일회용비밀번호발생기(One Time Password, OTP)의 난수를 발생시키기 위한 객체 지향 OTP 난수 생성 장치에 관한 것이다.

본 발명의 객체 지향 OTP의 난수 생성 장치는, 공인인증서, 등록 금융기관별 및 OTP 난수를 저장하기 위한 IC칩; 상기 IC칩과 전기적으로 연결되며, 상기 OTP 난수 생성 모듈, 상기 공인인증서 검증 모듈, 및 데이터 전송 모듈을 저장한 메모리 수단; 상기 IC칩 및 상기 메모리 수단에 전원을 공급하기 위한 전원 수단; 및 유무선 단말기와의 연결을 위한 연결 수단을 포함하는 것을 특징으로 한다.

대표도 - 도1



특허청구의 범위

청구항 1

공인인증서와 등록 금융기관별 OTP 난수를 저장하기 위한 IC칩;(OTP 난수를 저장하는가??? 아니면 OTP 난수 발생을 위한 OTP 키값을 저장하는가???)

상기 IC칩과 전기적으로 연결되며, 상기 OTP 난수 생성 모듈, 상기 공인인증서 검증 모듈, 및 데이터 전송 모듈을 저장한 메모리 수단;

상기 IC칩 및 상기 메모리 수단에 전원을 공급하기 위한 전원 수단; 및

유무선 단말기와의 연결을 위한 연결 수단을 포함하는 것을 특징으로 하는 OTP 난수 생성 장치.

청구항 2

제 1 항에 있어서,

상기 연결 수단은 USB 플러그인 것을 특징으로 하는 OTP 난수 생성 장치.

청구항 3

제 2 항에 있어서,

상기 OTP 난수 생성 장치의 일측에 액정디스플레이를 추가로 포함하는 것을 특징으로 하는 OTP 난수 생성 장치.

청구항 4

제 3 항에 있어서,

상기 OTP 난수 생성 장치의 일측에 지문입력부를 추가로 포함하며, 상기 메모리 수단은 지문인증모듈을 추가로 포함하는 것을 특징으로 하는 OTP 난수 생성 장치.

청구항 5

제 4 항에 있어서,

상기 OTP 난수 생성 모듈은 사용자가 선택한 다수의 난수 생성 객체로부터 상기 OTP 난수를 생성하며, 상기 난수 생성 객체는 OTP 핀번호, 주민등록번호, 계좌번호, 계좌비밀번호, 인증서DN값, 카드번호, 주소, 전화번호, 핸드폰번호, 생일, 차량번호 중에서 선택된 적어도 하나의 값과 OTP비밀번호를 포함하는 것을 특징으로 하는 OTP 난수 생성 장치.

청구항 6

제 1 항 내지 제 5 항 중 어느 한 항의 OTP 난수 생성 장치를 이용한 객체 지향 OTP 난수 생성 방법으로서,

상기 OTP 난수 생성 장치의 상기 연결 수단을 상기 유무선 단말기와 연결하는 단계;

상기 유무선 단말기의 디스플레이 화면에서 금융기관 및 난수 생성 객체를 선택하는 단계;

상기 OTP 난수 생성 모듈이 상기 선택된 난수 생성 객체를 이용하여 난수를 생성하고, 생성된 상기 난수를 상기 IC칩에 저장하는 단계를 포함하는 것을 특징으로 하는 객체 지향 OTP 난수 생성 방법.

청구항 7

제 6 항에 있어서,

상기 유무선 단말기를 이용하여 상기 등록 금융기관 중 하나의 서버에 접속하는 단계;

상기 유무선 단말기와 상기 OTP 난수 생성 장치를 접속하는 단계;

상기 IC칩에 저장된 상기 등록 금융기관에 관련된 난수가 상기 서버로 전송되는 단계를 추가로 포함하는 것을 특징으로 하는 객체 지향 OTP 난수 생성 방법.

청구항 8

제 6 항에 있어서,

상기 지문입력부를 통해 지문을 입력하는 단계;

상기 지문입력결과 이상이 없으면, 상기 등록 금융기관 리스트가 디스플레이되는 단계;

전자금융거래를 수행하고자 하는 금융기관을 선택하는 단계;

선택된 금융기관에 관련된 난수들이 디스플레이되는 단계; 및

상기 디스플레이되는 난수 중의 하나를 텔레뱅킹용 난수로 입력하는 단계를 포함하는 것을 특징으로 하는 객체 지향 OTP 난수 생성 방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<7> 본 발명은 전자금융거래의 보안 장치에 관한 것으로서, 특히 전자금융거래의 보안수단으로 이용되는 일회용비밀번호발생기(One Time Password, OTP)의 난수를 발생시키기 위한 객체 지향 OTP 난수 생성 장치에 관한 것이다.

<8> 전자금융거래의 활성화와 더불어 전자금융거래 해킹 사고가 발생하면서 전자금융거래에 대한 불안감이 고조되는 가운데, 전자금융거래시마다 새로운 일회용비밀번호를 생성하는 OTP, 키보드 입력정보를 암호화해 주는 키보드 보안, 고객의 웹브라우저와 금융기관의 웹서버간 전송정보를 암호화해주는 웹암호화, 고객정보 데이터베이스 자체를 보호하기 위한 DB보안 등 다양한 종류의 보안 솔루션들이 제공되고 있다.

<9> 최근 정부에서는 해킹방지, 전자금융, 전자상거래 및 공인인증서의 4개 분야에 대해 전자금융거래 안전성 강화 종합대책을 마련하고 있으며, 이와 관련하여 금융감독원에서는 OTP 단말기의 도입을 권고사항으로 발표하였다.

<10> OTP란 사용자가 인증을 받고자할 때마다 매번 새로운 비밀번호를 생성하여 사용하는 보안 시스템으로서, 이러한 일회용비밀번호를 OTP라고 하고 확장된 의미로 이러한 비밀번호를 생성해 주는 단말기를 OTP라고 부르기도 한다. OTP를 이용하면 사용자 인증 과정에 이용되는 비밀번호의 노출 가능성을 제거함으로써 전자금융거래를 해킹으로부터 보호할 수 있게 된다.

<11> 그러나, 기존의 OTP 방식은 각 금융기관마다 개별적으로 OTP와 관련 단말기를 지급하고 있어서, 사용자가 복수의 OTP를 보관해야 하는 불편함이 있으며, 금융기관도 각 고객에 대한 OTP 및 관련 단말기 발급 비용이 부담이 되고 있는 상황이다.

