(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[8]
G06F 15/00 (2006.01)
G06Q 99/00 (2006.01)

(45) 공고일자 2006년02월02일
(11) 등록번호 10-0548638
(24) 등록일자 2006년01월25일

(21) 출원번호 10-2005-0070994
(22) 출원일자 2005년08월03일

(65) 공개번호
(43) 공개일자

(73) 특허권자 주식회사 하이스마텍
서울 종로구 운니동 98-20

(72) 발명자 신귀현
경기 고양시 일산구 일산동 중산마을 107-1003

(74) 대리인 이은철

심사관 : 여원현

(54) 스마트카드를 이용한 원 타임 패스워드 생성 및 인증방법그리고 이를 위한 스마트카드

요약

본 발명은 스마트카드에 원 타임 패스워드 생성 기능을 구현함으로써, 원 타임 패스워드 생성 및 인증을 위한 시스템의 규모를 줄이고, 이와 아울러 시스템 구축에 소요되는 비용을 절감시킬 수 있는, 스마트카드를 이용한 원 타임 패스워드 생성 및 인증방법을 제공함에 그 목적이 있다.

이러한 특징적인 목적을 달성하기 위한 본 발명은, 단말기가 호스트서버에 접속 및 로그인 한 후, 보안 서비스를 요청하는 단계와, 단말기가 호스트서버로부터 요구정보가 포함된 소정의 입력 요청 메시지를 전송받는 단계와, 단말기가 요구정보에 대응하는 응답정보를 사용자로부터 획득하여 스마트카드로 전송하는 단계와, 스마트카드가 응답정보를 초기값으로 원 타임 패스워드를 생성하여 단말기로 전송하는 단계와, 단말기가 원 타임 패스워드를 호스트서버로 전송하는 단계와, 호스트서버가 인증서버로 원 타임 패스워드에 대한 인증을 요청하는 단계, 및 인증서버가 원 타임 패스워드에 대한 인증을 수행하는 단계로 이루어진다.

대표도

도 4

색인어

스마트카드, 원 타임 패스워드, ONE TIME PASSWORD, 인증, 보안

명세서

도면의 간단한 설명

도 1 은 본 발명의 제 1 실시예에 따른 스마트카드를 이용한 원 타임 패스워드 생성 및 인증을 위한 시스템을 나타낸 구성도.

도 2 는 본 발명에 따른 OTP 애플리케이션을 나타내는 개략적인 구성도.

도 3 은 본 발명의 제 2 실시예에 따른 스마트카드를 이용한 원 타임 패스워드 생성 및 인증을 위한 시스템을 나타내는 구성도.

도 4 는 본 발명에 따른 원 타임 패스워드 생성 및 인증 방법을 나타내는 흐름도.

< 도면의 주요 부분에 대한 부호의 설명 >

SC : 스마트카드 R : 리더기

100, 100' : 단말기 M : 접속모듈

200 : 호스트서버 210 : 회원DB

300 : 인증서버 400 : 이동통신사서버

HSM : Hardware Security Module

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 스마트카드를 이용한 원 타임 패스워드 생성 및 인증방법 그리고 이를 위한 스마트카드에 관한 것이다.

유무선 정보통신망(인터넷망)을 통해 각종 컨텐츠 서버에서의 사용자 식별 및 인증 방법으로서, 주로 아이디/패스워드 방식이 이용되고 있다. 이러한 방식의 경우, 아이디/패스워드 도용을 방지하기 위하여 해당 단말기 상에 입력되는 아이디/패스워드가 실제 입력정보가 아닌 '********' 의 형태로 표시된다. 그러나 상기 보안처리 방법은 부정사용자에 의하여 해킹 프로그램(예; '피싱')이 설치된 단말기의 경우, 사용자가 입력하는 아이디/패스워드가 부정사용자에게 실시간으로 전송될 수 있다는 치명적인 문제점을 내포하고 있다. 즉, 종래 소정의 패스워드(다수의 난수)는 반복 사용이 가능하기 때문에 해킹을 통하여 아이디/패스워드를 획득한 부정사용자에 의하여 부정한 목적으로 사용될 위험성이 상존하고 있다. 따라서 고도의 보안성을 유지하여야 하는 경우, 반복 사용이 불가능한 1회용 아이디/패스워드를 적용할 필요성이 있다.

근래 들어, 전자금융, 전자결제 등과 같이 철저한 보안이 요구되는 각종 서비스들이 이루어지고 있으며, 이에 따라 사용자들은 이러한 서비스를 이용하기 위해 다소 복잡한 패스워드를 설정하거나, 거래은행 또는 공인인증기관으로부터 인증서를 발급받아 설치하고, 소정의 패스워드(다수의 난수)들이 수록된 카드 등을 통하여 본인 확인과정을 수차례 통과하여야만 해당 서비스를 이용할 수 있도록 하고 있다. 물론, 이러한 일련의 본인 확인과정은 사용자에게 개인정보 보안이라는 측면에서 긍정적인 효과를 제공하고 있으나, 그 과정이 다소 번잡하여 서비스 이용에 불편한 점이 있었다.

