

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2014년 1월 9일 (09.01.2014)



(10) 국제공개번호
WO 2014/007516 A1

- (51) 국제특허분류:
H04W 12/06 (2009.01)
- (21) 국제출원번호: PCT/KR2013/005859
- (22) 국제출원일: 2013년 7월 2일 (02.07.2013)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2012-0071623 2012년 7월 2일 (02.07.2012) KR
10-2012-0071624 2012년 7월 2일 (02.07.2012) KR
- (71) 출원인: 에스케이플래닛 주식회사 (SK PLANET CO., LTD.) [KR/KR]; 100-999 서울시 중구 을지로 65 (을지로 2가), Seoul (KR).
- (72) 발명자: 주재영 (JU, Jaeyoung); 435-755 경기도 군포시 오금로 16, 다산아파트 326 동 301호 (금정동), Gyeonggi-do (KR). 고정완 (KO, Kyungwan); 143-758 서울시 광진구 아차산로 262, 더샵스타시티아파트 A 동 3503호 (자양동), Seoul (KR). 엄봉수 (UM, Bongsu); 133-724 서울시 성동구 상원길 80, 동아그린아파트 101동 708호 (성수동 1가), Seoul (KR).
- (74) 대리인: 박종한 (PARK, Chonghan); 152-740 서울시 구로구 디지털로 26길 5, 319 (구로동, 에이스하이엔드 타워), 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, BN, 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, 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, PA, 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.

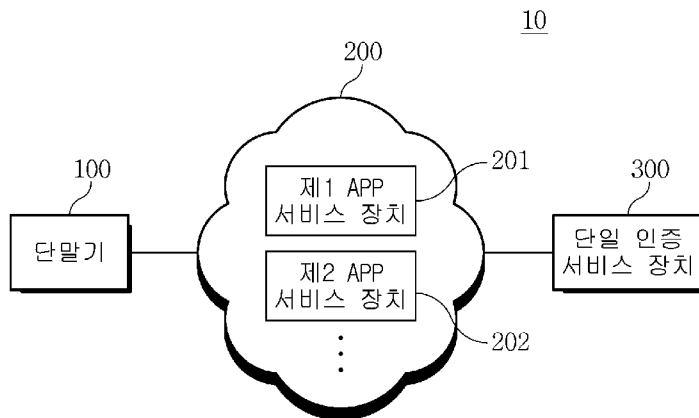
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE,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

공개:

- 국제조사보고서와 함께 (조약 제 21 조(3))
- 청구범위 보정 기한 만료 전의 공개이며, 보정서를 접수하는 경우 그에 관하여 별도 공개함 (규칙 48.2(h))

(54) Title: SINGLE CERTIFICATE SERVICE SYSTEM AND OPERATIONAL METHOD THEREOF

(54) 발명의 명칭: 단일 인증 서비스 시스템 및 이의 운용 방법



100 ... TERMINAL
201 ... FIRST APP SERVICE DEVICE
202 ... SECOND APP SERVICE DEVICE
300 ... SINGLE CERTIFICATE SERVICE DEVICE

(57) Abstract: The present invention relates to single certificate service support, and more particularly to a single certificate service system which includes: a terminal for accessing at least one of a plurality of application service devices in response to an activation request of at least one of a plurality of applications to receive a service token used for the service operation from the application service device on the basis of a single certificate token without additional certificate information; an application service device for providing the data for the application service operation of the terminal showing the service token and for delivering a message received in connection with single certificate to a single certificate service device; and a single certificate service device for delivering the information for the single certificate service operation to the application service device or through the application service device to the terminal if receiving the message from the application service device in connection with single certificate, and to each structure of the system, and an operational method thereof.

(57) 요약서:

[다음 쪽 계속]



본 발명은 단일 인증 서비스 지원에 관한 것으로, 특히 본 발명은 복수개의 어플리케이션 중 적어도 하나의 활성화 요청에 따라 복수의 어플리케이션 서비스 장치 중 적어도 하나의 어플리케이션 서비스 장치 접속을 수행하되 단일 인증 토큰을 기반으로 별도의 인증 정보 입력 없이 각각의 어플리케이션 서비스 장치로부터 서비스 운용을 위해 사용되는 서비스 토큰을 수신하는 단말기, 상기 서비스 토큰을 제시하는 단말기의 어플리케이션 서비스 운용을 위한 데이터를 제공하며 단일 인증 관련 메시지 수신 시 해당 메시지를 단일 인증 서비스 장치에 제공하는 어플리케이션 서비스 장치, 상기 어플리케이션 서비스 장치로부터 단일 인증 관련 메시지를 수신하면 상기 단말기의 단일 인증 서비스 운용을 위한 정보를 상기 어플리케이션 서비스 장치에 제공하거나 또는 상기 어플리케이션 서비스 장치를 통하여 상기 단말기에 제공하는 단일 인증 서비스 장치를 포함하는 것을 특징으로 하는 단일 인증 서비스 시스템과 시스템의 각 구성들 및 이의 운용 방법의 구성을 개시한다.

명세서

발명의 명칭: 단일 인증 서비스 시스템 및 이의 운용 방법 기술분야

- [1] 본 발명은 단말기의 단일 인증에 관한 것으로, 특히 단말기에서 운용되는 다수의 어플리케이션들의 단일 인증 운용을 위한 단일 인증 서비스 시스템 및 이의 운용 방법에 관한 것이다.

배경기술

- [2] 통신 단말기는 휴대가 가능한 형태로 제작되면서 그 이용의 편리성과 휴대의 용이성 등으로 인하여 매우 폭넓은 분야에서 이용되고 있다. 이러한 통신 단말기는 최근 들어 다양한 사용자 기능을 탑재한 스마트폰의 형태로 발전하면서 편리성과 오락성을 제공하고 있다.
- [3] 한편 스마트폰의 보급과 함께 사용자들은 다양한 사용자 기능을 이용하고 있으며, 특히 스마트폰 기반의 다양한 통신 서비스를 이용하고 있다. 예를 들어 종래 사용자들은 스마트폰을 이용하여 채팅 서비스를 이용하거나, 특정 웹 서비스를 이용하거나, 타 사용자와 이메일을 주고받는 서비스를 이용한다. 이때 사용자는 스마트폰 기반의 다양한 어플리케이션을 운용하여 특정 통신 서비스를 이용하고 있다. 그런데 이 과정에서 사용자는 각각의 어플리케이션이 제공하는 특정 통신 서비스 이용을 위해서는 해당 어플리케이션 운용을 지원하는 서비스 장치와 인증 과정을 수행하여 정당한 사용자인지를 확인하고 이용 권한을 획득해야 한다. 이러한 인증 과정은 각 스마트폰 사용자들의 정상적인 통신 서비스 이용 및 보안을 위해서 필요한 사항이다.
- [4] 그런데 이러한 정보 인증 과정은 때로는 사용자에게 매우 큰 불편함을 주는 경우가 있다. 이를 보다 상세히 설명하면, 사용자는 특정 어플리케이션 기반의 통신 서비스 이용을 위하여 각각의 서비스 장치와 인증 정보를 송수신하고 이를 인증 받는 과정을 수행해야 한다. 이때 어플리케이션의 종류가 늘어나는 경우 그리고 한정적인 화면 상태에서 인증 정보를 입력해야 하는 경우 불편한 입력 조건에서 사용자에게 반복적인 인증 정보 입력 과정을 수행하도록 강요하는 문제가 있었다. 더욱이 각 어플리케이션별로 인증 정보를 다르게 설정한 경우 사용자는 각 어플리케이션별로 정확한 인증 정보 입력을 수행해야 하며, 이 과정에서 적절한 정보 기억을 수행할 수 없는 경우 사용자는 잘못된 인증 정보 입력을 수행하고 이를 정정하기 위한 부차적인 절차를 수행해야만 한다. 이러한 불편함 때문에 많은 사용자들이 단말기를 기반으로 한 특정 통신 서비스 이용을 포기하는 사례가 빈번하게 발생하고 있다.

발명의 상세한 설명

기술적 과제

- [5] 따라서 본 발명의 목적은 전술된 바와 같은 종래 기술의 문제점을 해결하기

위한 것으로, 어플리케이션들을 통합적으로 인증할 수 있도록 하여 특정 통신 서비스들을 보다 용이하고 간편하게 운용하면서도 적절한 보안성을 확보할 수 있도록 지원하는 단일 인증 서비스 시스템 및 이의 운용 방법을 제공함에 있다.

과제 해결 수단

- [6] 상기 목적을 달성하기 위한 본 발명은 복수개의 어플리케이션 중 적어도 하나의 활성화 요청에 따라 복수의 어플리케이션 서비스 장치 중 적어도 하나의 어플리케이션 서비스 장치와의 접속을 수행하되 단일 인증 토큰을 기반으로 별도의 인증 정보 입력 없이 각각의 어플리케이션 서비스 장치로부터 서비스 운용을 위해 사용되는 서비스 토큰을 수신하는 단말기, 서비스 토큰을 제시하는 단말기의 어플리케이션 서비스 운용을 위한 데이터를 제공하며 단일 인증 관련 메시지 수신 시 해당 메시지를 단일 인증 서비스 장치에 제공하는 어플리케이션 서비스 장치, 어플리케이션 서비스 장치로부터 단일 인증 관련 메시지를 수신하면 단말기의 단일 인증 서비스 운용을 위한 정보를 어플리케이션 서비스 장치에 제공하거나 또는 어플리케이션 서비스 장치를 통하여 단말기에 제공하는 단일 인증 서비스 장치를 포함하는 것을 특징으로 하는 단일 인증 서비스 시스템의 구성을 개시한다.
- [7] 본 발명은 또한, 단말기의 특정 어플리케이션으로부터 통합 ID 로그인 정보 또는 단일 인증 토큰 기반의 세션 조회 메시지를 수신하는 제1 통신부, 단말기의 특정 어플리케이션 기능 지원을 위한 데이터를 저장하며, 단말기의 특정 어플리케이션 기능 운용을 위한 서비스 토큰을 저장하는 제1 저장부, 특정 어플리케이션으로부터 통합 ID 로그인 정보 수신 시 단일 인증 토큰 생성을 위한 메시지를 단일 인증 서비스 장치에 전달하며, 세션 조회 메시지 수신 시 이를 단일 인증 서비스 장치로 전송하고 단일 인증 서비스 장치로부터 세션 조회 메시지와 관련된 통합 서비스 번호를 수신 하여 해당 어플리케이션의 별도 인증 정보 확인 없이 서비스 토큰을 단말기의 특정 어플리케이션에게 제공하는 제1 제어부를 포함하는 것을 특징으로 하는 단일 인증 서비스를 지원하는 어플리케이션 서비스 장치의 구성을 개시한다.
- [8] 여기서 제1 제어부는, 통합 ID 로그인 정보에 해당하는 메시지 또는 세션 조회 메시지에 대응하는 메시지를 단일 인증 서비스 장치에 전달하고, 단일 인증 서비스 장치로부터 웹 브라우저의 단일 인증 쿠키 정보 획득을 위한 단일 인증 토큰과 1회용 접속키를 수신하는 경우 단말기의 어플리케이션에 전달하도록 제어한다.
- [9] 또한, 제1 제어부는 통합 ID 로그인 정보 수신 시, 단일 인증 서비스 장치가 제공하는 단일 인증 토큰을 기반으로 서비스 토큰을 생성하고 단일 인증 토큰 및 서비스 토큰, 어플리케이션 기능 지원을 위한 데이터를 단말기의 특정 어플리케이션에 제공하도록 제어하며, 단말기의 특정 어플리케이션으로부터 서비스 토큰 만료 요청 메시지 수신 시 해당 어플리케이션의 서비스 로그아웃을

- 위한 서비스 토큰 만료 응답 메시지를 단말기에 제공하도록 제어할 수 있다.
- [10] 또한, 제1 제어부는, 통합 ID 로그인 정보 수신 시, 단일 인증 서비스 장치가 제공하는 단일 인증 토큰을 기반으로 서비스 토큰을 생성하고 단일 인증 토큰, 1회용 접속키 및 서비스 토큰, 어플리케이션 기능 지원을 위한 데이터를 단말기의 어플리케이션에 제공하도록 제어하며, 세션 조회 메시지 수신 시 단일 인증 서비스 장치가 제공하는 통합 서비스 번호를 기반으로 서비스 토큰을 생성하고 서비스 토큰을 상기 단말기의 어플리케이션에 제공하도록 제어한다.
- [11] 또한 제1 제어부는 상기 단말기의 특정 어플리케이션으로부터 서비스 토큰 및 단일 인증 토큰 만료 요청 메시지 수신 시 단일 인증 토큰 만료 요청 메시지를 단일 인증 서비스 장치에 제공하고 그에 대응하는 응답 메시지를 수신하는 경우, 서비스 토큰 및 상기 단일 인증 토큰의 만료 응답 메시지를 단말기에 제공하도록 제어할 수 있다.
- [12] 또한, 제1 제어부는, 상기 단말기로부터 웹 브라우저 종료 또는 웹 브라우저 기반의 단일 인증 쿠키 만료 요청 메시지 수신 시 단일 인증 쿠키 만료 요청 메시지를 상기 단일 인증 서비스 장치에 제공하고, 그에 대응하는 응답 메시지를 상기 단말기에 제공하도록 제어한다.
- [13] 본 발명은 또한, 적어도 하나의 어플리케이션 서비스 장치와 통신 채널을 형성하고 단말기의 특정 어플리케이션이 상기 어플리케이션 서비스 장치를 통해 전송하는 단일 인증 세션 요청 메시지 또는 단일 인증 세션 검사 메시지를 수신하는 장치 통신부, 특정 어플리케이션 서비스 장치를 별도 인증 정보 입력 없이 접속할 수 있도록 하는 단일 인증 지원을 위해 상기 단말기에 제공되는 단일 인증 토큰을 저장하는 제2 저장부, 상기 단일 인증 세션 요청 메시지 수신 시 상기 단일 인증 토큰을 상기 어플리케이션 서비스 장치를 통하여 단말기에 제공하며, 상기 단일 인증 세션 검사 메시지 수신 시 상기 단일 인증 토큰 기반의 통합 서비스 번호를 상기 어플리케이션 서비스 장치에 제공하도록 제어하는 제2 제어부를 포함하는 것을 특징으로 하는 단일 인증 서비스 장치의 구성을 개시한다.
- [14] 여기서 상기 제2 제어부는 상기 어플리케이션 서비스 장치로부터 단일 인증 토큰 만료 요청 메시지 수신 시 상기 단일 인증 토큰 만료에 대응하는 응답 메시지를 상기 어플리케이션 서비스 장치에 제공할 수 있다.
- [15] 또한, 제2 제어부는, 상기 단말기의 웹 브라우저에 제공할 단일 인증 쿠키 정보 생성을 위한 단일 인증 세션 요청 메시지를 수신하면, 상기 단일 인증 세션 요청 메시지에 대응하는 단일 인증 토큰 및 1회용 접속키를 상기 어플리케이션 서비스 장치를 통해 상기 단말기에 제공하도록 제어하고, 상기 1회용 접속키를 통해 접속하는 웹 브라우저에게 단일 인증 쿠키 정보를 제공하도록 제어한다.
- [16] 또한, 상기 제2 제어부는, 상기 웹 브라우저의 상기 1회용 접속키 기반의 접속 이후 상기 1회용 접속키를 삭제하도록 제어한다.
- [17] 또한, 상기 제2 제어부는, 상기 단말기의 웹 브라우저가 제공하는 단일 인증

쿠키 정보를 이용하여 작성된 상기 어플리케이션의 단일 인증을 위한 메시지를 수신하면, 상기 메시지에 대응하는 통합 서비스 번호를 상기 어플리케이션 서비스 장치에 제공하도록 제어하며, 상기 단말기의 웹 브라우저로부터 상기 단일 인증 쿠키 만료 요청 메시지를 수신하면, 상기 만료 요청 메시지에 대응하는 응답 메시지를 상기 웹 브라우저에 제공하고, 상기 제2 저장부에 저장된 단일 인증 쿠키 정보를 삭제하도록 제어한다.

- [18] 본 발명은 또한, 복수개의 어플리케이션 중 적어도 하나의 어플리케이션 기능 수행을 위해 복수개의 어플리케이션 서비스 장치 중 적어도 하나와 통신 채널을 형성하는 통신부, 복수개의 어플리케이션, 복수개의 어플리케이션 서비스 장치의 서비스 이용을 위한 서비스 토큰, 복수개의 어플리케이션 서비스 장치에 접속할 수 있도록 지원하는 단일 인증 토큰을 저장하는 저장부, 단일 인증 토큰 부재 시 단일 인증 토큰 획득을 위한 요청 메시지를 상기 어플리케이션 서비스 장치를 통해 단일 인증 서비스 장치에 제공하여 단일 인증 토큰을 획득하도록 제어하며, 단일 인증 토큰이 존재하면 단일 인증 토큰을 기반으로 특정 어플리케이션 서비스 장치 접속 및 이용을 위한 통합 서비스 번호 제공을 위한 단일 인증 세션 조회 메시지를 어플리케이션 서비스 장치를 통하여 단일 인증 서비스 장치에 제공하도록 제어하는 제어부를 포함하는 것을 특징으로 하는 단일 인증 서비스를 지원하는 단말기의 구성을 개시한다.
- [19] 여기서 단말기는 어플리케이션 서비스 장치 접속을 위한 일반 인증 정보 입력을 위한 영역, 상기 단일 인증 토큰 획득을 위한 통합 ID 로그인을 위한 영역, 상기 단일 인증 토큰 기반으로 특정 어플리케이션 서비스 장치 접속을 위한 인증 정보가 자동 입력된 영역 중 적어도 하나를 출력하는 표시부를 더 포함할 수 있다.
- [20] 또한 단말기는 서비스 토큰 만료 요청을 위한 로그아웃 항목, 단일 인증 토큰 만료 요청을 위한 팝업창, 어플리케이션 서비스 장치로부터 수신된 데이터를 출력하는 서비스 영역 중 적어도 하나를 포함하는 화면을 제공하는 표시부를 더 포함할 수 있다.
- [21] 한편 제어부는 단일 인증 토큰 운용을 위한 어카운트 매니저 계정 생성을 제어하거나 또는 클라우드 서비스 기능의 활성화 제어를 지원할 수 있으며, 이때 상기 단일 인증 토큰 만료 시 상기 어카운트 매니저 계정을 삭제하도록 제어할 수 있다.
- [22] 또한, 제어부는, 특정 어플리케이션 활성화를 위한 선택 시 웹 브라우저의 단일 인증 쿠키 정보 운용 여부를 확인하고, 상기 단일 인증 쿠키 정보를 통해 제공되는 단일 인증 토큰을 이용하여 상기 어플리케이션의 자동 로그인 수행을 위한 메시지를 해당 어플리케이션 서비스 장치에 전송하도록 제어한다.
- [23] 또한, 특정 어플리케이션은, 웹 브라우저의 상기 단일 인증 쿠키 운용 불가 시, 통합 ID 로그인을 수행하여 1회용 접속키를 단일 인증 서비스 장치로부터 수신하여 상기 웹 브라우저에게 제공하며, 상기 웹 브라우저는, 상기 1회용

접속키를 기반으로 상기 단일 인증 서비스 장치에 접속하여 상기 단일 인증 쿠키 정보를 수신한다.

- [24] 본 발명은 또한, 단말기가 특정 어플리케이션 기능 운용을 위하여 어플리케이션 서비스 장치 접속 과정에서 통합 ID 로그인을 수행하거나 사전 저장된 단일 인증 토큰 기반의 단일 인증을 위한 세션 조회 메시지를 어플리케이션 서비스 장치에 제공하는 단계, 어플리케이션 서비스 장치가 상기 통합 ID 로그인을 수행한 후 단일 인증 토큰 생성을 위한 요청 메시지를 상기 단일 인증 서비스 장치에 전송하거나 상기 세션 조회 메시지를 단일 인증 서비스 장치에 전송하는 단계, 어플리케이션 서비스 장치가 단일 인증 서비스 장치로부터 단일 인증 토큰 또는 세션 조회 메시지에 따른 통합 서비스 번호를 수신하는 단계, 어플리케이션 서비스 장치가 단일 인증 토큰 수신 시 단일 인증 토큰과 어플리케이션 서비스 장치 이용을 위한 서비스 토큰 및 데이터를 상기 단말기에 제공하고, 통합 서비스 번호 수신 시 어플리케이션의 자동 로그인을 수행하고 상기 서비스 토큰 및 데이터를 상기 단말기에 제공하는 단계를 포함하는 것을 특징으로 하는 단일 인증 서비스 운용 방법의 구성을 개시한다.
- [25] 상기 방법은 단말기가 서비스 토큰 만료를 위한 요청 메시지 또는 서비스 토큰과 단일 인증 토큰 만료를 위한 요청 메시지를 어플리케이션 서비스 장치에 전송하는 단계, 상기 어플리케이션 서비스 장치가 서비스 토큰 만료에 따른 응답 메시지를 단말기에 제공하거나 단일 인증 토큰 만료를 위한 요청 메시지를 단일 인증 서비스 장치에 전송하고 그에 대응하는 응답을 상기 서비스 토큰 만료 응답 메시지와 함께 상기 단말기에 제공하는 단계, 단말기가 서비스 로그아웃 또는 단일 인증 로그아웃 중 어느 하나를 수행하는 단계를 더 포함할 수 있다.
- [26] 본 발명은 또한, 단말기의 웹 브라우저가 특정 어플리케이션 활성화를 위한 입력 신호 수신 시 해당 어플리케이션 호출과 함께 해당 어플리케이션에게 단일 인증 쿠키 정보 기반의 단일 인증 토큰을 제공하는 단계; 상기 어플리케이션이 상기 단일 인증 토큰을 이용하여 자동 로그인을 위한 세션 조회 메시지를 어플리케이션 서비스 장치를 통해 단일 인증 서비스 장치에 제공하는 단계; 상기 단일 인증 서비스 장치가 상기 세션 조회 메시지에 대응하는 통합 서비스 번호를 생성하여 상기 어플리케이션 서비스 장치에 제공하는 단계; 상기 어플리케이션 서비스 장치가 상기 통합 서비스 번호를 기반으로 어플리케이션 서비스 운용을 위한 서비스 토큰을 생성하는 단계; 및 상기 어플리케이션 서비스 장치가 상기 서비스 토큰 및 상기 어플리케이션 서비스 운용을 위한 사용자 데이터를 상기 어플리케이션에 제공하는 단계를 포함한다.
- [27] 상기 방법은 상기 웹 브라우저의 단일 인증 쿠키 정보 운용 불가 시, 상기 어플리케이션이 입력된 통합 ID 로그인을 위한 정보를 상기 어플리케이션 서비스 장치를 통해 상기 단일 인증 서비스 장치에 제공하는 단계; 상기 단일 인증 서비스 장치가 1회용 접속키를 상기 어플리케이션에 제공하는 단계; 상기 어플리케이션이 상기 웹 브라우저에 상기 1회용 접속키를 제공하는 단계; 및

상기 웹 브라우저가 상기 1회용 접속키를 이용하여 상기 단일 인증 서비스 장치에 접속하여 상기 단일 인증 쿠키 정보를 수신하는 단계를 더 포함한다.