<12> 또한, 기존의 OTP 방식은 계좌 비밀번호, 공인인증서, 보안카드번호 등 금융기관에서 일방적으로 지정한 요소에 의해 OTP 값이 부여되므로, 해커에 의한 OTP 값의 재구성 내지 금융기관 내부자의 고객 정보 유용과 같은 정보 누출의 가능성이 있었다.

<13> 또한, 기존의 OTP 방식으로 사용자가 전자금융거래를 하기 위해서는 공인인증서를 하드디스크와 같은 저장수단에 저장하는 동시에 별도로 보안카드를 안전하게 보관해야 하는 등 사용자 입장에서는 전자금융거래에 상당한 불편함이 있었다.

<14> 또한, 기존의 OTP 방식은 전자금융거래시 OTP를 키보드 등의 입력수단을 이용하여 입력하기 때문에, 키보드 해킹 등에 따른 OTP 노출 가능성에 대해서는 대처할 수 없었다.

발명이 이루고자 하는 기술적 과제

<15> 본 발명은 상기한 문제점을 해결하고자, 객체 지향 OTP 난수 생성 장치(이하, 'OTP 기기'라 함)를 발급하는 경우 및 이미 발급된 OTP 기기를 타 금융기관이 이용할 때 발급 및 이용에 관련된 정보를 OTP 등록 센터에 등록하도록 함으로써, 하나의 금융기관에서 발급한 OTP 기기를 타 금융기관에서도 공동으로 이용하도록 하여 OTP 발급 비용을 최소화하고, 사용자에게는 단일 OTP 기기를 이용하여 다수의 금융기관과의 전자금융거래를 가능하게 하

는 것을 목적으로 한다.

<16> 또한, 본 발명은 스마트카드와 USB드라이브의 기능을 구비한 OTP USB 형태의 OTP 기기를 제공하고, OTP 값을 입력하는 것이 아니라 OTP 기기에서 직접 금융기관의 서버로 전송하도록 함으로써, OTP와 관련 단말기 또는 보안카드를 별도로 관리해야 하는 부담을 줄이고 OTP를 이용한 전자금융거래절차를 간소화하는 것을 목적으로 한다.

<17> 또한, 본 발명은 OTP 난수 생성시 각각의 다른 객체를 다수개 이용하여 객체 지향 OTP 알고리즘으로 하나의 고유한 난수를 생성하여 OTP 키값으로 사용하고, 각 금융기관의 서버와 사용자의 OTP 기기에서만 OTP 난수가 생성되도록 함으로써, 해커에 의한 OTP 값의 재구성 내지 정보누출의 가능성을 최소화하는 것을 목적으로 한다.

<18> 또한, 본 발명은 본 발명은 하나의 OTP 기기를 이용하여 사용자는 복수의 금융기관에 자신의 OTP USB를 사실상 횟수의 제한없이 등록할 수 있으며, 향후 OTP 기기를 이용한 전자금융거래시 금융기관은 해당 OTP 기기의 고유 OTP 핀번호를 확인하고 자사에 해당하는 난수 값을 OTP 기기로부터 자사의 서버로 전송받음으로써 사용자 인증절차를 완료하고, 금융관련거래 서비스를 제공할 수 있는 안전하고, 비용효율적으로 수행할 수 있도록 하는 것을 목적으로 한다.

<19> 또한, 본 발명은 유무선 고객 단말기와의 USB 포트를 이용한 접속이 가능한 OTP USB의 형태로서 스마트카드와 USB드라이브의 기능을 결합한 OTP 기기를 제공하여, OTP 기기를 사용자의 유무선 단말기와 접속시키는 간단한 절차를 통해 OTP 난수의 생성 및 전송을 완료함으로써 간단한 방법으로 보안성이 강화된 전자금융거래를 수행할 수 있도록 하는 것을 목적으로 한다.

<20> 또한, 본 발명은 다수의 금융기관에 관련된 OTP 키값을 저장하고, 사용자의 금융기관 선택시 저장된 OTP 키값을 이용하여 복수의 OTP를 생성하여 디스플레이함으로써, 보안성이 강화된 텔레뱅킹을 수행할 수 있도록 하는 것을 목적으로 한다.

발명의 구성 및 작용

<21> 본 발명의 객체 지향 OTP 난수 생성 장치는, 공인인증서, 등록 금융기관별 및 OTP 난수를 저장하기 위한 IC칩; 상기 IC칩과 전기적으로 연결되며, 상기 OTP 난수 생성 모듈, 상기 공인인증서 검증 모듈, 및 데이터 전송 모듈을 저장한 메모리 수단; 상기 IC칩 및 상기 메모리 수단에 전원을 공급하기 위한 전원 수단; 및 유무선 단말기와의 연결을 위한 연결 수단을 포함하는 것을 특징으로 한다.

<22> 이하 본 발명의 일 실시예를 도시한 첨부도면을 참조하여 본 발명을 상세히 설명하기로 한다.

<23> 도 1은 본 발명의 일 실시예에 따른 OTP 기기의 블록도이다.

<24> 도 1의 OTP 기기는 PC나 핸드폰, PDA와 같은 유무선 고객 단말기와의 USB 포트를 이용한 접속이 가능한 OTP USB의 형태로서 스마트카드와 USB드라이브의 기능을 결합한 것이다.

<25> 스마트카드의 IC칩과 동일유사한 기능을 수행하는 스마트칩과, OTP 기기에서 수행되는 프로세스 모듈들을 저장하기 위한 플래쉬 메모리, OTP 기기의 구동을 위한 ROM BIOS 정보 등을 저장한 EEPROM, 및 USB 통신을 제어하기 위한 USB 컨트롤러로 구성된다. IC칩은 공인인증서와 OTP 난수를 저장하며, 플래쉬 메모리는 OTP 난수 생성 알고리즘을 구비한 객체 지향 난수 발생 모듈, 데이터 전송 모듈, 인증서 검증 모듈, 지문 인증 모듈 등을 저장한다.(각 구성요소의 도 3a, 3b에서의 위치는???)

<26> 도 2a와 도 2b는 각각 도 1의 OTP 기기 외부의 전면 및 배면도이며, 도 3a와 도 3b는 각각 도 1의 OTP 기기의 내부의 전면 및 배면도이다.