최근에는 사용자가 인증을 요청할 경우 그 패스워드를 수시로 바꿔주는 보안 솔루션으로서 시간동기방식, 챌린지/레스펀스(CHALLENGE/RESPONSE) 방식 또는 호스트 난수 입력 방식으로 이루어진 원 타임 패스워드 시스템이 널리 채용되고 있다. 구체적으로 원 타임 패스워드 시스템은, 패스워드가 본의 아니게 유출되더라도 패스워드의 사용가능 횟수가 단 1회로 한정되어 있기 때문에 악의적인 타인에 의해 재사용이 불가하다는 장점이 있다. 이러한 특유의 장점으로 인해 전자금융을 비롯한 전자결제, 그리고 각종 컨텐츠 제공 업자들로부터 각광받고 있는 추세이다.

전술한 원 타임 패스워드 시스템에 관련해서는, 대한민국 공개특허 제10-2004-0000078호(발명의 명칭: 원 타임 패스워드 시스템 및 방법)(이하, '선행특허'라 한다) 외에 다수 출원 및 등록되어 있는 상태이다.

더욱 구체적으로, 상기 선행특허는 이동 통신 단말과의 무선 구간 통신을 담당하는 기지국, 상기 기지국을 제어하는 기지국 제어기, 상기 기지국 제어기와 연결되어 패킷 데이터 서비스를 제공하기 위한 패킷 데이터 서비스 노드 및 데이터 코어망을 포함하여 구성되는 이동통신 시스템의 상기 데이터 코어망과 접속되며, 이동통신 단말이 상기 데이터 코어망을 통해 접속 가능한 CP(Contents Provider)서버에서 인증 받기 위한 원 타임 패스워드를 발급하여 상기 이동통신 단말로 제공하는 OTP서버를 포함하여 구성되는 시스템으로서, 상기 OTP서버는, 일정한 시간마다 시간을 초기값으로 하여 생성되는 시간 동기 난수를 발생시키는 난수 발생부와; 이통 통신 단말로부터 OTP의 발급이 요청되면 상기 난수 발생부에서 발생된 시간 동기 난수와 개인 식별 정보를 이용하여 OTP를 생성하는 OTP생성부; 및 상기 생성된 OTP와 난수 발생 시간 정보를 상기 이동통신 단말로 전송하기 위한 OTP전송부; 를 포함하여 구성되어, 상기 이동통신 단말이 상기 OTP서버로부터 수신한 OTP를 이용하여 해당 CP서버를 이용할 수 있도록 하는 것을 특징으로 하고 있다.

그러나, 상술한 바와 같은 선행특허에 있어서, 원 타임 패스워드를 생성하기 위한 OTP서버가 별도로 구비되어야 하는바, 시스템이 비대해짐과 아울러 시스템 구축에 소요되는 비용이 높아지는 문제점이 있었다.

한편, 원 타임 패스워드 생성 기능이 구현된 전자계산기 형상의 휴대용 단말기가 출시되고 있으나 이 또한 개별적으로 소지하기가 번거로울 뿐만 아니라, 비교적 고가이며, 그리고 사용이 불편하다는 문제점도 있었다.

발명이 이루고자 하는 기술적 과제

본 발명은, 상기와 같은 문제점들을 해결하기 위해 창안된 것으로서, 스마트카드에 원 타임 패스워드 생성에 관련된 기능을 프로그램으로 구현함으로써, 원 타임 패스워드 생성 및 인증을 위한 시스템의 규모를 줄이고, 시스템 구축에 소요되는 비용을 절감시킬 수 있는, 스마트카드를 이용한 원 타임 패스워드 생성 및 인증방법그리고 이를 위한 스마트카드를 제공함에 그 특징적인 목적이 있다.

상기의 목적들을 달성하기 위하여 본 발명에 따른 스마트카드를 이용한 원 타임 패스워드 생성 및 인증방법은, (a) 상기 단말기가 상기 호스트서버에 접속 및 로그인 한 후, 보안 서비스를 요청하는 단계; (b) 상기 단말기가 상기 회원정보를 기반으로 생성된 요구정보를 포함한 소정의 입력 요청 메시지를 상기 호스트서버로부터 전송받는 단계; (c) 상기 단말기가 상기 요구정보에 대응하는 응답정보를 사용자로부터 획득하여 스마트카드로 전송하는 단계; (d) 상기 스마트카드가 상기 응답정보를 초기값으로 원 타임 패스워드를 생성하여 단말기로 전송하는 단계; (e) 상기 단말기가 원 타임 패스워드를 호스트서버로 전송하는 단계; (f) 상기 호스트서버가 인증서버로 원 타임 패스워드에 대한 인증을 요청하는 단계; 및 (g) 상기 인증서버가 상기 원 타임 패스워드에 대한 인증을 수행하는 단계; 로 구성된다.