- [28] 상기 방법은 상기 웹 브라우저 종료 또는 상기 웹 브라우저 기반의 단일 인증 서비스 로그아웃을 위한 입력 신호를 수신하는 단계; 상기 입력 신호에 따른 요청 메시지를 상기 단일 인증 서비스 장치에 전송하는 단계; 상기 단일 인증 서비스 장치가 저장된 단일 인증 쿠키 정보를 삭제하고 상기 요청 메시지에 대응하는 응답 메시지를 상기 단말기에 제공하는 단계; 및 상기 단말기가 상기 서비스 로그아웃을 수행하는 단계를 더 포함한다.

- [29] 본 발명은 또한, 상술한 방법을 실행하는 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체의 구성을 개시한다.

발명의 효과

- [30] 이상에서 살펴본 바와 같이 본 발명에 따른 단일 인증 서비스 시스템 및 방법에 따르면, 본 발명은 특정 어플리케이션 운용을 위한 간단한 입력만으로도 다양한 어플리케이션들의 운용을 위한 인증 과정을 신속하고 편리하게 할 수 있으며, 인증 상태 관리를 보다 용이하게 운용할 수 있도록 지원한다.

- [31] 또한 본 발명은 특정 서비스 제공업자가 다양하게 제공하는 어플리케이션들을 단일 인증 정보를 토대로 공통적으로 이용할 수 있도록 지원하여 인증 정보의 관리 투명성과 신뢰도를 높이면서도 인증 정보 관리를 위한 비용을 절감하고 인증 정보 관리의 효율성을 개선할 수 있다.

도면의 간단한 설명

- [32] 도 1은 본 발명의 실시 예들에 따른 단일 인증 서비스 시스템의 구성을 개략적으로 나타낸 도면이다.

- [33] 도 2는 본 발명의 실시 예들에 따른 단말기의 구성을 보다 상세히 나타낸 블록도이다.

- [34] 도 3은 본 발명의 실시 예들에 따른 어플리케이션 서비스 장치의 구성을 보다 상세히 나타낸 블록도이다.

- [35] 도 4는 본 발명의 실시 예들에 따른 단일 인증 서비스 장치의 구성을 보다 상세히 나타낸 블록도이다.

- [36] 도 5 및 도 6은 본 발명의 제1 실시 예에 따른 단일 인증 운용 방법을 설명하기 위한 신호 흐름도이다.

- [37] 도 7 및 도 8은 본 발명의 제2 실시 예에 따른 단일 인증 운용 방법을 설명하기 위한 신호 흐름도이다.

- [38] 도 9는 본 발명의 실시 예들에 따른 단일 인증 서비스 시스템의 서비스 로그아웃 운용을 설명하기 위한 도면이다.

- [39] 도 10은 본 발명의 실시 예들에 따른 단일 인증 서비스 시스템의 단일 인증 로그아웃 운용을 설명하기 위한 도면이다.

- [40] 도 11은 본 발명의 제3 실시 예에 따른 웹 브라우저 기반의 단말기의 구성을

개략적으로 나타낸 블록도이다.

- [41] 도 12는 본 발명의 실시 예에 따른 웹 브라우저 기반의 단일 인증 서비스 장치의 구성을 보다 상세히 나타낸 블록도.
- [42] 도 13는 본 발명의 제3 실시 예에 따른 웹 브라우저 기반의 단일 인증 운용 방법 중 단일 인증 초기화 과정을 설명하기 위한 도면이다.
- [43] 도 14은 본 발명의 제3 실시 예에 따른 웹 브라우저 기반의 단일 인증 운용 방법 중 단일 인증 운용 과정을 설명하기 위한 도면이다.
- [44] 도 15은 본 발명의 제3 실시 예에 따른 단일 인증 기능 운용에 따른 단말기의 화면 인터페이스의 일예를 개략적으로 나타낸 도면이다.

발명의 실시를 위한 형태

- [45] 이하, 본 발명의 실시 예를 첨부된 도면에 의거하여 상세히 설명한다.
- [46] 실시 예를 설명함에 있어서 본 발명이 속하는 기술분야에 익히 알려져 있고 본 발명과 직접적으로 관련이 없는 기술 내용에 대해서는 설명을 생략한다. 또한, 실질적으로 동일한 구성과 기능을 가진 구성 요소들에 대해서는 상세한 설명을 생략하도록 한다.
- [47] 마찬가지로의 이유로 첨부 도면에 있어서 일부 구성요소는 과장되거나 생략되거나 또는 개략적으로 도시되었으며, 각 구성요소의 크기는 실제 크기를 전적으로 반영하는 것이 아니다. 따라서 본 발명은 첨부한 도면에 그려진 상대적인 크기나 간격에 의해 제한되어지지 않는다.
- [48] 도 1은 본 발명의 실시 예들에 따른 단일 인증 서비스 시스템의 구성을 개략적으로 나타낸 블록도이다.
- [49] 도 1을 참조하면, 본 발명의 단일 인증 서비스 시스템(10)은 단말기(100), 어플리케이션 서비스 장치들(200) 및 단일 인증 서비스 장치(300)의 구성을 포함할 수 있다. 여기서 단말기(100)는 특정 어플리케이션(이하 어플리케이션) 운용을 위하여 어플리케이션 서비스 장치들(200)과 통신 채널을 형성하며, 어플리케이션 서비스 장치들(200)은 단말기(100)의 어플리케이션들 간 단일 인증 지원을 위하여 단일 인증 서비스 장치(300)와 통신 채널을 형성한다.
- [50] 특히 본 발명의 단일 인증 서비스 시스템(10)은 단말기(100)가 특정 어플리케이션을 통하여 접속한 어플리케이션 서비스 장치 예를 들면 제1 어플리케이션 서비스 장치(201)로부터 서비스 토큰과 단일 인증 토큰(Single-Sign On Token : SSO 토큰)을 수신하고, 이를 기반으로 단일 인증 관리를 수행하는 인증 관리자(Authenticator)를 운용하도록 지원한다. 여기서 인증 관리자는 각각의 모바일 어플리케이션이 활성화될 때 단일 인증 토큰 추출을 지원한다. 이에 따라 인증 관리자가 유지되는 모바일 환경에서는 단말기(100)에서 특정 어플리케이션 예를 들면 제2 어플리케이션 지원을 위한 특정 어플리케이션 서비스 장치 예를 들면 제2 어플리케이션 서비스 장치(202)로부터 자동으로 서비스 토큰을 수신할 수 있다. 그러면 단말기(100)의

제2 어플리케이션은 수신된 서비스 토큰을 이용하여 제2 어플리케이션 서비스 장치(202)가 지원하는 서비스 이용을 지원할 수 있다. 여기서 인증 관리자는 단말기(100)가 지원하는 운영체제에 따라 다르게 구현될 수 있으며, 이와 같이 인증 관리자는 각 단말기(100)의 운용 체제에 따라 특정 형태의 소프트웨어 모듈 등으로 구현되어 인증 정보 관리를 지원하는 구성이 될 수 있다.

- [51] 상술한 바와 같이 본 발명의 단일 인증 서비스 시스템(10)은 단말기(100)가 특정 어플리케이션 운용을 위하여 어플리케이션 서비스 장치들(200) 접속을 수행하는데 있어서 단일 인증 서비스 장치(300)가 발행하는 단일 인증 토큰을 어플리케이션 서비스 장치들(200)이 운용할 수 있도록 설계하고, 어플리케이션 서비스 장치들(200)은 단일 인증 토큰을 기반으로 단말기(100)의 각 어플리케이션들에게 서비스 토큰을 할당하여 어플리케이션 서비스 장치들(200) 접속 및 서비스 이용을 수행할 수 있도록 지원한다. 이에 따라 본 발명의 단일 인증 서비스 시스템(10)은 단말기(100)에서 다양한 어플리케이션들 중 적어도 하나가 운용될 경우, 사전 생성된 인증 관리자가 제공하는 단일 인증 토큰을 이용하여 해당 어플리케이션 서비스 장치들(200)로부터 서비스 토큰을 수신하여 이용할 수 있도록 지원한다. 결과적으로 본 발명의 단일 인증 서비스 시스템(10)은 각 어플리케이션별로 별다른 인증 정보 송수신 과정을 수행하지 않고도 단일 인증 토큰 기반으로 제공되는 서비스 토큰을 이용하여 자유로운 어플리케이션 서비스 장치들(200) 접속 및 서비스 이용을 수행하도록 지원한다. 상술한 단일 인증 서비스 시스템(10)을 구성하는 각 구성들에 대하여 도 2 내지 도 4를 참조하여 보다 상세히 설명하기로 한다.
- [52] 먼저, 도 2는 본 발명의 실시 예들에 따른 단말기(100)의 구성을 보다 상세히 나타낸 도면이다.
- [53] 도 2를 참조하면, 본 발명의 단말기(100)는 통신부(110), 입력부(120), 오디오 처리부(130), 표시부(140), 저장부(150) 및 제어부(160)의 구성을 포함할 수 있다.
- [54] 이와 같은 구성을 가지는 본 발명의 단말기(100)는 저장부(150)에 저장된 특정 어플리케이션 예를 들면 제1 어플리케이션(151) 활성화 요청에 따라 통신부(110)를 이용하여 제1 어플리케이션 서비스 장치(201) 접속을 수행할 수 있다. 이 과정에서 단말기(100)는 단일 인증 서비스 운용을 위하여 사전 생성된 인증 관리자가 존재하는지를 확인하고, 인증 관리자가 존재하지 않는 경우 제1 어플리케이션 서비스 장치(201)를 통하여 어플리케이션들 간의 단일 인증에 이용되는 단일 인증 토큰 제공을 위한 인증 관리자 운용을 수행할 수 있다. 한편, 단말기(100)는 인증 관리자가 단일 인증 토큰을 제공할 수 있는 경우, 해당 인증 관리자로부터 단일 인증 토큰을 추출하고, 추출된 단일 인증 토큰을 기반으로 다른 어플리케이션 서비스 장치 예를 들면 제2 어플리케이션 서비스 장치(202) 접속을 수행할 수 있다. 이에 따라 본 발명의 단말기(100)는 다수개의 어플리케이션들(151, 153) 중에 특정 어플리케이션을 기반으로 단일 인증 토큰을 제공하는 인증 관리자 운용이 선행된 경우 다른 어플리케이션 서비스 이용을

위한 제2 어플리케이션 서비스 장치(202) 접속은 별도의 인증 정보 제공 없이 가능하도록 지원받을 수 있다. 이를 위하여 통신부(110)는 단말기(100)의 통신 기능을 지원하여 어플리케이션 서비스 장치들(200)과 통신 채널을 형성하는 구성이다. 이러한 통신부(110)는 단말기(100)의 이동성 지원을 위하여 이동통신 모듈로 구성될 수 있다. 이에 따라 통신부(110)는 통신 서비스를 지원하기 위하여 설치된 기지국이나 무선 액세스 포인트에 접속을 수행하고, 기지국 또는 무선 액세스 포인트와 연결된 네트워크 장치를 통하여 어플리케이션 서비스 장치들(200) 접속을 수행할 수 있다. 그리고 통신부(110)는 단일 인증 토큰을 제공하는 인증 관리자 운용이 불가능한 경우 제어부(160) 제어에 따라 통합 ID 정보를 기반으로 하는 로그인을 요청하는 요청 메시지를 예를 들면 제1 어플리케이션 서비스 장치(201)에 전송할 수 있다.

- [55] 또한 통신부(110)는 이에 대응하여 제1 어플리케이션 서비스 장치(201)로부터 서비스 토큰과 사용자 데이터 및 단일 인증 토큰을 수신할 수 있다. 통신부(110)는 인증 관리자 운용이 가능한 경우 인증 관리자로부터 추출된 단일 인증 토큰을 기반으로 단일 인증 세션 조회를 위한 조회 메시지를 예를 들면 제2 어플리케이션 서비스 장치(202)에 전송하고, 제2 어플리케이션 서비스 장치(202)로부터 해당 조회 메시지에 대응하는 서비스 토큰 및 사용자 데이터를 수신할 수 있다. 통신부(110)가 수신한 정보는 제어부(160)에 전달되며, 제어부(160)는 수신된 정보를 토대로 특정 어플리케이션 기반의 사용자 기능 수행을 지원할 수 있다. 입력부(120)는 단말기(100) 운용에 필요한 입력 신호 생성을 지원하는 구성으로서, 예를 들면 홈 키, 사이드 키 등의 키 버튼으로 형성될 수 있으며 또한 터치스크린으로 구현된 표시부(140) 상에 가상 키 맵 형태로 출력될 수 있다. 입력부(120)는 단말기(100)가 지원하는 어플리케이션들(151, 153) 중 적어도 하나의 어플리케이션을 활성화하기 위한 입력 신호를 생성할 수 있으며, 이러한 입력 신호는 제어부(160)에 전달되어 해당 어플리케이션 활성화를 위한 명령어로 이용될 수 있다. 추가로 입력부(120)는 특정 어플리케이션 활성화에 따라 어플리케이션 서비스 장치에서 요구하는 인증 정보 입력을 수행할 수 있다.

- [56] 특히 입력부(120)는 본 발명의 실시 예에 따른 단일 인증 토큰 획득을 위해 통합 ID 로그인을 위한 인증 정보 입력을 사용자 제어에 따라 수행할 수 있다. 단일 인증 토큰이 획득된 이후 또는 단일 인증 토큰을 기반으로 인증 관리자가 생성된 이후 입력부(120)는 추가적으로 활성화되는 어플리케이션들의 인증 정보 확인을 위해서 사전 정의되고 단순화된 특정 입력 신호를 생성할 수 있다. 예를 들면 특정 입력 신호는 특정 어플리케이션 서비스 장치 접속을 요청하는 단일 인증 화면에서 확인 키 버튼을 선택하기 위한 입력 신호가 될 수 있다. 오디오 처리부(130)는 단말기(100) 운용 과정에서 발생하는 다양한 오디오 데이터를 출력하기 위한 스피커(SPK)와 오디오 데이터 수집을 위한 마이크(MIC)를 포함할 수 있다. 특히 오디오 처리부(130)는 단말기(100)가 지원하는 특정

어플리케이션들(151, 153)이 활성화되는 과정에서 발생하는 다양한 오디오 신호를 출력할 수 있다. 이 과정에서 오디오 처리부(130)는 특정 어플리케이션 활성화 및 어플리케이션 서비스 장치 접속 과정에서 잘못된 인증 정보 입력이 발생하는 경우 이를 경고하는 안내음을 출력할 수 있다. 한편 오디오 처리부(130)는 특정 어플리케이션 활성화에 따라 어플리케이션 서비스 장치가 오디오 데이터를 제공하는 경우 해당 오디오 데이터 출력을 지원할 수 있다.

[57] 표시부(140)는 단말기(100)의 각종 메뉴를 비롯하여 사용자가 입력한 정보 또는 사용자에게 제공하는 정보를 표시한다. 즉 표시부(140)는 단말기(100) 이용에 따른 다양한 화면 예를 들면, 대기화면, 메뉴 화면, 메시지 작성 화면, 통화 화면, 단말기 종료 화면, 단말기 부팅 화면 등을 제공할 수 있다. 이러한 표시부(140)는 액정 표시 장치(Liquid Crystal Display), OLED(Organic Light Emitted Diode) 등의 평판 표시 패널의 형태로 형성될 수 있다. 표시부(140)는 제조 형태에 따라 표시 패널과 터치 패널을 포함하는 구조로 제작될 수 있다.

[58] 특히 본 발명의 표시부(140)는 특정 어플리케이션 활성화에 따라 어플리케이션 서비스 장치 접속을 위하여 인증 정보를 입력하는 화면을 출력할 수 있다. 이때 표시부(140)가 출력하는 인증 정보 입력 화면은 일반 인증 정보 또는 통합 인증 정보를 입력할 수 있는 ID 입력 영역과 패스워드 입력 영역을 포함할 수 있다. 그리고 인증 정보 입력 화면은 입력된 인증 정보를 기반으로 통합 ID 로그인을 위한 간편 로그인 선택 항목을 포함할 수 있다. 통합 ID 로그인이 수행된 경우 단일 인증 서비스 장치(300)는 단일 인증 토큰을 어플리케이션 서비스 장치에 전달할 수 있고, 표시부(140)는 어플리케이션 서비스 장치로부터 단일 인증 토큰에 의하여 생성된 서비스 토큰, 사용자 데이터 및 단일 인증 토큰 수신 화면을 출력할 수 있다. 또한 표시부(140)는 단일 인증 토큰을 기반으로 생성된 단일 인증 토큰 기반의 로그인 화면을 출력할 수 있다.

[59] 한편 단말기(100)는 어플리케이션 서비스 장치로부터 단일 인증 토큰을 수신하는 경우 이를 기반으로 인증 관리자 운용을 지원할 수 있으며, 이 인증 관리자 운용은 표시부(140)를 통하여 알람될 수 있다. 또는 인증 관리자 운용은 별도의 알람 없이 백그라운드 프로세싱을 통하여 수행될 수 있다. 다만 표시부(140)는 인증 관리자를 통하여 다양한 어플리케이션들을 별도의 인증 정보 입력 없이 접속할 수 있음을 안내하기 위한 특정 이미지 효과 또는 지시자를 출력할 수도 있다.

[60] 예를 들어 표시부(140)는 일측에 인증 관리자 운용 상태를 안내하는 또는 단일 인증 토큰 기반으로 어플리케이션 서비스 장치 접속이 가능함을 안내하는 지시 아이콘이나 안내 메시지 등을 출력할 수 있다. 한편 상술한 안내 메시지나 아이콘 또는 이미지 효과 등은 설계자의 의도에 따라 표시부(140)에 고정적으로 제공되지 않을 수 있으며, 인증 관리자 운용 상태에서 인증 정보 입력이 필요한 특정 어플리케이션 활성화 시 해당 어플리케이션 활성화 화면에 출력될 수 있다. 표시부(140)를 통하여 제공되는 인증 정보 입력 화면에 대해서 후술하는 도면을

참조하여 보다 상세히 설명하기로 한다. 저장부(150)는 본 발명의 실시 예에 따른 기능 동작에 필요한 응용 프로그램을 비롯하여, 표시부(140)에 출력될 화면 이미지 등을 저장한다. 그리고 저장부(150)는 표시부(140)가 터치스크린으로 구성되는 경우 터치스크린 운용을 위한 키 맵이나 메뉴 맵 등을 저장할 수 있다. 여기서 키 맵, 메뉴 맵은 각각 다양한 형태가 될 수 있다. 즉, 키맵은 키보드 맵이나, 3*4 키 맵, 쿼터 키 맵 등이 될 수 있고, 현재 활성화되고 있는 응용 프로그램의 운용 제어를 위한 제어키 맵이 될 수도 있다. 또한, 메뉴 맵은 현재 활성화되고 있는 응용 프로그램 운용 제어를 위한 메뉴 맵이 될 수도 있다. 이러한 저장부(150)는 단말기(100)의 부팅 및 상술한 각 구성의 운용을 위한 운영체제(OS, Operating System), 다양한 사용자 기능 예를 들면, 단말기(100)의 통화기능 지원을 위한 사용자 기능, 기타 음원을 재생하기 위한 MP3 사용자 기능, 사진 등을 재생하기 위한 이미지 출력 기능, 동영상 재생 기능 등을 각각 지원하기 위한 응용 프로그램 등을 저장할 수 있다.

