(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2012 년 8 월 16 일 (16.08.2012)

WIPO | PCT

(10) 국제공개번호
WO 2012/108661 A2

(51) 국제특허분류:
H04L 9/32 (2006.01) *G06K 9/18* (2006.01)
H04W 12/06 (2009.01)

(21) 국제출원번호: PCT/KR2012/000879

(22) 국제출원일: 2012 년 2 월 7 일 (07.02.2012)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2011-0011190 2011 년 2 월 8 일 (08.02.2011) KR

(72) 발명자; 겸
(71) 출원인 : **홍승의 (HONG, Seung Ui)** [KR/KR]; 서울특별시 관악구 신림 9 동 1524-9 호, 151-895 Seoul (KR).

(74) 대리인: **이준성 (LEE, Joonsung)**; 서울특별시 강남구 대치동 894-3 대치빌딩 4 층, 135-840 Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

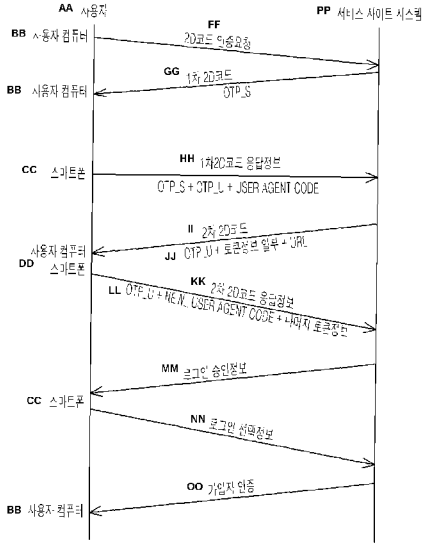
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

공개:
— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

(54) **Title**: SYSTEM AND METHOD FOR SECURITY AUTHENTICATION OF A BI-DIRECTIONAL SUBSCRIBER ON A COMMUNICATION NETWORK, AND RECORDING MEDIUM ON WHICH THE METHOD IS RECORDED

(54) **발명의 명칭** : 네트워크 통신망에서의 쌍방향 가입자 보안 인증 시스템과 방법 및 이 방법을 기록한 기록매체

[Fig. 3]



AA ... User
BB ... User computer
CC ... Smart phone
DD ... User computer
Smart phone
FF ... 2D code authentication request
GG ... First 2D code
HH ... First 2D code response information
II ... Second 2D code
JJ ... OTP_U + Part of token information + URL
KK ... Second 2D code response information
LL ... OTP_U + NEW_USER AGENT CODE + rest of token information
MM ... Login approval information
NN ... Login selection information
OO ... Subscriber authentication
PP ... Service site system
QQ ... OTP_S + OTP_U + USER AGENT CODE

(57) **Abstract**: The present invention relates to an authentication method for a subscriber accessing a network page provided on a communication network such as the internet. Generally, a method is used in which a user inputs information through a keyboard on a user's personal computer so as to access a website and log into the website. However, this method always has a risk that the confidential information can be leaked through a phishing tool that provides a function of intercepting typing performed on a keyboard. In order to solve the problem mentioned above, the present invention relates to a method for security authentication of a subscriber in a page accessed on a network without using tools in a user computer such as a keyboard and a mouse, and more particularly, a system and method for security authentication of a subscriber on a communication network, which fundamentally removes the risk of phishing by being able to authenticate a subscriber for accessing a network page throught the use of a smart phone operated by a predetermined operating system. The present invention also relates to a system and method for security authentication of a bi-directional subscriber on a communication network, wherein for performing an authentication of a subscriber on a communication network, a user is allowed to recognize whether a network page (website) which the user has accessed is a correct network page, by performing an authentication for the network page which the user is attempting to access.

(57) **요약서**:

[다음 쪽 계속]

WO 2012/108661 A2

본 발명은 인터넷과 같은 네트워크 통신망에서 제공하는 네트워크페이지의 접속 가입자 인증방법에 관한 것이다. 일반적으로 웹페이지에 접속하여 로그인하는 방법으로 사용자 개인 컴퓨터 상 에서 사용자가 키보드를 통하여 입력하는 방법을 이용하게 된다. 따라서 키보드 타이핑 가로채기 기능을 제공하는 피싱 툴에 의하여 외부 유출될 수 있는 위험성이 항상 존재한다. 본 발명에서는 이와 같은 문제점을 해소하기 위하여, 키보드, 마우스와 같이 사용자 컴퓨터 단말기내의 수단을 이용하지 않는 네트워크 접속 페이지의 가입자 인증 방법을 제시하고자 한 것으로, 소정의 운영체제에 의해 운용되는 스마트폰을 이용하여 네트워크 페이지의 접속을 위한 가입자 인증이 가능하도록 함으로써, 피싱의 위험을 근본적으로 해소한 네트워크 통신망에서의 가입자 보안 인증시스템 과 그 방법을 제공하고자 한다. 또한, 본 발명은 네트워크 통신망에서의 가입자 인증을 수행함에 있어서, 사용자가 접속 시도하는 네트워크 페이지에 대한 인증을 수행함으로써, 사용자로 하여금 자신이 접속한 네트워크 페이지(사이트)가 정당한 네트워크 페이지임을 인식할 수 있도록 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증시스템과 그 방법을 제공하고자 한다.

명세서

발명의 명칭: 네트워크 통신망에서의 쌍방향 가입자 보안 인증 시스템과 방법 및 이 방법을 기록한 기록매체

기술분야

[1] 본 발명은 인터넷과 같은 네트워크 통신망에서 제공하는 네트워크페이지의 접속 가입자 인증방법에 관한 것으로, 더 상세하게는 접속이 허용되는 가입자에 대한 보안 인증 프로세스를 제공하기 위한 것이며, 소정의 정해진 운영체제에 따라 운영되는 스마트폰을 이용하여 사용자가 접속에 이용하는 개인 단말장치(PC)에서의 보안접속이 가능하도록 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 시스템과 방법 및 이 방법을 기록한 기록매체에 관한 것이다.

배경기술

[2] 일반적으로 인터넷의 웹사이트에서는 접속자에 대한 가입자 인증과정을 수행하여 접속자가 정당한 사용자인지 여부를 확인하고 접속을 허용하고 있다.

[3] 예컨대 가입자 회원의 아이디 및 패스워드를 미리 설정하여 두고, 접속하고자 하는 사용자에게 정해진 아이디 및 패스워드를 입력하는 방식으로 가입자 인증을 수행하는 것이 일반적이다.

[4] 또한 인터넷 뱅킹이나 온라인 카드결제 등을 이용하는 경우에는 가입자 본인을 입증하는 인증서의 존부 확인과 더불어 이에 설정된 패스워드 확인을 통하여 접속을 허용하는 인증서를 이용한 인증 방법이 이용되며, 이러한 인증서를 이용하는 방법에 있어서도 OTP(One-Time Password)생성기에서 생성된 일회용 패스워드를 이용하여 부차적인 가입자를 확인하여 인증하는 보안 인증방법이 이용되고 있다.

[5] 그러나 이와 같은 모든 방법 들은 모두 사용자 개인 컴퓨터 상에서 사용자가 키보드를 통하여 입력하는 정보를 이용하는 방법으로, 키보드 타이핑 가로채기 기능을 제공하는 피싱 툴에 의하여 외부에 유출될 수 있는 위험성이 항상 존재한다.

[6] 근래에는 이와 같은 키보드 피싱 툴에 대한 문제를 해소하기 위하여 스크린 상에 가상 키패드를 나타내고, 이를 사용자가 마우스로 클릭하여 사용자 인증정보를 입력하도록 하는 방식도 제시된 바 있으나, 이러한 방식 또한 스크린 상의 마우스 입력위치의 좌표를 계산하여 해당 값을 가로채기 하는 피싱 툴에 의해 정보유출의 위험성은 항상 존재한다.

[7] 이와 같이 사용자가 이용하는 컴퓨터 단말장치를 통하여 키보드 값 또는 스크린 상에서의 마우스 좌표 입력 값을 피싱하여 사용자가 입력하는 인증정보를 언제든지 외부로 유출될 수 있는 점을 감안하여 개인 컴퓨터 단말장치만을 통한 네트워크 페이지의 접속자 인증을 수행하는 것은 더 이상 안전한

접속인증 방법이 아니어서, 새로운 가입자 인증방법이 요구되고 있다.

[8]

[9] *이에 따라서 액티브엑스 등의 방식을 통하여 피싱방지 프로그램이 유저단말에 설치되도록 하여 피싱을 방지하려는 기술이 사용되고 있다.

[10] 그러나, 피싱방지 프로그램은 고가의 프로그램에 속하므로, 모든 웹사이트에서 피싱방지프로그램을 구비하여 유저단말에 제공하기가 쉽지않다.

[11] 또한, 피싱의 유형은 날로 발전함으로써, 이에 대한 신속한 대응을 위한 피싱방지 프로그램의 빠른 업데이트가 필요하다.

[12] 따라서 사용자가 해당 페이지에 접속할 때마다 피싱방지 프로그램의 업데이트가 이루어질 수 밖에 없어서, 사용자는 안전한 접속 보안을 위하여 업데이트 시간에 대한 불편함을 감수할 수 밖에 없다.

[13] 그러나 무엇보다 각종 웹사이트를 웹 서핑하는 사용자 입장에서는, 접속된 웹사이트에서 설치를 유도하는 프로그램의 실체가 피싱 방지 프로그램인지 피싱을 하기 위하여 피싱방지 프로그램을 가장한 피싱 툴 인지의 여부를 판별하기 어렵다는 문제점이다.

[14] 이를 감안하여 가짜 웹사이트가 아닌 정당한 웹사이트 임을 알려주기 위한 미리 정해진 그래픽 씰을 미리 정하여 두고, 키보드나 마우스의 입력에 의한 로그인이나 인증 시에 미리 정해진 그래픽 씰을 표시하여 사용자가 접속한 웹사이트가 정당한 웹사이트 임을 알리는 소위 '보안 씰' 기술(야후, 옥션 등)이 제시되었다.

[15] 그러나, 이러한 방법에서도 상기에서 설명한 바와 같이, 키보드나 마우스와 같이 사용자 컴퓨터의 일 수단을 이용하는 방법으로, 피싱의 대상일 수 밖에 없어서 안전한 보안 인증방법으로 인정되기 어려운 점이 있다.

발명의 상세한 설명

기술적 과제

[16] 본 발명에서는 이와 같은 문제점을 해소하기 위하여, 키보드, 마우스와 같이 사용자 컴퓨터 단말기내의 수단을 이용하지 않는 네트워크 접속 페이지의 가입자 인증 방법을 제시하고자 한 것으로, 소정의 운영체제에 의해 운용되는 스마트폰을 이용하여 네트워크 페이지의 접속을 위한 가입자 인증이 가능하도록 함으로써, 피싱의 위험을 근본적으로 해소한 네트워크 통신망에서의 가입자 보안 인증시스템 과 그 방법을 제공하고자 한 것이다.

[17] 또한, 본 발명은 네트워크 통신망에서의 가입자 인증을 수행함에 있어서, 사용자가 접속 시도하는 네트워크 페이지에 대한 인증을 수행함으로써, 사용자로 하여금 자신이 접속한 네트워크 페이지(사이트)가 정당한 네트워크 페이지임을 인식할 수 있도록 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증시스템과 그 방법을 제공하고자 한 것이다.