한편, 본 발명에 따른 원 타임 패스워드 생성을 위한 스마트카드는, 사용자의 단말기(100)(100')와, 상기 사용자의 회원정보가 저장된 회원DB(210)를 구비하며, 유무선 인터넷망(N)을 통해 접속된 상기 단말기가 보안 서비스를 요청할 경우, 상기 회원정보를 기반으로 생성한 요구정보를 상기 단말기로 전송하는 호스트서버(200)와, 상기 호스트서버와 연동되어 상기 단말기로부터 전송된 원 타임 패스워드에 대한 인증을 수행하며 상기 회원DB(210)를 공유하는 인증서버(300)로 구성되는 시스템의 단말기에 접속되어 원 타임 패스워드 생성을 수행하는 스마트카드(SC)에 있어서, 상기 요구정보에 대응하는 응답정보를 단말기로부터 전송받아 이를 초기값으로 하여 원 타임 패스워드를 생성하는 OTP 애플리케이션을 포함하고 있는 것을 특징으로 한다.

발명의 구성 및 작용

도 1 을 참조하면, 본 발명의 제 1 실시예에 따른 스마트카드를 이용한 원 타임 패스워드 생성 및 인증을 위한 시스템(이하, '제 1 시스템'이라 한다)은, 스마트카드(Smart Card, SC), 단말기(100), 리더기(Reader, R), 호스트서버(200) 및 인증서버(300)를 포함하여 구성된다.

스마트카드(SC)는 접촉식(Contact Type), 비접촉식(Contact-less Type) 또는 하이브리드식(Hybrid Type)의 스마트카드로서, 내부에서 실행되는 원 타임 패스워드(이하, 'OTP'라 한다) 생성에 관련한 애플리케이션(Application)(이하, 'OTP 애플리케이션'이라 한다)을 포함한다.

더욱 구체적으로 OTP 애플리케이션은, 도 2 에 도시된 바와 같이, 기본적으로 제 1 OTP를 생성하기 위한 OTP생성 알고리즘(10)과, OTP 애플리케이션의 접근 인증을 위한 개인식별정보(20), 및 OTP 애플리케이션 별로 부여되는 고유정보(바람직하게는, 일련번호)(30)로 구성된 애플리케이션 정보를 포함하고 있다. 부연하면, OTP생성 알고리즘(10)은 OTP 애플리케이션 별로 상이하게 설정될 수 있으며, 하기에서 설명될 응답정보를 초기값으로 제 1 OTP를 생성하는 알고리즘이다.

여기서 OPT생성 알고리즘은 해쉉(Hashing) 알고리즘을 포함한 소정의 비밀키 암호화 방식이 구현된 알고리즘일 수 있으며, 그 암호화 방식은 DES, T-DES 및 아리아(ARIA) 등을 포함하여 다양하게 설정될 수 있다. 그리고 개인식별정보(20)는 PIN정보(Personal Identification Number) 또는 지문정보와 같은 생체인식정보로 설정될 수 있다.

또한, 단말기(100)는 유무선 인터넷망(Network, N)과 접속 가능한 통상의 사용자 컴퓨터와 PDA를 비롯한 통신단말 등이며, 본 발명의 일양상에 따라 하기의 호스트서버(200)에 보안 서비스를 요청할 경우, 호스트서버(200)로부터 전송된 보안 서비스에 관련한 입력화면 또는 메시지들을 디스플레이하며, 사용자로부터 개인식별정보(20)를 입력받아 스마트카드(SC)로 전송한다. 또한 스마트카드(SC)에서 개인식별정보(20)에 대한 인증이 정상적으로 이루어졌을 경우, 호스트서버(200)에서 전송된 소정의 요구정보에 대응하는 응답정보를 사용자로부터 획득한 후 스마트카드(SC)로 전송하여, 응답정보를 초기값으로 하여 생성된 제 1 OTP와 고유정보(30)를 스마트카드(SC)로부터 전송받아 기본정보 및/또는 기타정보와 함께 하기의 호스트서버(200)로 전송하는 기능을 수행한다.

부연하여, 상기 기본정보는 사용자의 계좌정보이며, 기타정보는 금액과 관련된 결제정보이고, 그리고 요구정보는 호스트서버(200)가 하기의 회원정보를 기반으로 생성한 랜덤화된 정보이되, 사용자가 추정 가능한 정보이다. 예컨대 계좌번호, 주민등록번호, 신용카드번호, 또는 전화번호 중에서 그 일부분 또는 이들의 조합을 요구하는 정보와 같이 다양하게 설정될 수 있다. 한편, 상기 요구정보는 응답정보와 표형식으로 관계화된 정보일 수 있다. 예들 들어, 요구정보로서 다수의 인덱스(INDEX)와 이 인덱스에 대응하는 응답정보로서 소정 자릿수의 숫자/문자로 구성된 카드 형상의 표(이하, '관계표'라 한다)일 수 있다. 이러한 관계표는 스마트카드(SC)와 함께 사용자에게 발급되고, 하기의 회원정보에 정보화된 상태로 포함되는 것이 바람직하다.