<27> OTP 기기 하우징(130)의 전면에는 액정디스플레이(120)가 구비되어 있으며, 상하이동 버튼(140)과 확인버튼(150)이 제공되어 있다. 하우징(130)의 일측에는 사용자의 유무선 단말기의 USB 소켓에 결합될 수 있는 USB 플러그(110)가 구비되어 있다.

<28> OTP 기기 하우징(130)의 배면에는 지문인증모듈에서의 지문인식을 위한 지문입력부(160)가 구비된다.

<29> OTP 기기의 내부를 보면, 액정디스플레이(120) 아래에 위치하는 전면에는 IC칩(170), 플래쉬 메모리(180) 및 OTP 기기의 충전을 위한 충전용 배터리(190)가 제공되며, 지문입력부(160) 아래에 위치하는 배면에는 상기 IC칩(170), 플래쉬 메모리(180) 등을 장착한 인쇄회로기판(210) 및 충전용 콘덴서(200)가 제공된다.(충전용 콘덴서는 어떻게 동작합니까???)

<30> 본 발명에 따른 OTP 기기는 상기한 OTP USB의 형태인 것이 바람직하지만, 그것이 본 발명의 범위를 제한하는 것

은 아니며, 따라서 본 발명의 OTP 기기는 고객 인증에 필요한 데이터를 자체적으로 저장하고 있어서 전자금융거래에 필요한 데이터가 PC나 핸드폰과 같은 고객 단말기의 메모리에서 실행되지 않고 별도의 OTP 기기에서 실행될 수 있는 것이면 무방하다. 다만, 본 실시예에서는 바람직한 OTP 기기의 형태인 OTP USB를 예로 들어 설명하기로 한다.

<31> 도 4는 본 발명의 일 실시예에 따른 객체 지향 OTP 난수 생성을 위한 객체 입력용 사용자 인터페이스 구조를 도시하고 있다.

<32> OTP USB의 초기화를 위해, OTP USB를 PC 등 USB 포트가 구비된 유선 또는 무선 단말기에 삽입하면, OTP USB에 내장된 객체 지향 난수 발생 모듈이 구동되며 고객이 등록한 공인인증서의 비밀번호를 OTP USB 자체로 한번 검증하게 된다.

<33> 이어서, OTP USB가 접속된 사용자의 유무선 단말기의 디스플레이 화면에는, 도 4와 같이, 선택가능한 금융기관의 종류와 선택가능한 난수 생성 객체의 종류(OTP 비밀번호, 계좌번호, 주민등록번호, 계좌비밀번호, 핸드폰번호, 인증서DN(Distinguish Name)값, 카드번호, 전화번호, 생일, 차량번호 등)가 디스플레이되며, 사용자는 자신의 금융기관 및 자신이 선택한 난수 생성 객체들을 체크할 수 있다.

<34> 사용자의 선택이 완료되면, OTP USB에 있는 플레쉬 메모리(180)에 저장된 객체 지향 난수 생성 모듈이 구동되어 난수를 생성한 후 OTP USB에 내장된 스마트칩(170)에 생성된 난수 값을 해당 금융기관의 OTP 키(Key)값으로 저장한다. 이렇게 저장된 난수는 이후 해당 금융기관과의 전자금융거래에서 일회용 비밀번호 즉, OTP를 생성하기 위한 OTP 키값으로 이용되다. 이 과정에서 난수의 생성을 위해서는 공지의 난수 생성 알고리즘이 이용될 수 있다.

<35> 도 5는 본 발명의 일 실시예에 따른 객체 지향 OTP 기기 사용시의 웹사이트 정보입력화면을 도시하고 있다.

<36> 향후 사용자가 인터넷 뱅킹 등 OTP USB를 이용한 금융관련거래를 하고자 하는 경우, OTP 키값이 생성된 해당 금융기관의 서버에 접속하면 예컨대 도 5와 같은 정보 입력 화면이 제공되며, 이때 자신의 유무선 단말기에 OTP USB를 삽입하여 금융기관의 서버와 자신의 OTP USB를 동기시키면 OTP USB의 스마트칩(170)에 저장된 OTP 키값이 금융기관의 서버로 전송되어 OTP 동기가 이루어지며, 이후 금융거래를 수행할 수 있다. 도 5의 화면은 OTP 생성을 위해 OTP USB 삽입을 지시할 뿐, 키보드 등의 입력 수단을 이용한 보안카드번호 등의 정보 입력을 요하지 않는 점에서 통상의 OTP용 보안카드 이용시의 입력화면과 구별되며, 이 과정에 따르면 키보드 해킹 등을 이용한 OTP 도난을 방지할 수 있다.

<37> 도 6은 도 1의 OTP 기기를 이용한 전자금융거래 시스템의 구성도이다.

<38> 도 6을 참조하여, 객체 지향 OTP USB 난수 발생 및 이용 절차를 설명하기로 한다. (난수 및 OTP 키에 대한 정의와 사용이 올바른지 확인 바랍니다.!!!)

<39> 먼저 객체 지향 OTP USB 신청 단계(110)이다.

<40> 개인 또는 법인 사용자(이하, '고객'(10)이라 함)가 제1 금융기관(20)을 방문하여 객체 지향 OTP USB(40)를 신청한다. 금융기관이라 함은 은행, 증권사, 보험사, 카드사 등 유무선 인터넷을 이용하여 금융관련거래를 하는 모든 종류의 기관을 말한다. 제1 금융기관(20)은 객체 지향 OTP USB(40)의 발급에 필요한 난수를 발생시킬 복수의 난수 생성 객체를 고객(10)이 선택하게 한다.

<41> 이때 사용되는 난수 생성 객체는 예컨대, OTP핀번호, 주민등록번호, 계좌번호, 계좌비밀번호, 인증서DN(Distinguish Name)값, 카드번호, OTP비밀번호, 주소, 전화번호, 핸드폰번호, 생일, 차량번호 등 해당 고객(10)과 관련한 객체로서 제1 금융기관(20)에서 사용할 수 있는 어떠한 정보라도 상관없다. 다만, 고객(10)이 복수(바람직하게는 3개 이상)의 난수 생성 객체를 선택할 때 OTP비밀번호는 반드시 포함되어야 한다.

<42> 이어서 난수 생성 및 저장 단계(120)가 수행된다.

<43> 고객(10)으로부터 난수 생성 객체를 선택받은 제1 금융기관(20)이 해당 고객(10)에게 발급할 OTP USB(40)를 먼저 제1 금융기관(20)의 자체 단말기의 USB 포트에 삽입하면, 단말기는 해당 OTP USB(40)의 고유한 OTP 핀번호를 자체 서버로 전송한 후 고객(10)이 선택한 난수 생성 객체를 체크한다(난수 생성 객체 또한 서버로 전송하는 것은 아닌지???).