- [61] 특히, 본 발명의 저장부(150)는 특정 어플리케이션 서비스 장치와 통신하여 특정 사용자 기능을 제공하도록 설계된 다양한 어플리케이션들(151, 153)을 저장할 수 있다. 예를 들어, 저장부(150)는 제1 어플리케이션(151) 및 제2 어플리케이션(153)을 저장할 수 있다. 제1 어플리케이션(151) 및 제2 어플리케이션(153) 중 적어도 하나는 단말기(100)가 지원 가능한 특정 사용자 기능을 지원하기 위하여 설계된 어플리케이션으로서 본 발명에서는 각각의 어플리케이션 서비스 장치들(200)과 통신 채널을 형성하되 단일 인증 토큰을 기반으로 어플리케이션 서비스 장치들(200)과의 자동 인증 정보 확인을 통하여 특정 데이터를 제공하는 어플리케이션들이 될 수 있다. 특히 제1 어플리케이션(151) 및 제2 어플리케이션(153)은 단일 인증 토큰을 기반으로 해당 서비스를 지원할 수 있도록 하나 사업자 또는 공동 서비스 사업자가 관리할 수 있는 어플리케이션 서비스 장치들에 의해 지원되는 사용자 기능이 될 수 있다.
- [62] 예를 들어, 제1 어플리케이션(151)은 제1 어플리케이션 서비스 장치(201)와의 통신을 기반으로 사용자 기능을 지원하고, 제2 어플리케이션(153)은 제2 어플리케이션 서비스 장치(202)와의 통신을 기반으로 사용자 기능을 지원할 수 있다. 이 경우 제1 어플리케이션 서비스 장치(201) 및 제2 어플리케이션 서비스 장치(202)는 각각 단일 인증 서비스 장치(300)에 의하여 인증 정보 관리가 가능하도록 통합된 장치가 될 수 있다. 즉 제1 어플리케이션 서비스 장치(201) 및 제2 어플리케이션 서비스 장치(202)는 인증 정보를 특정 서비스 제공 사업자가 함께 관리하는 어플리케이션 서비스 장치들(200)이 될 수 있다.
- [63] 서비스 형태의 예로서 제1 어플리케이션(151)은 채팅 서비스 어플리케이션이 될 수 있으며, 제2 어플리케이션(153)은 쇼핑물 어플리케이션이 될 수 있다. 이때 채팅 서비스 및 쇼핑물을 지원하는 어플리케이션 서비스 장치는 공통적으로 인증 정보 관리가 가능하도록 협약될 수 있다. 또 다른 서비스 형태의 예로서 제1 어플리케이션(151)은 제1 게임 어플리케이션이 될 수 있으며, 제2

어플리케이션(153)은 제2 게임 어플리케이션이 될 수 있다. 여기서 제1 게임 어플리케이션을 지원하는 어플리케이션 서비스 장치 및 제2 게임 어플리케이션을 지원하는 어플리케이션 서비스 장치는 보급자가 동일한 또는 계정 관리를 공동으로 수행할 수 있는 서비스 사업자일 수 있으며, 이에 따라 해당 서비스 사업자가 제공하는 단일 인증 토큰을 토대로 접속이 가능한 형태로 설계될 수 있다. 한편 각 어플리케이션 서비스 장치는 사용자 요청에 따라 개별적인 인증 정보 입력 및 확인 통하여 접속을 지원할 수도 있다.

- [64] 한편 상술한 설명에서는 저장부(150)에 두 개의 어플리케이션이 저장되는 것으로 하여 설명하였지만 본 발명이 이에 한정되는 것은 아니다. 즉 상기 저장부(150)는 보다 많은 어플리케이션들을 저장할 수 있으며, 이러한 어플리케이션들은 모두 단일 인증 토큰을 기반으로 접속이 가능한 어플리케이션 서비스 장치들과 관련된 어플리케이션들이 될 수 있다.

제어부(160)는 본 발명의 실시 예에 따른 단일 인증 서비스 기능 지원을 위한 다양한 신호 흐름 제어와 데이터 처리 및 데이터 전송과 수신을 제어할 수 있다. 예를 들어, 제어부(160)는 저장부(150)에 저장된 제1 어플리케이션(151) 및 제2 어플리케이션(153) 중 적어도 하나를 활성화할 수 있는 메뉴, 아이콘, 위젯 중 적어도 하나를 출력할 수 있다. 또는 제어부(160)는 제1 어플리케이션(151) 및 제2 어플리케이션(153) 활성화를 위한 핫 키 등을 사전 설정된 스케줄 방식에 따라 할당할 수도 있다.

- [65] 그리고 제어부(160)는 특정 어플리케이션을 활성화하기 위한 입력 신호가 발생하면, 해당 어플리케이션 지원을 위한 어플리케이션 서비스 장치 주소 정보를 수집하고, 통신부(110)를 활성화하여 어플리케이션 서비스 장치 접속을 제어할 수 있다. 이때 제어부(160)는 해당 어플리케이션 서비스 장치 접속이 가능한 서비스 토큰이 있는지 여부를 확인하고, 서비스 토큰이 없는 경우 단일 인증 토큰 지원이 가능한 인증 관리자가 있는지 여부를 확인한다. 그리고 인증 관리자가 없는 경우 단일 인증 토큰을 요청하기 위한 요청 메시지를 사용자가 입력한 정보를 포함하여 작성하고, 이를 특정 어플리케이션 기능 지원을 위한 특정 어플리케이션 서비스 장치에 전송할 수 있다. 여기서 요청 메시지에 포함되는 입력 정보는 해당 어플리케이션 활성화를 위하여 사전에 어플리케이션 서비스 장치에 등록한 입력 정보 예를 들면 ID 정보 및 패스워드 정보이거나 사전에 단일 인증을 위해 설정한 통합 ID 정보 및 패스워드 정보가 될 수 있다.

- [66] 이후, 어플리케이션 서비스 장치로부터 단일 인증 서비스 장치(300)가 발생한 단일 인증 토큰과, 어플리케이션 서비스 장치를 이용하는데 필요한 서비스 토큰 및 사용자 데이터를 수신하면, 제어부(160)는 해당 정보들을 토대로 어플리케이션 활성화에 따른 사용자 기능을 지원한다. 이와 함께 제어부(160)는 단일 인증 토큰을 이용하여 인증 관리자 운용을 지원할 수 있다. 그리고 제어부(160)는 다른 어플리케이션 활성화를 요청받는 경우 인증 관리자를

통하여 단일 인증 토큰을 제공한다. 인증 관리자에 의하여 제공된 단일 인증 토큰은 어플리케이션 서비스 장치에 제공될 수 있으며, 단일 인증 서비스 장치(300) 지원에 따라 사용자는 별도의 인증 정보 입력과정 없이 해당 어플리케이션 서비스 장치의 인증 정보 확인 과정을 자동으로 수행하도록 지원받을 수 있다. 제어부(160)는 활성화를 위해 선택된 다른 어플리케이션 지원을 위한 데이터를 해당 어플리케이션 서비스 장치로부터 수신하고 이를 표시부(140)에 출력하거나 오디오 데이터인 경우 오디오 처리부(130)를 통하여 출력하도록 제어할 수 있다.

- [67] 또한, 제어부(160)는 특정 어플리케이션 종료 또는 로그아웃을 위한 입력 신호가 발생하면, 해당 종료 또는 로그아웃 과정에서 해당 어플리케이션 서비스만을 종료 또는 로그아웃할 것인지 또는 인증 관리자를 통한 단일 인증 서비스까지 종료 또는 로그아웃할 것인지를 확인 받고, 그에 따른 종료 또는 로그아웃 절차 진행을 제어할 수 있다. 여기서 제어부(160)는 인증 관리자를 통하여 활성화된 어플리케이션들에 대한 종료 또는 로그아웃 신호가 발생하면 각 어플리케이션들을 종료 신호 또는 로그아웃 신호에 따라 종료하되, 마지막으로 어플리케이션을 종료 또는 로그아웃하는 과정에서 인증 관리자 제거 및 단일 인증 토큰 제거를 수행하도록 제어할 수 있다. 또는 제어부(160)는 단일 인증 토큰을 기반으로 활성화된 어플리케이션들 중 최초 종료 또는 로그아웃되는 어플리케이션의 종료 또는 로그아웃 수행 시 인증 관리자 제거 및 단일 인증 토큰 제거를 위한 신호 처리를 수행할 수 있다. 또는 제어부(160)는 최초 단일 인증 토큰을 단일 인증 서비스 장치(300)로부터 수신하도록 기여한 어플리케이션 종료 또는 로그아웃 시에 해당 단일 인증 토큰의 제거 및 인증 관리자 제거를 지원할 수 있다. 도 3은 본 발명의 실시 예에 따른 어플리케이션 서비스 장치(200) 구성을 보다 상세히 나타낸 도면이다. 설명에 앞서, 어플리케이션 서비스 장치(200)는 제1 어플리케이션 서비스 장치(201) 및 제2 어플리케이션 서비스 장치(202) 중 적어도 하나가 될 수 있으며, 이에 따라 이하에서는 어플리케이션 서비스 장치로 명명하며, 도면 번호 200을 할당하여 공통적으로 설명하기로 한다. 도 3을 참조하면, 본 발명의 어플리케이션 서비스 장치(200)는 제1 통신부(210), 제1 저장부(230) 및 제1 제어부(220)의 구성을 포함할 수 있다. 추가로 어플리케이션 서비스 장치(200)는 어플리케이션 서비스 지원 및 관리를 위하여 입력부, 표시부 등 다양한 구성을 더 포함할 수도 있다.

- [68] 제1 통신부(210)는 단말기(100)의 특정 어플리케이션 활성화에 따른 사용자 기능 지원을 위하여 단말기(100)와 통신 채널을 형성할 수 있다. 제1 통신부(210)는 단말기(100)로부터 접속 요청 메시지를 수신할 수 있으며, 이에 대응하여 인증 정보 요청 메시지를 전송할 수 있다. 그리고 제1 통신부(210)는 단말기(100)로부터 인증 정보를 포함하는 메시지 또는 단일 인증을 요청하는 요청 메시지를 수신할 수 있다.

- [69] 수신된 메시지들은 제1 제어부(220)에 전달되어 해당 단말기(100)의

어플리케이션 기능 지원을 위한 인증 과정에 이용될 수 있으며, 통합 ID 로그인을 요청하는 요청 메시지 또는 단일 인증 수행을 위한 조회 메시지의 경우 단일 인증 서비스 장치(300)에 제공될 수 있다. 이를 위하여 제1 통신부(210)는 단일 인증 서비스 장치(300)와 통신 채널을 형성할 수 있다. 제1 통신부(210)는 통합 ID 로그인 또는 단일 인증을 요청하는 요청 메시지를 단일 인증 서비스 장치(300)에 제공하고, 단일 인증 서비스 장치(300)로부터 해당 요청 메시지 처리에 따른 단일 인증 토큰 또는 통합 서비스 번호를 수신할 수 있다. 수신된 단일 인증 토큰은 단말기(100)에 제공될 수 있으며 수신된 통합 서비스 번호는 해당 단말기(100)의 어플리케이션 기능 지원을 위해 자동 로그인 서비스에 이용될 수 있다.

- [70] 제1 통신부(210)는 단말기(100)와 통신 채널을 형성하기 위한 통신 모듈 및 단일 인증 서비스 장치(300)와 통신 채널을 형성하기 위한 통신 모듈을 각각 포함할 수 있다. 또는 제1 통신부(210)는 단말기(100) 및 단일 인증 서비스 장치(300)와 통신 채널을 형성할 수 있는 하나의 통신 모듈을 포함할 수도 있다. 이를 위하여 단말기(100) 및 단일 인증 서비스 장치(300) 접속을 위한 통신 인터페이스가 호환이 가능하거나 또는 동일한 방식으로 구현될 수 있다.
- [71] 제1 저장부(230)는 어플리케이션 서비스 장치(200) 운용에 필요한 운영체제와 다양한 응용 프로그램을 저장한다. 특히 제1 저장부(230)는 단말기(100)의 특정 어플리케이션 기능 지원을 위하여 어플리케이션 지원 프로그램(231)을 포함할 수 있으며, 단말기(100)의 서비스 이용을 위해 할당되는 서비스 토큰(233)을 저장할 수 있다. 그리고 제1 저장부(230)는 단말기(100)의 사전 등록 과정을 통하여 단말기(100)의 식별 정보를 저장할 수 있다. 단말기(100)의 식별 정보는 해당 단말기(100)가 정상적인 서비스 이용이 가능하도록 등록된 단말기인지를 확인하는데 이용될 수 있으며, 이를 위하여 제1 저장부(230)는 사전 협의된 규칙에 따라 단말기(100)가 등록한 ID 정보와 패스워드 정보를 식별 정보에 포함하여 저장할 수 있다.
- [72] 어플리케이션 지원 프로그램(231)은 단말기(100)의 접속 요청에 따라 해당 단말기가 사전 등록된 단말기인지 확인하기 위한 인증 처리 루틴, 인증된 단말기(100)의 어플리케이션 활성화에 대응한 서비스 토큰 및 사용자 데이터를 제공하는 루틴을 포함할 수 있다. 특히 어플리케이션 지원 프로그램(231)은 단말기(100)의 통합 ID 로그인 처리 또는 모바일 단일 인증 토큰 기반의 단일 인증 요청 처리를 위한 루틴, 통합 ID 로그인 처리에 따른 단일 인증 토큰을 단말기(100)에 전달하도록 처리하는 루틴 및 통합 서비스 번호 기반의 자동 로그인 기능 지원 루틴 등을 저장할 수 있다.
- [73] 서비스 토큰(233)은 단말기(100)가 어플리케이션 서비스 장치(200)가 제공하는 서비스를 이용할 수 있도록 제공되는 정보이다. 이러한 서비스 토큰(233)은 단말기(100)가 접속을 요청하고 정상적인 인증 과정이 수행되면 해당 단말기(100)에 할당되고, 해당 어플리케이션 서비스 기능 종료 시 회수 또는

폐기될 수 있다. 한편 서비스 토큰(233)은 단말기(100)가 단일 인증 서비스를 요구하는 경우 단일 인증 서비스 장치(300)가 제공하는 단일 인증 토큰과 연계되어 또는 단일 인증 토큰을 기반으로 생성될 수 있다.

- [74] 제1 제어부(220)는 어플리케이션 서비스 장치(200) 운용을 위한 다양한 신호 처리와 데이터 처리 및 전달을 제어하는 구성이다. 단말기(100)로부터 접속을 요청받는 경우 제1 제어부(220)는 사전 정의된 스케줄 정보에 따라 인증 정보를 단말기(100)에 요청하도록 제어할 수 있다. 단말기(100)로부터 인증 정보를 수신하면, 제1 제어부(220)는 해당 인증 정보가 사전 등록된 정보와 일치하는지 확인하고, 그에 따른 어플리케이션 서비스 기능에 필요한 데이터를 제공할 수 있다.
- [75] 여기서 제1 제어부(220)는 단말기(100)의 특정 어플리케이션으로부터 단일 인증을 위한 요청 메시지를 수신한 경우, 해당 요청 메시지를 단일 인증 서비스 장치(300)에 제공하도록 제어할 수 있다. 그리고 단일 인증 서비스 장치(300)로부터 단일 인증 토큰을 수신하면, 단일 인증 토큰과 함께 서비스 토큰 및 사용자 데이터를 단말기(100)에 제공할 수 있다. 여기서 제1 제어부(220)는 단일 인증을 위한 요청 메시지에 포함된 통합 ID 정보 및 패스워드 정보를 기반으로 해당 단말기(100)의 인증 과정을 수행할 수 있다. 그리고 제1 제어부(220)는 단말기(100)의 서비스 이용을 위한 서비스 토큰을 단일 인증 토큰을 기반으로 또는 단일 인증 토큰과 연계하여 생성할 수 있다.
- [76] 한편 제1 제어부(220)는 단말기(100)의 특정 어플리케이션으로부터 단일 인증 토큰 기반의 세션 조회 메시지를 수신하면, 조회 메시지를 단일 인증 서비스 장치(300)에 전달할 수 있다. 그리고 단일 인증 서비스 장치(300)로부터 단일 인증에 따른 통합 서비스 번호를 수신하면, 이를 기반으로 단말기(100)의 로그인을 수행하고 서비스 토큰을 생성할 수 있다. 제1 제어부(220)는 생성된 서비스 토큰 및 어플리케이션 서비스 기능 지원을 위한 사용자 데이터를 단말기(100)에 제공할 수 있다. 즉 제1 제어부(220)는 단일 인증 토큰을 기반으로 접속을 요청하는 단말기(100)에 대해서 단일 인증 서비스 장치(300)의 확인에 따라 별도의 인증 정보 확인 과정 없이 로그인을 수락하고 해당 어플리케이션에 따른 서비스 기능을 지원할 수 있다.
- [77] 상술한 어플리케이션 서비스 장치(200) 설명에서는 특정 어플리케이션 서비스 장치(200)가 단일 인증 요청 메시지를 기반으로 하는 로그인 지원, 단일 인증 토큰을 기반으로 하는 로그인 지원을 모두 수행하는 것으로 설명하였지만, 본 발명이 이에 한정되는 것은 아니다. 즉 시스템 설계자의 설계 방식에 따라 단일 인증 요청 메시지 기반의 로그인 지원의 어플리케이션 서비스 장치는 예를 들면 제1 어플리케이션 서비스 장치(201)로 고정될 수 있다. 예를 들어, 단말기(100)의 제1 어플리케이션(151)을 지원하는 제1 어플리케이션 서비스 장치(201)는 단일 인증 요청 메시지 기반으로 로그인 수행을 지원하며, 제2 어플리케이션(153)을 지원하는 제2 어플리케이션 서비스 장치(202)는 단일 인증 토큰 기반의 로그인

수행 및 일반 인증 정보 기반의 로그인 수행만을 지원하도록 설계될 수 있다. 또는 제2 어플리케이션 서비스 장치(202)가 단일 인증 토큰을 제공하기 위한 장치가 될 수 있으며, 제1 어플리케이션 서비스 장치(201)는 단일 인증 세션 조회 메시지 기반으로 로그인을 수행하는 장치가 될 수 있다.

- [78] 도 4는 본 발명의 실시 예에 따른 단일 인증 서비스 장치(300)의 구성을 보다 상세히 나타낸 도면이다.
- [79] 도 4를 참조하면, 본 발명의 단일 인증 서비스 장치(300)는 장치 통신부(310), 제2 제어부(320), 및 제2 저장부(330)의 구성을 포함할 수 있다. 추가로 단일 인증 서비스 장치(300)는 어플리케이션 서비스 장치(200)와 유사하게 장치 관리를 위하여 또는 특정 데이터 갱신 등을 위하여 입력부, 표시부 등의 구성을 더 포함할 수 있다.
- [80] 장치 통신부(310)는 어플리케이션 서비스 장치(200)와 통신 채널을 형성하는 구성이다. 이를 위하여 장치 통신부(310)는 어플리케이션 서비스 장치(200)와 데이터 송수신이 가능한 형태의 통신 모듈 또는 어플리케이션 서비스 장치(200)가 접속된 네트워크 장치에 데이터를 전송하고 해당 네트워크 장치로부터 데이터를 수신할 수 있는 통신 모듈로 구성될 수 있다. 이러한 장치 통신부(310)는 어플리케이션 서비스 장치(200)로부터 단일 인증 요청 메시지를 수신하거나, 단일 인증 세션 조회 메시지를 수신할 수 있다. 그리고 장치 통신부(310)는 제2 제어부(320)가 생성한 단일 인증 토큰 및 통합 서비스 번호 중 어느 하나를 어플리케이션 서비스 장치(200)에 제공한다.
- [81] 제2 저장부(330)는 단일 인증 서비스 장치(300) 운용을 위한 프로그램들을 저장한다. 특히 제2 저장부(330)는 본 발명의 단일 인증 서비스 지원을 위한 프로그램인 단일 인증 지원 프로그램(331) 및 단일 인증 토큰(332)을 저장할 수 있다.
- [82] 단일 인증 지원 프로그램(331)은 어플리케이션 서비스 장치(200)로부터 수신되는 메시지에 따라 통합 서비스 번호를 생성하거나, 단일 인증 토큰을 생성하도록 지원할 수 있다. 이를 위하여 단일 인증 지원 프로그램(331)은 어플리케이션 서비스 장치(200)로부터 수신되는 메시지의 종류를 구분하는 루틴, 수신된 메시지가 단일 인증 세션 조회 메시지인 경우 해당 조회 메시지에 대응하여 통합 서비스 번호를 생성하는 루틴, 생성된 통합 서비스 번호를 어플리케이션 서비스 장치(200)에 제공하는 루틴을 포함할 수 있다. 또한 단일 인증 지원 프로그램(331)은 수신된 메시지가 단일 인증 요청 메시지인 경우 단일 인증 토큰을 생성하는 루틴, 생성된 단일 인증 토큰을 어플리케이션 서비스 장치(200)에 제공하는 루틴을 포함할 수 있다.
- [83] 단일 인증 토큰(332)은 특정 단말기(100)가 다수의 어플리케이션 서비스 장치를 접속하고 이용할 수 있도록 지원하는 정보이다. 이러한 단일 인증 토큰(332)은 특정 단말기(100)가 단일 인증 서비스를 이용하기 위하여 요청하는 경우 생성되어 어플리케이션 서비스 장치(200)를 통하여 단말기(100)에

전송되는 한편 제2 저장부(330)에 저장될 수 있다. 이후 단일 인증 토큰(332)은 단일 인증 세션 조회 메시지의 유효성 확인을 위하여 이용될 수 있다. 이를 위하여 단말기(100)는 단일 인증 세션 조회 메시지 작성 시 이전에 어플리케이션 서비스 장치(200)를 통하여 단일 인증 서비스 장치(300)로부터 수신한 단일 인증 토큰을 인증 관리자로부터 제공받고, 이를 해당 메시지에 포함하여 전송할 수 있다. 상기 단일 인증 토큰(332)은 단말기(100)의 단일 인증 서비스 종료 요청에 따라 폐기될 수 있다.