또한, 리더기(R)는 단말기(100)와 접속되어 스마트카드(SC)에 데이터를 읽고 쓸 수 있게 하는 매개체로서의 기능을 제공한다. 여기에서, 리더기(R)는 스마트카드(SC)의 작동 방식, 다시 말해 접촉식, 비접촉식 또는 하이브리드식 중 적어도 어느 하나를 지원할 수 있도록 설정되는 것이 바람직하다. 본 실시예에서 리더기(R)는, USB(Universal Serial Bus) 방식의 접속수단을 통해 단말기(100)에 접속되는 것으로 설정하겠으나, 본 발명이 접속수단의 방식에 국한되는 것은 아니다.

또한, 호스트서버(200)는 사용자가 유무선 인터넷망(N)을 통해 접속하고자 하는 금융기관, 예를 들어 은행의 서버로서, 사용자에게 스마트카드(SC)를 발급하고 은행에 계설된 계좌로부터 잔금확인, 결제, 또는 이체 등과 같이 보안이 요구되는 서비스(이하, '보안 서비스'라 한다)를 제공한다. 이때, 통상의 인터넷 뱅킹 서비스와 마찬가지로 사용자와 은행 사이에는 사용자 인증을 위한 회원가입 또는 로그인(Log IN) 절차가 이루어지는 것이 바람직하며, 로그인을 위한 정보와 발급된 스마트카드(SC)의 애플리케이션 정보는 회원정보로서 취합되어 회원DB(210)에 저장된다.

그리고, 인증서버(300)는 전술한 호스트서버(200)와 연동된 서버이거나 또는호스트서버(200)에 의해 운용되는 서버로서, 호스트서버(200)로부터 제 1 OTP에 대한 인증이 요청되면, 회원DB(210)에 기저장된 회원정보에서 요구정보와 대응하는 응답정보를 찾아 이를 초기값으로 하여 제 2 OTP를 생성하고, 제 1 OTP를 제 2 OTP와 비교하여 제 1 OTP의 유효성을 판단하며, 이것이 유효할 경우 단말기(100)가 호스트서버(200)를 통한 보안 서비스 절차를 제공 받도록 하는 본 발명의 특징적인 기능을 수행한다.

한편, 본 발명의 일양상에 따른 인증서버(300)는, 바람직하게 도 1 에 도시된 호스트서버(200)의 회원DB(210)를 공유하고 있으며, 전술한 바와 같은 일련의 OPT 유효성 판단 절차를 전담하는 HSM(Hardware Security Module)(310)을 더 포함할 수 있다.

지금까지 설명한 본 발명의 제 1 시스템을 통해 이루어지는 원 타임 패스워드 생성 및 인증 방법에 대한 보다 상세한 절차는 후술하기로 하며, 이하에서는 도 3 을 참조하여 본 발명의 제 2 실시예에 따른 스마트카드를 이용한 원 타임 패스워드 생성 및 인증을 위한 시스템에 대해 살펴본다. 도 3 을 참조하면, 스마트카드를 이용한 원 타임 패스워드 생성 및 인증을 위한 시스템(이하, '제 2 시스템'이라 한다)은, 스마트카드(SC), 단말기(100'), 호스트서버(200), 인증서버(300) 및 이동통신사서버(400)로 구성된다.

상술한 구성의 제 2 시스템은 제 1 시스템과 대비하여 전체적으로 동일한 기능 및 절차를 수행하되, 단말기(100')는 스마트카드(SC)를 탈착 가능하게 수용하고 스마트카드(SC)의 데이터를 읽고 쓸 수 있게 하는 접속모듈(M)이 구비된 통상의 모바일 뱅킹용 이동통신단말기이며, 이동통신사서버(400)는 단말기(100')가 호스트서버(200) 또는 인증서버(300)에 접속할 수 있도록 하는 기능을 수행한다.

이하, 도 4 를 참조하여 전술한 특징적인 구성과 기능을 갖는 본 발명의 제 1 또는 제 2 시스템을 통한 원 타임 패스워드 생성 및 인증 방법에 대해 상세히 살펴본다. 먼저, 도 4 를 참조하면, 사용자의 단말기(100)(100')가 유무선 인터넷망(N)을

통해 호스트서버(200)에 접속 및 로그인 한 후(S401), 보안 서비스를 요청하면인증서버(300)로부터 보안 서비스를 위한 소정의 입력 요청 메시지를 수신한다(S403). 여기에서, 제 S401 단계 이전에 사용자와 호스트서버(200) 사이에 스마트카드(SC) 발급을 포함한 일련의 회원가입 절차들이 이루어진 상태이며, 제 S403 단계의 입력 요청 메시지에는 전술한 바와 같이 호스트서버(200)로부터 전송된 요구정보가 포함되어 있다.