과제 해결 수단

[18] 본 발명 네트워크 통신망에서의 쌍방향 가입자 보안 인증 시스템은,

[19] 서비스 사이트 시스템의 페이지에 접속하기 위한 사용자 단말수단과, 서비스 사이트 시스템에서 제공하는 2D코드를 이용한 사용자 단말수단의 로그인을 수행하기 위한 가입자 보안인증 서비스 어플리케이션이 설치된 스마트폰과, 스마트폰으로 부터의 2D코드를 이용한 로그인요청에 대하여 기가입자 보안인증과정을 수행하여 사용자 컴퓨터의 로그인을 판단 관리하는 서비스사이트시스템을 포함하여 구성되며,

[20] 서비스 사이트 시스템은 서비스 사이트의 접속을 관리하기 위한 웹서버와, 2D코드를 이용한 로그인 요청에 대하여 가입자 보안인증을 수행관리하기 위한 보안인증관리서버를 포함하여 구성되며,

[21] 보안인증관리서버는 서비스사이트 패스워드 정보를생성하기 위한 패스워드정보생성부와, 서비스 사이트에 표시할 패스워드정보를 포함하는 2D 코드를 생성하는 2D코드생성부와, 스마트폰에 전송할 정보의 생성 및 관리를 제어하고 등록된 토큰 정보에 대한 편집정보를 제공하여 스마트폰으로부터 응답된 정보를 확인하여 가입자 보안인증 요청한 가입자의 페이지 로그인을 관리제어하는 보안인증제어부와, 토큰정보 등록관리 및 사용자 관리정보(USER AGENT CODE)를 등록 관리하는 가입자식별정보관리부와, 토큰정보 및 사용자 관리정보(USER AGENT CODE)가 등록 관리되는 데이터베이스를 포함하여 구성되고,

[22] 가입자 보안인증 서비스 어플리케이션은, 서비스 사이트에 접속하여 가입자 인증을 위한 토큰정보 등록과정을 제어하는 토큰정보 등록프로세스와, 사용자의 가입자 보안인증 모드가 선택 됨을 판단하여 카메라수단을 구동하여 서비스 사이트 시스템에서 제공하는 2D코드를 스캔하기 위한 스캔관리프로세스와, 보안인증을 위한 사용자 패스워드정보를 생성하기 위한 패스워드정보생성프로세스와, 스캔된 2D코드정보를 해독하여 이에 대한 응답정보를 생성하고 생성된 정보를 전송 관리하기 위한 응답정보 생성 및 전송 프로세스와, 서비스 사이트 시스템에서의 로그인 승인정보를 사용자에게 제공하고 사용자의 선택에 따라 사용자의 로그인 선택정보를 서비스 사이트 시스템에 제공하는 로그인 승인정보 제공프로세스를 포함하는 것을 특징으로 한다.

[23] 그리고, 본 발명의 보안인증제어부는 등록된 사용자의 토큰정보 중 어느 하나를 선택하여 토큰정보의 일부정보를 가입자 확인용 편집정보로 구성하고, 스마트폰으로부터의 응답정보에 포함된 상기 가입자 확인용 편집정보를 채워줄 토큰정보로 가입자를 인증 확인하도록 프로세스를 포함하는 것을 특징으로 한다.

[24] 본 발명 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법은,

[25] 스마트폰에 설치된 어플리케이션을 통해 서비스 사이트에 접속하여 가입자 인증을 위한 토큰정보를 등록하는 스마트폰에서의 토큰정보 등록과정과,

[26] 사용자의 가입자 보안인증 모드 시도를 판단하여 서비스사이트 패스워드정보를 포함하는 2D코드를 서비스 사이트 페이지에 표시하는 서비스사이트시스템에서의 1차 2D코드생성 및 표시과정과,

[27] 사용자가 가입자 보안 인증모드를 선택하였는 가를 판단하여 구동되고 스캔입력이 확인되는 1차 2D코드를 스캔하여 서비스사이트 패스워드정보를 확인하고 사용자 패스워드정보를 생성하여 서비스사이트 패스워드 정보와 생성한 사용자 패스워드정보 및 사용자 관리정보를 미리 설정되어있는 위치정보(URL)로 전송하는 사용자 스마트폰에서의 1차 2D코드 응답정보 생성 및 전송과정과,

[28] 상기 스마트폰의 2D코드 응답정보 생성 및 전송과정을 통해 스마트폰으로부터 2D코드에 대한 응답정보가 수신되면, 수신된 2D코드에 대한 응답정보로부터 상기 서비스사이트의 1차 2D코드생성 및 표시과정을 통해 전송한 서비스사이트 패스워드정보인지를 확인하고 사용자 관리정보(USER AGENT CODE)와 매칭되는 토큰정보를 로드하여 로드된 토큰정보를 편집하여 2D코드에 대한 응답정보에 포함된 사용자 패스워드정보와 편집된 토큰정보와 최종 사용자정보를 제공받을 위치정보(URL)를 포함하는 2차 2D코드를 생성하여 사용자의 접속페이지에 표시하는 서비스사이트시스템에서의 2차 2D코드 생성 및 표시과정과,

[29] 사용자의 스캔선택 입력을 판단하여 확인되는 2차 2D코드를 스캔하여 2차 2D코드에 포함된 정보로부터 자신이 전송했던 사용자 패스워드정보를 확인하고 편집된 토큰정보로부터 해당하는 토큰정보를 판단하여 전송한 편집된 토큰정보에 대한 응답정보를 생성하고, 새롭게 교체할 사용자 관리정보(NEW_USER AGENT CODE)를 생성하여 사용자 패스워드정보와 생성된 응답 토큰정보 및 새롭게 교체할 사용자관리정보를 2차 2D코드에 대한 응답정보로 전송하는 사용자 스마트폰에서의 2차 2D코드 응답정보 생성 및 전송과정과,

[30] 사용자 스마트폰으로부터 2차 2D코드 응답정보가 수신되면, 수신된 2차 2D코드 응답정보로부터 토큰정보를 확인하여 응답 토큰정보가 전송한 올바른 토큰정보인 지를 판단하여 올바른 응답정보로 판단되면 토큰정보에 해당하는 사용자에 등록된 사용자 관리정보(USER AGENT CODE)를 수신된 새롭게 교체할 사용자 관리정보(NEW_USER AGENT CODE)로 교체하여 등록하고 사용자 스마트폰의 어플리케이션으로 로그인 승인정보를 전송하는 서비스사이트시스템에서의 접속허가 판단 및 인증과정과,

[31] 서비스 사이트 시스템에서 전송한 로그인승인정보로부터 사용자가 로그인 할 수 있도록 로그인 선택수단을 생성하여 표시하고, 사용자가 로그인 선택수단을 입력하면 로그인 선택정보를 서비스사이트로 전송하는 사용자 스마트폰에서의 로그인과정과,

[32] 사용자스마트폰으로부터 로그인 선택정보가 입력되면 해당 서비스사이트

시스템의 웹페이지의 로그인을 허가하여 접속 인증을 완료하는 서비스 사이트시스템에서의 접속완료과정을 포함하여 이루어지는 것을 특징으로 한다.

발명의 효과

[33] 이와 같은 본 발명에 따르면, 사용자의 컴퓨터단말기의 디바이스를 이용하지 않고 스마트폰을 이용하여 간단히 서비스 사이트의 페이지에 접속할 수 있어, 그 편의성을 더 할 수 있음은 물론, 네트워크 상의 인증에 대한 불안감을 해소할 수 있는 보안인증을 수행할 수 있다.

[34] 또한 사용자가 접속하고자 하는 서비스 사이트 시스템과 가입자 간의 쌍방향 보안인증이 이루어질 수 있도록 함으로써, 안전한 이중 보안 시스템을 제공할 수 있다.

[35] 가입자 보안인증과정에 있어서, 스마트폰에 인증과정의 가입자 맞춤형 광고정보 및 공지정보를 제공함으로써, 효과적인 광고정보 제공 및 공지안내가 가능해지며, 사용자는 스마트폰에 적절한 안내정보를 저장해두고 손쉽게 접근할 수 있다.

도면의 간단한 설명

[36] 도 1은 본 발명 네트워크 통신망에서의 쌍방향 가입자 보안 인증 시스템의 개략적인 구성을 나타낸 도면.

[37] 도 2는 본 발명 네트워크 통신망에서의 쌍방향 가입자 보안 인증 시스템의 구성을 나타낸 블록도.

[38] 도 3은 본 발명에 있어서, 가입자 보안 인증과정을 나타낸 챠트.

[39] 도 4는 본 발명에 있어서, 스마트폰에서 이루어지는 토큰 등록과정을 나타낸 플로우챠트.

[40] 도 5는 본 발명에 있어서, 서비스 사이트 시스템에서 이루어지는 토큰 등록과정을 나타낸 플로우챠트.

[41] 도 6은 본 발명에 있어서, 2D코드가 표시된 사용자 컴퓨터 로그인 화면의 일 예를 나타낸 도면.

[42] 도 7은 본 발명에 있어서, 사용자 스마트폰을 이용하여 사용자 컴퓨터에 표시된 2D 코드를 스캔하는 상태를 나타낸 도면.

[43] 도 8은 본 발명에 있어서, 서비스 사이트 시스템의 로그인 허용에 대하여 사용자 스마트폰에 나타난 로그인 허용의 일 예를 나타낸 도면.

[44] 도 9는 본 발명에 있어서, 스마트폰을 이용하여 로그인 서비스를 수행하여 로그인된 사용자 컴퓨터의 일 예를 나타낸 도면.

[45] 도 10은 본 발명 네트워크 통신망에서의 쌍방향 가입자 보안 인증 시스템의 다른 실시 예 구성을 나타낸 블록도.

발명의 실시를 위한 최선의 형태

[46] 이와 같은 본 발명 네트워크 통신망에서의 쌍방향 가입자 보안 인증 시스템과 방법을 첨부된 도면 도 1 내지 도 5에 도시된 실시 예를 참조하여 그 구성 및

작용을 설명하면 다음과 같다.

[47] 서비스 사이트 시스템(300)의 웹페이지에 접속하기 위한 사용자 컴퓨터(100)와, 서비스 사이트 시스템(300)에서 제공하는 2D코드를 이용한 사용자 컴퓨터(100)의 로그인을 수행하기 위한 가입자 보안인증 서비스 어플리케이션이 설치된 스마트폰(200)과, 스마트폰(200)으로 부터의 2D코드를 이용한 로그인요청에 대하여 가입자 보안인증과정을 수행하여 사용자 컴퓨터(100)의 로그인을 판단 관리하는 서비스사이트시스템(300)을 포함하여 구성된다.

[48] 서비스사이트 시스템(300)은 서비스 사이트의 접속을 관리하기 위한 웹서버(310)와, 2D코드를 이용한 로그인 요청에 대하여 가입자 보안인증을 수행관리하기 위한 보안인증관리서버(320)를 포함하여 구성되며,

[49] 보안인증관리서버(320)는 서비스사이트 OTP정보(OTP_S)를 생성하기 위한 OTP생성부(321)와, 서비스 사이트에 표시할 2D 코드를 생성하는 2D코드생성부(322)와, 생성된 OTP정보 및 2D코드를 전송 관리하고 스마트폰(200)로부터 수신되는 정보를 확인하여 가입자 보안인증 요청한 가입자의 웹페이지 로그인을 관리제어하는 보안인증제어부(323)와, 토큰정보 등록관리 및 사용자 관리정보(USER AGENT CODE)를 등록 관리하는 가입자식별정보관리부(324)와, 토큰정보 및 사용자 관리정보(USER AGENT CODE)가 등록 관리되는 데이터베이스(325)를 포함하여 구성된다.

[50] 이와 같은 본 발명에 있어서,

[51] 상기 사용자 컴퓨터(100)는 네트워크를 통해 서비스 사이트에 접속하기 위한 사용자 단말수단으로, 네트워크 접속수단 및 웹페이지 표시수단을 포함하는 데스크탑, 노트북, 타블렛 PC 등을 포함할 수 있다.

[52]

[53] *상기 스마트폰(200)은 소정의 운영체제로 운영되는 개인 휴대용 통신단말수단이며, 무선인터넷접속수단, 외부 이미지를 스캔 취득하기 위한 카메라수단을 포함하여 구성되고, 상기 운영체제에 의해 운용되는 가입자 보안인증 서비스 어플리케이션이 설치된다.

[54] 상기 가입자 보안인증 서비스 어플리케이션은 사용자가 해당 운영체제에 대한 어플리케이션 또는 서비스 사이트 시스템(300)에서 운영하는 시스템으로부터 제공받아 설치 가능한 것으로, 일명 '어플'이라한다.

[55] 가입자 보안인증 서비스 어플리케이션은, 서비스 사이트에 접속하여 가입자 인증을 위한 토큰정보 등록과정을 제어하는 토큰정보 등록프로세스와, 사용자의 가입자 보안인증 모드가 선택 됨을 판단하여 카메라수단을 구동하여 서비스 사이트 시스템(300)에서 제공하는 2D코드를 스캔하기 위한 스캔관리프로세스와, 보안인증을 위한 사용자 OTP정보를 생성하기 위한 OTP정보생성프로세스와, 스캔된 2D코드정보를 해독하여 이에 대한 응답정보를 생성하고 생성된 정보를 전송 관리하기 위한 응답정보 생성 및 전송 프로세스와,

서비스 사이트 시스템에서의 로그인 승인정보를 사용자에게 제공하고 사용자의 선택에 따라 사용자의 로그인 선택정보를 서비스 사이트 시스템에 제공하는 로그인 승인정보 제공프로세스를 포함한다.