- [84] 제2 제어부(320)는 단일 인증 서비스 장치(300) 운용에 필요한 다양한 신호의 처리와 전달을 제어할 수 있다. 특히 제2 제어부(320)는 본 발명의 단일 인증 서비스 지원을 위한 단일 인증 토큰(332)의 생성과 제공 및 관리, 단일 인증 토큰(332) 기반의 통합 서비스 번호의 생성과 제공 및 관리를 지원할 수 있다. 이를 보다 상세히 설명하면, 제2 제어부(320)는 어플리케이션 서비스 장치(200)로부터 단일 인증 요청 메시지를 수신하면, 해당 요청에 따라 단일 인증 토큰(332)을 생성할 수 있다. 제2 제어부(320)는 단일 인증 토큰(332)이 생성되면, 이를 어플리케이션 서비스 장치(200)에 제공할 수 있다.
- [85] 여기서 단일 인증 요청 메시지를 전송한 단말기(100)의 유효성 인증은 어플리케이션 서비스 장치(200)의 통합 ID 정보 인증을 통하여 수행될 수 있기 때문에 제2 제어부(320)가 별도로 유효성 검증을 수행하지 않을 수 있다. 그러나 시스템 설계자의 설계 방식에 따라 제2 제어부(320)는 단일 인증 요청 메시지에 포함된 단말기(100) 관련 정보를 토대로 해당 단말기(100)가 단일 인증 서비스를 이용하도록 사전 등록된 단말기인지 여부를 확인할 수 있다. 이를 위하여 단일 인증 서비스 장치(300)는 단일 인증 서비스를 이용하기 위하여 사전 등록된 단말기(100)들의 정보를 보관 및 관리할 수 있다.
- [86] 한편, 제2 제어부(320)는 어플리케이션 서비스 장치(200)로부터 단일 인증 세션 조회 메시지를 수신하는 경우, 해당 조회 메시지에 포함된 단일 인증 토큰을 확인한다. 그리고 조회 메시지에 포함된 단일 인증 토큰이 사전 저장된 단일 인증 토큰(332)과 동일한지 또는 단일 인증 토큰(332)과 비교하여 유효한지 여부를 확인할 수 있다. 여기서 유효성 여부는 단일 인증 토큰(332)의 생성 시간을 고려한 것이다. 즉 조회 메시지에 포함된 단일 인증 토큰이 사전 저장된 단일 인증 토큰(332)과 동일하다 하더라도 제2 제어부(320)는 사전 설계된 임계 시간을 경과한 단일 인증 토큰의 경우 유효성을 상실한 것으로 결정하고, 해당 단일 인증 토큰 기반의 단일 인증 서비스 지원을 차단할 수 있다. 이러한 단일 인증 토큰(332)에 대한 유효성 설계는 시스템 설계자의 설계 방식에 따라 적용되지 않을 수도 있다. 제2 제어부(320)는 수신된 조회 메시지의 단일 인증 토큰이 유효한 경우 또는 사전 저장된 단일 인증 토큰(332)과 동일한 경우 어플리케이션 서비스 장치 이용을 지원하기 위한 통합 서비스 번호를 생성하고 이를 어플리케이션 서비스 장치(200)에 제공할 수 있다. 이 통합 서비스 번호는 어플리케이션 서비스 장치(200)에 접속하고자하는 단말기(100)의 로그인 수락을

지원하는 정보로 이용될 수 있다.

- [87] 한편 제2 제어부(320)는 어플리케이션 서비스 장치(200)로부터 단일 인증 토큰 제거를 위한 메시지를 수신할 수 있다. 이 경우 제2 제어부(320)는 해당 단일 인증 토큰 제거를 수행하고, 단일 인증 토큰이 제거되었음을 어플리케이션 서비스 장치(200)에 전달할 수 있다.
- [88] 이상에서 설명한 바와 같이 본 발명의 단일 인증 서비스 시스템(10) 및 이를 지원하는 각 구성들은 토큰을 기반으로 단말기의 어플리케이션들 간의 단일 인증 서비스를 이용할 수 있도록 지원한다. 이에 따라 사용자는 다양한 어플리케이션들을 활성화하고 해당 서비스를 이용하는 과정에서 불필요하게 반복적인 인증 정보의 입력과 인증 획득 과정 없이 필요한 서비스를 즉각적으로 이용할 수 있다.
- [89] 도 5는 본 발명의 제1 실시 예에 따른 단일 인증 서비스 시스템의 운용 방법 중 인증 관리자 기반의 운용 방법을 설명하기 위한 도면이다.
- [90] 도 5를 참조하면, 단일 인증 서비스 시스템 운용 방법은 먼저, 단말기(100) 사용자가 저장부(150)에 저장된 특정 어플리케이션 예를 들면 제1 어플리케이션(151)을 활성화하기 위한 입력 신호를 생성하면, 단말기(100)는 S101 단계에서 제1 어플리케이션(151) 지원을 위한 서비스 토큰이 존재하는지 여부를 확인할 수 있다. 여기서 서비스 토큰은 제1 어플리케이션(151)의 사용자 기능 지원을 위하여 제1 어플리케이션 서비스 장치(201)를 이용할 수 있는 정보가 될 수 있다. 만약 단말기(100)는 제1 어플리케이션 서비스 장치(201)에 대한 사용 이력을 가지고 있으며, 재접속 시간이 사전 정의된 유효 기간 이내 또는 제1 어플리케이션 서비스 장치(201)에 대한 로그인을 유지한 경우 단말기(100)는 서비스 토큰을 유지할 수 있다. 결과적으로 단말기(100)는 서비스 토큰이 존재하는 경우 별도의 인증 과정 수행 없이 이전 이력을 기반으로 제1 어플리케이션 서비스 장치(201) 접속을 수행할 수 있다(S103).
- [91] 한편 S101 단계에서 서비스 토큰이 없는 경우 단말기(100)는 S105 단계로 분기하여 어카운트 매니저(Account Manager) 계정이 존재하는지 여부를 확인할 수 있다. S105 단계에서 어카운트 매니저 계정이 존재하는 경우에 대한 설명은 도 6을 참조하여 설명하기로 한다.
- [92] 한편 S105 단계에서 어카운트 매니저 계정이 존재하지 않는 경우, 단말기(100)는 단일 인증을 위한 통합 ID 로그인 요청을 위한 요청 메시지를 작성하고 이 요청 메시지를 S107 단계에서 제1 어플리케이션 서비스 장치(201)에 전송할 수 있다. 제1 어플리케이션 서비스 장치(201)는 제1 어플리케이션(151) 사용자 기능 지원을 위한 데이터를 제공하는 장치가 될 수 있다. 제1 어플리케이션 서비스 장치(201)는 단말기(100)로부터 단일 인증을 위한 요청 메시지를 수신하면, 해당 메시지에 포함된 로그인 정보를 이용하여 통합 ID 인증을 S109 단계에서 수행할 수 있다. 그리고 제1 어플리케이션 서비스 장치(201)는 단일 인증 토큰 획득을 위한 단일 인증 세션 생성 요청

메시지(createSSOSessionForMoblie)를 작성하고, 이를 S111 단계에서 단일 인증 서비스 장치(300)에 전송할 수 있다. 여기서 단일 인증 세션 생성 요청 메시지는 통합 로그인 정보를 포함할 수 있다.

- [93] 단일 인증 서비스 장치(300)는 제1 어플리케이션 서비스 장치(201)로부터 단일 인증 세션 생성 요청 메시지를 수신하면, 해당 요청 메시지 수신에 따라 S113 단계에서 단일 인증(SSO: Single-Sign On) 세션을 생성할 수 있다. 그리고 단일 인증 서비스 장치(300)는 단일 인증 세션 운용을 위한 단일 인증 토큰을 생성하고 S115 단계에서 단일 인증 토큰을 제1 어플리케이션 서비스 장치(201)에 제공할 수 있다. 또한 단일 인증 서비스 장치(300)는 생성된 단일 인증 토큰 및 단말기(100)가 제공한 통합 로그인 정보를 추후 단말기(100)의 식별 또는 유효성 검사 등을 위하여 보관 관리할 수 있다.
- [94] 제1 어플리케이션 서비스 장치(201)는 단일 인증 서비스 장치(300)로부터 단일 인증 토큰을 수신하면, 단일 인증 토큰과 연계된 또는 단일 인증 토큰을 기반으로 하는 제1 어플리케이션 서비스 장치(201) 이용을 위한 서비스 토큰을 생성하고, S117 단계에서 해당 단일 인증 토큰, 서비스 토큰 및 서비스 지원에 따른 사용자 데이터를 단말기(100)에 제공할 수 있다. 그러면 단말기(100)는 S119 단계에서 수신된 단일 인증 토큰을 기반으로 어카운트 매니저 계정을 생성하고 단일 인증 토큰을 저장부(150)에 저장하도록 지원할 수 있다. 한편 단말기(100)는 수신된 서비스 토큰을 이용하여 제1 어플리케이션(151) 기능을 지원할 수 있다.
- [95] 도 6은 본 발명의 제1 실시 예에 따른 단일 인증 서비스 시스템의 운용 방법 중 단일 인증 토큰 기반의 운용 방법을 설명하기 위한 도면이다.
- [96] 도 6을 참조하면, 본 발명의 단일 인증 서비스 시스템(10)의 운용 방법은 단말기(100)가 제2 어플리케이션(153) 활성화를 요청받는 경우 S201 단계에서 제2 어플리케이션(153) 지원을 위한 제2 어플리케이션 서비스 장치(202) 접속 및 서비스 이용을 위한 서비스 토큰이 있는지 여부를 확인한다. 이 단계에서 단말기(100)는 서비스 토큰이 있는 경우에는 해당 서비스 토큰을 기반으로 제2 어플리케이션 서비스 장치(202) 접속을 수행하고 서비스 이용을 위한 데이터 송수신을 지원할 수 있다(S203).
- [97] 한편 단말기(100)는 제2 어플리케이션(153) 운용을 위한 서비스 토큰이 없는 경우, S205 단계로 분기하여 어카운트 매니저 계정이 존재하는지 확인한다. 이 단계에서 어카운트 매니저 계정이 존재하지 않는 경우 단말기(100)는 앞서 도 5에서 설명한 운용 방법에 따른 절차를 수행하도록 지원할 수 있다. 한편 S205 단계에서 어카운트 매니저 계정이 존재하면 단말기(100)는 S207 단계에서 어카운트 매니저로부터 단일 인증 토큰을 추출할 수 있다. 그리고 단말기(100)는 단일 인증 토큰 기반의 단일 인증 세션 조회를 위한 조회 메시지를 작성하고, 작성된 조회 메시지를 S209 단계에서 제2 어플리케이션 서비스 장치(202)에 전송할 수 있다.
- [98] 제2 어플리케이션 서비스 장치(202)는 단말기(100)로부터 조회 메시지를

수신하는 경우, 조회 메시지에 대응하는 단일 인증 세션 검사 메시지(checkSSOSessionForMobile)를 작성하고, 작성된 단일 인증 세션 검사 메시지(checkSSOSessionForMobile)를 S211 단계에서 단일 인증 서비스 장치(300)에 전달할 수 있다. 단일 인증 서비스 장치(300)는 단일 인증 세션 검사 메시지(checkSSOSessionForMobile)를 제2 어플리케이션 서비스 장치(202)로부터 수신하면, 해당 단일 인증 세션 검사 메시지(checkSSOSessionForMobile)에 포함된 조회 메시지 내용을 확인하여 단말기(100)가 제공한 단일 인증 토큰이 유효한지 여부를 확인할 수 있다. 그리고 단일 인증 서비스 장치(300)는 유효한 단일 인증 토큰을 기반으로 작성된 메시지를 수신하였다고 판단되면, 단일 인증 토큰에 대응하는 S213 단계에서 통합 서비스 번호를 생성할 수 있다. 이 단계에서 단일 인증 서비스 장치(300)는 단일 인증 토큰이 유효하지 않은 것으로 판단되면, 에러 메시지를 작성하고, 이를 제2 어플리케이션 서비스 장치(202)를 통하여 단말기(100)에 제공할 수 있다. 그러면 단말기(100)는 앞서 설명한 도 5의 운용 방법을 통하여 새로운 단일 인증 토큰을 획득하는 과정을 수행하도록 지원할 수 있다. 한편, 단일 인증 서비스 장치(300)는 생성된 통합 서비스 번호를 S215 단계에서 제2 어플리케이션 서비스 장치(202)에 제공한다.

- [99] 제2 어플리케이션 서비스 장치(202)는 통합 서비스 번호를 수신하면, S217 단계에서 통합 ID 인증 및 서비스 토큰 생성을 수행할 수 있다. 여기서 통합 서비스 번호는 단말기(100)의 통합 로그인 정보를 포함할 수 있다. 단일 인증 서비스 장치는 통합 서비스 번호 생성 시 사전 저장한 단말기(100) 관련 통합 로그인 정보를 확인하고 이를 통합 서비스 번호에 포함하도록 작성할 수 있다. 한편 제2 어플리케이션 서비스 장치(202)는 S219 단계에서 서비스 토큰 및 제2 어플리케이션(153) 기능 지원을 위한 사용자 데이터를 단말기(100)에 제공할 수 있다.
- [100] 도 7은 본 발명의 제2 실시 예에 따른 단일 인증 서비스 시스템의 운용 방법 중 인증 관리자 기반의 운용 방법을 설명하기 위한 도면이다.
- [101] 도 7을 참조하면, 본 발명의 단일 인증 서비스 시스템(10) 운용 방법은 먼저 앞서 설명한 S101 단계와 유사하게 단말기(100)가 제1 어플리케이션(151) 활성화 요청 시 S301 단계에서 서비스 토큰 존재 여부를 확인한다. 서비스 토큰이 존재하면 존재하는 서비스 토큰을 이용하여 제1 어플리케이션 서비스 장치(201)에 접속하여 동작할 수 있다.
- [102] 그리고 서비스 토큰이 없는 경우, 단말기(100)는 S305 단계에서 인증 관리자 기능을 수행하는 클라우드 서비스 저장소에 단일 인증 토큰 정보가 존재하는지 확인한다. 이를 위하여 단말기(100)는 클라우드 클라이언트를 활성화할 수 있다. 클라우드 서비스는 단말기(100)에 저장된 콘텐츠를 별도의 통신 서비스 장치에 공유하여 운용할 수 있는 서비스가 될 수 있다. 이때 클라우드 서비스는 정보 공유를 위하여 단말기(100)의 계정을 관리할 수 있으며, 특히 본 발명의 실시 예에 따른 단일 인증 기반의 어플리케이션 기능 지원을 위한 단일 인증 토큰을

관리할 수 있다.

- [103] 한편 S305 단계에서 단일 인증 토큰 정보가 없는 경우, 단일 인증 서비스 시스템(10)의 각 구성들 즉 단말기(100), 제1 어플리케이션 서비스 장치(201) 및 단일 인증 서비스 장치(300)는 앞서 도 5에서 설명한 S107 단계 내지 S119 단계와 동일한 동작을 수행하게 된다. 즉 S307 단계에서 단말기(100)는 통합 ID 로그인 요청 메시지를 제1 어플리케이션 서비스 장치(201)에 전송하고, S309 단계에서 제1 어플리케이션 서비스 장치(201)는 통합 ID 인증 수행과 함께 단일 인증 세션 요청 메시지(createSSOSessionForMobile) 작성을 수행하고 S310 단계에서 단일 인증 세션 요청 메시지(createSSOSessionForMobile)를 단일 인증 서비스 장치(300)에 전송한다. 그러면 단일 인증 서비스 장치(300)는 S311 단계에서 단일 인증 세션을 생성하고, S313 단계에서 단일 인증 토큰을 제1 어플리케이션 서비스 장치(201)에 전송할 수 있다. 제1 어플리케이션 서비스 장치(201)는 서비스 토큰을 생성하고 제1 어플리케이션(151) 서비스 지원을 위한 사용자 데이터를 단일 인증 토큰과 함께 S315 단계에서 단말기(100)에 제공할 수 있다.
- [104] 결과적으로 단말기(100)는 상술한 단계들을 걸쳐 S317 단계에서 수신된 단일 인증 토큰을 클라우드 저장소에 저장하도록 제어할 수 있다. 한편 단말기(100)는 수신된 서비스 토큰을 기반으로 제1 어플리케이션(151) 기능 지원을 수행한다.
- [105] 도 8은 본 발명의 제2 실시 예에 따른 단일 인증 서비스 시스템의 운용 방법 중 단일 인증 토큰 기반의 운용 방법을 설명하기 위한 도면이다.
- [106] 도 8을 참조하면, 본 발명의 단일 인증 서비스 시스템의 운용 방법은 제2 어플리케이션(153) 활성화 요청이 발생하는 경우, 단말기(100)가 S401 단계에서 해당 제2 어플리케이션(153) 서비스 지원을 위해 제2 어플리케이션 서비스 장치(202) 이용을 가능하도록 하는 서비스 토큰이 존재하는지 확인한다. 이 단계에서 서비스 토큰이 없는 경우 단말기(100)는 S405 단계로 분기하여 클라우드 저장소에 단일 인증 토큰 정보가 존재하는지 여부를 확인할 수 있다. 이를 위하여 단말기(100)는 클라우드 클라이언트를 활성화한 상태를 유지할 수 있다. S405 단계에서 단일 인증 토큰이 존재하는 경우 단말기(100)는 S407 단계에서 클라우드 저장소에서 단일 인증 토큰을 추출하는 과정을 수행한다. 여기서 단말기(100)는 클라우드 서비스 장치에 단일 인증 토큰 보유 여부를 확인하고, 보유한 경우 단일 인증 토큰 정보를 클라우드 서비스 장치에 요청할 수 있다. 한편 단말기(100)는 단일 인증 토큰이 클라우드 클라이언트에 저장된 경우, 해당 클라이언트 활성화에 따라 단일 인증 토큰 정보를 수집하도록 제어할 수 있다. 단일 인증 토큰의 관리 등은 클라우드 시스템 설계자 설계 방식에 따라 변경될 수 있으며, 본 발명의 단말기(100)는 해당 시스템 설계 방식에 따라 단일 인증 토큰 정보를 수집하도록 설계될 수 있을 것이다.
- [107] 한편 이하 단일 인증 서비스 시스템(10)이 수행하는 S409 단계 내지 S419 단계는 앞서 설명한 도 6의 S209 단계 내지 S219 단계와 실질적으로 동일한 동작을 수행함으로 그에 대한 상세한 설명은 생략하기로 한다.

- [108] 도 9는 본 발명의 실시 예에 따른 단일 인증 서비스 시스템에서의 서비스 로그아웃을 설명하기 위한 도면이다.
- [109] 도 9를 참조하면, 단말기(100)는 활성화 상태인 특정 어플리케이션을 종료하기 이전에 로그아웃을 위한 절차를 수행할 수 있다. 이를 위하여 사용자는 표시부(140)에 출력된 어플리케이션 활성화 화면에서 로그아웃을 지시하는 가상 키버튼을 활성화는 입력 신호를 생성할 수 있다. 또는 단말기(100)는 활성화된 어플리케이션 종료를 위한 입력 신호가 발생하면 해당 어플리케이션의 로그인 상태를 사전 정의된 시간 동안 유지한 후 추가적인 입력 신호 예를 들면 종료시킨 어플리케이션을 재활성화하기 위한 입력 신호 발생이 없는 경우 로그아웃 이벤트 발생으로 간주할 수 있다. 또는 단말기(100)는 특정 어플리케이션 종료를 위한 입력 신호를 로그아웃 이벤트 발생으로 간주할 수 있다.
- [110] 단말기(100)는 사용자의 로그아웃 지시에 해당하는 입력 신호가 수신되거나 상술한 기 설정된 방식의 로그아웃 이벤트가 발생하면 S501 단계에서 서비스 토큰 만료 요청 메시지를 작성하고, 서비스 토큰 만료 요청 메시지를 어플리케이션 서비스 장치(200)에 전송할 수 있다. 단말기(100)로부터 서비스 토큰 만료 요청 메시지를 수신한 어플리케이션 서비스 장치(200)는 해당 요청 메시지 수신에 대응하여 S503 단계에서 서비스 토큰 만료 처리를 수행한다. 그리고 어플리케이션 서비스 장치(200)는 서비스 토큰 만료 응답 메시지를 작성하고, 해당 응답 메시지를 S505 단계에서 단말기(100)에 전송할 수 있다.
- [111] 단말기(100)는 S507 단계에서 서비스 토큰 만료 요청 메시지에 대응하는 서비스 토큰 만료 응답 메시지를 수신하면, 이를 기반으로 해당 어플리케이션의 로그인 상태를 로그아웃 상태로 처리할 수 있다. 한편 단말기(100)는 어플리케이션 종료를 위한 입력 신호 수신 시, 표시부(140)에 출력 중인 어플리케이션 활성화 화면을 우선적으로 종료시키면서 상술한 메시지 송수신에 따른 로그아웃처리를 백그라운드 프로세싱 방식으로 처리할 수 있다.
- [112] 상술한 바와 같이 본 발명의 단일 인증 서비스 시스템(10)은 특정 어플리케이션의 로그인 상태를 로그아웃 상태로 처리하는 과정에서 단일 인증 토큰은 유지하도록 지원할 수 있다. 이에 따라 단일 인증 서비스 시스템(10)은 종료된 특정 어플리케이션을 재활성화하는 경우 만료되지 않은 단일 인증 토큰을 기반으로 해당 어플리케이션 서비스 장치로부터 서비스 토큰을 자동으로 발급받아 운용하도록 지원한다.
- [113] 도 10은 본 발명의 실시 예에 따른 단일 인증 서비스 시스템에서의 단일 인증 로그아웃을 설명하기 위한 도면이다.
- [114] 도 10을 참조하면, 단말기(100)는 특정 어플리케이션의 로그아웃과 함께 단일 인증 로그아웃을 지시하는 입력 신호가 수신되면, 서비스 토큰 및 단일 인증 토큰 만료를 요청하는 만료 요청 메시지를 작성하고 S601 단계에서 만료 요청 메시지를 어플리케이션 서비스 장치(200)에 전송할 수 있다. 여기서 특정

어플리케이션의 로그아웃과 함께 단일 인증 로그아웃을 지시하는 입력 신호의 수신은 특정 어플리케이션 종료 시 단일 인증 로그아웃을 확인하는 과정을 수행함으로써 발생할 수 있다. 또는 특정 어플리케이션 로그아웃 시 자동으로 단일 인증 로그아웃이 수행되도록 설계된 경우 단말기(100)는 해당 어플리케이션 로그아웃을 위한 입력 신호 수신을 단일 인증 로그아웃까지 수행하는 입력 신호로 결정할 수 있다. 또는 단일 인증 기반으로 운용된 어플리케이션들이 종료되면서 활성화 상태를 유지하던 마지막 어플리케이션이 종료되는 경우 또는 마지막 어플리케이션을 로그아웃하는 경우 단말기(100)는 자동으로 단일 인증 로그아웃을 수행하도록 메시지 작성을 수행할 수 있다.