<44> 제1 금융기관(20)의 서버에서는 고객(10)에게 발급된 OTP USB(40)의 고유 OTP 핀번호와 고객(10)이 선택한 난수 생성 객체를 사용하여 객체 지향 OTP 알고리즘을 이용하여 해당 OTP USB(40)에서 제1 금융기관(20)과 관련하여

사용될 고유한 난수를 생성한 후 생성된 난수를 서버에 저장한다. 이렇게 생성된 난수는 이후의 금융관련거래에서 일회용 비밀번호 즉, OTP를 생성하기 위한 OTP 키(Key)값으로 이용된다.

<45> 난수의 생성을 위해서는 다양한 공지의 알고리즘이 이용될 수 있으며, 예컨대 국내의 암호화 알고리즘 중 SEED 및 HASH 함수의 값을 이용하여 수행될 수 있다. 난수 생성을 위한 객체를 입력하면 특정 입력 값에 따른 고유의 난수 값이 생성된다. 본 발명에 따르면, 난수 생성용 객체 지향 OTP 알고리즘이 기본적으로 OTP USB(40)에 내장되기 때문에, 어떠한 알고리즘을 사용하더라도 보안상의 문제가 발생하지 않게 된다.

<46> 이어서 OTP USB 등록 단계(130)가 수행된다.

<47> 제1 금융기관(20)의 서버는 OTP USB(40)의 고유한 OTP 핀번호를 제1 금융기관(20)의 명칭(또는 인증값 내지 전자서명)과 함께 OTP 등록센터(30)의 OTP 등록서버에 전송하여 해당 OTP USB가 어느 금융기관에서 발급된 것인지를 OTP 등록서버에 등록한다. 이상의 온라인 등록 과정을 통해 해당 OTP USB(40)가 OTP 등록센터(30)에 등록되면, 제1 금융기관(20)에서는 등록된 OTP USB(40)를 고객(10)에게 전달하여 고객이 향후 금융관련거래에 이용할 수 있도록 한다.

<48> 이후 OTP USB 초기화 단계(140)가 수행된다.

<49> 고객(10)이 발급된 OTP USB(40)의 초기화를 위해, OTP USB(40)를 PC 등 USB 포트가 구비된 유선 또는 무선 단말기에 삽입하면, OTP USB(40)에 내장된 객체 지향 난수 발생 모듈이 구동되며 고객(10)이 등록한 공인인증서(41)의 비밀번호를 OTP USB(40) 자체로 한번 검증하게 된다. 단말기의 디스플레이 화면에는 도 4와 같이 선택가능한 금융기관의 종류와 선택가능한 난수 생성 객체의 종류가 디스플레이되며, 고객(10)은 자신의 제1 금융기관(20) 및 선택한 난수 생성 객체들을 체크할 수 있다.

<50> 고객(10)의 선택이 완료되면, OTP USB(40)에 있는 플레쉬메모리(180) 등의 메모리 수단에 저장된 난수 생성 모듈이 구동되어 난수를 생성한 후 OTP USB(40)에 내장된 스마트칩(170)에 생성된 난수 값을 저장한다. 난수는 OTP USB(40)에 내장된 칩 영역 즉, 제1 금융기관 OTP 영역(42)에 제1 금융기관(20)의 OTP 키(Key)값으로 저장된다. 즉, 저장된 난수는 이후의 금융관련거래에서 일회용 비밀번호 즉, OTP를 생성하기 위한 OTP 키값으로 이용되며, 이 과정에서 난수의 생성을 위해서는 공지의 알고리즘이 이용될 수 있다.

<51> 마지막으로 OTP USB(40)를 이용한 전자금융거래를 위한 OTP 동기 단계(150)이다.

<52> 향후 고객(10)이 인터넷 뱅킹 등 OTP USB(40)를 이용한 금융관련거래를 하고자 하는 경우, 제1 금융기관(20)의 서버에 접속하고 자신의 유무선 단말기에 OTP USB(40)를 삽입하여 제1 금융기관(20)의 서버와 자신의 OTP USB(40)를 동기시키면 OTP USB(40)의 스마트칩에 저장된 난수 값 즉, OTP 키값이 제1 금융기관(20)의 서버로 전송되는 OTP 동기 단계(160)가 수행된다. OTP 동기 단계(160)에서의 구현 방식으로는 S/Key 방식, 챌린지 리스펀스(Challenge Response) 방식, 시간 동기화(Time Synchronous) 방식, 이벤트 동기화(Event Synchronous) 방식 등 다양한 방법이 공지되어 있으나, 본 발명의 경우에는 챌린지 리스펀스 방식으로 진행되는 것이 바람직하다(?????).

<53> 이제, 고객(10)에 동일 OTP USB(40)를 이용하여 다른 금융기관 즉, 제2 금융기관(25)을 통한 금융거래를 하고자 하는 경우를 설명한다.

<54> 먼저, 제2 금융기관(25)에서의 OTP USB 2차 신청 단계(210)이다.

<55> 고객(10)이 제2 금융기관(25)을 방문하여 자신의 객체 지향 OTP USB(40)의 등록을 신청하는 OTP USB 2차 신청 단계(210)가 수행된다. OTP USB 신청 단계(110)가 OTP USB(40)의 발급 및 사용처(즉, 제1 금융기관(20))의 등록을 신청하는 단계라면, 이번의 OTP USB 2차 신청 단계(210)는 이미 발급된 OTP USB(40)의 다른 사용처(즉, 제2 금융기관(25))를 등록하는 단계라는 점이 차이가 있다.

<56> 고객(10)의 OTP USB(40) 등록 신청을 받은 제2 금융기관(25)이 소정의 내부 절차를 거쳐서 해당 OTP USB(40)의 등록을 결정하고, 제2 금융기관(25)과의 거래에 필요한 난수를 발생시킬 복수의 난수 생성 객체를 고객(10)이 선택하게 한다. 제2 금융기관(25)에서 선택가능한 난수 생성 객체의 개수는 제1 금융기관(20)의 경우와 상이할 수 있지만, 적어도 각 금융기관에서 선택가능한 난수 생성 객체의 종류는 동일해야 한다. 또한, 제2 금융기관(25)에서 선택되는 난수 생성 객체에도 OTP비밀번호는 반드시 포함되어야 한다.