[56] 웹서버(310)는 일반적인 웹페이지의 접속관리를 위한 서버수단이며, 보안인증관리서버(320)는 2D코드를 이용한 로그인 요청에 대하여 스마트폰(200)을 이용한 가입자 보안인증을 수행관리하기 위한 서버수단이다.

[57] 보인인증관리서버(320)는 웹서버(310) 내에 보안인증관리수단으로 통합하여 구성될 수 있다.

[58] OTP 생성부(321)는 보안인증을 수행하기 위한 일회용 패스워드정보를 생성하기 위한 수단으로, 본 실시 예에서는 패스워드정보생성수단으로 OTP생성프로세스로 OTP생성부(321)를 구성하며, OTP 정보외에도 다양한 패스워드 생성프로세스를 이용하여 구현 가능하다.

[59] OTP 생성부(321)는 2D코드 생성시 서비스 사이트 OTP정보(OTP_S)를 생성하기 위한 수단이다.

[60] OTP 정보의 생성은 난수 발생 기술을 기반으로 하여 종래의 다양한 기법에 의하여 구현가능하다.

[61] 2D코드생성부(322)는 서비스 사이트에 표시할 2D 코드를 생성하기 위한 수단으로 보안인증제어부(323)의 제어에 따라서 가입자 인증 서비스를 수행함에 있어, 1차 2D코드 및 2차 2D코드를 생성한다.

[62] 2D코드는 화면상에 표시되는 그래픽 태그를 총칭하는 것으로서, 정보를 그래픽 태그로 표현한 것이다.

[63] 이와 같은 2D코드는 종래의 바코드, QR코드, MS_Tag는 물론 향후 구현될 어떠한 코드나 태그도 포함될 수 있는 것으로, 정보를 화면상의 그래픽요소로 표현된 것을 나타낸다.

[64] 보안인증제어부(323)는 가입자 보안인증서비스의 전반적인 실행을 제어하기 위한 제어수단으로, 2D코드생성부(322) 및 OTP생성부(321)을 제어하여 OTP 정보(OTP_S)의 생성, 생성된 OTP정보(OTP_S)를 포함하는 2D코드의 생성 및 전송 관리하고 스마트폰(200)로부터 수신되는 정보를 확인하여 보안인증 요청한 가입자의 웹페이지 로그인을 관리제어하는 프로세스를 제공한다.

[65] 가입자식별정보관리부(324)는 가입자가 스마트폰(200)의 가입자 보안인증 서비스 어플을 이용하여 등록하는 토큰정보 및 어플에 부여된 사용자 관리정보(USER AGENT CODE)를 등록 관리하는 수단이다.

[66] 데이터 베이스(325)는 토큰정보 및 사용자 관리정보(USER AGENT CODE)가 등록 관리된다.

[67] 이와 같은 구성으로 이루어진 본 발명 시스템은 다음과 같은 과정을 통하여 쌍방향 가입자 보안 인증을 수행한다.

[68] 스마트폰(200)을 이용한 가입자 보안인증 서비스를 이용하기 위하여 스마트폰(200)에 설치된 어플리케이션을 통해 서비스 사이트에 접속하여 가입자

인증을 위한 토큰정보를 등록하는 스마트폰(200)에서의 토큰정보 등록과정과,

[69] 사용자의 가입자 보안인증 모드 시도를 판단하여 서비스사이트 OTP정보(OTP_S)를 포함하는 2D코드를 웹페이지에 표시하는 서비스사이트시스템(300)에서의 1차 2D코드생성 및 표시과정과,

[70] 사용자가 가입자 보안 인증모드를 선택하였는 가를 판단하여 구동되고 스캔입력 확인되는 1차 2D코드를 스캔하여 서비스사이트 OTP정보(OTP_S)를 확인하고 사용자 OTP정보(OTP_U)를 생성하여 서비스사이트 OTP 정보(OTP_S)와 생성된 사용자 OTP정보(OTP_U) 및 사용자 관리정보(USER AGENT CODE)를 미리 설정되어있는 위치정보(URL)로 전송하는 사용자 스마트폰(200)에서의 1차 2D코드 응답정보 생성 및 전송과정과,

[71] 상기 스마트폰(200)의 2D코드 응답정보 생성 및 전송과정을 통해 스마트폰(200)으로부터 2D코드에 대한 응답정보가 수신되면, 수신된 2D코드에 대한 응답정보로부터 상기 서비스사이트의 1차 2D코드생성 및 표시과정을 통해 전송한 서비스사이트 OTP정보(OTP_S)인지를 확인하고 사용자 관리정보(USER AGENT CODE)와 매칭되는 토큰정보를 로드하여 로드된 토큰정보의 일부만을 편집하여 2D코드에 대한 응답정보에 포함된 사용자 OTP정보(OTP_U)와 토큰정보의 일부와 최종 사용자정보를 제공받을 위치정보(URL)를 포함하는 2차 2D코드를 생성하여 사용자의 접속페이지에 표시하는 서비스사이트시스템(300)에서의 2차 2D코드 생성 및 표시과정과,

[72] 사용자의 스캔선택 입력을 판단하여 확인되는 2차 2D코드를 스캔하여 2차 2D코드에 포함된 정보로부터 자신이 전송했던 사용자 OTP정보(OTP_U)를 확인하고 수신된 토큰정보의 일부로부터 해당하는 토큰정보를 판단하여 전송한 나머지 토큰정보를 생성하고, 새롭게 교체할 사용자 관리정보(NEW_USER AGENT CODE)를 생성하여 사용자 OTP정보(OTP_U)와 생성된 나머지 토큰정보 및 새롭게 교체할 사용자관리정보를 2차 2D코드에 대한 응답정보로 전송하는 사용자 스마트폰(200)에서의 2차 2D코드 응답정보 생성 및 전송과정과,

[73] 사용자 스마트폰(200)으로부터 2차 2D코드 응답정보가 수신되면, 수신된 2차 2D코드 응답정보로부터 나머지 토큰정보를 확인하여 나머지 토큰정보가 전송한 토큰정보를 채울 수 있는 정보인 지를 판단하여 채울 수 있는 정보로 판단되면 토큰정보에 해당하는 사용자에 등록된 사용자 관리정보(USER AGENT CODE)를 수신된 새롭게 교체할 사용자 관리정보(NEW_USER AGENT CODE)로 교체하여 등록하고 사용자 스마트폰의 어플리케이션으로 로그인 승인정보를 전송하는 서비스사이트시스템(300)에서의 접속허가 판단 및 인증과정과,

[74] 서비스 사이트 시스템(300)에서 전송한 로그인승인정보로부터 사용자가 로그인 할 수 있도록 로그인 선택수단을 생성하여 표시하고, 사용자가 로그인 선택수단을 입력하면 사용자가 로그인 선택수단을 입력했음을 알리는 로그인 선택정보를 서비스 사이트 시스템(300)으로 전송하는 사용자

스마트폰(200)에서의 로그인과정과,

[75] 사용자스마트폰(200)으로부터 로그인 선택정보가 입력되면 해당 서비스사이트 시스템(300)의 웹페이지의 로그인을 허가하여 접속 인증을 완료하는 서비스 사이트시스템(300)에서의 접속완료과정을 포함하여 이루어진다.

[76] 이와 같은 수행과정으로 이루어지는 본 발명에 있어서,

[77] 스마트폰(200)에서의 토큰정보 등록과정은, 가입자의 식별정보로서 토큰정보를 서비스 사이트 시스템(300) 및 스마트폰(200)에 등록하기 위한 과정이다.

[78] 토큰정보는 가입자를 식별하기 위하여 등록되는 정보로서, 숫자조합, 문장(텍스트), 이미지(image) 등의 정보로 구성되며, 사용자가 필요에 따라서 스마트폰(200)을 통하여 등록한다.

[79] 도 4는 스마트폰에서 이루어지는 토큰등록정보 등록과정을 나타낸 플로우 챠트이다.

[80] 사용자로부터 토큰정보 등록 모드가 선택되면, 서비스 사이트 시스템(300)의 가입자 아이디와 패스워드를 요청하여 서비스 사이트 시스템에 접속 요구하는 로그인 요청과정과,

[81] 서비스 사이트 시스템(300)에 접속되면, 토큰정보로 등록할 수 있는 토큰정보선택메뉴를 제공하여 사용자로 하여금 등록할 토큰정보를 선택하여 입력하도록 하는 사용자 토큰정보 입력과정과,

[82] 사용자가 선택 입력한 토큰정보를 저장하고, 이를 기반으로 서비스 사이트 시스템에 전송하기 위한 토큰정보를 생성하는 토큰정보생성과정과,

[83] 생성된 토큰정보를 정해진 서비스 사이트 시스템(300)의 위치정보(URL)로 전송하는 토큰정보 전송과정과,

[84] 서비스 사이트 시스템(300)으로부터 사용자 관리정보(USER AGENT CODE)가 수신되면 새로운 사용자 관리정보(USER AGENT CODE)로 기존의 사용자 관리정보(USER AGENT CODE)를 새로운 사용자 관리정보(USER AGENT CODE)로 교체하는 사용자관리정보 관리과정으로 이루어진다.

[85] 여기에서 최초구동상태인 지를 확인하고, 최초 구동 상태인 경우에는 어플리케이션 구동에 필요한 가입자 설정 등록모드를 수행하도록 하는 사용자 설정등록모드설정과정을 더 포함할 수 있다.

[86] 즉, 토큰정보 등록과정이 아니더라도 가입자 보안인증 서비스 어플리케이션을 최초 구동하면 가입자 설정등록모드를 수행하도록 그 수행과정을 구성할 수 있다.

[87] 사용자 설정등록모드는 가입자 보안인증 서비스 어플리케이션의 구동 및 삭제방지를 위한 비밀번호 설정 및 어플리케이션에서 스마트폰의 위치정보를 이용할 수 있도록 하는 위치정보사용동의 정보를 포함하는 것으로, 사용자 설정등록모드는 필요에 따라서 서비스 사이트 시스템(300)과의 접속과 상관없이

가입자 보안인증서비스 어플리케이션을 구동하여 수행가능하다.

[88] 사용자 설정등록모드는 어플리케이션을 사용함에 있어서의 다양한 사용자 옵션 항목을 더 설정하여 구성할 수 있다.

[89] 도 5는 서비스 사이트 시스템에서 이루어지는 토큰정보 등록과정을 나타낸다.

[90] 접속된 스마트폰(200)의 가입자 보안인증 서비스 어플리케이션으로부터 등록할 토큰정보가 수신되면, 접속된 스마트폰(200)의 아이디와 패스워드에 맞추어 토큰정보를 매칭시켜 등록하는 토큰정보등록과정과,

[91] 토큰정보를 매칭시킨 접속 스마트폰(200)의 가입자 보안인증 서비스 어플리케이션의 새로운 사용자관리정보(USER AGENT CODE)를 생성하여 전송하는 사용자관리정보 전송과정을 포함하여 이루어진다.

[92] 이와 같이 등록되는 사용자 토큰정보 대신 가입자의 휴대전화번호, 맥어드레스와 같은 서비스 사이트시스템(300)에 등록된 정보로 자동 구성할 수 있다.

[93] 서비스사이트시스템(300)의 1차 2D코드생성 및 표시과정은 사용자의 접속시도에 대하여 2차코드를 통한 로그인을 수행하도록 하기 위하여 스마트폰(200)에서 스캔할 수 있도록 사용자 컴퓨터(100) 상에 표시되는 접속 페이지에 제공하는 과정이다.

[94] 상기 서비스사이트시스템(300)의 1차 2D코드생성 및 표시과정에서의, 1차로 사용자 컴퓨터(100)상의 접속 웹페이지 로그인창에 표시되는 1차 2D코드는 서비스 사이트 시스템(300)의 OTP 정보(OTP_S)만을 포함한다.

[95] 사용자 스마트폰(200)에서의 1차 2D코드 응답정보 생성 및 전송과정은, 상기 서비스 사이트시스템(300)에서 제공하는 1차 2D코드에 대한 응답정보를 전송하는 과정이다.

[96] 스마트폰(200)에서는 웹페이지에 표시된 1차 2D 코드에 대한 스캔입력으로부터 서비스 사이트 시스템(300)의 OTP 정보(OTP_S)를 확인하고, 가입자 보인인증 서비스 어플리케이션에 설정되어 있는 URL 정보에 따라 1차 2D 코드에 대한 응답정보를 전송한다.