이어서, 단말기(100)(100')는 사용자로부터 개인식별정보(20)를 입력받아 스마트카드(SC)로 전송하며(S405), 전술한 바와 같이 OTP 애플리케이션에 따라 작동하는 스마트카드(SC)를 통해 개인식별정보(20)에 대한 인증이 이루어지고(S407), 상기 개인식별정보(20)에 대한 정당성이 인증되면 단말기(100)(100')는 사용자로부터 요구정보에 따른 응답정보를 획득하여 이를 스마트카드(SC)로 전송한다(S409).

다음으로, 스마트카드(SC)는 전송받은 응답정보를 초기값으로 제 1 OTP를 생성한 후(S411), 고유정보(30)와 함께 단말기(100)(100')로 전송한다(S413).

이후, 단말기(100)(100')는 사용자로부터 기본정보와 기타정보를 입력받아 제 S413 단계에서 전송받은 고유정보(30) 및 제 1 OTP와 함께 호스트서버(200)로 전송하고(S415), 이를 수신한 호스트서버(200)가 제 1 OTP에 대한 인증을 인증서버(300)에 요청한다(S417).

제 S417 단계 이후에, 인증서버(300)는 회원DB(210)에서 상기 제 S403 단계의 요구정보에 대응하는 응답정보를 찾아 이를 초기값으로 제 2 OTP를 생성하고(S419), 생성된 제 2 OTP와 제 1 OTP가 동일한지 여부를 비교 판단한다(S421, S423). 여기에서 제 2 OTP는 스마트카드(SC)에서 사용된 OTP생성 알고리즘과 동일한 알고리즘을 통해 생성된다. 본 실시예에서 OTP생성 알고리즘은 스마트카드(SC)마다 다르게 설정될 수 있으므로, 제 S419 단계 이전에 인증서버(300)가 회원정보를 기반으로 해당 OTP생성 알고리즘을 선택하는 단계가 포함될 수 있다. 또한, 제 S419 단계 이전에 인증서버(300)는 제 1 OTP가 제 S401 단계에서 로그인한 사용자에 의해 생성된 것인지 여부를 확인하기 위하여 전송받은 고유정보(30)와 회원정보의 고유정보를 비교하는 부가적인 단계가 더 포함될 수 있으나, 본 발명이 이에 한정되는 것은 아니다.

이어서, 제 S423 단계의 판단결과, 제 1 OTP와 제 2 OTP가 동일하다면 인증서버(300)는 단말기(100)(100')가 호스트서버(200)의 보안 서비스 절차를 제공받도록 하고(S425), 그에 따른 소정의 결과 화면 또는 메시지를 단말기(100)(100')로 전송한다(S427). 한편, 제 S423 단계의 판단결과, 동일하지 않다면 인증서버(300)는 소정의 실패 화면 또는 메시지를 단말기(100)(100')로 전송한다(S429).

이상으로 본 발명의 기술적 사상을 예시하기 위한 바람직한 실시예와 관련하여 설명하고 도시하였지만, 본 발명은 이와 같이 도시되고 설명된 그대로의 구성 및 작용에만 국한되는 것이 아니며, 기술적 사상의 범주를 일탈함이 없이 본 발명에 대해 다수의 변경 및 수정이 가능함을 당업자들은 잘 이해할 수 있을 것이다. 따라서, 그러한 모든 적절한 변경 및 수정과 균등물들도 본 발명의 범위에 속하는 것으로 간주되어야 할 것이다.

발명의 효과

제 1 실시예 및 제 2 실시예를 통해 살펴본 본 발명에 따르면, 원 타임 패스워드 생성에 관련된 기능이 프로그램으로써 스마트카드에 구현되어 있는 바, 보안 서비스를 위한 원 타임 패스워드 생성 및 그 인증 과정이 종래에 비해 간결해지며, 이를 위한 시스템의 규모와 시스템 구축에 소요되는 비용을 줄일 수 있는 효과가 있다.

또한, 본 발명의 특징적인 양상에 따른 스마트카드는 이동통신단말기 또는 컴퓨터에 용이하게 접속 또는 채용될 수 있는 바, 종래와 같이 고가의 휴대용 단말기를 별도로 구비하지 않아도 된다.

(57) 청구의 범위

청구항 1.