[115] 어플리케이션 서비스 장치(200)는 단말기(100)로부터 서비스 토큰 및 단일 인증 토큰 만료를 요청하는 만료 요청 메시지를 수신하면, S603 단계에서 서비스 토큰 만료를 수행함과 아울러, S605 단계에서 단일 인증 토큰 만료 요청 메시지를 단일 인증 서비스 장치(300)에 전송할 수 있다. 단일 인증 서비스 장치(300)는 수신된 단일 인증 토큰 만료 요청 메시지에 따라 S607 단계에서 단일 인증 토큰 만료를 수행하고, S609 단계에서 단일 인증 토큰 만료에 대한 응답 메시지를 어플리케이션 서비스 장치(200)에 전달할 수 있다.

[116] 어플리케이션 서비스 장치(200)는 단일 인증 서비스 장치(300)로부터 단일 인증 토큰 만료 응답 메시지를 수신하면, 서비스 토큰 및 단일 인증 토큰 만료 응답 메시지를 작성하고, 작성된 만료 응답 메시지를 S611 단계에서 단말기(100)에 전송할 수 있다. 만료 응답 메시지를 수신한 단말기(100)는 S613 단계에서 운용 체제별로 어카운트 매니저 계정 및 단일 인증 토큰 정보를 삭제하거나 클라우드 저장소에서 단일 인증 토큰 정보를 삭제한다. 그리고 단말기(100)는 S615 단계에서 서비스 로그아웃을 수행할 수 있다.

[117] 이상에서 설명한 바와 같이 본 발명의 제1 및 제2 실시예에서는 다수의 어플리케이션들의 단일 인증을 위한 단일 인증 시스템 및 이의 운용 방법에 대해 설명하였으며, 이하, 본 발명의 제3 실시예에서는 다수의 어플리케이션들의 단일 인증 운용을 웹 브라우저를 기반으로 수행하기 위한 단일 인증 시스템 및 이의 운용 방법에 대해 설명하기로 한다.

[118] 본 발명의 제3 실시예에 따른 단일 인증 시스템은 본 발명의 제1 및 제2 실시예에 따른 단일 인증 시스템의 구성과 동일하나, 웹 브라우저를 기반으로 단일 인증을 수행하기 위한 구성이 포함될 수 있다. 따라서, 본 발명의 제3 실시예에 따른 단일 인증 시스템의 단말 장치, 어플리케이션 서비스 장치 및 단일 인증 서비스 장치의 구성은 제1 및 제2 실시예의 단말 장치, 어플리케이션 서비스 장치 및 단일 인증 서비스 장치의 구성과 동일한 참조 부호를 적용하여 설명하기로 한다. 다만, 본 발명의 제3 실시예에 따른 단말 장치 및 단일 인증 서비스 장치는 웹 브라우저에 관련한 구성이 더 포함되어 구성되므로 이를 도시한 첨부된 도 11 및 도 12를 참조하여 설명하기로 한다. 그리고 본 발명의 제3 실시예에 따른 어플리케이션 서비스 장치는 첨부된 도 3을 참조하여

설명하기로 한다.

- [119] 우선, 본 발명의 제3 실시예에 따른 단일 인증 시스템(10)은 제1 및 제2 실시예에 따른 단일 인증 시스템(10)과 같이, 단말기(100), 어플리케이션 서비스 장치들(200) 및 단일 인증 서비스 장치(300)의 구성을 포함할 수 있다.
- [120] 본 발명의 제3 실시예에 따른 단말기(100)는 적어도 하나의 특정 어플리케이션(이하 어플리케이션) 운용을 위하여 웹 브라우저를 활성화하며, 웹 브라우저를 통하여 다수의 어플리케이션들을 선택적으로 운용할 수 있도록 지원한다. 특히 본 발명의 단일 인증 서비스 시스템(10)은 특정 어플리케이션 운용 과정에서 통합 ID 로그인을 통하여 단일 인증 초기화를 수행한 경우, 동일한 웹 브라우저를 기반으로 하는 다른 어플리케이션들의 활성화 시 단일 기능 운용에 따른 자동 로그인 기능을 지원할 수 있다.
- [121] 이를 위하여 단말기(100)는 웹 브라우저와 다수개의 어플리케이션을 저장할 수 있으며, 웹 브라우저 활성화에 따라 다수개의 어플리케이션을 선택적으로 운용할 수 있도록 지원할 수 있다. 그리고 단말기(100)는 웹 브라우저를 기반으로 단일 인증 쿠키 정보를 획득하도록 지원하고, 단일 인증 쿠키 정보에 포함된 단일 인증 토큰을 이용하여 단일 인증 서비스 장치(300)의 승인에 따라 별도의 로그인 정보 입력 없이 새로운 어플리케이션 운용을 수행하도록 지원할 수 있다.
- [122] 본 발명의 제3 실시예에 따른 어플리케이션 서비스 장치들(200)은 단말기(100)에 포함된 각 어플리케이션들의 서비스 지원을 위하여 복수개의 서비스 장치들을 포함할 수 있다. 예를 들어, 어플리케이션 서비스 장치들(200)은 단말기(100)의 제1 어플리케이션 지원을 위하여 제1 어플리케이션 서비스 장치(201)를 포함할 수 있으며, 또한 단말기(100)의 제2 어플리케이션 지원을 위하여 제2 어플리케이션 서비스 장치(202)를 포함할 수 있다. 이러한 어플리케이션 서비스 장치들(200)은 단말기(100)의 특정 어플리케이션 활성화에 따라 접속이 요청되는 경우 인증 정보 확인을 위한 과정을 수행할 수 있다. 특히 본 발명의 어플리케이션 서비스 장치들(200) 중 적어도 하나는 웹 브라우저가 제공한 단일 인증 토큰 기반의 통합 서비스 번호를 이용하여 단말기(100)의 자동 로그인 서비스를 지원할 수 있다.
- [123] 본 발명의 제3 실시예에 따른 단일 인증 서비스 장치(300)는 특정 어플리케이션이 활성화된 단말기(100)가 제공한 통합 ID 정보를 기반으로 어플리케이션 서비스 장치들(200)이 세션 생성 요청 메시지를 제공하면 해당 요청에 따라 단일 인증 토큰과 1회용 접속키를 단말기(100)의 특정 어플리케이션에 제공할 수 있다. 이후 단일 인증 서비스 장치(300)는 1회용 접속키를 이용하여 접속하는 단말기(100)의 웹 브라우저에 단일 인증 쿠키를 제공하고, 단일 인증 쿠키에 포함된 단일 인증 토큰을 기반으로 세션 조회를 요청한 어플리케이션에 대해서는 통합 서비스 번호 할당을 지원할 수 있다. 결과적으로 단일 인증 서비스 장치(300)는 단말기(100)의 웹 브라우저를 기반으로 다양한 어플리케이션들이 자동 로그인 기능을 수행할 수 있도록

지원한다.

- [124] 상술한 바와 같이 본 발명의 실시 예에 의한 단일 인증 서비스 시스템(10)은 단말기(100)가 특정 어플리케이션 운용을 위하여 어플리케이션 서비스 장치들(200) 접속을 수행하는데 있어서 단일 인증 서비스 장치(300)가 발행하는 단일 인증 쿠키 정보의 단일 인증 토큰을 웹 브라우저를 통해 특정 어플리케이션들에게 제공함으로써 반복적인 인증 정보 확인 과정을 수행하지 않고도 자동 로그인을 통하여 손쉬운 서비스 접속 및 운용을 수행할 수 있도록 지원한다. 상술한 웹 브라우저 기반의 단일 인증 서비스 시스템(10)을 구성하는 각 구성들에 대하여 도 3, 도 11 및 도 12를 참조하여 보다 상세히 설명하기로 한다.
- [125] 먼저, 도 11은 본 발명의 제3 실시 예에 따른 단말기의 구성을 보다 상세히 나타낸 도면이다.
- [126] 도 11을 참조하면, 본 발명의 제3 실시 예에 따른 단말기(100)는 통신부(110), 입력부(120), 오디오 처리부(130), 표시부(140), 저장부(150) 및 제어부(160)의 구성을 포함할 수 있다.
- [127] 이와 같은 구성을 가지는 본 발명의 제3 실시 예에 따른 단말기(100)는 저장부(150)에 저장된 웹 브라우저(155)를 기반으로 다양한 어플리케이션, 예를 들면 제1 어플리케이션(151) 활성화 요청에 따라 통신부(110)를 이용하여 제1 어플리케이션 서비스 장치(201) 접속을 수행할 수 있다. 이 과정에서 단말기(100)는 단일 인증 서비스 운용을 위하여 제1 어플리케이션(151)을 기반으로 단일 인증 서비스 운용을 위한 초기화 과정을 수행할 수 있다. 즉 단말기(100)는 제1 어플리케이션(151) 운용 과정에서 단일 인증 서비스 장치(300)로부터 단일 인증 쿠키 정보를 웹 브라우저(155)가 획득할 수 있도록 지원한다. 그리고 다른 어플리케이션 예를 들면 제2 어플리케이션(153) 활성화 요청이 발생하면, 웹 브라우저(155)는 단일 인증 쿠키 정보에 포함된 단일 인증 토큰을 제2 어플리케이션(153)에 제공하고, 이를 기반으로 제2 어플리케이션 서비스 장치(202)의 자동 로그인 기능을 수행하도록 지원한다.
- [128] 이를 위하여 통신부(110)는 단말기(100)의 통신 기능을 지원하여 어플리케이션 서비스 장치들(200)과 통신 채널을 형성하는 구성이다. 이러한 통신부(110)는 단말기(100)의 이동성 지원을 위하여 이동통신 모듈로 구성될 수 있다. 이에 따라 통신부(110)는 통신 서비스를 지원하기 위하여 설치된 기지국이나 무선 액세스 포인트에 접속을 수행하고, 기지국 또는 무선 액세스 포인트와 연결된 네트워크 장치를 통하여 어플리케이션 서비스 장치들(200)와의 접속을 수행할 수 있다.
- [129] 특히 통신부(110)는 웹 브라우저(155) 활성화에 의해 지정된 특정 어플리케이션들의 서비스 지원을 위하여 어플리케이션 서비스 장치들(200)과의 통신 채널을 형성할 수 있다. 이때 웹 브라우저(155)가 단일 인증 토큰을 제공하지 않는 경우 통신부(110)는 활성화를 위해 선택된 특정 어플리케이션의 요청에 따라 통합 ID 정보를 이용한 로그인을 요청하는 요청 메시지를 예를 들면

제1 어플리케이션 서비스 장치(201)에 전송할 수 있으며, 이에 대응하여 제1 어플리케이션 서비스 장치(201)로부터 서비스 토큰과 사용자 데이터, 단일 인증 토큰 및 1회용 접속키를 수신할 수 있다.

- [130] 여기서 단일 인증 토큰 및 1회용 접속키는 단일 인증 서비스 장치(300)가 제1 어플리케이션 서비스 장치(201)를 통하여 제공할 수 있다. 한편 수신된 1회용 접속키는 웹 브라우저(155)에 제공될 수 있다. 웹 브라우저(155)는 통신부(110)가 단일 인증 서비스 장치(300)와 형성한 통신 채널 및 1회용 접속키를 이용하여 단일 인증 서비스 장치(300) 접속하고, 단일 인증 서비스 장치(300)로부터 단일 인증 쿠키 정보를 수신한다. 웹 브라우저(155)는 수신된 단일 인증 쿠키 정보를 이용하여 어플리케이션들의 자동 로그인을 지원할 수 있다.
- [131] 입력부(120)는 단말기(100) 운용에 필요한 입력 신호 생성을 지원하는 구성으로서, 예를 들면 홈 키, 사이드 키 등의 키 버튼으로 형성될 수 있으며 또한 터치스크린으로 구현된 표시부(140) 상에 가상 키 맵 형태로 출력될 수 있다. 입력부(120)는 단말기(100)가 지원하는 웹 브라우저(155) 및 어플리케이션들(151, 153) 중 적어도 하나를 활성화하기 위한 입력 신호를 생성할 수 있으며, 이러한 입력 신호는 제어부(160)에 전달되어 해당 웹 브라우저(155) 및 어플리케이션 활성화를 위한 명령어로 이용될 수 있다. 추가로 입력부(120)는 특정 어플리케이션 활성화에 따라 어플리케이션 서비스 장치에서 요구하는 인증 정보 입력을 수행할 수 있다.
- [132] 특히 입력부(120)는 본 발명의 실시 예에 따른 웹 브라우저 기반의 단일 인증을 위해 통합 ID 로그인을 위한 인증 정보 입력을 사용자 제어에 따라 수행할 수 있다. 웹 브라우저(155)가 단일 인증 쿠키 정보를 획득한 이후 입력부(120)는 추가적으로 활성화되는 어플리케이션들의 인증을 위해서 사전 정의되고 단순화된 특정 입력 신호 예를 들면 자동 로그인 선택을 위한 입력 신호를 생성할 수 있다.
- [133] 오디오 처리부(130)는 단말기(100)의 운용 과정에서 발생하는 다양한 오디오 데이터를 출력하기 위한 스피커(SPK)와 오디오 데이터 수집을 위한 마이크(MIC)를 포함할 수 있다. 특히 오디오 처리부(130)는 단말기(100)가 지원하는 웹 브라우저(155) 및 특정 어플리케이션들(151, 153)이 활성화되는 과정에서 발생하는 다양한 오디오 신호를 출력할 수 있다. 이 과정에서 오디오 처리부(130)는 특정 어플리케이션 활성화 및 어플리케이션 서비스 장치 접속 과정에서 잘못된 인증 정보 입력이 발생하는 경우 이를 경고하는 안내음을 출력할 수 있다. 한편 오디오 처리부(130)는 특정 어플리케이션 활성화에 따라 어플리케이션 서비스 장치가 오디오 데이터를 제공하는 경우 해당 오디오 데이터 출력을 지원할 수 있다.
- [134] 표시부(140)는 단말기(100)의 각종 메뉴를 비롯하여 사용자가 입력한 정보 또는 사용자에게 제공하는 정보를 표시한다. 즉 표시부(140)는 단말기(100) 이용에 따른 다양한 화면 예를 들면, 대기화면, 메뉴 화면, 메시지 작성 화면,

통화 화면, 단말기 종료 화면, 단말기 부팅 화면 등을 제공할 수 있다. 이러한 표시부(140)는 액정 표시 장치(Liquid Crystal Display), OLED(Organic Light Emitted Diode) 등의 평판 표시 패널의 형태로 형성될 수 있다. 표시부(140)는 제조 형태에 따라 표시 패널과 터치 패널을 포함하는 구조로 제작될 수 있다.

[135] 특히 본 발명의 표시부(140)는 웹 브라우저(155)의 활성화 화면, 웹 브라우저(155) 상에서 활성화를 위해 선택된 특정 어플리케이션 지원을 위해 어플리케이션 서비스 장치 접속 화면을 출력할 수 있다. 이때 접속 화면은 일반 인증 정보를 통한 접속 및 통합 ID 정보를 이용한 접속 중 어느 하나를 선택할 수 있는 인증 정보 입력 화면이 될 수 있다. 한편 통합 ID 정보는 특정 어플리케이션 서비스 장치를 통하여 단일 인증 서비스 장치(300)에 전달될 수 있다. 그리고 단일 인증 서비스 장치(300)가 단일 인증한 정보, 즉 단일 인증 토큰 및 1회용 접속키를 어플리케이션 서비스 장치에 전달하면, 표시부(140)는 어플리케이션 서비스 장치로부터 단일 인증 토큰에 의하여 생성된 서비스 토큰, 사용자 데이터 및 단일 인증 토큰, 1회용 접속키 수신을 확인할 수 있는 화면을 출력할 수 있다.

[136] 한편 어플리케이션 서비스 장치로부터 단일 인증 토큰과 1회용 접속키를 수신한 어플리케이션은 1회용 접속키를 웹 브라우저(155)에 전달할 수 있으며, 웹 브라우저(155)는 1회용 접속키를 이용하여 단일 인증 서비스 장치(300)로부터 단일 인증 쿠키 정보를 수신할 수 있다. 이 과정에서 표시부(140)는 웹 브라우저(155)가 단일 인증 쿠키 정보를 수신하고 이를 이용하여 특정 어플리케이션의 자동 로그인을 지원하는 과정에서 요구되는 다양한 화면을 제공할 수 있다. 그리고 표시부(140)는 웹 브라우저(155)를 통하여 단일 인증이 수행되고 있음을 지시하는 지시자나 이미지 효과를 웹 브라우저(155) 활성화 화면에 출력할 수 있다. 이러한 지시자나 이미지 효과의 적용은 설계자의 의도에 따라 표시부(140)에 고정적으로 제공되지 않을 수 있으며, 웹 브라우저(155) 상태에서 특정 어플리케이션이 선택되는 경우 자동 로그인 수행을 위한 화면 출력을 통해 대체될 수 있다. 표시부(140)를 통하여 제공되는 화면 인터페이스에 대해서 후술하는 도면을 참조하여 보다 상세히 설명하기로 한다.

[137] 저장부(150)는 본 발명의 실시 예에 따른 기능 동작에 필요한 응용 프로그램을 비롯하여, 표시부(140)에 출력될 화면 이미지를 포함하는 다양한 리소스를 저장한다. 특히, 본 발명의 저장부(150)는 다양한 어플리케이션들을 선택하여 운용할 수 있도록 제공되는 웹 브라우저(155), 특정 어플리케이션 서비스 장치와 통신하여 특정 사용자 기능을 제공하도록 설계된 다양한 어플리케이션들(151, 153)을 저장할 수 있다.

[138] 웹 브라우저(155)는 다수의 어플리케이션들(151, 153)의 웹 서비스 지원을 수행한다. 이러한 웹 브라우저(155)는 활성화 요청 시 등록된 다수의 어플리케이션들(151, 153)을 항목으로 하는 브라우저 화면을 제공할 수 있으며, 특정 어플리케이션 활성화 선택 시, 해당 어플리케이션 호출을 지원한다. 특히 본 발명의 웹 브라우저(155)는 단일 인증 서비스 지원을 위하여 단일 인증 서비스

장치(300)로부터 단일 인증 쿠키 정보를 수신하여 관리할 수 있다. 단일 인증 쿠키 정보를 보유한 웹 브라우저(155)는 입력부(120) 또는 입력 기능의 표시부(140)로부터 특정 어플리케이션 활성화를 위한 입력 신호가 발생하면, 해당 어플리케이션을 호출하면서 해당 어플리케이션의 통신 서비스 지원을 위하여 단일 인증 토큰을 제공할 수 있다.

- [139] 제1 어플리케이션(151) 및 제2 어플리케이션(153) 중 적어도 하나는 단말기(100)가 지원 가능한 특정 사용자 기능을 지원하기 위하여 설계된 어플리케이션으로서 본 발명에서는 각각의 어플리케이션 서비스 장치들(200)과 통신 채널을 형성하되 웹 브라우저(155)의 지원에 따라 단일 인증 쿠키 정보를 기반으로 어플리케이션 서비스 장치들(200)과의 자동 인증 정보 확인을 통하여 특정 데이터를 제공하는 어플리케이션들이 될 수 있다. 특히 제1 어플리케이션(151) 및 제2 어플리케이션(153)은 단일 인증 토큰을 기반으로 해당 서비스를 지원할 수 있도록 하나의 서비스 사업자 또는 공동 서비스 사업자가 관리할 수 있는 어플리케이션 서비스 장치들에 의해 지원되는 사용자 기능이 될 수 있다.
- [140] 예를 들어, 제1 어플리케이션(151)은 웹 브라우저(155) 상에 제공되는 항목으로서, 활성화를 위한 선택 시 제1 어플리케이션 서비스 장치(201)와의 통신을 기반으로 사용자 기능을 지원하고, 제2 어플리케이션(153) 역시 웹 브라우저(155) 상에 제공되는 항목으로서 활성화를 위한 선택 시 제2 어플리케이션 서비스 장치(202)와의 통신을 기반으로 사용자 기능을 지원할 수 있다. 상술한 제1 어플리케이션(151) 및 제2 어플리케이션(153)의 단일 인증 서비스를 지원하기 위해 제1 어플리케이션 서비스 장치(201) 및 제2 어플리케이션 서비스 장치(202)는 각각 단일 인증 서비스 장치(300)에 의하여 인증 정보 관리가 가능하도록 통합된 장치가 될 수 있다. 즉 제1 어플리케이션 서비스 장치(201) 및 제2 어플리케이션 서비스 장치(202)는 인증 정보를 특정 서비스 제공 사업자가 함께 관리하는 어플리케이션 서비스 장치들(200)이 될 수 있다.
- [141] 서비스 형태의 예로서 제1 어플리케이션(151)은 제1 어플리케이션 서비스 장치(201)가 운용하는 웹 페이지 접속을 위한 어플리케이션이 될 수 있으며, 제2 어플리케이션(153)은 제2 어플리케이션 서비스 장치(202)가 운용하는 웹 페이지 접속을 위한 어플리케이션이 될 수 있다. 여기서 제1 어플리케이션(151)에 따른 웹 페이지 및 제2 어플리케이션(153)에 따른 웹 페이지는 동일 사업자에 의해 인증 정보의 통합 운용이 가능한 웹 페이지들이 될 수 있으며 또는 사전 협약에 의해 협의된 사업자들에 의해 통합적으로 인증 정보 운용이 가능한 웹 페이지들이 될 수 있다.
- [142] 또 다른 서비스 형태의 예로서 제1 어플리케이션(151)은 제1 게임 어플리케이션이 될 수 있으며, 제2 어플리케이션(153)은 제2 게임 어플리케이션이 될 수 있다. 여기서 제1 게임 어플리케이션을 지원하는

어플리케이션 서비스 장치 및 제2 게임 어플리케이션을 지원하는 어플리케이션 서비스 장치는 보급자가 동일한 또는 계정 관리를 공동으로 수행할 수 있는 서비스 사업자일 수 있으며, 이에 따라 해당 서비스 사업자가 제공하는 단일 인증 서비스를 토대로 통합 접속이 가능한 형태로 설계될 수 있다. 한편 각 어플리케이션 서비스 장치는 사용자 요청에 따라 개별적인 인증 정보 입력 및 확인 통하여 접속을 지원할 수도 있다.