[97] 그 전송되는 응답정보는 생성된 사용자 OTP정보(OTP_U)와 1차 2D 코드에 포함된 서비스 사이트 OTP정보(OTP_S)와 가입자 보안인증 서비스 어플리케이션의 사용자관리정보(USER AGENT CODE)를 포함한다.

[98] 사용자관리정보(USER AGENT CODE)는 서비스 사이트 시스템(300)과 스마트폰(200)간에 정보를 주고 받음에 있어서, 접근한 어플리케이션의 인식 및 토큰정보를 등록한 가입자 확인을 위한 정보로 보안을 위하여 정보를 주고받으면서 로그인 또는 인증절차 1회 이후에는 교체되는 정보이다.

[99] 서비스 사이트 시스템(300)에서의 2차 2D코드 생성 및 표시과정은, 스마트폰(200)으로 부터의 응답정보를 이용하여 자신이 전송한 1차 2D코드 정보에 대한 응답정보인 지를 확인하고, 가입자 인증을 위하여 사용자 OTP정보(OTP_U)와 토큰정보의 일부와 최종 사용자정보를 제공받을

위치정보(URL)를 포함하는 2차 2D코드를 생성하여 사용자의 접속페이지에 표시하는 과정이다.

[100] 사용자 스마트폰(200)에서의 2차 2D코드 응답정보 생성 및 전송과정은,

[101] 사용자의 스캔선택 입력을 판단 확인되는 2차 2D코드를 스캔하여 2차 2D코드에 포함된 정보로부터 자신이 전송했던 사용자 OTP정보(OTP_U)를 확인하고 수신된 토큰정보에 대한 나머지 토큰 정보를 응답하여 가입자 인증을 받기 위한 과정이다.

[102] 새롭게 교체할 사용자 관리정보(NEW_USER AGENT CODE)를 생성하여 사용자 OTP정보(OTP_U)와 나머지 토큰정보 및 생성한 새롭게 교체할 사용자관리정보(NEW_USER AGENT CODE)를 2차 2D코드에 대한 응답정보로 전송한다.

[103] 서비스 사이트 시스템(300)에서의 접속허가 판단 및 인증과정은 사용자 스마트폰(200)으로 수신된 응답정보에서 나머지 토큰정보를 확인하여 정당한 사용자인지를 판단하여 가입자 보안인증을 수행하기 위한 과정이다.

[104] 사용자 스마트폰(200)에서 전송한 나머지 토큰정보가 전송한 토큰정보를 채울 수 있는 정보인 지를 판단하여 채울 수 있는 정보로 판단되면 토큰정보에 해당하는 사용자에 등록된 사용자 관리정보(USER AGENT CODE)를 수신된 새롭게 교체할 사용자 관리정보(NEW_USER AGENT CODE)로 교체하여 등록한다.

[105] 사용자 스마트폰(200)에서의 로그인과정은, 서비스 사이트 시스템(300)에서 전송한 로그인 승인정보로부터 사용자가 선택한 로그인 선택수단(로그인 버튼)을 표시하여 사용자가 로그인할 수 있도록 하는 과정이다.

[106] 서비스 사이트 시스템(300)에서의 접속완료과정은, 서비스 사이트 시스템(300)에서 사용자 스마트폰(200)으로부터 사용자가 로그인을 선택했는지 여부를 판단하여 해당 서비스 사이트의 로그인을 승인하는 과정이다.

[107] 이와 같은 구성을 특징으로 하는 본 발명의 동작과정을 상세히 설명하면 다음과 같다.

[108] 사용자는 본 발명에서 제안하는 스마트폰(200)을 이용하여 해당하는 웹사이트 페이지의 로그인을 하기 위한 가입자 보안 인증 서비스를 이용하기 위해서는 먼저 스마트폰(200)에 가입자 보안인증 서비스 어플리케이션(이하 '어플'이라고 함)을 설치해야한다.

[109] 사용자는 이와 같은 어플을 이용하여 서비스 사이트 시스템(300)의 2D코드를 이용한 로그인을 요청하여 가입자 인증을 받을 수 있다.

[110] 서비스 사이트 시스템(300)에서는

[111] 사용자는 상기와 같이, 스마트폰(200)을 이용한 웹페이지의 로그인을 수행하는 가입자 보안인증 서비스를 이용하기 위해서는 먼저 토큰정보를 서비스 사이트 시스템(300)에 등록해야 한다.

[112] 토큰정보의 등록과정은 도 4 및 도 5에 도시된 플로우 챠트에 나타낸 바와 같다.

[113] 사용자가 어플을 실행하여 토큰정보에 대한 등록을 선택하게 되면, 토큰등록을 위하여 서비스 사이트 시스템(300)에 접속하기 위한 어플에서는 아이디와 패스워드를 요청하게 된다.

[114] 이때, 어플을 설치하고 최초구동한 상태라면, 어플은 실행되면서 어플실행 및 삭제방지를 위한 비밀번호 설정 및 현재위치정보를 어플에서 이용가능 하도록 할 것인지를 설정하기 위한 사용자 설정등록 모드를 먼저 수행하게 된다.

[115] 사용자는 어플의 실행시 비밀번호를 이용하고자 하면 사용자 설정등록 모드에서 비밀번호를 설정하면 된다.

[116] 대부분의 사용자들은 스마트폰(200)을 전체적으로 록(LOCK)을 걸어 사용하는 경우가 대부분이어서 어플 단독에 대한 비밀번호를 설정하도록 할 필요는 없으나, 사용자가 필요에 따라서 설정할 수 있다.

[117] 토큰정보도 등록하지 않은 상태라면 어플에서는 최초 구동시에도 토큰정보 등록 모드를 자동 수행하도록 할 수 있다.

[118] 토큰정보는 사용자가 필요에 따라서 어플 내에서 토큰정보 등록모드를 수행하여 서비스 사이트 시스템(30) 및 어플 내에 등록 저장 관리할 수 있다.

[119] 토큰정보 등록모드를 실행하게 되면, 어플에서는 서비스 사이트 시스템(300)에 접속하기 위한 아이디와 패스워드를 사용자에게 요청한다.

[120] 사용자는 스마트폰(200)에 서비스 사이트 시스템(300)에 등록된 아이디와 패스워드를 입력하여 로그인을 요청한다.

[121] 서비스 사이트 시스템(300)에서는 입력된 아이디와 패스워드를 확인하여 정당한 사용자인 지를 확인하여 스마트폰(200)의 접속을 승인한다.

[122] 이후, 어플에서는 토큰정보선택메뉴를 제공하여 사용자로 하여금 등록할 토큰정보를 선택하여 입력할 수 있도록 한다.

[123] 사용자는 자신이 원하는 숫자조합 또는 스마트폰(200)을 이용하여 자신의 모습을 촬영하거나, 기 촬영된 이미지 또는 텍스트정보를 선택하여 토큰정보로 입력한다.

[124] 어플에서는 사용자가 입력한 토큰정보를 저장 및 토큰정보를 기반으로 하여 서비스 사이트 시스템(300)에 등록하기 위한 전송데이터를 생성한다.

[125] 생성된 토큰정보를 정해진 서비스 사이트 시스템(300)의 위치정보(URL)로 전송한다.

[126] 서비스 사이트 시스템(300)에서는 접속된 스마트폰(200)의 가입자 보안인증 서비스 어플리케이션으로부터 등록할 토큰정보가 수신되면, 접속된 스마트폰(200)의 아이디를 확인하여 해당 아이디에 맞추어 토큰정보를 매칭시켜 등록한다.

[127] 토큰정보의 등록이 완료되면, 토큰정보를 등록한 스마트폰(200)의 가입자 보안인증 서비스 어플리케이션의 새로운 사용자관리정보(USER AGENT CODE)를 생성하여 전송한다.

[128] 서비스 사이트 시스템(300)으로 부터 사용자 관리정보(USER AGENT CODE)가

수신되면 수신된 사용자 관리정보(USER AGENT CODE)를 기존의 사용자 관리정보(USER AGENT CODE) 대신에 교체하여 저장한다.

[129] 이와 같은 동작과정으로 토큰정보가 등록된다.

[130] 토큰정보 등록모드는 등록된 토큰정보의 삭제모드를 포함하는 것으로, 사용자가 토큰정보를 기 등록된 토큰정보의 삭제 및 새로운 토큰정보의 등록을 관리하도록 할 수 있다.

[131] 한편 가입자 보안인증 서비스 과정은 다음과 같은 동작으로 이루어진다.

[132] 도 3을 참조하여 설명하면 다음과 같다.

[133] 사용자가 사용자 컴퓨터(100)를 통해 서비스 사이트 시스템(300)의 웹사이트 페이지에 2D 코드를 통한 가입자 보안인증을 요청하게 되면, 서비스 사이트 시스템(300)의 OTP생성부(321)에서는 서비스 사이트 OTP정보(OTP_S)를 생성하고, 2D코드 생성부(322)에서는 상기와 같이 생성된 서비스 사이트 OTP정보(OTP_S)를 포함하는 1차 2D코드를 생성한다.

[134] 보안인증제어부(323)에서는 이와 같은 1차 2D를 웹서버(310)로 전송하여 웹페이지에 표시하여 사용자 컴퓨터(100)에 제공한다.

[135] 도 6은 사용자 컴퓨터(100)에 표시된 웹페이지에 2D코드를 나타낸다.

[136] 이때, 사용자 컴퓨터(100)의 가입자 보안인증 요청과 상관없이 서비스 사이트 웹페이지에 소정의 정해진 시간단위로 1차 2D코드를 생성하여 표시하도록 하여 사용자가 로그인을 원할 경우 해당하는 1차 2D코드를 이용하도록 구성할 수 있다.

[137] 사용자는 스마트폰(200)에 설치된 어플을 구동시켜 가입자 보안인증 모드를 실행하게 된다.

[138] 어플에서는 가입자 보안인증모드가 실행되면 스마트폰(200)의 카메라를 구동시켜 사용자 컴퓨터(100)에 표시된 웹페이지의 1차 2D코드를 스캔하기 위하여 대기한다.

[139] 이후 도 7에 도시된 바와 같이, 스마트폰(200)을 카메라 상에 사용자가 웹페이지의 1차 2D코드를 위치시키면 스캔하여 1차 2D코드를 입력한다.

[140] 이와 같이 1차 2D코드가 입력되면 이에 대한 응답정보를 생성하여 미리 어플에 정해져있는 URL정보로 전송하는 바, 먼저 사용자 OTP정보(OTP_U)를 생성하고, 1차 2D코드에 포함된 서비스사이트 OTP정보(OTP_S)와 생성된 OTP정보(OTP_U) 그리고 어플의 사용자관리정보(USER AGENT CODE)를 포함시켜 응답정보를 생성한다.

[141] 이와 같이 스마트폰(200)의 어플로부터 1차 2D코드에 대한 응답정보가 수신되면, 수신된 2D코드에 대한 응답정보로부터 자신이 전송한 서비스사이트 OTP정보(OTP_S)인지를 확인한다.

[142] 확인결과 서비스 사이트 시스템(300)에서 전송한 서비스 사이트 OTP정보(OTP_S)가 맞으면 응답정보를 통해 수신된 사용자 관리정보(USER AGENT CODE)와 매칭되는 토큰정보를 로드하여 가입자 확인을 위한 정보로

가공한다.

[143] 로드된 토큰정보의 일부만을 편집하여 가입자 확인을 위한 정보로 가공한다.

[144] 2D코드생성부(322)에서는 응답정보로 수신된 사용자 OTP정보(OTP_U)와 가공된 토큰정보의 일부 및 최종 사용자정보를 제공받을 URL 정보를 포함하는 2차 2D코드를 생성하여 사용자 컴퓨터(100)가 접속한 웹페이지에 표시한다.

[145] 이후 사용자는 스마트폰(100)으로 2차 2D코드를 스캔하여 2차 2D코드에 포함된 정보를 읽어들인다.

[146] 어플에서는 자신이 전송한 사용자 OTP정보(OTP_U)를 확인하고 2차 2D코드에 대한 응답정보를 준비한다.

[147] 스캔 입력된 토큰정보의 일부로부터 해당하는 토큰정보를 판단하고, 저장되어 있는 토큰정보로부터 나머지 토큰정보를 생성한다.

[148] 그리고, 새롭게 교체할 사용자 관리정보(NEW_USER AGENT CODE)를 생성하여 사용자 OTP정보(OTP_U)와 생성된 나머지 토큰정보와 함께 2차 2D코드에 대한 응답정보로 전송한다.