원 타임 패스워드(OTP) 생성 기능이 프로그램 형식으로 구현된 스마트카드(SC), 상기 스마트카드와 접속되는 사용자의 단말기(100)(100'), 상기 사용자의 회원정보를 저장하는 회원DB(210)를 구비하며 유무선 인터넷망(N)을 통해 상기 단말기에 소정의 보안 서비스를 제공하는 호스트서버(200), 상기 호스트서버와 연동되어 스마트카드에서 생성된 원 타임 패스워드에 대한 인증을 수행하며 상기 회원DB를 공유하는 인증서버(300)로 구성되는 시스템의 원 타임 패스워드 생성 및 인증방법에 있어서,

(a) 상기 단말기가 상기 호스트서버에 접속 및 로그인 한 후, 보안 서비스를 요청하는 단계; (b) 상기 단말기가 상기 회원정보를 기반으로 생성된 요구정보를 포함한 소정의 입력 요청 메시지를 상기 호스트서버로부터 전송받는 단계; (c) 상기 단말기가 상기 요구정보에 대응하는 응답정보를 사용자로부터 획득하여 스마트카드로 전송하는 단계; (d) 상기 스마트카드가 상기 응답정보를 초기값으로 원 타임 패스워드를 생성하여 단말기로 전송하는 단계; (e) 상기 단말기가 원 타임 패스워드를 호스트서버로 전송하는 단계; (f) 상기 호스트서버가 인증서버로 상기 원 타임 패스워드에 대한 인증을 요청하는 단계; 및 (g) 상기 인증서버가 상기 원 타임 패스워드에 대한 인증을 수행하는 단계; 로 구성되어, 상기 단말기에 보안 서비스가 제공되는 것을 특징으로 하는 스마트카드를 이용한 원 타임 패스워드 생성 및 인증방법.

청구항 2.

제 1 항에 있어서,

상기 제 (a) 단계 이전에,

(a-1) 상기 사용자와 호스트서버(200) 사이에 스마트카드(SC) 발급을 포함한 일련의 회원가입 단계; 를 더 포함하는 것을 특징으로 하는 스마트카드를 이용한 원 타임 패스워드 생성 및 인증방법.

청구항 3.

제 1 항에 있어서,

상기 제 (b) 단계 이전에,

(b-1) 상기 단말기가 사용자로부터 개인식별정보를 입력받아 스마트카드(SC)로 전송하는 단계; 및 (b-2) 상기 스마트카드가 개인식별정보에 대한 인증을 수행하는 단계; 를 더 포함하는 것을 특징으로 하는 스마트카드를 이용한 원 타임 패스워드 생성 및 인증방법.

청구항 4.

제 1 항에 있어서,

상기 제 (g) 단계의 인증은,

상기 인증서버가 상기 제 (b) 단계의 요구정보에 대응하는 회원정보의 응답정보를 초기값으로 하여 생성한 원 타임 패스워드와 상기 호스트서버로부터 전송된 원 타임 패스워드를 비교함으로써 이루어지는 것을 특징으로 하는 스마트카드를 이용한 원 타임 패스워드 생성 및 인증방법.

청구항 5.

제 3 항에 있어서,

상기 개인식별정보는,

PIN정보 또는 생체인식정보인 것을 특징으로 하는 스마트카드를 이용한 원 타임 패스워드 생성 및 인증방법.

청구항 6.

삭제

청구항 7.

제 1 항 또는 제 4 항에 있어서,

상기 요구정보는,

계좌번호, 주민등록번호, 신용카드번호, 또는 전화번호 중에서 그 일부분 또는 이들의 조합을 요구하는 정보인 것을 특징으로 하는 스마트카드를 이용한 원 타임 패스워드 생성 및 인증방법.

청구항 8.

제 1 항 또는 제 4 항에 있어서,

상기 요구정보는,

관계표에 의해 응답정보를 도출할 수 있는 정보인 것을 특징으로 하는 스마트카드를 이용한 원 타임 패스워드 생성 및 인증방법.

청구항 9.

제 8 항에 있어서,

상기 관계표는,

상기 요구정보로서 다수의 인덱스와 이 인덱스에 대응하는 응답정보로서 소정 자릿수의 숫자/문자로 구성된 카드 형상의 표이며, 스마트카드(SC)와 함께 사용자에게 발급되고, 회원정보에 정보화된 상태로 포함되는 것을 특징으로 하는 스마트카드를 이용한 원 타임 패스워드 생성 및 인증방법.

청구항 10.

제 1 항에 있어서,

상기 단말기가 사용자 컴퓨터일 경우,

상기 시스템은,

스마트카드와 사용자 컴퓨터 사이에서 접속기능을 제공하는 리더기(R)를 더 포함하는 것을 특징으로 하는 스마트카드를 이용한 원 타임 패스워드 생성 및 인증방법.

청구항 11.

제 1 항에 있어서,

상기 단말기가 이동통신단말기일 경우,

상기 이동통신단말기는,

스마트카드를 탈착 가능하게 수용하고 상기 스마트카드와 접속되는 접속모듈(M)을 구비하는 것을 특징으로 하는 스마트카드를 이용한 원 타임 패스워드 생성 및 인증방법.

청구항 12.

제 1 항에 있어서,

상기 제 (e) 단계는,

상기 단말기가 사용자로부터 기본정보 및 기타정보를 입력받아 상기 원 타임 패스워드와 함께 호스트서버로 전송하는 것을 특징으로 하는 스마트카드를 이용한 원 타임 패스워드 생성 및 인증방법.