- [143] 이에 따라 본 발명의 제1 어플리케이션(151) 및 제2 어플리케이션(153)은 특정 웹 페이지나 특정 게임, 특정 서비스 페이지 등에 한정되는 것이 아니라 통합 인증 정보를 통하여 단일 인증이 가능하도록 설계되는 어플리케이션 서비스 장치들에 접속을 위한 어플리케이션으로 이해될 수 있을 것이다. 또한 상술한 설명에서는 저장부(150)에 두 개의 어플리케이션이 저장되는 것을 예로 하여 설명하였지만 본 발명이 이에 한정되는 것은 아니다. 즉 상기 저장부(150)는 보다 많은 어플리케이션들을 저장할 수 있으며, 이러한 어플리케이션들은 모두 웹 브라우저(155)를 통하여 단일 인증 쿠키 정보를 이용하여 자동 로그인이 가능한 어플리케이션 서비스 장치들과 관련된 어플리케이션들이 될 수 있다.
- [144] 제어부(160)는 본 발명의 실시 예에 따른 단일 인증 서비스 기능 지원을 위한 다양한 신호 흐름 제어와 데이터 처리 및 데이터 전송과 수신을 제어할 수 있다. 예를 들어, 제어부(160)는 저장부(150)에 저장된 웹 브라우저(155), 제1 어플리케이션(151) 및 제2 어플리케이션(153) 중 적어도 하나를 활성화할 수 있는 메뉴, 아이콘, 위젯 중 적어도 하나를 출력할 수 있다. 또는 제어부(160)는 웹 브라우저(155), 제1 어플리케이션(151) 및 제2 어플리케이션(153) 활성화를 위한 핫 키 등을 사전 설정된 스케줄 방식에 따라 할당할 수도 있다.
- [145] 그리고 제어부(160)는 웹 브라우저(155)를 활성화하기 위한 입력 신호가 발생하면, 웹 브라우저(155)를 통해 지원되는 다수개의 어플리케이션들(151, 153)을 웹 브라우저(155) 지원 화면에 출력되도록 지원할 수 있다. 웹 브라우저(155)에 포함된 다수개의 어플리케이션들(151, 153) 중 특정 어플리케이션이 활성화를 위해 선택되면 제어부(160)는 해당 어플리케이션 기능 지원을 위한 어플리케이션 서비스 장치 주소 정보를 수집하고, 통신부(110)를 활성화하여 어플리케이션 서비스 장치 접속을 제어할 수 있다.
- [146] 이때 제어부(160)는 해당 어플리케이션 서비스 장치 접속이 가능한 서비스 토큰이 있는지 여부를 확인하고, 서비스 토큰이 없는 경우 웹 브라우저(155)가 해당 어플리케이션에게 단일 인증 쿠키 정보 기반의 단일 인증 토큰을 제공하도록 제어할 수 있다. 여기서 웹 브라우저(155)가 단일 인증 쿠키 정보 운용이 불가능한 경우 제어부(160)는 해당 어플리케이션 기능 지원을 위해 어플리케이션 서비스 장치 접속을 위한 로그인 화면을 표시부(140)에 출력하도록 지원할 수 있다. 그리고 제어부(160)는 사용자 선택에 따라 단일 인증 쿠키 정보 운용을 위한 통합 ID 로그인을 위한 인증 정보 전송을 수행하도록 제어할 수 있다. 한편 제어부(160)는 웹 브라우저(155)가 단일 인증 쿠키 정보를

운용할 수 있는 경우, 단일 인증 토큰 제공을 통하여 활성화를 위해 선택된 어플리케이션의 자동 로그인을 수행할 수 있도록 지원할 수 있다.

- [147] 즉 본 발명의 단말기(100) 제어부(160)는 웹 브라우저(155)를 통해 제공되는 다수개의 어플리케이션들에 대하여 웹 브라우저(155)의 단일 인증 쿠키 정보 운용 여부에 따라 자동 로그인 기능을 수행하도록 지원할 수 있다. 그리고 제어부(160)는 단일 인증 쿠키 정보 운용이 불가능한 경우 웹 브라우저(155)가 단일 인증 쿠키 정보를 단일 인증 서비스 장치(300)로부터 수신할 수 있도록 메시지의 전송과 데이터 수신 등을 처리할 수 있다.
- [148] 한편 제어부(160)는 특정 어플리케이션 종료 또는 로그아웃 등 서비스 해제를 위한 입력 신호가 발생하면, 해당 어플리케이션의 서비스만을 해제할 것인지 또는 웹 브라우저(155)의 단일 인증 쿠키 정보까지 제거할 것인지를 제어할 수 있다. 또는 제어부(160)는 특정 어플리케이션 서비스 해제 시에는 해당 서비스 운용을 위해 수집된 서비스 토큰의 만료만을 수행하고, 웹 브라우저(155) 종료를 위한 입력 신호 발생 시 단일 인증 쿠키 정보를 제거하도록 제어할 수 있다.
- [149] 도 3은 본 발명의 실시 예에 따른 어플리케이션 서비스 장치(200) 구성을 보다 상세히 나타낸 도면이다. 설명에 앞서, 어플리케이션 서비스 장치(200)는 제1 어플리케이션 서비스 장치(201) 및 제2 어플리케이션 서비스 장치(202) 중 적어도 하나가 될 수 있으며, 이에 따라 이하에서는 어플리케이션 서비스 장치로 명명하며, 도면 번호 200을 할당하여 공통적으로 설명하기로 한다. 또한 이하 설명에서는 필요에 따라 어플리케이션 서비스 장치를 각각의 어플리케이션 서비스 장치로 구분하여 설명하기로 한다.
- [150] 도 3을 참조하면, 본 발명의 어플리케이션 서비스 장치(200)는 제1 통신부(210), 제1 제어부(220), 및 제1 저장부(230)의 구성을 포함할 수 있다. 추가로 어플리케이션 서비스 장치(200)는 어플리케이션 서비스 지원 및 관리를 위하여 입력부, 표시부 등 다양한 구성을 더 포함할 수도 있다.
- [151] 제1 통신부(210)는 단말기(100)의 특정 어플리케이션 활성화에 따른 사용자 기능 지원을 위하여 단말기(100)와 통신 채널을 형성할 수 있다. 제1 통신부(210)는 특정 어플리케이션 활성화 시 단말기(100)의 웹 브라우저(155)가 제공하는 단일 인증 쿠키 정보에 의한 단일 인증 토큰을 기반으로 작성된 접속 요청 메시지를 수신할 수 있다. 또는 제1 통신부(210)는 단말기(100)로부터 특정 어플리케이션의 서비스 지원을 위한 접속 요청을 수신할 수 있으며, 단말기(100)로부터 일반 인증 또는 단일 인증을 위한 ID 및 패스워드 정보를 수신할 수 있다.
- [152] 수신된 메시지들은 제1 제어부(220)에 전달되어 해당 단말기(100)의 어플리케이션 기능 지원을 위한 인증 과정에 이용될 수 있으며, 특히 통합 ID 로그인을 요청하는 요청 메시지 또는 단일 인증을 위한 세션 조회 메시지의 경우 단일 인증 서비스 장치(300)에 제공될 수 있다. 이를 위하여 제1 통신부(210)는 단일 인증 서비스 장치(300)와 통신 채널을 형성할 수 있다. 제1 통신부(210)는

단일 인증 서비스 장치(300)로부터 해당 메시지 처리에 따른 단일 인증 토큰 또는 통합 서비스 번호를 수신할 수 있다. 수신된 단일 인증 토큰은 단말기(100)에 제공될 수 있으며, 통합 서비스 번호는 해당 어플리케이션의 기능 지원을 위한 자동 로그인 서비스에 이용될 수 있다. 상술한 메시지들의 수신과 처리 등에 대해서 후술하는 도면을 참조하여 보다 상세히 설명하기로 한다.

- [153] 한편 제1 통신부(210)는 단말기(100)와 통신 채널을 형성하기 위한 통신 모듈 및 단일 인증 서비스 장치(300)와 통신 채널을 형성하기 위한 통신 모듈을 각각 포함할 수 있다. 또는 제1 통신부(210)는 단말기(100) 및 단일 인증 서비스 장치(300)와 통신 채널을 형성할 수 있는 하나의 통신 모듈을 포함할 수도 있다. 이를 위하여 단말기(100) 및 단일 인증 서비스 장치(300) 접속을 위한 통신 인터페이스가 호환이 가능하거나 또는 동일한 방식으로 구현될 수 있다.
- [154] 제1 저장부(230)는 어플리케이션 서비스 장치(200) 운용에 필요한 운영체제와 다양한 응용 프로그램을 저장한다. 특히 제1 저장부(230)는 단말기(100)의 특정 어플리케이션 기능 지원을 위하여 어플리케이션 지원 프로그램(231)을 포함할 수 있으며, 단말기(100)의 서비스 이용을 위해 할당되는 서비스 토큰(233)을 저장할 수 있다. 그리고 제1 저장부(230)는 단말기(100)의 사전 등록 과정을 통하여 단말기(100)의 식별 정보를 저장할 수 있다. 단말기(100)의 식별 정보는 해당 단말기(100)가 정상적인 서비스 이용이 가능하도록 등록된 단말기인지를 확인하는데 이용될 수 있으며, 이를 위하여 제1 저장부(230)는 사전 협의된 규칙에 따라 단말기(100)가 등록한 ID 정보와 패스워드 정보를 식별 정보에 포함하여 저장할 수 있다.
- [155] 어플리케이션 지원 프로그램(231)은 단말기(100)의 접속 요청에 따라 해당 단말기가 사전 등록된 단말기인지 확인하기 위한 인증 처리 루틴, 인증된 단말기(100)의 어플리케이션 활성화에 대응한 사용자 데이터를 제공하는 루틴, 단말기(100)의 단일 인증 요청 처리를 위한 단일 인증 처리 루틴, 단말기(100)의 어플리케이션 서비스 이용을 위하여 서비스 토큰을 할당하는 루틴 등을 저장할 수 있다.
- [156] 단일 인증 처리 루틴은 단말기(100)로부터 통합 ID 로그인 요청 수신 시 통합 ID 인증을 위한 루틴, 단일 인증 토큰 생성을 단일 인증 서비스 장치(300)에 요청하는 루틴, 단일 인증 토큰 및 1회용 접속키를 단말기(100)에 제공하는 루틴을 포함할 수 있다. 또한 단일 인증 처리 루틴은 단말기(100)로부터 단일 인증 토큰 기반의 단일 인증 세션 조회 메시지를 수신하는 경우 이를 단일 인증 서비스 장치(300)에 전달하고 그에 대응하는 통합 서비스 번호를 수신하는 루틴, 통합 서비스 번호를 기반으로 자동 로그인 수행을 지원하는 루틴을 포함할 수 있다.
- [157] 서비스 토큰(233)은 단말기(100)의 특정 어플리케이션이 해당 어플리케이션 서비스 장치(200)가 제공하는 서비스를 이용할 수 있도록 제공되는 정보이다. 이러한 서비스 토큰(233)은 단말기(100)가 접속을 요청하고 정상적인 인증

과정이 수행되면 해당 단말기(100)에 할당되고, 해당 어플리케이션 서비스 기능 종료 시 회수 또는 폐기될 수 있다. 한편 서비스 토큰(233)은 단말기(100)가 단일 인증 서비스를 요구하는 경우 단일 인증 서비스 장치(300)가 제공하는 단일 인증 토큰과 연계되어 또는 단일 인증 토큰을 기반으로 생성될 수 있다.

- [158] 제1 제어부(220)는 어플리케이션 서비스 장치(200) 운용을 위한 다양한 신호 처리와 데이터 처리 및 전달을 제어하는 구성이다. 단말기(100)로부터 접속을 요청받는 경우 제1 제어부(220)는 사전 정의된 스케줄 정보에 따라 인증 정보를 단말기(100)에 요청하도록 제어할 수 있다. 단말기(100)로부터 인증 정보를 수신하면, 제1 제어부(220)는 해당 인증 정보가 사전 등록된 정보와 일치하는지 확인하고, 그에 따른 어플리케이션 서비스 기능에 필요한 데이터를 제공할 수 있다.
- [159] 여기서 제1 제어부(220)는 단말기(100)로부터 통합 ID 로그인 정보를 수신하는 경우 해당 정보를 기반으로 통합 ID 로그인을 수행하면서, 단일 인증 세션 생성을 위한 요청 메시지를 단일 인증 서비스 장치(300)에 제공한다. 그리고 제1 제어부(220)는 단일 인증 서비스 장치(300)로부터 단일 인증 토큰 및 1회용 접속키를 수신하는 경우 이를 단말기(100)의 특정 어플리케이션에게 전달하도록 지원할 수 있다.
- [160] 한편 제1 제어부(220)는 단말기(100)로부터 단일 인증 토큰 기반의 세션 조회 메시지를 수신하는 경우, 해당 조회 메시지를 단일 인증 서비스 장치(300)에 제공하도록 제어할 수 있다. 그리고 제1 제어부(220)는 단일 인증 서비스 장치(300)로부터 통합 서비스 번호를 수신하고, 이를 기반으로 해당 단말기(100)의 어플리케이션 기능 지원을 위한 자동 로그인 서비스를 지원할 수 있다. 즉 제1 제어부(220)는 통합 서비스 번호를 기반으로 통합 ID 로그인을 수행하고, 서비스 토큰을 할당한 후 이를 단말기(100)의 특정 어플리케이션에게 제공하도록 지원할 수 있다. 즉 제1 제어부(220)는 단일 인증 토큰을 기반으로 접속을 요청하는 단말기(100)의 어플리케이션에 대해서 단일 인증 서비스 장치(300)의 확인에 따라 별도의 인증 정보 확인 과정 없이 로그인을 수락하고 해당 어플리케이션에 따른 서비스 기능을 지원할 수 있다.
- [161] 도 12는 본 발명의 제3 실시 예에 따른 단일 인증 서비스 장치의 구성을 보다 상세히 나타낸 도면이다.
- [162] 도 12를 참조하면, 본 발명의 단일 인증 서비스 장치(300)는 제2 통신부(310), 제2 제어부(320)와, 제2 저장부(330)의 구성을 포함할 수 있다. 추가로 단일 인증 서비스 장치(300)는 어플리케이션 서비스 장치(200)와 유사하게 장치 관리를 위하여 또는 특정 데이터 갱신 등을 위하여 입력부, 표시부 등의 구성을 더 포함할 수 있다.
- [163] 제2 통신부(310)는 어플리케이션 서비스 장치(200)와 통신 채널을 형성하는 구성이다. 이를 위하여 제2 통신부(310)는 어플리케이션 서비스 장치(200)와 데이터 송수신이 가능한 형태의 통신 모듈 또는 어플리케이션 서비스

장치(200)가 접속된 네트워크 장치에 데이터를 전송하고 해당 네트워크 장치로부터 데이터를 수신할 수 있는 통신 모듈로 구성될 수 있다. 이러한 제2 통신부(310)는 어플리케이션 서비스 장치(200)로부터 단일 인증 요청 메시지를 수신하거나, 단일 인증 세션 조회 메시지를 수신할 수 있다. 그리고 제2 통신부(310)는 제2 제어부(320)가 생성한 단일 인증 토큰, 1회용 접속키, 단일 인증 쿠키 정보 및 통합 서비스 번호 중 적어도 하나를 어플리케이션 서비스 장치(200)에 제공한다.

[164] 제2 저장부(330)는 단일 인증 서비스 장치(300) 운용을 위한 프로그램들을 저장한다. 특히 제2 저장부(330)는 본 발명의 단일 인증 서비스 지원을 위한 프로그램인 단일 인증 지원 프로그램(331), 단일 인증 토큰(333), 1회용 접속키(335) 및 단일 인증 쿠키 정보(337)를 저장할 수 있다.

[165] 단일 인증 지원 프로그램(331)은 어플리케이션 서비스 장치(200)로부터 수신되는 메시지에 따라 통합 서비스 번호를 생성하거나, 단일 인증 토큰(333) 및 1회용 접속키(335)를 생성하도록 지원할 수 있다. 이를 위하여 단일 인증 지원 프로그램(331)은 어플리케이션 서비스 장치(200)로부터 수신되는 메시지의 종류를 구분하는 루틴, 수신된 메시지가 단일 인증 세션 조회 메시지인 경우 해당 조회 메시지에 대응하여 통합 서비스 번호를 생성하는 루틴, 생성된 통합 서비스 번호를 어플리케이션 서비스 장치(200)에 제공하는 루틴을 포함할 수 있다. 또한 단일 인증 지원 프로그램(331)은 수신된 메시지가 단일 인증 요청 메시지인 경우 단일 인증 토큰(333) 및 1회용 접속키(335)를 생성하는 루틴, 생성된 단일 인증 토큰(333) 및 1회용 접속키(335)를 어플리케이션 서비스 장치(200)에 제공하는 루틴을 포함할 수 있다. 또한 단일 인증 지원 프로그램(331)은 1회용 접속키(335) 기반의 접속이 발생하는 경우 해당 1회용 접속키(335)의 확인에 따른 단일 인증 쿠키 정보(337) 생성 및 전송 루틴을 포함할 수 있다.

[166] 단일 인증 토큰(333) 및 1회용 접속키(335)는 특정 단말기(100)의 단일 인증 토큰 생성을 위한 정보이다. 이러한 단일 인증 토큰(333) 및 1회용 접속키(335)는 특정 단말기(100)가 단일 인증 서비스를 이용하기 위하여 요청하는 경우 생성되어 어플리케이션 서비스 장치(200)를 통하여 단말기(100)의 특정 어플리케이션에 전송되는 한편 제2 저장부(330)에 저장될 수 있다. 제2 저장부(330)에 저장된 단일 인증 토큰(333) 및 1회용 접속키(335)는 단일 인증 쿠키 정보 생성 과정에서 해당 어플리케이션의 접속 유효성 확인을 위하여 이용될 수 있다. 1회용 접속키(335)는 단말기(100)의 웹 브라우저(155) 접속 이후 삭제될 수 있다.

[167] 단일 인증 쿠키 정보(337)는 단일 인증 쿠키 및 단일 인증 토큰을 포함한다. 이러한 단일 인증 쿠키 정보(337)는 1회용 접속키(335)를 기반으로 접속한 웹 브라우저(155)에 제공되는 정보이다. 단일 인증 쿠키 정보(337)에 포함된 단일 인증 토큰은 추후 단말기(100)의 특정 어플리케이션의 세션 조회 메시지 조회에

이용될 수 있다. 단일 인증 쿠키 정보(337)는 단말기(100)의 단일 인증 서비스 종료 예를 들면 웹 브라우저(155) 종료 시 폐기될 수 있다.

- [168] 제2 제어부(320)는 단일 인증 서비스 장치(300) 운용에 필요한 다양한 신호의 처리와 전달을 제어할 수 있다. 특히 제2 제어부(320)는 본 발명의 단일 인증 서비스 지원을 위한 단일 인증 토큰(333), 1회용 접속키(335) 및 단일 인증 쿠키 정보(337)의 생성과 제공 및 관리, 단일 인증 토큰 기반의 통합 서비스 번호의 생성과 제공 및 관리를 지원할 수 있다. 이를 보다 상세히 설명하면, 제2 제어부(320)는 어플리케이션 서비스 장치(200)로부터 단일 인증 요청 메시지를 수신하면, 해당 요청에 따라 단일 인증 토큰(333) 및 1회용 접속키(335)를 생성할 수 있다. 그리고 제2 제어부(320)는 단일 인증 토큰(333) 및 1회용 접속키(335)가 생성되면, 이를 어플리케이션 서비스 장치(200)를 통해 단말기(100)의 특정 어플리케이션에 제공할 수 있다.
- [169] 그리고 제2 제어부(320)는 1회용 접속키(335)를 이용한 웹 브라우저(155)의 접속이 발생하면 1회용 접속키(335)에 해당하는 단일 인증 토큰 조회를 통해 웹 브라우저(155) 접속의 유효성을 확인할 수 있다. 이후 제2 제어부(320)는 단일 인증 쿠키 정보 생성 및 전송을 제어하는 한편 1회용 접속키(335)의 삭제를 제어할 수 있다.
- [170] 여기서 단일 인증 요청 메시지를 전송한 단말기(100)의 유효성 인증은 어플리케이션 서비스 장치(200)의 통합 ID 정보 인증을 통하여 수행될 수 있기 때문에 제2 제어부(320)가 별도로 유효성 검증을 수행하지 않을 수 있다. 그러나 시스템 설계자의 설계 방식에 따라 제2 제어부(320)는 단일 인증 요청 메시지에 포함된 단말기(100) 관련 정보를 토대로 해당 단말기(100)가 단일 인증 서비스를 이용하도록 사전 등록된 단말기인지 여부를 확인할 수 있다. 이를 위하여 단일 인증 서비스 장치(300)는 단일 인증 서비스를 이용하기 위하여 사전 등록된 단말기(100)들의 정보를 보관 및 관리할 수 있다.
- [171] 한편, 제2 제어부(320)는 어플리케이션 서비스 장치(200)로부터 단일 인증 토큰 기반의 단일 인증 세션 조회 메시지를 수신하는 경우, 해당 조회 메시지에 포함된 단일 인증 토큰을 확인한다. 그리고 조회 메시지에 포함된 단일 인증 토큰이 사전 저장된 단일 인증 쿠키 정보(337)를 기반으로 유효한지 여부를 확인할 수 있다. 여기서 유효성 여부는 단일 인증 쿠키 정보(337)와의 일치 및 생성 시점 경과 등을 고려할 수 있다. 즉 조회 메시지에 포함된 단일 인증 토큰이 사전 저장된 단일 인증 쿠키 정보(337)에 부합된다 하더라도 제2 제어부(320)는 사전 설계된 임계 시간을 경과한 단일 인증 토큰의 경우 유효성을 상실한 것으로 결정하고, 해당 단일 인증 토큰 기반의 단일 인증 서비스 지원을 차단할 수 있다. 이러한 단일 인증 토큰에 대한 유효성 설계는 시스템 설계자의 설계 방식에 따라 적용되지 않을 수도 있다. 제2 제어부(320)는 수신된 조회 메시지가 유효한 경우 어플리케이션 서비스 장치 이용을 지원하기 위한 통합 서비스 번호를 생성하고 이를 어플리케이션 서비스 장치(200)에 제공할 수 있다. 이 통합 서비스 번호는

어플리케이션 서비스 장치(200)에 접속하고자 하는 단말기(100)의 자동 로그인 수락을 지원하는 정보로 이용될 수 있다.