[149] 서비스 사이트 시스템(300)에서는 사용자 스마트폰(200)으로부터 2차 2D코드 응답정보가 수신되면, 수신된 2차 2D코드 응답정보로부터 나머지 토큰정보를 확인하여 나머지 토큰정보가 전송한 토큰정보를 채울 수 있는 정보인 지를 판단한다.

[150] 나머지 토큰정보가 채울 수 있는 정보로 판단되면 토큰정보에 해당하는 사용자에 등록된 사용자 관리정보(USER AGENT CODE)를 새롭게 수신된 사용자 관리정보(NEW_USER AGENT CODE)로 교체하여 등록한다.

[151] 이후, 사용자 스마트폰(200)의 어플로 로그인을 허가하는 로그인 승인정보를 전송한다.

[152] 스마트폰(200)의 어플에서는 이와 같은 로그인 승인정보가 수신되면, 사용자가 로그인을 선택할 수 있도록 로그인 버튼을 표시하고, 사용자가 로그인 버튼을 선택하면 사용자가 그 로그인 버튼을 선택하였다는 것을 알리는 로그인 선택정보를 서비스 사이트 시스템(300)으로 전송한다.

[153] 로그인 선택정보가 수신되면, 서비스 사이트 시스템(300)에서는 사용자 컴퓨터(100)가 접속한 웹페이지에 가입자를 인증하여 로그인을 허락하게 된다.

[154] 도 8은 로그인을 허락하게 될 때, 사용자 스마트폰(200)에 나타난 화면의 일 실시예이다.

[155] 따라서 사용자는 스마트폰(200)의 로그인 선택만으로 사용자 컴퓨터(100)에서 요청했던 도 9에서와 같이 로그인 접속이 가능해진다.

[156] 여기서, 서비스 사이트 시스템(300)에서는 로그인 승인정보를 스마트폰(200)으로만 전송하는 것이 아니라, 해당 웹페이지에도 함께 전송하여 사용자가 선택하여 로그인을 수행하도록 할 수 있다.

[157] 이와 같은 경우에는 웹페이지의 로그인화면에 로그인 선택버튼이 표시되어 사용자는 웹페이지의 로그인 선택버튼을 선택하여도 로그인이 가능 하도록 할

수 있다.

[158] 한편 본 발명의 다른 실시 예로, 로그인을 허가할 때 스마트폰(200)으로 인증가입자에 맞춤 광고정보 및 안내정보를 제공하도록 구성할 수 있다.

[159] 도 10은 본 발명 네트워크 통신망에서의 쌍방향 가입자 보안 인증 시스템의 다른 실시 예 구성을 나타낸 블록도이다.

[160] 본 발명 다른 실시 예에서는 서비스 사이트 시스템(300)의 보안인증관리서버(320)는, 보안인증제어부(323)의 로그인 인증이 확인되면 웹서버(310)에서 제공되는 가입자 정보 및 스마트폰(200)으로부터 얻어지는 위치정보에 따라서 가입자에 따른 맞춤정보 생성을 위한 프로세스를 제공하는 광고제어부(326a)와, 웹서버(310)로부터 인증된 가입자에게 제공하기 위한 서비스 사이트의 공지정보(notification data)를 제공받아 제공될 공지정보를 생성하기 위한 프로세스를 제공하는 공지제어부(326b)를 포함하는 로그인 승인정보와 함께 제공될 안내정보를 생성하기 위한 안내정보생성수단(326)과, 광고정보가 저장관리 되는 광고정보 데이터베이스(327)를 더 포함하여 구성할 수 있다.

[161] 이는 스마트폰(200)은 항상 사용자가 소지하고, 또한 쉽게 찾아 확인할 수 있는 수단임에 따라서 스마트폰(200)에 그 정보를 제공하면 효과적인 정보전달이 됨은 물론 그 유효한 기간이 늘어날 것으로 기대됨을 감안한 것이다.

[162] 이에 따르면, 서비스사이트시스템(300)에서의 접속허가 판단 및 인증과정은 접속허가가 결정되면 해당 가입자의 아이디를 확인하여 웹서버(310)로 회원가입정보 및 서비스 사이트의 공지정보를 요청하고, 해당 가입자로부터 제공되는 위치정보수신여부를 확인하여 해당 가입자에게 제공할 광고정보 및 공지정보를 포함하는 안내정보를 생성하여 로그인승인정보에 첨가하여 사용자 스마트폰(200)의 어플리케이션으로 전송하도록 하는 안내정보 생성 및 전송과정을 더 포함하고,

[163] 사용자 스마트폰(200)에서의 로그인과정은, 서비스 사이트 시스템(300)에서 전송한 로그인승인정보로부터 사용자가 로그인 할 수 있도록 로그인 선택수단을 생성하여 표시할 때, 또는 사용자가 로그인 선택수단을 입력할 때 상기 안내정보를 표시하도록 하는 안내정보표시과정을 더 포함한다.

[164] 이와 같은 본 발명 실시 예는, 서비스 사이트 시스템(300)의 보안인증제어부(323)에서 로그인 인증이 결정되면, 안내정보제어수단(326)에서는 로그인승인정보에 첨가하여 스마트폰(200)에 전송할 안내정보를 생성하게 된다.

[165] 광고제어부(326a)에서는 웹서버(310)에 요청하여 서비스 사이트에 등록된 해당 가입자의 회원가입정보와 스마트폰(200)으로부터 위치정보가 제공되었는지를 확인하여 이에 따른 광고정보를 광고정보 데이터베이스(327)로부터 추출하여 광고정보를 생성하게 된다.

[166] 즉, 회원의 등록정보에 따라서 성별, 나이, 직업에 맞춘 광고정보 및

스마트폰(200)의 위치정보에 따른 가입자의 현재 위치 주변에 관한 광고정보를 제공할 광고정보로 생성하게 됨으로써, 가입자에 대한 맞춤 광고를 제공할 수 있게 된다.

[167] 또한 공지제어부(326b)는 서비스 사이트 시스템(300)에 등록되어 있는 공지정보가 있는 지를 웹서버(310)에 요청하여 제공받아 안내정보로 제공한다.

[168] 이러한 안내정보에는 가입자에게 제공할 유용한 생활정보, 가입자가 요청한 질문에 대한 답변정보, 뉴스 등 다양한 정보를 포함하여 작성될 수 있다.

[169] 이와 같이 생성된 안내정보는 사용자 스마트폰(200)의 어플로 제공될 로그인 승인정보에 첨가되어 사용자 스마트폰(200)으로 전송된다.

[170] 서비스 사이트 시스템(300)로부터 상기와 같이 로그인 승인정보가 수신되면, 상기에서와 같이, 사용자가 로그인을 선택할 수 있도록 로그인 버튼을 표시하면서, 안내정보를 표시하거나 안내정보의 일부(타이틀)만을 표시한다.

[171] 또는 사용자가 로그인 버튼을 선택할 때 안내정보를 표시하도록 할 수 있다.

[172] 사용자 스마트폰(200)의 어플은 사용자에게 필요에 따라서 이들 안내정보를 확인, 편집 또는 삭제할 수 있는 기능을 제공한다.

[173] 이에 따라서 사용자는 스마트폰(200)의 어플을 실행시켜 저장된 광고정보 및 공지정보를 확인할 수 있으며, 필요에 따라서 편집, 삭제가 가능하다.

[174] 이와 같은 본 발명 실시 예에 있어서는 단순히 서비스 사이트의 보안인증에 관련하여 설명을 하고 있으나, 본 발명 시스템 및 방법을 은행과 같은 보안이 필요한 시스템에 적용할 경우 쌍방향 보안인증이 가능함으로써, 신뢰있는 은행시스템을 제공할 수 있음은 물론 사용자들 또한 편리하고 안전하게 보안인증 가능한 방법을 제공받을 수 있게 된다.

[175] 특히 스마트폰에서 저장 가능한 정보로 스마트폰에 광고정보 및 공지정보를 제공할 수 있음에 따라서, 은행, 보험, 증권과 같이 지속적인 상품을 안내하여야 함은 물론, 각 가입자별 공지사항이 별도로 필요한 경우 본 발명이 유용하게 적용될 수 있다.

청구범위

[청구항 1] 서비스 사이트 시스템의 페이지에 접속하기 위한 **사용자 단말수단**, 서비스 사이트 시스템에서 제공하는 2D코드를 이용한 상기 사용자 단말수단의 로그인을 수행하기 위한 가입자 **보안인증 서비스 어플리케이션**이 설치된 **스마트폰**, 상기 스마트폰으로부터의 2D코드를 이용한 로그인요청에 대하여 가입자 보안인증 과정을 수행하여 사용자 컴퓨터의 로그인을 판단 관리하는 **서비스사이트시스템**을 포함하여 구성되며,
상기 **서비스 사이트 시스템**은 서비스 사이트의 접속을 관리하기 위한 **웹서버**, 2D코드를 이용한 로그인 요청에 대하여 상기 가입자 보안인증을 수행관리하기 위한 **보안인증관리서버**를 포함하여 구성되며,
상기 **보안인증관리서버**는 서비스 사이트 패스워드정보를 생성하기 위한 **패스워드 생성부**, 상기 서비스 사이트에 표시할 패스워드정보를 포함하는 2D 코드를 생성하는 **2D코드 생성부**, 스마트폰에 제공할 정보의 생성 및 관리를 제어하고 스마트폰으로부터 응답된 정보를 확인하여 가입자 보안인증을 요청한 가입자의 페이지 로그인을 관리제어하는 **보안인증제어부**, 토큰정보 등록관리 및 사용자 관리정보(USER AGENT CODE)를 등록 관리하는 **가입자 식별정보 관리부**, 토큰정보 및 상기 사용자 관리정보(USER AGENT CODE)가 등록 관리되는 **데이터베이스**를 포함하여 구성되고,
상기 보안인증관리서버의 **보인인증제어부**는, 접속된 사용자 단말기의 보안인증 모드 요청에 따라서 2D코드 생성부를 통해 2D코드를 생성하여 사용자 단말기에 표시제어, 스마트폰으로 수신된 2D코드에 대한 1차 응답정보에 포함된 상기 패스워드생성부를 통해 생성된 패스워드정보를 확인하여 서비스 사이트 시스템의 2D코드에 대한 스캔응답정보인가를 판단, 1차 응답정보에 포함된 사용자 관리정보(USER AGENT CODE)에 따라서 가입자를 판단하여 해당 가입자의 상기 데이터베이스에 등록된 토큰정보를 로드하여 가입자 확인용 편집 토큰정보로 편집, 가입자 확인용 편집 토큰정보와 1차 응답정보에 포함된 사용자 패스워드정보를 포함하는 2D코드를 2D코드 생성부를 통해 생성하여 사용자 단말기에 표시, 2차 2D코드에 대한 2차 2D코드 응답정보에 포함된 응답토큰 정보를 확인하여 가입자 확인용 편집 토큰정보에 올바른 응답토큰 정보 인가를 확인하여 가입자를 인증 확인하는 프로세스가 포함되고,

상기 **가입자 보안인증 서비스 어플리케이션**은, 상기 서비스 사이트에 접속하여 가입자 인증을 수행하기 위한 토큰정보에 대한 등록과정을 제어하는 **토큰정보 등록프로세스**, 사용자의 가입자 보안인증 모드가 선택됨을 판단하여 카메라수단을 구동하여 서비스 사이트 시스템에서 제공하는 2D코드를 스캔하기 위한 **스캔관리프로세스**, 보안인증을 위한 사용자 패스워드정보를 생성하기 위한 **패스워드정보생성프로세스**, 스캔관리프로세스를 통해 스캔된 1차 2D코드 정보에 포함된 패스워드 정보와 상기 패스워드정보생성프로세스에서 생성된 사용자 패스워드 정보와 사용자관리정보(USER AGENT CODE)를 포함하는 **1차 2D코드 응답정보의 생성 및 전송 프로세스**, 사용자 단말기에 표시된 2차 2D코드에 포함되어 있는 가입자 확인용 편집 토큰정보에 대한 토큰정보를 2차 2D코드 응답정보로 생성하되 2D 코드에 포함되어 있는 서비스 사이트 패스워드정보를 함께 응답정보에 포함하여 2차 2D코드 응답정보를 생성하여 전송하는 **2차 2D코드 응답정보 생성 및 전송 프로세스**, 상기 서비스 사이트 시스템에서 제공된 로그인 승인정보를 상기 사용자에게 제공하고 상기 사용자의 선택에 따라 상기 사용자의 로그인 선택정보를 상기 서비스 사이트 시스템에 제공하는 **로그인 승인정보 제공프로세스**를 포함하는 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 시스템.