청구항 13.

사용자의 단말기(100)(100')와, 상기 사용자의 회원정보가 저장된 회원DB(210)를 구비하며, 유무선 인터넷망(N)을 통해 접속된 상기 단말기가 보안 서비스를 요청할 경우, 상기 회원정보를 기반으로 생성한 요구정보를 상기 단말기로 전송하는 호스트서버(200)와, 상기 호스트서버와 연동되어 상기 단말기로부터 전송된 원 타임 패스워드에 대한 인증을 수행하며 상기 회원DB(210)를 공유하는 인증서버(300)로 구성되는 시스템의 단말기에 접속되어 원 타임 패스워드 생성을 수행하는 스마트카드(SC)에 있어서,

상기 요구정보에 대응하는 응답정보를 단말기로부터 전송받아 이를 초기값으로 하여 원 타임 패스워드를 생성하는 OTP 애플리케이션을 포함하고 있는 것을 특징으로 하는 원 타임 패스워드 생성을 위한 스마트카드.

청구항 14.

제 13 항에 있어서,

상기 OTP 애플리케이션은,

OTP생성 알고리즘(10), OTP 애플리케이션의 접근 인증을 위한 개인식별정보(20) 및 사용자 별로 부여되는 고유정보(30)로 구성된 애플리케이션 정보를 포함하는 것을 특징으로 하는 원 타임 패스워드 생성을 위한 스마트카드.

청구항 15.

제 14 항에 있어서,

상기 개인식별정보(20)는,

PIN정보 또는 생체인식정보인 것을 특징으로 하는 원 타임 패스워드 생성을 위한 스마트카드.

청구항 16.

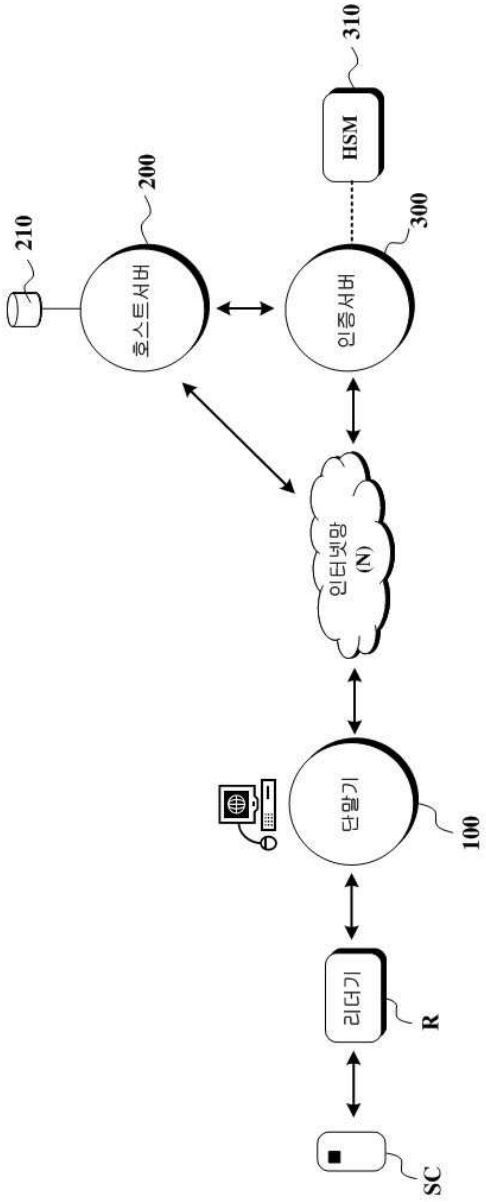
제 14 항에 있어서,

상기 OTP생성 알고리즘(10)은,

비밀키 암호화 방식이 구현된 알고리즘인 것을 특징으로 하는 원 타임 패스워드 생성을 위한 스마트카드.