[172] 한편 제2 제어부(320)는 어플리케이션 서비스 장치(200)로부터 단일 인증 쿠키 정보(337) 제거를 위한 메시지를 수신할 수 있다. 이 경우 제2 제어부(320)는 해당 단일 인증 쿠키 정보(337) 제거를 수행하고, 단일 인증 쿠키 정보(337)가 제거되었음을 어플리케이션 서비스 장치(200)에 전달할 수 있다.

[173] 이상에서 설명한 바와 같이 본 발명의 단일 인증 서비스 시스템(10) 및 이를 지원하는 각 구성들은 단일 인증 쿠키 정보를 단말기의 웹 브라우저(155)가 다양한 어플리케이션들의 단일 인증 서비스 지원을 수행할 수 있도록 지원한다. 이에 따라 사용자는 웹 브라우저(155)를 기반으로 다양한 어플리케이션들을 활성화하고 해당 서비스를 이용하는 과정에서 불필요하게 반복적인 인증 정보의 입력과 인증 획득 과정 없이 필요한 서비스를 즉각적으로 이용할 수 있다.

[174] 도 13는 본 발명의 제3 실시 예에 따른 웹 브라우저 기반의 단일 인증 서비스 운용 방법 중 단일 인증 쿠키 생성 과정을 설명하기 위한 도면이다.

[175] 도 13을 참조하면, 단일 인증 서비스 시스템 운용 방법은 먼저, 단말기(100) 사용자가 저장부(150)에 저장된 웹 브라우저(155)를 활성화하면, 웹 브라우저(155)는 등록된 다수개의 어플리케이션들을 활성화할 수 있는 화면을 표시부(140)에 출력할 수 있다. 사용자는 웹 브라우저(155)에 등록된 어플리케이션들 중 특정 어플리케이션 예를 들면 제1 어플리케이션(151)을 활성화하기 위한 입력 신호를 생성하면, 단말기(100)는 제1 어플리케이션(151) 지원을 위한 서비스 토큰이 존재하는지 여부를 확인할 수 있다. 여기서 서비스 토큰은 제1 어플리케이션(151)의 사용자 기능 지원을 위하여 제1 어플리케이션 서비스 장치(201)를 이용할 수 있는 정보가 될 수 있다. 만약 단말기(100)는 제1 어플리케이션 서비스 장치(201)에 대한 사용 이력을 가지고 있으며, 재접속 시간이 사전 정의된 유효 기간 이내 또는 제1 어플리케이션 서비스 장치(201)에 대한 로그인을 유지한 경우 단말기(100)는 서비스 토큰을 유지할 수 있다. 결과적으로 단말기(100)는 서비스 토큰이 존재하는 경우 별도의 인증 과정 수행 없이 이전 이력을 기반으로 제1 어플리케이션 서비스 장치(201) 접속을 수행할 수 있다.

[176] 한편 서비스 토큰이 없지만 단일 인증 쿠키 정보(337) 운용이 가능한 경우 웹 브라우저(155)는 단일 인증 토큰을 제1 어플리케이션(151)에 제공할 수 있다. 이에 대한 설명은 도 13을 참조하여 보다 상세히 설명하기로 한다. 웹 브라우저(155)가 단일 인증 쿠키 정보(337) 운용이 불가능한 경우 제1 어플리케이션(151)은 단일 인증을 위한 통합 ID 로그인 요청을 위한 요청 메시지를 작성하고 이 요청 메시지를 S701 단계에서 제1 어플리케이션 서비스 장치(201)에 전송할 수 있다. 제1 어플리케이션 서비스 장치(201)는 제1 어플리케이션(151) 사용자 기능 지원을 위한 데이터를 제공하는 장치가 될 수

있다. 제1 어플리케이션 서비스 장치(201)는 단말기(100)로부터 단일 인증을 위한 요청 메시지를 수신하면, 해당 메시지에 포함된 로그인 정보를 이용하여 통합 ID 인증을 S703 단계에서 수행할 수 있다. 그리고 제1 어플리케이션 서비스 장치(201)는 단일 인증 토큰 획득을 위한 단일 인증 세션 생성 요청 메시지(createSSOSessionForMoblie)를 작성하고, 이를 S705 단계에서 단일 인증 서비스 장치(300)에 전송할 수 있다. 여기서 단일 인증 세션 생성 요청 메시지(createSSOSessionForMoblie)는 통합 로그인 정보를 포함할 수 있다.

[177] 단일 인증 서비스 장치(300)는 제1 어플리케이션 서비스 장치(201)로부터 단일 인증 세션 생성 요청 메시지(createSSOSessionForMoblie)를 수신하면, 해당 요청 메시지 수신에 따라 S707 단계에서 단일 인증(SSO: Single-Sign On) 세션을 생성할 수 있다. 그리고 단일 인증 서비스 장치(300)는 단일 인증 세션 운용을 위한 단일 인증 토큰 및 1회용 접속키를 생성하고 S709 단계에서 단일 인증 토큰 및 1회용 접속키를 제1 어플리케이션 서비스 장치(201)에 제공할 수 있다. 여기서 단일 인증 서비스 장치(300)는 생성된 단일 인증 토큰 및 1회용 접속키를 추후 웹 브라우저(155)의 접속 유효성 검사 등을 위하여 보관 관리할 수 있다.

[178] 제1 어플리케이션 서비스 장치(201)는 단일 인증 서비스 장치(300)로부터 단일 인증 토큰 및 1회용 접속키를 수신하면, 단일 인증 토큰과 연계된 또는 단일 인증 토큰을 기반으로 하는 제1 어플리케이션 서비스 장치(201) 이용을 위한 서비스 토큰을 생성하고, S711 단계에서 해당 단일 인증 토큰, 1회용 접속키, 서비스 토큰 및 서비스 지원에 따른 사용자 데이터를 단말기(100)의 제1 어플리케이션(151)에 제공할 수 있다. 그러면 단말기(100)의 제1 어플리케이션(151)은 S713 단계에서 수신된 단일 인증 토큰 정보를 저장할 수 있다. 그리고 제1 어플리케이션(151)은 웹 브라우저(155)가 비활성화된 경우 S715 단계에서 웹 브라우저(155)를 호출하고 웹 브라우저(155)에 1회용 접속키(335)를 제공할 수 있다. 여기서 웹 브라우저(155)가 활성화된 경우 웹 브라우저(155)에 1회용 접속키(335)를 제공할 수 있다. 이러한 경우는 사용자가 웹 브라우저(155) 호출 없이 제1 어플리케이션(151)을 활성화하여 제1 어플리케이션 서비스 장치(201)에 접속한 경우를 가정할 것이다.

[179] 한편 웹 브라우저(155)는 제1 어플리케이션(151)으로부터 1회용 접속키를 수신하면, 이를 기반으로 S717 단계에서 단일 인증 서비스 장치(300) 접속을 수행할 수 있다. 이때 웹 브라우저(155)는 제1 어플리케이션 서비스 장치(201)를 거치지 않고 직접적으로 단일 인증 서비스 장치(300) 접속을 수행할 수 있다. 제1 어플리케이션 서비스 장치(201)를 거치는 경우, 제1 어플리케이션 서비스 장치(201)는 웹 브라우저(155)와 단일 인증 서비스 장치(300) 사이에서 데이터 중계를 지원할 수 있다.

[180] 단일 인증 서비스 장치(300)는 단말기(100)의 웹 브라우저(155)로부터 1회용 접속키 기반의 접속을 수신하면, S719 단계에서 1회용 접속키를 기반으로 단일 인증 토큰을 조회하고, 이를 기반으로 쿠키 정보를 생성하도록 제어할 수 있다.

그리고 단일 인증 서비스 장치(300)는 S721 단계에서 1회용 접속키 삭제를 수행할 수 있다. 한편 단일 인증 서비스 장치(300)는 S723 단계에서 생성된 단일 인증 쿠키 정보를 단말기(100)의 웹 브라우저(155)에 제공할 수 있다. 여기서 쿠키 정보는 단일 인증 쿠키(SSO Cookie) 및 단일 인증 토큰(Mobile SSO Token)을 포함할 수 있다.

- [181] 웹 브라우저(155)는 단일 인증 토큰 정보를 수신하면, 이를 기반으로 S125 단계에서 단일 인증 쿠키를 생성하는 한편, S727 단계에서 선택되는 특정 어플리케이션 예를 들면 제1 어플리케이션(151)을 호출하고, 제1 어플리케이션(151)에 단일 인증 토큰(Mobile SSO Token)을 전달할 수 있다.
- [182] 도 14는 본 발명의 제3 실시 예에 따른 웹 브라우저 기반의 단일 인증 서비스 운용 방법 중 단일 인증 토큰 운용을 설명하기 위한 도면이다.
- [183] 도 14를 참조하면, 본 발명의 단일 인증 서비스 시스템(10)의 운용 방법은 웹 브라우저(155)가 활성화된 상태에서 특정 어플리케이션(App) 예를 들면 제2 어플리케이션(153) 활성화를 위한 입력 신호가 수신되면, 웹 브라우저(155)는 S801 단계에서 해당 제2 어플리케이션(153) 호출을 수행하는 한편, 제2 어플리케이션(153)에게 단일 인증 토큰(Mobile SSO Token)을 제공할 수 있다. 그러면 제2 어플리케이션(153)은 단일 인증 토큰을 기반으로 단일 인증 세션 조회 메시지를 작성하고, 세션 조회 메시지를 S803 단계에서 제2 어플리케이션 서비스 장치(202)에 전달할 수 있다.
- [184] 제2 어플리케이션 서비스 장치(202)는 세션 조회 메시지 수신에 대응하여 단일 인증 세션 검사 메시지(checkSSOSessionForMobile)를 작성하고, S805 단계에서 해당 단일 인증 세션 검사 메시지(checkSSOSessionForMobile)를 단일 인증 서비스 장치(300)에 전달할 수 있다. 단일 인증 서비스 장치(300)는 제2 어플리케이션 서비스 장치(202)로부터 단일 인증 세션 확인 메시지(checkSSOSessionForMobile)를 수신하면, 단일 인증 세션 확인 메시지(checkSSOSessionForMobile)에 포함된 정보들 특히 단일 인증 토큰을 기반으로 S807 단계에서 통합 서비스 번호를 할당할 수 있다.
- [185] 통합 서비스 번호는 S809 단계에서 제2 어플리케이션 서비스 장치(202)에 전달될 수 있다. 그러면 제2 어플리케이션 서비스 장치(202)는 수신된 통합 서비스 번호를 기반으로 S811 단계에서 통합 ID 로그인을 수행하고, 제2 어플리케이션 서비스 장치(202) 이용을 위한 서비스 토큰을 생성한다. 생성된 서비스 토큰 및 제2 어플리케이션 서비스 장치(202) 운용을 위한 사용자 데이터는 S813 단계에서 단말기(100)의 제2 어플리케이션(153)에 제공될 수 있다.
- [186] 상술한 바와 같이 본 발명의 웹 브라우저 기반의 단일 인증 서비스 운용 방법은 웹 브라우저가 단일 인증 쿠키를 기반으로 활성화를 지시 받은 어플리케이션에게 단일 인증 토큰을 할당함으로써, 특정 어플리케이션 서비스 장치 접속 과정에서 자동 로그인 서비스가 제공되도록 지원할 수 있다.

- [187] 도 15는 본 발명의 제3 실시 예에 따른 웹 브라우저 기반의 단일 인증 서비스 지원 과정에서의 단말기 화면 인터페이스의 일 예를 나타낸 도면이다.
- [188] 도 15를 참조하면, 단말기(100)는 전원이 공급되면 기 설정된 스케줄 정보 또는 사용자 입력에 따라 701 화면에서와 같이 웹 브라우저 항목(701a)을 선택할 수 있는 화면을 표시부(140)에 출력할 수 있다. 도시된 도면에서는 웹 브라우저 항목(701a)만이 표시되는 것으로 나타내었지만 사용자 설정 등에 따라 단말기(100)가 지원하는 다양한 기능들을 운용하기 위한 어플리케이션 항목들이 더 표시될 수 있다. 예를 들어 단말기(100)는 제1 어플리케이션(703a) 또는 제2 어플리케이션(703b)을 바로 실행할 수 있도록 지원하는 어플리케이션 항목들을 표시부(140)에 출력할 수 있다.
- [189] 한편 사용자가 웹 브라우저 항목(701a)을 선택하는 경우 단말기(100)는 703 화면에서와 같이 다수개의 어플리케이션 항목들(703a, 703b)을 선택할 수 있는 화면을 출력할 수 있다. 도시된 도면에서는 3개의 어플리케이션 항목들(703a, 703b)이 표시된 상태를 나타내었으나 사용자 설정에 따라 또는 단말기 지원에 따라 어플리케이션 항목들(703a, 703b)의 개수는 더 늘어나거나 줄어들 수 있을 것이다.
- [190] 한편 사용자가 제1 어플리케이션 항목(703a)을 선택하는 경우, 단말기(100)는 제1 어플리케이션 항목(703a) 지원을 위한 제1 어플리케이션 서비스 장치(201) 접속을 수행하도록 제어한다. 이때 웹 브라우저(155)가 앞서 설명한 단일 인증 서비스 수행을 위한 단일 인증 토큰을 제공할 수 없는 경우, 단말기(100)는 제1 어플리케이션 서비스 장치(201)의 접속을 위한 제1 어플리케이션 로그인 화면(705a)을 표시부(140)에 출력할 수 있다. 그러면 사용자는 제1 어플리케이션 로그인 화면(705a)을 통하여 ID 및 패스워드 입력을 수행할 수 있다. 특히 사용자는 제1 어플리케이션 로그인 화면(705a)을 통하여 웹 브라우저(155)가 단일 인증 쿠키를 생성 및 운용할 수 있도록 하기 위하여 통합 로그인 항목(705b)을 선택하고, 사전 등록된 통합 ID 및 패스워드 입력을 수행할 수 있다. 단말기(100)는 통합 로그인 항목(705b) 선택 시, 입력되는 ID 및 패스워드 정보를 기반으로 통합 ID 로그인을 위한 요청 메시지 작성을 수행하고, 이를 제1 어플리케이션 서비스 장치(201)에 전송할 수 있다. 이후 단말기(100)는 앞서 설명한 절차에 따라 웹 브라우저(155)가 단일 인증 쿠키 정보를 획득할 수 있도록 지원할 수 있다. 한편 통합 로그인 항목(705b)이 선택되지 않는 경우 제1 어플리케이션(151)은 일반 인증 정보 송수신을 통하여 제1 어플리케이션 서비스 장치(201)와의 인증만을 수행하도록 지원할 수 있다.
- [191] 단말기(100)의 웹 브라우저(155)가 단일 인증 쿠키 정보(337)를 운용할 수 있는 상태의 703 화면을 가정할 경우, 웹 브라우저(155)는 제2 어플리케이션 항목(703b)이 선택되면, 제2 어플리케이션(153) 호출을 수행하고 아울러 제2 어플리케이션(153)에게 단일 인증 토큰을 제공할 수 있다. 그러면 제2 어플리케이션(153)은 제2 어플리케이션 서비스 장치(202) 접속을 수행하는

과정에서 단일 인증 토큰 기반의 세션 조회 메시지 제2 어플리케이션 서비스 장치(202)를 통해 단일 인증 서비스 장치(300)에 전송한다. 제2 어플리케이션 서비스 장치(202)는 단일 인증 서비스 장치(300)로부터 통합 서비스 번호를 수신하여 제2 어플리케이션(153)의 통합 ID 로그인을 수행하도록 제어할 수 있다. 이때 제2 어플리케이션 서비스 장치(202)는 단말기(100)의 제2 어플리케이션(153)에게 통합 ID 로그인 실행을 수행할 것인지 문의할 수 있으며, 단말기(100)는 707 화면에서와 같이 단일 인증 로그인 항목(707b)을 포함하는 제2 어플리케이션 로그인 화면(707a)을 출력할 수 있다. 사용자는 단일 인증 로그인 항목(707b)을 선택하는 동작으로 제2 어플리케이션(153)의 지원을 위한 제2 어플리케이션 서비스 장치(202)로의 자동 로그인을 수행할 수 있다.

- [192] 한편 단말기(100)는 특정 어플리케이션의 로그아웃을 위한 입력 신호 또는 종료를 위한 입력 신호 발생 시 해당 어플리케이션의 로그아웃 또는 종료를 위한 서비스 토큰 만료 요청 메시지를 어플리케이션 서비스 장치에 전송할 수 있다. 그리고 단말기(100)는 어플리케이션 서비스 장치로부터 서비스 토큰 만료 응답 메시지를 수신하면 서비스 로그아웃을 수행하도록 제어할 수 있다. 또한 단말기(100)는 웹 브라우저(155) 종료 또는 웹 브라우저(155) 기반의 단일 인증 서비스 로그아웃을 위한 입력 신호가 발생하면, 해당 입력 신호에 해당하는 서비스 토큰 만료 및 단일 인증 쿠키 만료 요청 메시지를 해당 어플리케이션 서비스 장치 및 단일 인증 서비스 장치(300)에 전송할 수 있다. 그리고 단말기(100)는 어플리케이션 서비스 장치 및 단일 인증 서비스 장치(300)로부터 서비스 토큰 만료 및 단일 인증 쿠키 만료 응답 메시지를 수신하면 서비스 로그아웃을 수행할 수 있다. 단일 인증 서비스 장치(300)는 단일 인증 쿠키 만료 요청 메시지 수신에 대응하여 응답 메시지를 제공하면서 저장된 단일 인증 쿠키 정보를 삭제할 수 있다.

- [193] 이상에서 설명한 바와 같이 본 발명의 단일 인증 서비스 시스템 및 방법과 이를 지원하는 화면 인터페이스에서는 단일 인증 토큰 및 어플리케이션 서비스 장치 운용을 위한 서비스 토큰을 운용함으로써 다양한 어플리케이션들에 대한 반복적인 인증 정보 입력을 제거하며, 인증 정보의 관리를 보다 용이하게 할 수 있도록 지원한다. 또한 본 발명은 다양한 어플리케이션 수행을 위한 어플리케이션 서비스 장치 접속을 단일 인증 토큰으로 수행하도록 함으로써 인증 정보 재입력이나 아이디 및 패스워드 질의 상황을 최소화하도록 지원할 수 있다.

- [194] 한편 상술한 단말기(100)는 그 제공 형태에 따라 다양한 추가 모듈을 더 포함할 수 있다. 즉 상기 단말기(100)는 통신 단말기인 경우 근거리 통신을 위한 근거리통신모듈, 상기 단말기(100)의 유선통신방식 또는 무선통신방식에 의한 데이터 송수신을 위한 인터페이스, 인터넷 네트워크와 통신하여 인터넷 기능을 수행하는 인터넷통신모듈 및 디지털 방송 수신과 재생 기능을 수행하는 디지털방송모듈 등과 같이 상기에서 언급되지 않은 구성들을 더 포함할 수도

있다. 이러한 구성 요소들은 디지털 기기의 컨버전스(convergence) 추세에 따라 변형이 매우 다양하여 모두 열거할 수는 없으나, 상기 언급된 구성 요소들과 동등한 수준의 구성 요소가 상기 디바이스에 추가로 더 포함되어 구성될 수 있다. 또한 본 발명의 단말기(100)는 그 제공 형태에 따라 상기한 구성에서 특정 구성들이 제외되거나 다른 구성으로 대체될 수도 있음은 물론이다. 이는 본 기술분야의 통상의 지식을 가진 자에겐 쉽게 이해될 수 있을 것이다.

[195] 또한 본 발명의 실시 예에 따른 상기 단말기(100)는 어플리케이션 서비스 장치 기반의 어플리케이션 기능을 이용할 수 있는 모든 형태의 디바이스를 포함할 수 있다. 예를 들면, 상기 단말기(100)는 다양한 통신 시스템들에 대응되는 통신 프로토콜들(communication protocols)에 의거하여 동작하는 모든 이동통신 단말기들(mobile communication terminals)을 비롯하여, PMP(Portable Multimedia Player), 디지털방송 플레이어, PDA(Personal Digital Assistant), 음악 재생기(예컨대, MP3 플레이어), 휴대게임단말, 스마트 폰(Smart Phone), 노트북(Notebook) 및 핸드헬드 PC 등 모든 정보통신기기와 멀티미디어기기 및 그에 대한 응용기기를 포함할 수 있다.