<57> 이어서, 제2 금융기관(25)에서의 2차 난수 생성 및 저장 단계(220)가 수행된다.

<58> 해당 고객(10)에게서 전달받은 OTP USB(40)를 제2 금융기관(25)의 자체 단말기의 USB 포트에 삽입하면, 해당 단

말기는 해당 OTP USB(40)의 고유한 OTP 핀번호를 자체 서버로 전송한 후 고객(10)이 선택한 난수 생성 객체를 체크한다(난수 생성 객체 또한 서버로 전송하는 것은 아닌지???).

<59> 제2 금융기관(25)의 서버에서는 OTP USB(40)의 고유 OTP 핀번호와 고객(10)이 선택한 난수 생성 객체를 사용하여 객체 지향 OTP에서 사용될 고유한 난수를 생성한 후 생성된 난수를 서버에 저장한다. 여기서 이용되는 난수 생성 알고리즘은 제1 금융기관(20)의 경우와 마찬가지로 공지의 알고리즘을 이용할 수 있다.

<60> 이어서, 제2 금융기관(25)에 관련된 OTP USB 2차 등록 단계(230)가 수행된다.

<61> 제2 금융기관(25)의 서버는 OTP USB(40)의 고유한 OTP 핀번호를 제2 금융기관(25)의 명칭(즉, 인증값 내지 전자서명)과 함께 OTP 등록센터(30)의 서버에 전송하여 해당 OTP USB(40)를 어느 금융기관에서 사용할 것인지를 OTP 등록센터(30)의 서버에 등록한다. 이상의 2차 등록 과정을 통해 해당 OTP USB(40)가 OTP 등록센터(30)에 등록되면, 제2 금융기관(25)에서는 등록된 OTP USB(40)를 고객(10)에게 반환하여 고객(10)이 향후 금융관련거래에 이용할 수 있도록 한다.

<62> 이후, OTP USB 2차 초기화 단계(240)가 수행된다.

<63> 고객(10)이 OTP USB(40)를 유무선 단말기에 삽입하면, OTP USB(40)에 내장된 객체 지향 난수 생성 모듈이 구동되며 고객(10)이 등록한 공인인증서(41)의 비밀번호를 OTP USB(40) 자체로 한번 검증하게 된다. 한편, 단말기의 디스플레이 화면에는 선택가능한 금융기관의 종류와 선택가능한 난수 생성 객체의 종류가 디스플레이되며, 고객(10)이 자신의 제2 금융기관(25) 및 선택한 난수 생성 객체들을 체크하면, OTP USB(40)에 있는 메모리 수단에 저장된 난수 생성 모듈이 구동되어 난수를 생성한 후 OTP USB에 내장된 스마트칩에 생성된 난수 값을 저장하게 된다. 이와 같은 난수 생성 단계의 결과 생성된 난수는 OTP USB(40)에 내장된 칩 영역 즉, 제2 금융기관 OTP 영역(43)에 제2 금융기관(20)의 OTP 키(Key)값으로 저장된다.

<64> 이와 같이 본 발명의 OTP USB(40)는 자체 칩에 인증서를 저장하기 위한 인증서 영역과, 제1, 제2 금융기관 등 다수의 금융기관에 관련된 OTP 키값을 저장하기 위한 각 금융기관별 OTP 영역을 확보하고 있다.

<65> 향후 고객(10)이 인터넷 뱅킹 등 OTP USB(40)를 이용한 금융관련거래를 하고자 하는 경우, 제2 금융기관(25)의 서버에 접속하고 자신의 유무선 단말기에 OTP USB를 삽입하여 제2 금융기관(25)의 서버와 자신의 OTP USB를 동기시키면 OTP USB의 스마트칩에 저장된 제2 금융기관(25)에 관련된 OTP 키값이 제2 금융기관(25)의 서버로 전송된다(단계 250).

<66> 한편, 제1 금융기관(20)에서 OTP USB를 발급받은 고객(10)이 제2 금융기관(25)에 해당 OTP USB(40)를 등록하고자 하는 경우, 제2 금융기관(25)을 방문하지 않고 제2 금융기관(25)의 서버에 접속하여 자신의 OTP USB(40)를 삽입하고 난수 생성 객체를 선택함으로써 제2 금융기관(25)에서의 등록과정을 온라인으로 처리할 수도 있다. 즉, 상기한 OTP USB 2차 신청 단계(210), 2차 난수 생성 및 저장 단계(220), OTP USB 2차 등록 단계(230), OTP USB 2차 초기화 단계(240) 및 OTP 동기 단계(250)가 모두 온라인으로 수행될 수 있다. 이는 향후 동일 OTP USB(40)를 이용하게 되는 제3, 제4 금융기관의 경우에도 마찬가지이다.

<67> 한편, 고객(10)이 텔레뱅킹을 위해 OTP USB(40)를 이용하는 경우에는, 도 3a의 충전용 배터리(190)에 의해 제공되는 OTP USB(40)의 자체 전원 공급을 통해 OTP 난수를 액정에 표시할 수 있다. 이때의 OTP 키값 전송의 예시적 과정은 다음과 같다.

<68> 먼저, 확인버튼(150)을 소정의 시간(약 3초) 동안 누르면 액정디스플레이(120)에 지문을 입력하라는 코멘트가 제공된다. 이어서, 도 2b에 도시된 배면의 지문입력부(160)에 고객의 지문을 입력하면, OTP USB(40)의 액정디스플레이(120)에 고객이 등록한 금융기관의 리스트가 출력된다. 고객은 전면에 제공된 상하이동버튼(140)을 이용하여 전자금융거래를 수행하고자 하는 금융기관을 선택한 후 확인버튼(150)을 누른다. 그러면, 해당 금융기관에 관련된 OTP 난수들(예컨대 24개)이 액정디스플레이(120) 상에 출력된다. 이어서, 텔레뱅킹 시스템에서 요청하는 난수번호를 확인하고 이를 텔레뱅킹을 위한 OTP 번호로 사용하면 된다. 종료시에는 다시 한번 확인버튼(150)을 소정의 시간 동안 누름으로써 종료하거나 또는 아무런 조작이 없을 경우 예컨대 약 10초 이후에 자동적으로 종료될 수 있다.

<69> 이후의 금융관련거래는 공지의 인터넷 뱅킹 절차로 진행될 수 있으며, 이러한 과정은 본 발명의 요지를 벗어나는 것이므로 이에 대한 설명은 생략하기로 한다.