[청구항 2] 제 1항에 있어서,
상기 데이터베이스에 등록된 토큰정보는 숫자조합, 텍스트정보, 이미지정보 중 하나 이상 등록된 정보로 구성되고, 상기 보안인증제어부는 이들 중 어느 하나를 선택하여 2차 2D 코드에 포함될 가입자 확인용 편집 토큰정보로 구성하는 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 시스템.

[청구항 3] 제 1항에 있어서,
상기 데이터베이스에 등록된 토큰정보는 상기 서비스 사이트시스템에 등록된 가입자의 휴대전화번호, 맥어드레스 정보 중 어느 하나 이상으로 구성되고, 상기 보안인증제어부는 이들 중 어느 하나를 선택하여 2차 2D 코드에 포함될 가입자 확인용 편집 토큰정보로 구성하는 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 시스템.

[청구항 4] 제 2항에 있어서,
상기 보안인증제어부는, 가입자 확인용 편집 토큰정보를 구성함에 있어서, 등록된 상기 토큰정보 중 어느 하나를 선택하고 선택된 토큰정보의 일부를 잘라내어 가입자 확인용 편집정보로 구성하고,

스마트폰으로부터의 2차 2D코드 응답정보에 포함된 응답토큰정보의 나머지 토큰정보가 토큰정보를 구성할 수 있는 가입자 확인용 편집토큰정보의 나머지 토큰정보인 가를 판단하여 가입자가 인증 확인되도록 하고,
상기 가입자 보안인증 서비스 어플리케이션의 2차 2D코드 응답정보 생성 및 전송 프로세스에서 가입자 확인용 편집 토큰정보에 대한 응답정보를 생성함에 있어서, 가입자 확인용 편집 토큰정보로 부터 해당하는 토큰정보를 판단하고 잘려진 정보를 제외한 나머지 토큰정보를 응답정보로 생성하도록 한 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 시스템.

[청구항 5] 제 1항에 있어서,
상기 서비스 사이트 시스템의 보안인증관리서버는, 로그인 승인정보와 함께 제공될 안내정보를 생성하기 위한 안내정보생성수단과, 광고정보가 저장관리 되는 광고정보 데이터베이스를 더 포함하여 구성되며,
상기 안내정보생성수단은 보안인증제어부의 로그인 인증이 확인되면 상기 웹서버에서 제공되는 가입자 정보 및 스마트폰으로부터 얻어지는 위치정보에 따라서 가입자에 따른 맞춤정보 생성을 위한 프로세스를 제공하는 광고제어부를 포함하여 구성되는 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 시스템.

[청구항 6] 제 1항 또는 제 5항에 있어서,
상기 서비스 사이트 시스템의 보안인증관리서버는, 로그인 승인정보와 함께 제공될 안내정보를 생성하기 위한 안내정보생성수단을 더 포함하여 구성되며,
상기 안내정보생성수단은 상기 웹서버로부터 인증된 가입자에게 제공하기 위한 서비스 사이트의 공지정보를 제공받아 제공될 공지정보를 생성하기 위한 프로세스를 제공하는 공지제어부를 포함하여 구성되는 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 시스템.

[청구항 7] 제 1항에 있어서,
상기 패스워드생성부는 OTP정보 생성수단으로 구성되고, 상기 2D코드에 포함되는 패스워드 정보는 OTP정보생성수단으로부터 생성된 OTP정보이고,
상기 가입자 보안인증 서비스 어플리케이션의 패스워드정보생성프로세스를 통해 생성된 패스워드정보는 OTP 정보인 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자

보안 인증 시스템.

[청구항 8] 스마트폰에 설치된 가입자 보안인증 서비스 어플리케이션의 토큰정보등록프로세스를 통해 서비스 사이트에 접속하여 토큰정보를 등록하는 스마트폰의 **가입자 보안인증 서비스 어플리케이션에서 이루어지는토큰정보 등록과정**,
사용자의 가입자 보안인증 모드 시도를 판단하여 보안인증관리서버의 패스워드생성부에서 생성된 서비스 사이트 패스워드 정보를 포함하는 2D코드를 2D코드 생성부를 통해 생성하고, 생성된 2D코드를 서비스 사이트 페이지에 표시하는 서비스사이트시스템의 **보안인증관리서버를 통해 이루어지는 1차 2D코드생성 및 표시과정**,
사용자가 가입자 보안 인증모드를 선택하였는가를 판단하여 구동되는 **스캔관리프로세스를 통해** 스캔입력 확인되는 상기 1차 2D코드에 포함된 상기 서비스 사이트 패스워드정보를 확인하고 **패스워드정보생성프로세스를 통해** 사용자 패스워드정보를 생성하여 1차 2D코드 응답정보 생성하되 사용자관리정보(USER AGENT CODE), 상기 확인된 서비스 사이트 패스워드정보, 상기 생성된 사용자패스워드정보를 포함하여 1차 2D코드 응답정보를 생성하고 생성된 2차 2D코드 응답정보를 미리 설정되어 있는 위치정보(URL)로 전송하는 사용자 스마트폰의 **가입자 보안인증 서비스 어플리케이션에서 이루어지는 1차 2D코드 응답정보 생성 및 전송과정**,
스마트폰으로부터 상기 1차 2D코드 응답정보가 수신되면 수신된 1차 2D코드 응답정보로부터 상기 서비스사이트의 1차 2D코드생성 및 표시과정을 통해 전송한 서비스사이트 패스워드정보인지를 확인하고 상기 사용자 관리정보와 매칭되는 토큰정보를 로드하여 로드된 토큰정보를 가입자 확인용 편집 토큰정보로 구성하고 가입자 확인용 편집 토큰정보, 1차 2D코드 응답정보에 포함된 사용자 패스워드 정보, 최종 사용자정보를 제공받기 위한 위치정보(URL)를 포함하는 2차 2D코드를 2D코드 생성부를 통해 생성하여 사용자의 접속페이지에 표시하는 서비스사이트시스템의 **보안인증관리서버를 통해 이루어지는 2차 2D코드생성 및 표시과정**,
사용자의 스캔선택 입력을 판단하여 확인된 2차 2D코드를 스캔하고 상기 2차 2D코드에 포함된 정보로부터 전송했던 사용자 패스워드정보를 확인하고 2차 2D코드에 포함된 가입자 확인용 편집 토큰정보를 확인하여 응답 토큰정보를 생성하고, 새롭게 교체할 사용자 관리정보(NEW_USER AGENT CODE)를 생성하여,

사용자 패스워드정보, 상기 생성된 응답토큰정보, 상기 생성된 새롭게 교체할 사용자관리정보를 포함하는 2차 2D코드 응답정보를 생성하여 전송하는 사용자 스마트폰의 **가입자 보안인증 서비스 어플리케이션에서 이루어지는 2차 2D코드 응답정보 생성 및 전송과정**,

스마트폰으로부터 상기 2차 2D코드 응답정보가 수신되면 수신된 2차 2D코드 응답정보로부터 응답토큰정보를 확인하여 응답토큰정보가 2차 2D코드에 포함된 가입자 확인용 편집 토큰정보에 대한 올바른 토큰정보인 가를 판단하여 올바른 토큰정보인 경우에는 상기 가입자 확인용 편집 토큰정보로 이용된 토큰정보에 대하여 데이터베이스에 등록된 가입자의 사용자 관리정보(USER AGENT CODE)를 수신된 새롭게 교체할 사용자 관리정보(NEW_USER AGENT CODE)로 교체하여 데이터베이스에 등록하고 상기 사용자 스마트폰의 가입자 보안인증 서비스 어플리케이션으로 로그인 승인정보를 전송하는 **서비스 사이트 시스템의 보안인증관리서버를 통해 이루어지는 접속허가 판단 및 인증과정**,

상기 서비스 사이트 시스템의 보안인증관리서버를 통해 이루어지는 접속허가 판단 및 인증과정을 통해 서비스 사이트 시스템에서 전송한 로그인 승인정보로부터 사용자가 로그인 할 수 있도록 로그인 선택수단을 생성하여 표시하고, 상기 사용자가 로그인 선택수단을 입력하면 로그인 선택정보를 상기 서비스사이트로 전송하는 로그인 승인정보 제공프로세스에 의해 수행되는 **사용자 스마트폰의 가입자 보안인증 서비스 어플리케이션에서 이루어지는 로그인과정,**

상기 사용자 스마트폰으로부터 로그인 선택정보가 입력되면 해당 서비스사이트 시스템의 웹페이지의 로그인을 허가하여 접속 인증을 완료하는 **서비스 사이트 시스템의 보안인증관리서버를 통해 이루어지는 접속완료과정**을 포함하여 이루어지는 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법.

[청구항 9] 제 8항에 있어서,

상기 토큰등록과정에 있어서, 상기 토큰정보는 가입자를 식별하기 위하여 등록되는 정보로서, 숫자조합, 문장(텍스트), 이미지(image) 중 스마트폰을 통해 등록 구성되는 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법.

[청구항 10] 제 8항에 있어서,

상기 토큰정보는 사용자 등록 토큰정보 대신 상기 서비스

사이트시스템에 등록된 가입자의 휴대전화번호, 맥어드레스 정보 중 어느 하나 이상으로 구성된 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법.

[청구항 11] 제 8항에 있어서,
상기 **서비스 사이트 시스템의 보안인증관리서버를 통해 이루어지는** 2차 2D코드 생성 및 표시과정은, 상기 토큰정보의 일부 정보를 잘라내어 가입자 확인용 편집 토큰정보로 구성하고,
상기 사용자 스마트폰의 **사용자 스마트폰의 가입자 보안인증 서비스 어플리케이션에서 이루어지는** 2차 2D코드 응답정보 생성 및 전송과정에 있어서, 수신된 가입자 확인용 편집 토큰정보로 부터 해당하는 토큰정보를 판단하고 해당하는 토큰정보로 부터 가입자 확인용 편집 토큰정보의 잘려진 토큰정보의 나머지 토큰정보를 가입자 확인용 편집토큰 정보의 응답토큰정보로 생성하도록 하고,
상기 서비스사이트시스템의 **보안인증관리서버를 통해 이루어지는** 접속허가 판단 및 인증과정에 있어서, 응답토큰정보로 구성된 나머지 토큰정보를 확인하여 나머지 토큰정보가 토큰정보를 구성할 수 있는 가입자 확인용 편집토큰정보의 나머지 토큰정보인 가를 판단하여 가입자의 보안인증요청을 승인하도록 한 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법.

[청구항 12] 제 8항에 있어서,
상기 **스마트폰에서의 가입자 보안인증 서비스 어플리케이션에서 이루어지는토큰정보 등록과정은**, 상기 사용자로부터 토큰정보 등록 모드가 선택되면, 상기 서비스 사이트 시스템의 가입자 아이디와 패스워드를 요청하여 상기 서비스 사이트 시스템에 접속을 요구하는 로그인 요청과정과,
상기 서비스 사이트 시스템에 접속되면, 토큰정보로 등록할 수 있는 토큰정보 선택메뉴를 제공하여 상기 사용자로 하여금 등록할 토큰정보를 선택하여 입력하도록 하는 사용자 토큰정보 입력과정과,
상기 사용자가 선택 입력한 토큰정보를 저장하고, 이를 기반으로 서비스 사이트 시스템에 전송하기 위한 토큰정보를 생성하는 토큰정보생성과정과,
상기 토큰정보생성과정을 통해 생성된 토큰정보를 정해진 서비스 사이트 시스템의 위치정보(URL)로 전송하는 토큰정보 전송과정과,
상기 서비스 사이트 시스템으로부터 사용자 관리정보(USER

AGENT CODE)가 수신되면 새로운 사용자 관리정보(USER AGENT CODE)로 기존의 사용자 관리정보(USER AGENT CODE)를 새로운 사용자 관리정보(USER AGENT CODE)로 교체하는 사용자관리정보 관리과정으로 이루어지는 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법.

[청구항 13] 제 8항 또는 제 12항에 있어서,
상기 스마트폰에 설치된 **가입자 보안인증 서비스 어플리케이션은 사용자의 실행명령이 입력되면** 최초구동상태인 지를 확인하고, 최초 구동 상태인 경우에는 어플리케이션 구동에 필요한 스마트폰의 가입자 보안인증 서비스 어플리케이션에서 이루어지는 가입자 설정 등록모드를 수행하도록 하는 사용자 설정등록모드설정과정을 더 포함하여 구성하는 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법.