도면

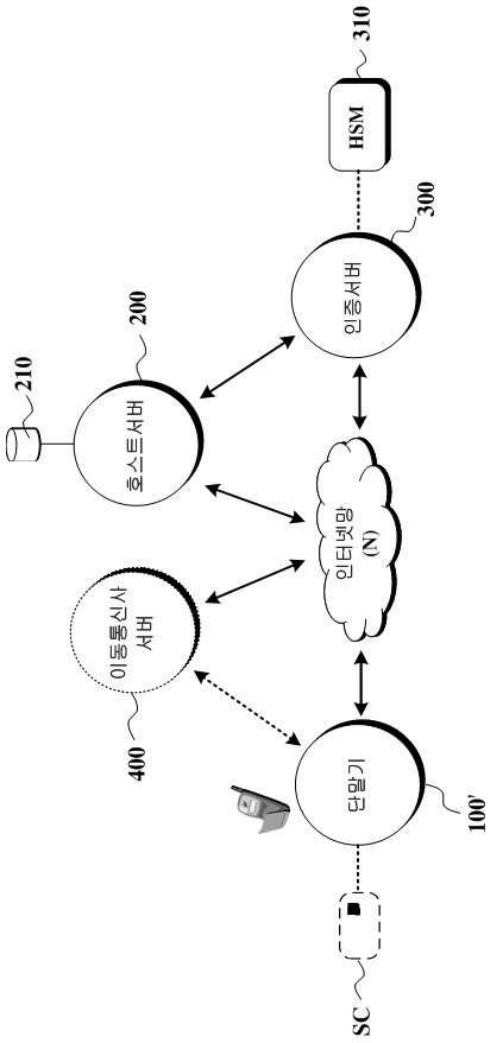
도면1



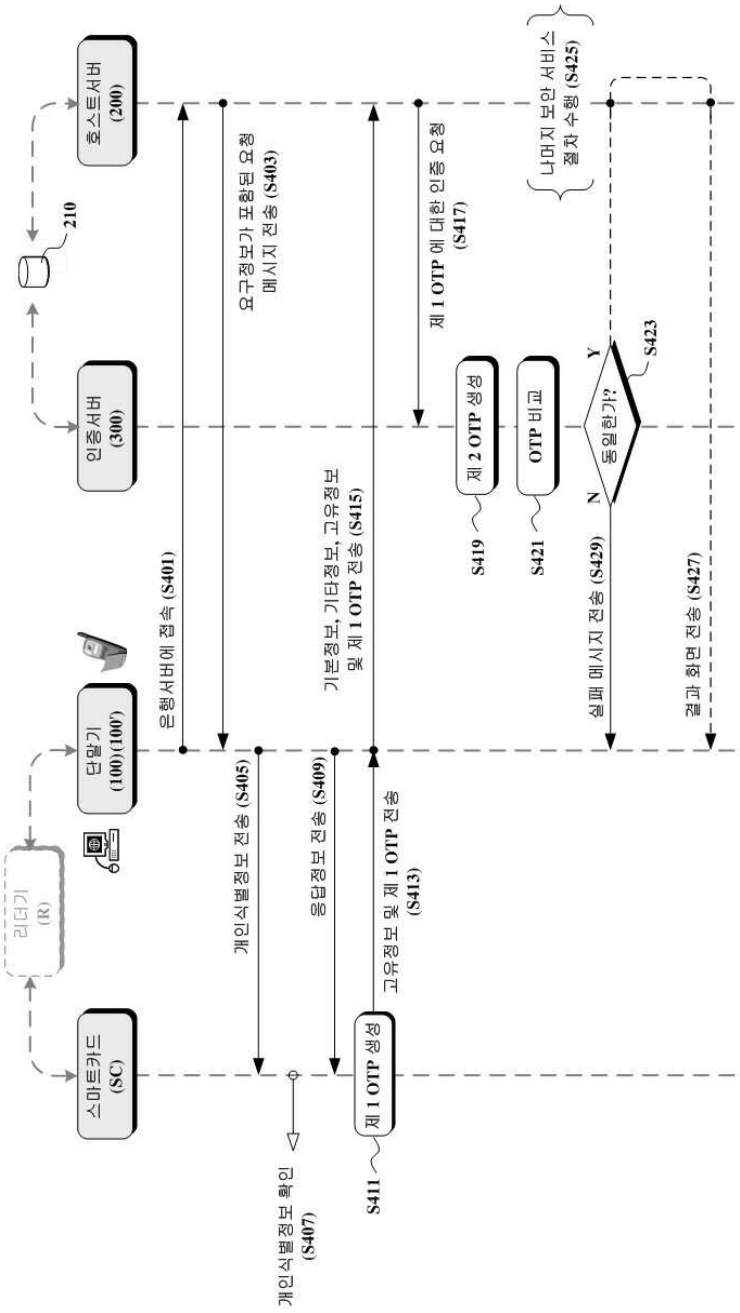
도면2


OTP생성 알고리즘
10
개인식별정보
20
고유정보
30
OTP 애플리케이션

도면3


310
HSM
300
인증서버
200
210
호스트서버
인터넷망
(N)
이동통신사
서버
400
단말기
100'
SC

도면4


호스트서버 (200)
210
인증서버 (300)
단말기 (100)(100')
리더기 (R)
스마트카드 (SC)
은행서버에 접속 (S401)
요구정보가 포함된 요청 메시지 전송 (S403)
제 1 OTP 에 대한 인증 요청 (S417)
나머지 보안 서비스 절차 수행 (S425)
제 2 OTP 생성
S419
OTP 비교
S421
동일한가?
Y
N
S423
실패 메시지 전송 (S429)
결과 화면 전송 (S427)
기본정보, 기타정보, 고유정보 및 제 1 OTP 전송 (S415)
개인식별정보 전송 (S405)
응답정보 전송 (S409)
고유정보 및 제 1 OTP 전송 (S413)
제 1 OTP 생성
S411
개인식별정보 확인 (S407)