<70> 한편, 본 발명에서 OTP USB를 발급한 제1 금융기관(20)은 OTP USB의 하드웨어 비용을 부담하는 대신 해당 OTP USB의 발급 금융기관으로 등록되며, 향후 해당 OTP USB를 등록하는 복수의 타 금융기관에 해당 OTP USB의 공동

사용에 대한 비용을 청구할 수 있다.

<71> 도 6에서, 제1 금융기관(20)은 OTP USB(40) 발급시 자체 서버에 해당 OTP USB(40)의 OTP 핀번호 및 제1 금융기관(20)의 명칭(즉, 인증값 또는 전자서명)을 저장함으로써 각 OTP USB에 대한 발급 기록을 저장하고, 저장된 OTP 핀번호와 제1 금융기관의 명칭을 OTP USB 등록센터(30)의 서버로 전송하고, OTP USB 등록센터(30)의 서버는 전송된 정보에 OTP USB 등록 센터(30)에 관한 정보를 추가하여 저장하여 등록한다. 이후, 고객(20)이 제2 금융기관(25)에 OTP USB(40)의 이용 등록 신청을 하게 되면 제2 금융기관(25)과 OTP USB 등록 센터(30) 사이에도 동일한 절차가 진행되며, 이에 따라 OTP USB 등록 센터(30)의 서버에는 해당 OTP USB(40)가 제1 금융기관(20)에서 발급 및 이용되고 있으며, 이후에 제2 금융기관(25)에서도 이용되고 있다는 정보가 기록된다.

<72> 그러면, OTP USB 등록센터(30)는 해당 OTP 핀번호와 제1 금융기관(20)을 확인하여 제2 금융기관(25)에 해당 OTP USB(40)의 사용료를 과금하고, 제2 금융기관(25)으로부터 징수한 해당 OTP USB(40)의 사용료를 발급기관인 제1 금융기관(20)에 지불하는 정산 절차를 진행한다(단계 300).

<73> 이상의 사용료 과금 및 등록 사용료 지불 단계(300)는 제2 금융기관(25)의 등록(단계230)과 함께 실시간으로 수행될 수도 있으며, 소정의 정산 방식을 통해 정기적 또는 부정기적으로 행해질 수도 있다.

발명의 효과

<74> 본 발명에 따르면, 객체 지향 OTP 난수 생성 장치를 발급하는 경우 및 이미 발급된 OTP 기기를 타 금융기관이 이용할 때 발급 및 이용에 관련된 정보를 OTP 등록 센터에 등록하도록 함으로써, 하나의 금융기관에서 발급한 OTP 기기를 타 금융기관에서도 공동으로 이용하도록 하여 OTP 발급 비용을 최소화하고, 사용자에게는 단일 OTP 기기를 이용하여 다수의 금융기관과의 전자금융거래를 가능하게 할 수 있다.

<75> 또한, 본 발명에 따르면, 스마트카드와 USB드라이브의 기능을 구비한 OTP USB 형태의 OTP 기기를 제공하고, OTP 값을 입력하는 것이 아니라 OTP 기기에서 직접 금융기관의 서버로 전송하도록 함으로써, OTP와 관련 단말기 또는 보안카드를 별도로 관리해야 하는 부담을 줄이고 OTP를 이용한 전자금융거래절차를 간소화할 수 있다.

<76> 또한, 본 발명에 따르면, OTP 난수 생성시 각각의 다른 객체를 다수개 이용하여 객체 지향 OTP 알고리즘으로 하나의 고유한 난수를 생성하여 OTP 키값으로 사용하고, 각 금융기관의 서버와 사용자의 OTP 기기에서만 OTP 난수가 생성되도록 함으로써, 해커에 의한 OTP 값의 재구성 내지 정보누출의 가능성을 최소화할 수 있다.

<77> 또한, 본 발명에 따르면, 하나의 OTP 기기를 이용하여 사용자는 복수의 금융기관에 자신의 OTP USB를 사실상 횟수의 제한없이 등록할 수 있으며, 향후 OTP 기기를 이용한 전자금융거래시 금융기관은 해당 OTP 기기의 고유 OTP 핀번호를 확인하고 자사에 해당하는 난수 값을 OTP 기기로부터 자사의 서버로 전송받음으로써 사용자 인증 절차를 완료하고, 금융관련거래 서비스를 제공할 수 있는 안전하고, 비용효율적으로 수행할 수 있다.

<78> 또한, 본 발명에 따르면, 유무선 고객 단말기와의 USB 포트를 이용한 접속이 가능한 OTP USB의 형태로서 스마트카드와 USB드라이브의 기능을 결합한 OTP 기기를 제공하여, OTP 기기를 사용자의 유무선 단말기와 접속시키는 간단한 절차를 통해 OTP 난수의 생성 및 전송을 완료함으로써 간단한 방법으로 보안성이 강화된 전자금융거래를 수행할 수 있다.

<79> 또한, 본 발명에 따르면, 다수의 금융기관에 관련된 OTP 키값을 저장하고, 사용자의 금융기관 선택시 저장된 OTP 키값을 이용하여 복수의 OTP를 생성하여 디스플레이함으로써, 보안성이 강화된 텔레뱅킹을 수행할 수 있다.

<80> 이상에서 본 발명의 바람직한 실시예에 따라 본 발명을 설명하였지만, 본 발명의 권리범위는 상기 실시예나 첨부된 도면에 의해 한정되지 않으며, 첨부된 특허청구범위에 기재된 본 발명의 권리범위를 벗어나지 않는 범위에서 다양한 변형이 가능하다.

도면의 간단한 설명

<1> 도 1은 본 발명의 일 실시예에 따른 OTP 기기의 블록도이다.

<2> 도 2a와 도 2b는 각각 도 1의 OTP 기기 외부의 전면 및 배면도이다.

<3> 도 3a와 도 3b는 각각 도 1의 OTP 기기 내부의 전면 및 배면도이다.

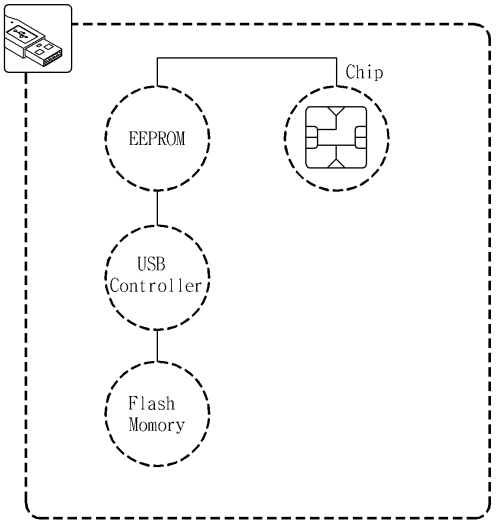
<4> 도 4는 본 발명의 일 실시예에 따른 객체 지향 OTP의 난수 생성을 위한 객체 입력용 사용자 인터페이스 구조를 도시하고 있다.