[청구항 14] 제 13항에 있어서,
상기 사용자 설정등록모드는 가입자 보안인증 서비스 어플리케이션의 구동 및 삭제방지를 위한 비밀번호 설정 및 가입자 보안인증 서비스 어플리케이션에서 스마트폰의 위치정보를 이용할 수 있도록 하는 위치정보사용동의 정보를 포함하여 이루어지며, 사용자의 필요에 따라서 서비스 사이트 시스템과의 접속과 상관없이 가입자 보안인증 서비스 어플리케이션을 구동시켜 실행하는 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법.

[청구항 15] 제 8항 또는 제 11항에 있어서,
상기 서비스 사이트 패스워드 정보와 상기 사용자 패스워드 정보는 OTP정보인 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법.

[청구항 16] 제 8항 또는 제 11항에 있어서,
상기 서비스사이트시스템**의 보안인증관리서버를 통해 이루어지는** 접속허가 판단 및 인증과정은, 접속허가가 결정되면 해당 가입자의 아이디를 확인하여 웹서버로 회원가입정보를 요청하고, 해당 가입자로부터 제공되는 위치정보수신여부를 확인하여 해당 가입자에게 제공할 광고정보 포함하는 안내정보를 생성하여 로그인승인정보에 첨가하여 사용자 스마트폰의 가입자 보안인증 서비스 어플리케이션으로 전송하도록 하는 안내정보 생성 및 전송과정을 더 포함하고,
상기 사용자 스마트폰의 가입자 보안인증 서비스 어플리케이션에서 이루어지는 로그인과정은, 서비스 사이트

시스템에서 전송한 로그인승인정보로부터 사용자가 로그인 할 수 있도록 로그인 선택수단을 생성하여 표시할 때 상기 안내정보를 표시하도록 하는 안내정보표시과정을 더 포함하는 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법.

[청구항 17] 제 8항 또는 제 11항에 있어서,
상기 서비스사이트시스템의 보안인증관리서버를 통해 이루어지는 접속허가 판단 및 인증과정은, 접속허가가 결정되면 웹서버에 공지정보를 요청하여 제공받은 공지정보를 포함하는 안내정보를 생성하여 로그인승인정보에 첨가하여 사용자 스마트폰의 가입자 보안인증 서비스 어플리케이션으로 전송하도록 하는 안내정보 생성 및 전송과정을 더 포함하고,
상기 사용자 스마트폰의 가입자 보안인증 서비스 어플리케이션에서 이루어지는 로그인과정은, 서비스 사이트 시스템에서 전송한 로그인승인정보로부터 사용자가 로그인 할 수 있도록 로그인 선택수단을 생성하여 표시할 때 상기 안내정보를 표시하도록 하는 안내정보표시과정을 더 포함하는 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법.

[청구항 18] 제 17항에 있어서,
상기 안내정보는 가입자에게 제공할 생활정보, 가입자가 요청한 질문에 대한 답변정보, 뉴스 정보를 포함하는 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법.

[청구항 19] 제 16항에 있어서,
상기 사용자 스마트폰의 가입자 보안인증 서비스 어플리케이션에서 이루어지는 로그인과정에 있어서,
안내정보표시과정은, 사용자가 로그인 선택수단을 입력할 때 상기 안내정보를 표시하도록 하는 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법.

[청구항 20] 제 17항에 있어서,
상기 사용자 스마트폰의 가입자 보안인증 서비스 어플리케이션에서 이루어지는 로그인과정에 있어서
안내정보표시과정은, 사용자가 로그인 선택수단을 입력할 때 상기 안내정보를 표시하도록 하는 것을 특징으로 하는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법.

[청구항 21] 청구항 제 8항 내지 청구항 10항 또는 청구항 12항 중 어느 한 항의 과정을 수행하기 위한 프로세스를 포함하는 프로그램이 기록된 컴퓨터로 읽을 수 있는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법을 기록한 기록매체.

[청구항 22] 청구항 제 14항의 과정을 수행하기 위한 프로세스를 포함하는

프로그램이 기록된 컴퓨터로 읽을 수 있는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법을 기록한 기록매체.

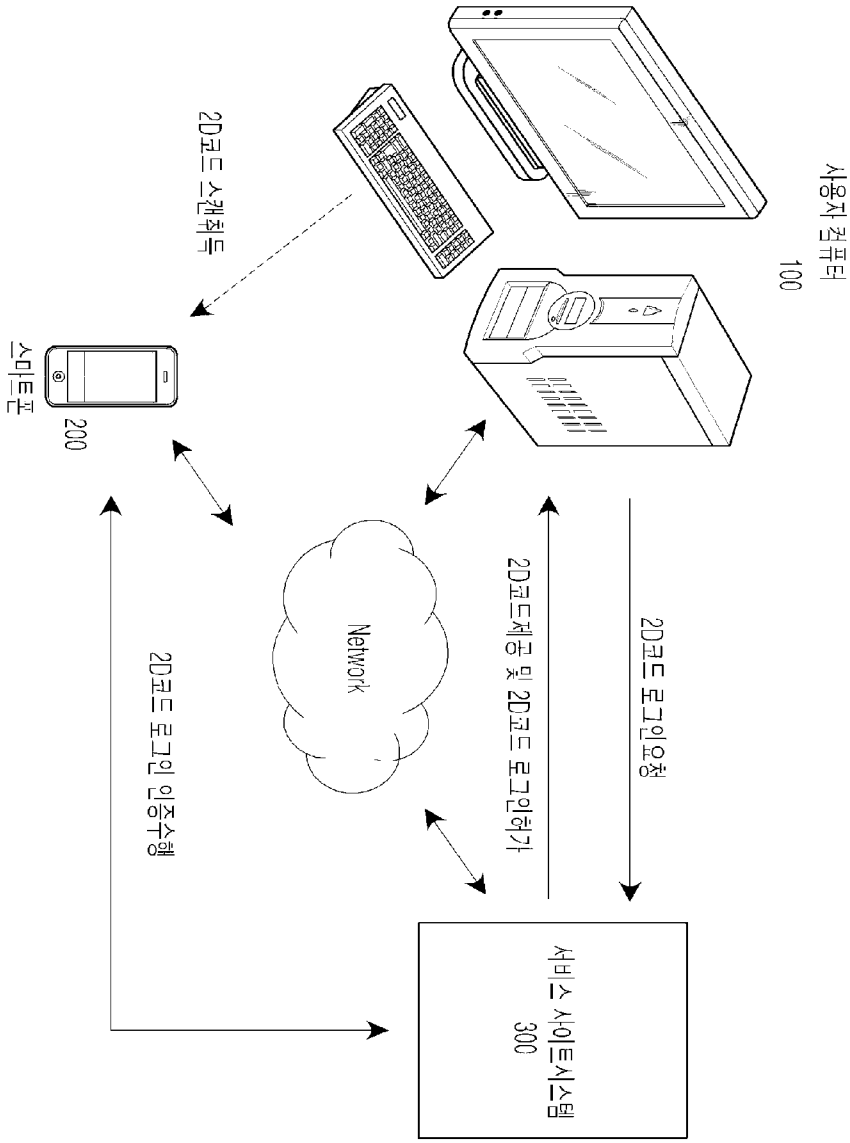
[청구항 23] 청구항 제 16항의 과정을 수행하기 위한 프로세스를 포함하는 프로그램이 기록된 컴퓨터로 읽을 수 있는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법을 기록한 기록매체.

[청구항 24] 청구항 제 17항의 과정을 수행하기 위한 프로세스를 포함하는 프로그램이 기록된 컴퓨터로 읽을 수 있는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법을 기록한 기록매체.

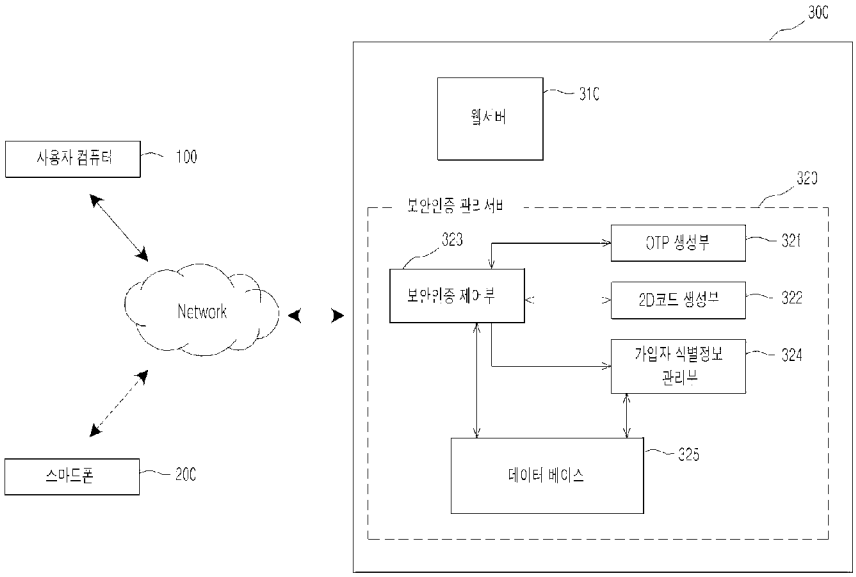
[청구항 25] 청구항 제 19항의 과정을 수행하기 위한 프로세스를 포함하는 프로그램이 기록된 컴퓨터로 읽을 수 있는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법을 기록한 기록매체.

[청구항 26] 청구항 제 20항의 과정을 수행하기 위한 프로세스를 포함하는 프로그램이 기록된 컴퓨터로 읽을 수 있는 네트워크 통신망에서의 쌍방향 가입자 보안 인증 방법을 기록한 기록매체.

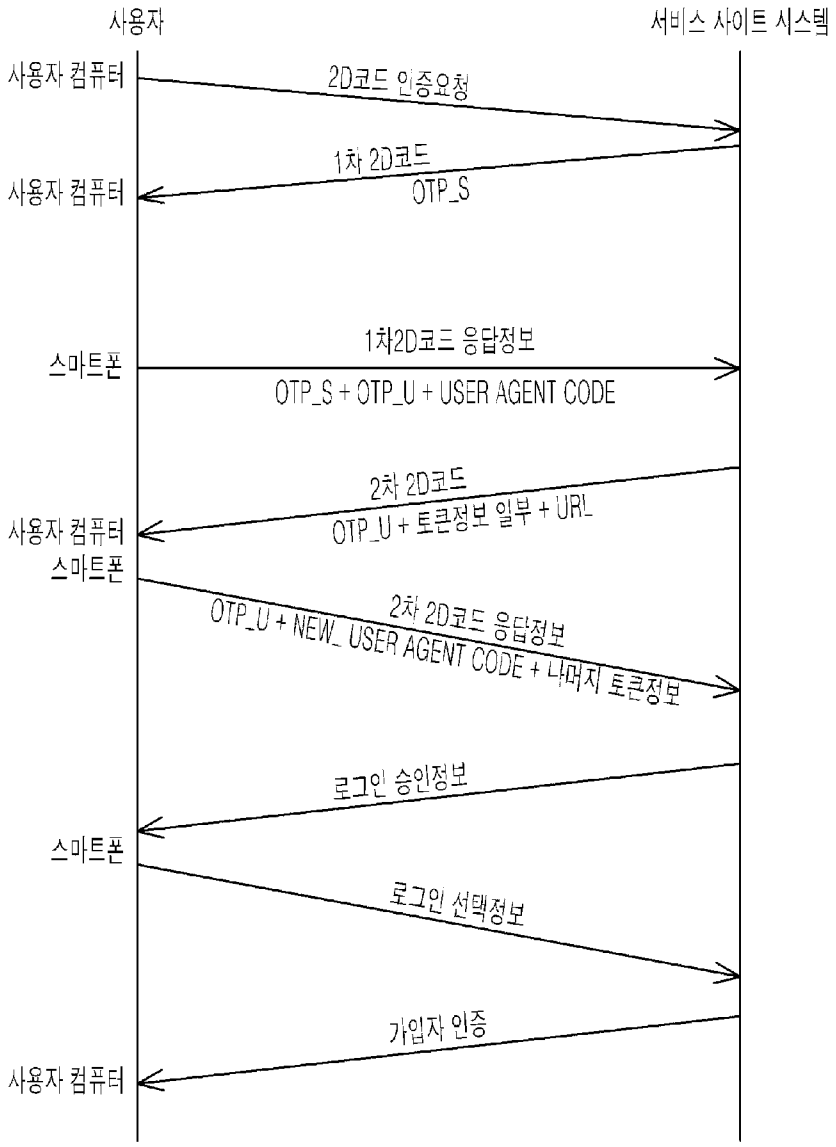
[Fig. 1]


2D코드 스캔취득
사용자 컴퓨터
100
스마트폰
200
Network
2D코드 로그인 인증수행
2D코드제공 및 2D코드 로그인허가
2D코드 로그인요청
서비스 사이트시스템
300

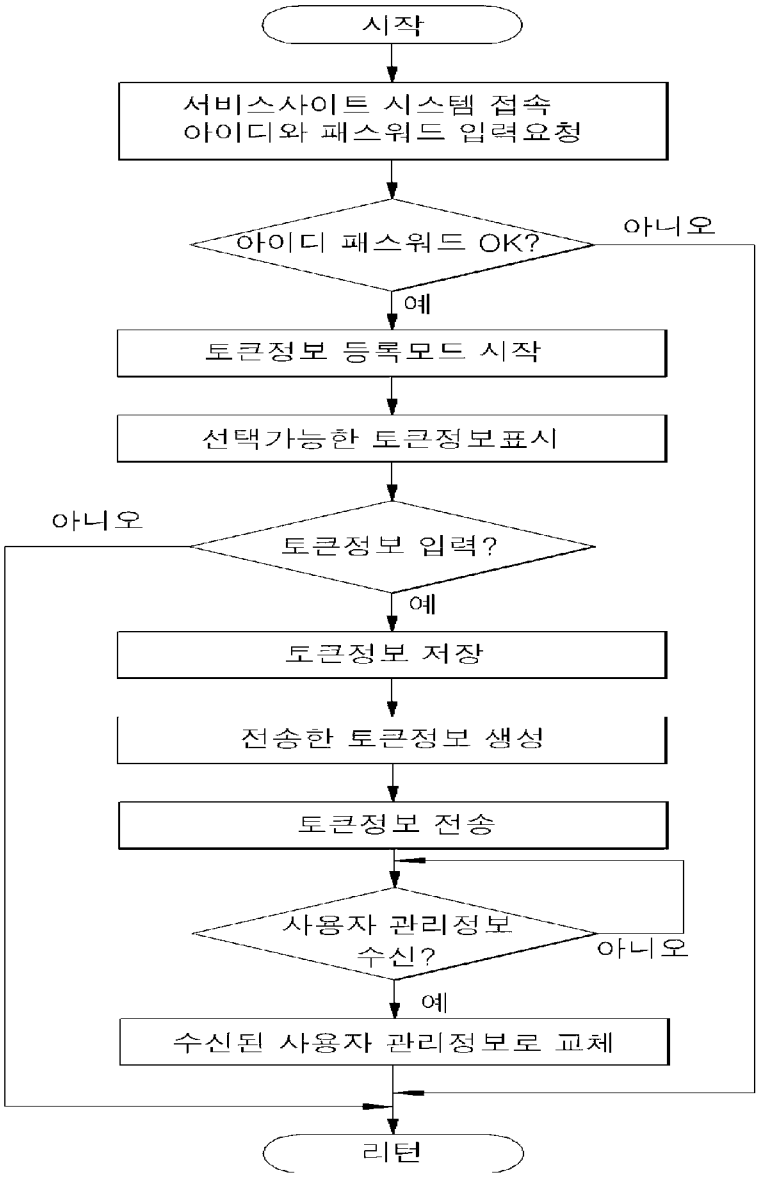
[Fig. 2]


300
웹서버
310
사용자 컴퓨터
100
보안인증 관리서버
320
323
OTP 생성부
321
보안인증 제어부
2D코드 생성부
322
가입자 식별정보 관리부
324
데이터 베이스
325
Network
스마트폰
200

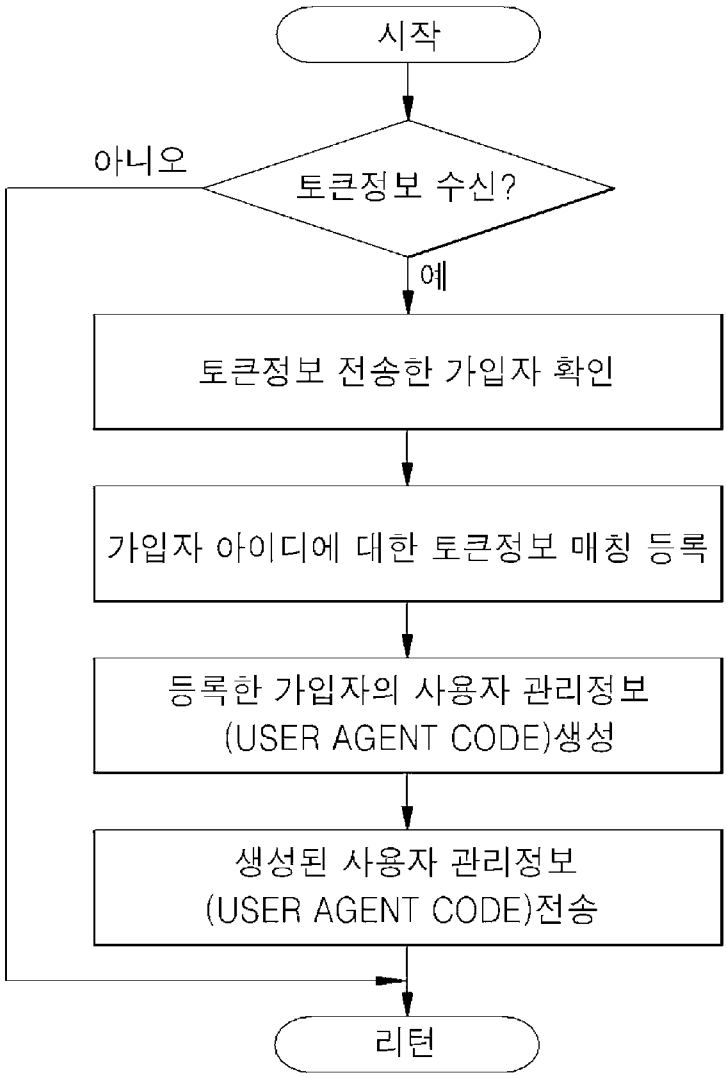
[Fig. 3]


사용자
서비스 사이트 시스템
사용자 컴퓨터
2D코드 인증요청
1차 2D코드
사용자 컴퓨터
OTP_S
스마트폰
1차2D코드 응답정보
OTP_S + OTP_U + USER AGENT CODE
2차 2D코드
사용자 컴퓨터
OTP_U + 토큰정보 일부 + URL
스마트폰
2차 2D코드 응답정보
OTP_U + NEW_ USER AGENT CODE + 나머지 토큰정보
로그인 승인정보
스마트폰
로그인 선택정보
가입자 인증
사용자 컴퓨터

[Fig. 4]


시작
서비스사이트 시스템 접속
아이디와 패스워드 입력요청
아이디 패스워드 OK?
아니오
예
토큰정보 등록모드 시작
선택가능한 토큰정보표시
아니오
토큰정보 입력?
예
토큰정보 저장
전송한 토큰정보 생성
토큰정보 전송
사용자 관리정보
수신?
아니오
예
수신된 사용자 관리정보로 교체
리턴

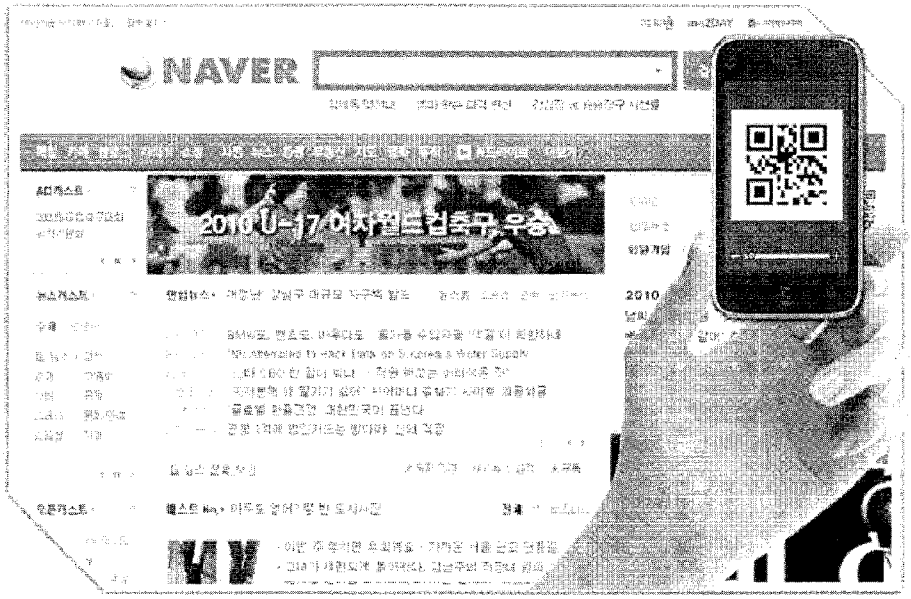
[Fig. 5]


시작
토큰정보 수신?
아니오
예
토큰정보 전송한 가입자 확인
가입자 아이디에 대한 토큰정보 매칭 등록
등록한 가입자의 사용자 관리정보
(USER AGENT CODE)생성
생성된 사용자 관리정보
(USER AGENT CODE)전송
리턴

[Fig. 6]

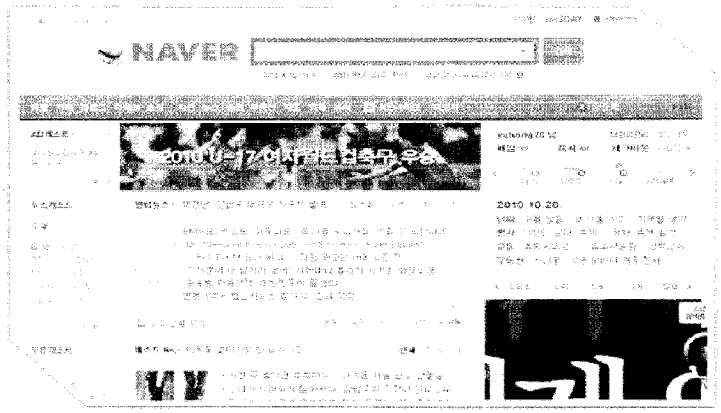

NAVER

[Fig. 7]

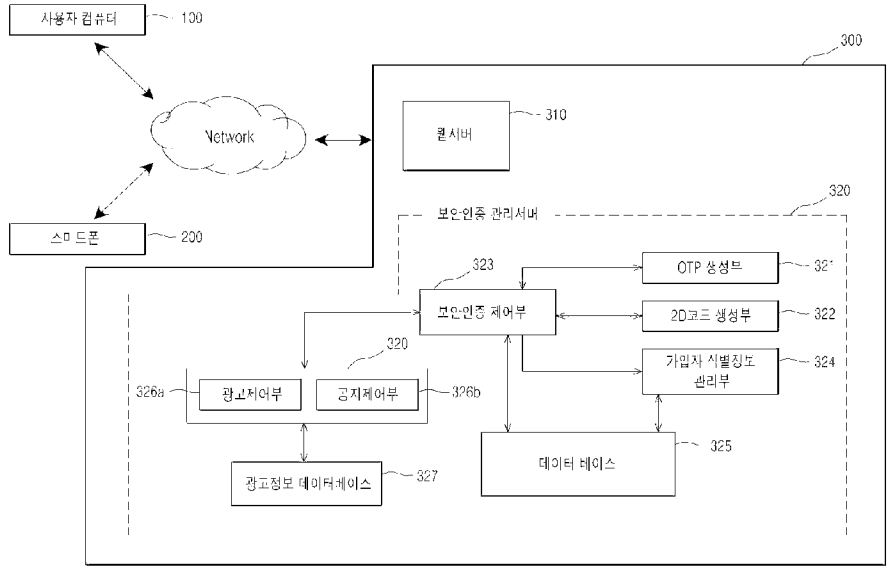


[Fig. 8]

[Fig. 9]


NAVER

[Fig. 10]


사용자 컴퓨터
100
Network
스마트폰
200
300
웹서버
310
보안인증 관리서버
320
323
OTP 생성부
321
보안인증 제어부
2D코드 생성부
322
가입자 식별정보 관리부
324
320
326a
광고제어부
공지제어부
326b
데이터 베이스
325
광고정보 데이터베이스
327