<5> 도 5은 본 발명의 일 실시예에 따른 객체 지향 OTP 기기 사용시의 웹사이트 정보입력화면을 도시하고 있다.

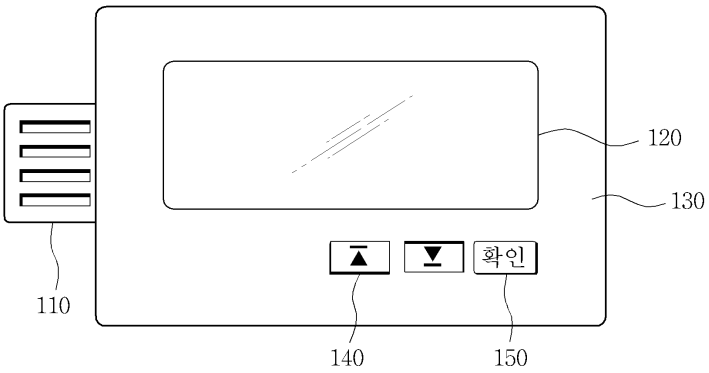
<6> 도 6은 본 발명의 일 실시예에 따른 객체 지향 OTP 기기 사용시의 전자금융거래 시스템의 구성도이다.

도면

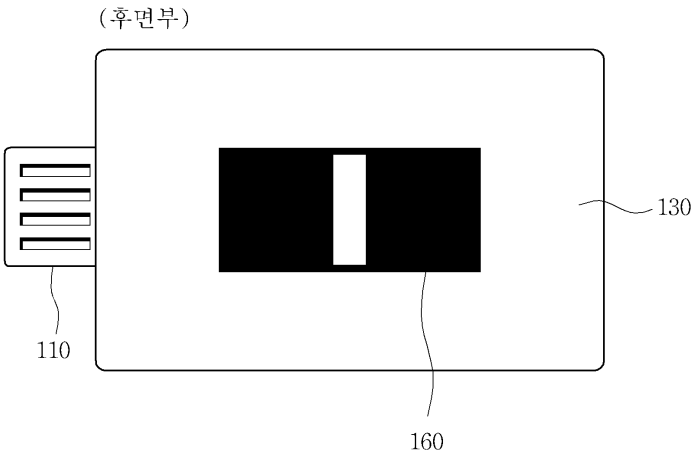
도면1



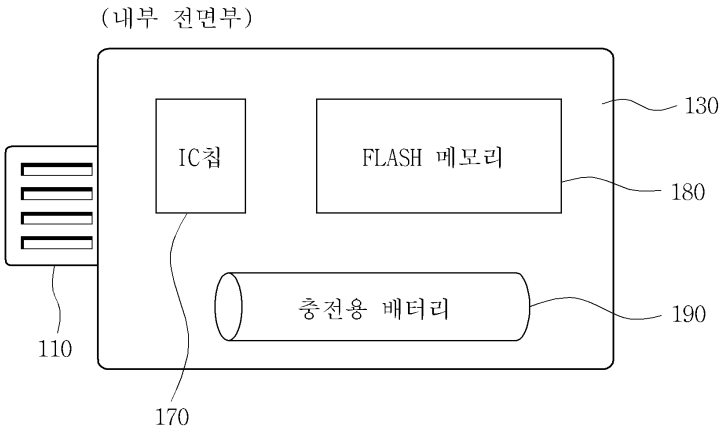
도면2a



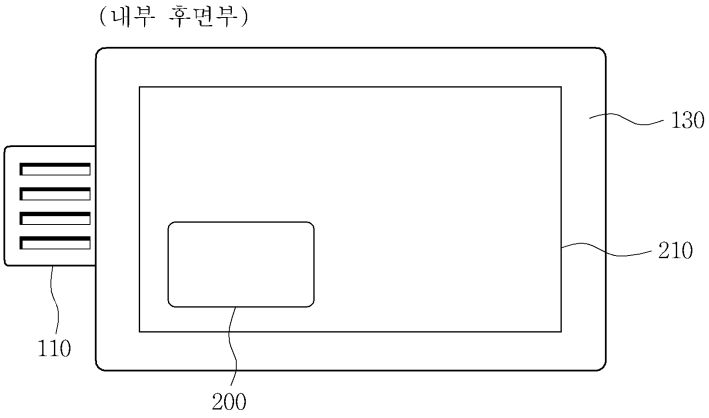
도면2b



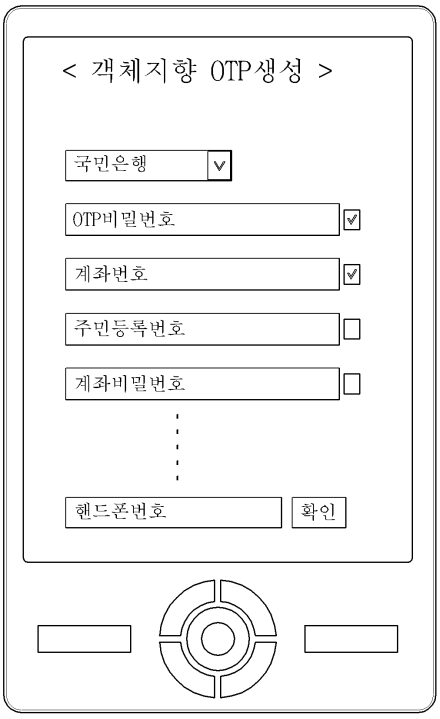
도면3a



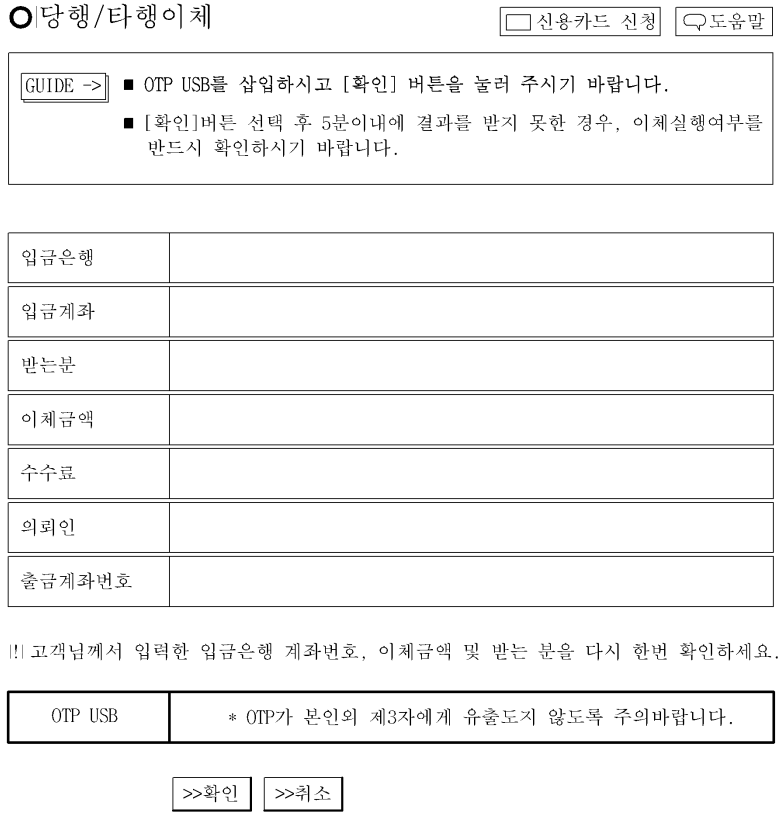
도면3b



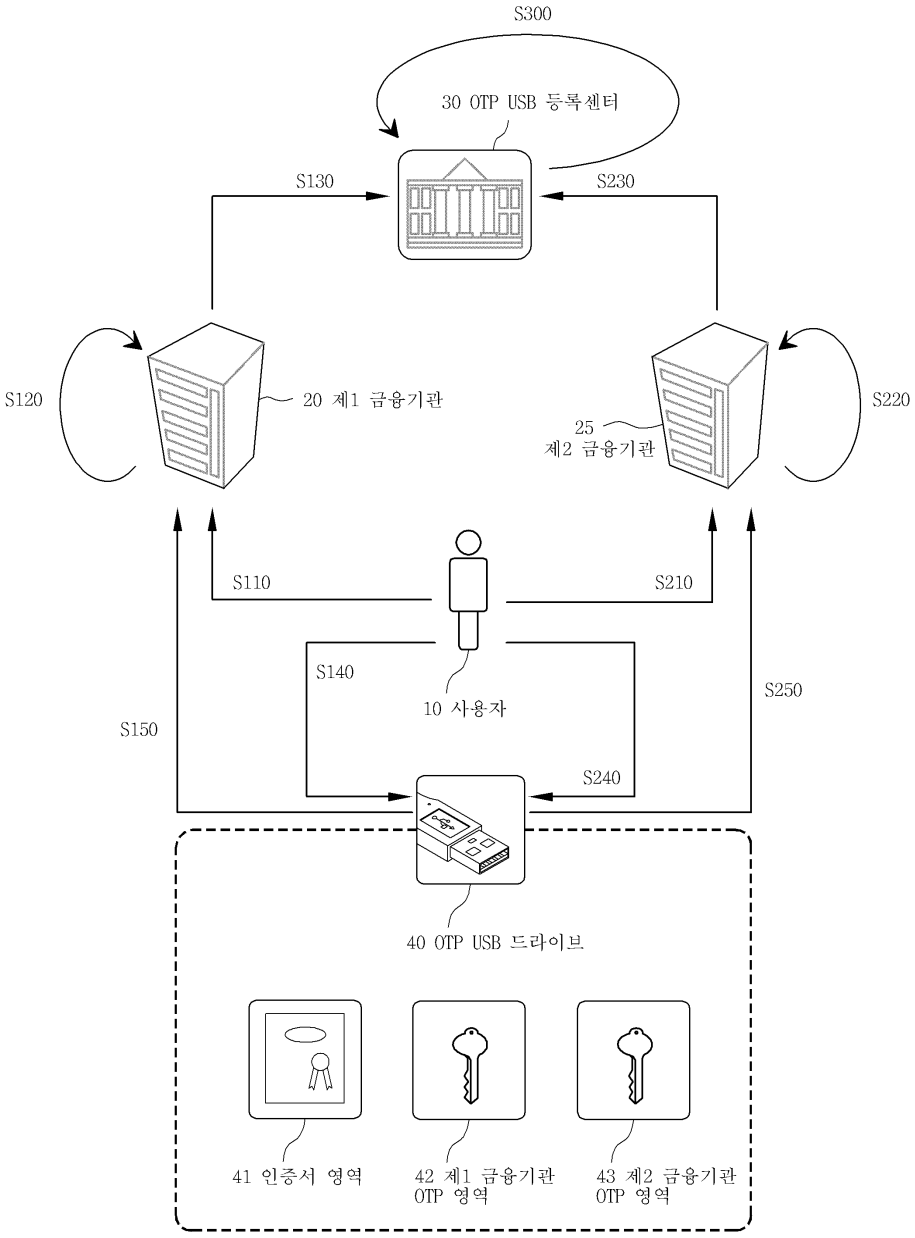
도면4


< 객체지향 OTP생성 >
국민은행
OTP비밀번호
계좌번호
주민등록번호
계좌비밀번호
핸드폰번호
확인

도면5


O|당행/타행이체
신용카드 신청
도움말
GUIDE ->
■ OTP USB를 삽입하시고 [확인] 버튼을 눌러 주시기 바랍니다.
■ [확인]버튼 선택 후 5분이내에 결과를 받지 못한 경우, 이체실행여부를 반드시 확인하시기 바랍니다.
입금은행
입금계좌
받는분
이체금액
수수료
의뢰인
출금계좌번호
!| 고객님께서 입력한 입금은행 계좌번호, 이체금액 및 받는 분을 다시 한번 확인하세요.
OTP USB
* OTP가 본인외 제3자에게 유출되지 않도록 주의바랍니다.
>>확인
>>취소

도면6


S300
30 OTP USB 등록센터
S130
S230
S120
20 제1 금융기관
25
제2 금융기관
S220
S110
S210
S140
10 사용자
S150
S250
S240
40 OTP USB 드라이브
41 인증서 영역
42 제1 금융기관
OTP 영역
43 제2 금융기관
OTP 영역