[196] 아울러 상술한 본 발명의 단일 인증 서비스 운용 방법은, 어플리케이션 서비스 장치 또는 단말기를 포함하는 다양한 컴퓨터 수단을 통하여 판독 가능한 소프트웨어 형태로 구현되어 기록매체에 기록될 수 있다. 이때, 상기 기록매체에 기록되는 프로그램은, 상술한 본 발명의 단일 인증 서비스 운용 방법 중에서, 하나 이상의 과정을 또는 기능을 실행하도록 구현될 수 있다. 여기서, 기록매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 기록매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 예컨대 기록매체는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM(Compact Disk Read Only Memory), DVD(Digital Video Disk)와 같은 광 기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media), 및 롬(ROM), 램(RAM, Random Access Memory), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함한다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다. 이러한 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[197] 한편, 본 명세서와 도면을 통해 본 발명의 바람직한 실시 예들에 대하여 설명하였으며, 비록 특정 용어들이 사용되었으나, 이는 단지 본 발명의 기술 내용을 쉽게 설명하고 발명의 이해를 돕기 위한 일반적인 의미에서 사용된 것일 뿐, 본 발명의 범위를 한정하고자 하는 것은 아니다. 여기에 개시된 실시

예외에도 본 발명의 기술적 사상에 바탕을 둔 다른 변형 예들이 실시 가능하다는 것은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 자명한 것이다.

산업상 이용가능성

- [198] 본 발명에 따른 단일 인증 서비스 시스템 및 방법은, 특정 어플리케이션 운용을 위한 한번의 입력만으로 다양한 어플리케이션들의 운용을 위한 인증 과정을 신속하고 편리하게 할 수 있으며, 인증 상태 관리를 보다 용이하게 운용할 수 있도록 지원한다. 또한 본 발명은 특정 서비스 제공업자가 다양하게 제공하는 어플리케이션들을 단일 인증 정보를 토대로 공통적으로 이용할 수 있도록 지원하여 인증 정보의 관리 투명성과 신뢰도를 높이면서도 인증 정보 관리를 위한 비용을 절감하고 인증 정보 관리의 효율성을 개선할 수 있다.
- [199] 따라서, 본 발명은 단말 장치에서 설치되는 다양한 어플리케이션들의 운용을 위한 인증 분야에 적용되어, 인증 처리를 위한 비용을 절감시키면서 효율성을 개선할 수 있으므로, 산업상 이용 가능성이 있다.

청구범위

[청구항 1]

복수개의 어플리케이션 중 적어도 하나의 활성화 요청에 따라 복수의 어플리케이션 서비스 장치 중 적어도 하나의 어플리케이션 서비스 장치 접속을 수행하되 단일 인증 토큰을 기반으로 별도의 인증 정보 입력 없이 각각의 어플리케이션 서비스 장치로부터 서비스 운용을 위해 사용되는 서비스 토큰을 수신하는 단말기; 상기 서비스 토큰을 제시하는 단말기의 어플리케이션 서비스 운용을 위한 데이터를 제공하며 상기 단말기로부터 단일 인증 관련 메시지 수신 시 해당 메시지를 단일 인증 서비스 장치에 제공하고, 상기 단일 인증 서비스 장치로부터 통합 서비스 번호를 수신한 경우 별도의 인증 정보 확인 없이 상기 단일 인증 토큰을 기반으로 상기 서비스 토큰을 생성하고, 생성된 서비스 토큰 및 상기 단말기의 어플리케이션 서비스 운용을 위한 데이터를 상기 단말기로 제공하는 어플리케이션 서비스 장치; 상기 어플리케이션 서비스 장치로부터 단일 인증 관련 메시지를 수신하면 상기 단말기의 단일 인증 서비스 운용을 위한 통합 서비스 번호를 상기 어플리케이션 서비스 장치로 제공하고, 단일 인증 서비스 장치;

를 포함하는 것을 특징으로 하는 단일 인증 서비스 시스템.

[청구항 2]

단말기의 특정 어플리케이션으로부터 통합 ID 로그인 정보 또는 단일 인증 토큰 기반의 세션 조회 메시지를 수신하는 제1 통신부; 상기 단말기의 특정 어플리케이션 기능 지원을 위한 데이터를 저장하며, 상기 단말기의 특정 어플리케이션 기능 운용을 위한 서비스 토큰을 저장하는 제1 저장부;

상기 특정 어플리케이션으로부터 통합 ID 로그인 정보 수신 시 단일 인증 토큰 생성을 위한 메시지를 단일 인증 서비스 장치에 전달하며, 상기 세션 조회 메시지 수신 시 이를 상기 단일 인증 서비스 장치로 전송하고 상기 단일 인증 서비스 장치로부터 상기 세션 조회 메시지와 관련된 통합 서비스 번호를 수신하여 해당 어플리케이션의 별도 인증 정보 확인 없이 상기 서비스 토큰을 상기 단말기의 특정 어플리케이션에게 제공하는 제1 제어부; 를 포함하는 것을 특징으로 하는 단일 인증 서비스를 지원하는 어플리케이션 서비스 장치.

[청구항 3]

제2항에 있어서, 상기 제1 제어부는,

상기 통합 ID 로그인 정보에 해당하는 메시지 또는 상기 세션 조회 메시지에 대응하는 메시지를 단일 인증 서비스 장치에 전달하고, 상기 단일 인증 서비스 장치로부터 상기 웹 브라우저의 단일 인증

쿠키 정보 획득을 위한 단일 인증 토큰과 1회용 접속키를 수신하는 경우 상기 단말기의 어플리케이션에 전달하도록 제어함을 특징으로 하는 단일 인증 서비스를 지원하는 어플리케이션 서비스 장치.

[청구항 4]

제2항에 있어서, 상기 제1 제어부는,
상기 통합 ID 로그인 정보 수신 시, 상기 단일 인증 서비스 장치가 제공하는 단일 인증 토큰을 기반으로 상기 서비스 토큰을 생성하고 상기 단일 인증 토큰 및 상기 서비스 토큰, 상기 어플리케이션 기능 지원을 위한 데이터를 상기 단말기의 특정 어플리케이션에 제공하도록 제어하는 것을 특징으로 하는 단일 인증 서비스를 지원하는 어플리케이션 서비스 장치.

[청구항 5]

제2항에 있어서, 상기 제1 제어부는,
상기 통합 ID 로그인 정보 수신 시, 상기 단일 인증 서비스 장치가 제공하는 단일 인증 토큰을 기반으로 상기 서비스 토큰을 생성하고 상기 단일 인증 토큰, 1회용 접속키 및 상기 서비스 토큰, 상기 어플리케이션 기능 지원을 위한 데이터를 상기 단말기의 어플리케이션에 제공하도록 제어하며,
상기 세션 조회 메시지 수신 시 상기 단일 인증 서비스 장치가 제공하는 통합 서비스 번호를 기반으로 상기 서비스 토큰을 생성하고 상기 서비스 토큰을 상기 단말기의 어플리케이션에 제공하도록 제어하는 것을 특징으로 하는 단일 인증 서비스를 지원하는 어플리케이션 서비스 장치.

[청구항 6]

제2항에 있어서, 상기 제1 제어부는,
상기 단말기의 특정 어플리케이션으로부터 상기 서비스 토큰 만료 요청 메시지 수신 시 해당 어플리케이션의 서비스 로그아웃을 위한 서비스 토큰 만료 응답 메시지를 상기 단말기에 제공하도록 제어하는 것을 특징으로 하는 단일 인증 서비스를 지원하는 어플리케이션 서비스 장치.

[청구항 7]

제2항에 있어서, 상기 제1 제어부는,
상기 단말기의 특정 어플리케이션으로부터 상기 서비스 토큰 및 상기 단일 인증 토큰 만료 요청 메시지 수신 시 단일 인증 토큰 만료 요청 메시지를 상기 단일 인증 서비스 장치에 제공하고 그에 대응하는 응답 메시지를 수신하는 경우, 상기 서비스 토큰 및 상기 단일 인증 토큰의 만료 응답 메시지를 상기 단말기에 제공하도록 제어하는 것을 특징으로 하는 단일 인증 서비스를 지원하는 어플리케이션 서비스 장치.

[청구항 8]

제2항에 있어서, 상기 제1 제어부는,
상기 단말기로부터 웹 브라우저 종료 또는 웹 브라우저 기반의

단일 인증 쿠키 만료 요청 메시지 수신 시 단일 인증 쿠키 만료 요청 메시지를 상기 단일 인증 서비스 장치에 제공하고, 그에 대응하는 응답 메시지를 상기 단말기에 제공하도록 제어하는 것을 특징으로 하는 단일 인증 서비스를 지원하는 어플리케이션 서비스 장치.

[청구항 9]

적어도 하나의 어플리케이션 서비스 장치와 통신 채널을 형성하고 단말기의 특정 어플리케이션이 상기 어플리케이션 서비스 장치를 통해 전송하는 단일 인증 세션 요청 메시지 또는 단일 인증 세션 검사 메시지를 수신하는 장치 통신부;
특정 어플리케이션 서비스 장치를 별도 인증 정보 입력 없이 접속할 수 있도록 하는 단일 인증 지원을 위해 상기 단말기에 제공되는 단일 인증 토큰을 저장하는 제2 저장부;
상기 단일 인증 세션 요청 메시지 수신 시 상기 단일 인증 토큰을 상기 어플리케이션 서비스 장치를 통하여 단말기에 제공하며, 상기 단일 인증 세션 검사 메시지 수신 시 상기 단일 인증 토큰 기반의 통합 서비스 번호를 상기 어플리케이션 서비스 장치에 제공하도록 제어하는 제2 제어부;
를 포함하는 것을 특징으로 하는 단일 인증 서비스 장치.

[청구항 10]

제9항에 있어서, 상기 제2 제어부는,
상기 어플리케이션 서비스 장치로부터 단일 인증 토큰 만료 요청 메시지 수신 시 상기 단일 인증 토큰 만료에 대응하는 응답 메시지를 상기 어플리케이션 서비스 장치에 제공하는 것을 특징으로 하는 단일 인증 서비스 장치.

[청구항 11]

제9항에 있어서, 상기 제2 제어부는,
상기 단말기의 웹 브라우저에 제공할 단일 인증 쿠키 정보 생성을 위한 단일 인증 세션 요청 메시지를 수신하면, 상기 단일 인증 세션 요청 메시지에 대응하는 단일 인증 토큰 및 1회용 접속키를 상기 어플리케이션 서비스 장치를 통해 상기 단말기에 제공하도록 제어하고, 상기 1회용 접속키를 통해 접속하는 웹 브라우저에게 단일 인증 쿠키 정보를 제공하도록 제어함을 특징으로 하는 단일 인증 서비스 장치.

[청구항 12]

제11항에 있어서, 상기 제2 제어부는,
상기 웹 브라우저의 상기 1회용 접속키 기반의 접속 이후 상기 1회용 접속키를 삭제하도록 제어하는 것을 특징으로 하는 단일 인증 서비스 장치.

[청구항 13]

제11항에 있어서, 상기 제2 제어부는,
상기 단말기의 웹 브라우저가 제공하는 단일 인증 쿠키 정보를 이용하여 작성된 상기 어플리케이션의 단일 인증을 위한 메시지를

수신하면, 상기 메시지에 대응하는 통합 서비스 번호를 상기 어플리케이션 서비스 장치에 제공하도록 제어하며, 상기 단말기의 웹 브라우저로부터 상기 단일 인증 쿠키 만료 요청 메시지를 수신하면, 상기 만료 요청 메시지에 대응하는 응답 메시지를 상기 웹 브라우저에 제공하고, 상기 제2 저장부에 저장된 단일 인증 쿠키 정보를 삭제하도록 제어하는 것을 특징으로 하는 단일 인증 서비스 장치.

[청구항 14]

복수개의 어플리케이션 중 적어도 하나의 어플리케이션 기능 수행을 위해 복수개의 어플리케이션 서비스 장치 중 적어도 하나와 통신 채널을 형성하는 통신부; 상기 복수개의 어플리케이션, 상기 복수개의 어플리케이션 서비스 장치의 서비스 이용을 위한 서비스 토큰, 상기 복수개의 어플리케이션 서비스 장치에 접속할 수 있도록 지원하는 단일 인증 토큰을 저장하는 저장부; 상기 단일 인증 토큰 부재 시 상기 단일 인증 토큰 획득을 위한 요청 메시지를 상기 어플리케이션 서비스 장치를 통해 단일 인증 서비스 장치에 제공하여 상기 단일 인증 토큰을 획득하도록 제어하며, 상기 단일 인증 토큰이 존재하면 상기 단일 인증 토큰을 기반으로 특정 어플리케이션 서비스 장치 접속 및 이용을 위한 통합 서비스 번호 제공을 위한 단일 인증 세션 조회 메시지를 상기 어플리케이션 서비스 장치를 통하여 상기 단일 인증 서비스 장치에 제공하도록 제어하는 제어부; 를 포함하는 것을 특징으로 하는 단일 인증 서비스를 지원하는 단말기.

[청구항 15]

제14항에 있어서
상기 어플리케이션 서비스 장치 접속을 위한 일반 인증 정보 입력을 위한 영역;
상기 단일 인증 토큰 획득을 위한 통합 ID 로그인을 위한 영역;
상기 단일 인증 토큰 기반으로 특정 어플리케이션 서비스 장치 접속을 위한 인증 정보가 자동 입력된 영역; 중 적어도 하나를 출력하는 표시부; 를 더 포함하는 것을 특징으로 하는 단일 인증 서비스를 지원하는 단말기.

[청구항 16]

제15항에 있어서
상기 서비스 토큰 만료 요청을 위한 로그아웃 항목;
상기 단일 인증 토큰 만료 요청을 위한 팝업창;
상기 어플리케이션 서비스 장치로부터 수신된 데이터를 출력하는 서비스 영역; 중 적어도 하나를 포함하는 화면을 제공하는 표시부;

를 더 포함하는 것을 특징으로 하는 단일 인증 서비스를 지원하는 단말기.

[청구항 17]

제15항에 있어서, 상기 제어부는,
상기 단일 인증 토큰 운용을 위한 어카운트 매니저 계정 생성을 제어하거나 또는 클라우드 서비스의 활성화 제어를 지원하는 것을 특징으로 하는 단일 인증 서비스를 지원하는 단말기.

[청구항 18]

제15항에 있어서, 상기 제어부는,
상기 단일 인증 토큰 만료 시 상기 어카운트 매니저 계정을 삭제하도록 제어하는 것을 특징으로 하는 단일 인증 서비스를 지원하는 단말기.

[청구항 19]

제15항에 있어서, 상기 제어부는,
특정 어플리케이션 활성화를 위한 선택 시 웹 브라우저의 단일 인증 쿠키 정보 운용 여부를 확인하고, 상기 단일 인증 쿠키 정보를 통해 제공되는 단일 인증 토큰을 이용하여 상기 어플리케이션의 자동 로그인 수행을 위한 메시지를 해당 어플리케이션 서비스 장치에 전송하도록 제어함을 특징으로 하는 단일 인증 서비스를 지원하는 단말기.

[청구항 20]

제19항에 있어서, 상기 특정 어플리케이션은,
상기 웹 브라우저의 상기 단일 인증 쿠키 운용 불가 시, 통합 ID 로그인을 수행하여 1회용 접속키를 단일 인증 서비스 장치로부터 수신하여 상기 웹 브라우저에게 제공하며,
상기 웹 브라우저는,
상기 1회용 접속키를 기반으로 상기 단일 인증 서비스 장치에 접속하여 상기 단일 인증 쿠키 정보를 수신하는 것을 특징으로 하는 단일 인증 서비스를 지원하는 단말기.

[청구항 21]

단말기가 특정 어플리케이션 기능 운용을 위하여 어플리케이션 서비스 장치 접속 과정에서 통합 ID 로그인을 수행하거나 사전 저장된 단일 인증 토큰 기반의 단일 인증을 위한 세션 조회 메시지를 어플리케이션 서비스 장치에 제공하는 단계;
상기 어플리케이션 서비스 장치가 상기 통합 ID 로그인을 수행한 후 단일 인증 토큰 생성을 위한 요청 메시지를 상기 단일 인증 서비스 장치에 전송하거나 상기 세션 조회 메시지를 상기 단일 인증 서비스 장치에 전송하는 단계;
상기 어플리케이션 서비스 장치가 상기 단일 인증 서비스 장치로부터 상기 단일 인증 토큰 또는 상기 세션 조회 메시지에 따른 통합 서비스 번호를 수신하는 단계; 및
상기 어플리케이션 서비스 장치가 상기 단일 인증 토큰 수신 시 상기 단일 인증 토큰과 상기 어플리케이션 서비스 장치 이용을

위한 서비스 토큰 및 데이터를 상기 단말기에 제공하고, 상기 통합 서비스 번호 수신 시 상기 어플리케이션의 자동 로그인을 수행하고 상기 서비스 토큰 및 데이터를 상기 단말기에 제공하는 단계;

를 포함하는 것을 특징으로 하는 단일 인증 서비스 운용 방법.

[청구항 22]

제21항에 있어서

상기 단말기가 상기 서비스 토큰 만료를 위한 요청 메시지 또는 상기 서비스 토큰과 상기 단일 인증 토큰 만료를 위한 요청 메시지를 상기 어플리케이션 서비스 장치에 전송하는 단계; 상기 어플리케이션 서비스 장치가 상기 서비스 토큰 만료에 따른 응답 메시지를 상기 단말기에 제공하거나 상기 단일 인증 토큰 만료를 위한 요청 메시지를 상기 단일 인증 서비스 장치에 전송하고 그에 대응하는 응답을 상기 서비스 토큰 만료 응답 메시지와 함께 상기 단말기에 제공하는 단계; 및

상기 단말기가 상기 서비스 로그아웃 또는 상기 단일 인증 로그아웃 중 어느 하나를 수행하는 단계;

를 더 포함하는 것을 특징으로 하는 단일 인증 서비스 운용 방법.

[청구항 23]

단말기의 웹 브라우저가 특정 어플리케이션 활성화를 위한 입력 신호 수신 시 해당 어플리케이션 호출과 함께 해당 어플리케이션에게 단일 인증 쿠키 정보 기반의 단일 인증 토큰을 제공하는 단계;

상기 어플리케이션이 상기 단일 인증 토큰을 이용하여 자동 로그인을 위한 세션 조회 메시지를 어플리케이션 서비스 장치를 통해 단일 인증 서비스 장치에 제공하는 단계;

상기 단일 인증 서비스 장치가 상기 세션 조회 메시지에 대응하는 통합 서비스 번호를 생성하여 상기 어플리케이션 서비스 장치에 제공하는 단계;

상기 어플리케이션 서비스 장치가 상기 통합 서비스 번호를 기반으로 어플리케이션 서비스 운용을 위한 서비스 토큰을 생성하는 단계; 및

상기 어플리케이션 서비스 장치가 상기 서비스 토큰 및 상기 어플리케이션 서비스 운용을 위한 사용자 데이터를 상기 어플리케이션에 제공하는 단계;

를 포함하는 것을 특징으로 하는 단일 인증 서비스 운용 방법.

[청구항 24]

제23항에 있어서,

상기 웹 브라우저의 단일 인증 쿠키 정보 운용 불가 시, 상기 어플리케이션이 입력된 통합 ID 로그인을 위한 정보를 상기 어플리케이션 서비스 장치를 통해 상기 단일 인증 서비스 장치에

제공하는 단계;

상기 단일 인증 서비스 장치가 1회용 접속키를 상기

어플리케이션에 제공하는 단계;

상기 어플리케이션이 상기 웹 브라우저에 상기 1회용 접속키를 제공하는 단계; 및

상기 웹 브라우저가 상기 1회용 접속키를 이용하여 상기 단일 인증 서비스 장치에 접속하여 상기 단일 인증 쿠키 정보를 수신하는 단계;

를 더 포함하는 것을 특징으로 하는 단일 인증 서비스 운용 방법.

[청구항 25]

제23항에 있어서,

상기 웹 브라우저 종료 또는 상기 웹 브라우저 기반의 단일 인증 서비스 로그아웃을 위한 입력 신호를 수신하는 단계;

상기 입력 신호에 따른 요청 메시지를 상기 단일 인증 서비스 장치에 전송하는 단계;

상기 단일 인증 서비스 장치가 저장된 단일 인증 쿠키 정보를 삭제하고 상기 요청 메시지에 대응하는 응답 메시지를 상기 단말기에 제공하는 단계; 및

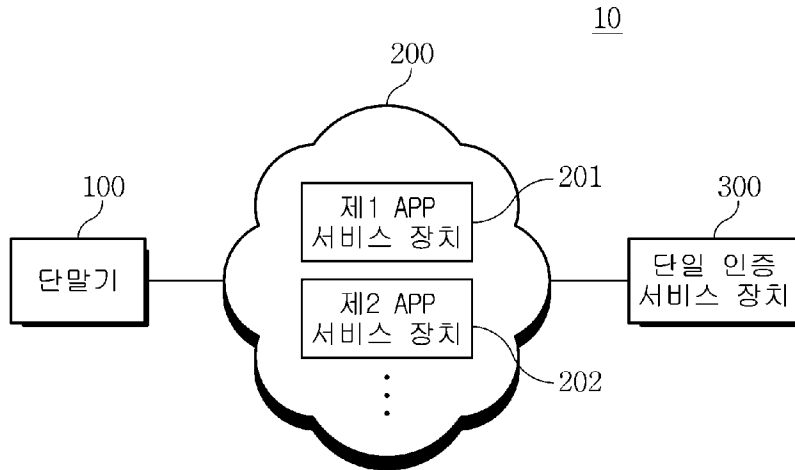
상기 단말기가 상기 서비스 로그아웃을 수행하는 단계;

를 더 포함하는 것을 특징으로 하는 단일 인증 서비스 운용 방법.

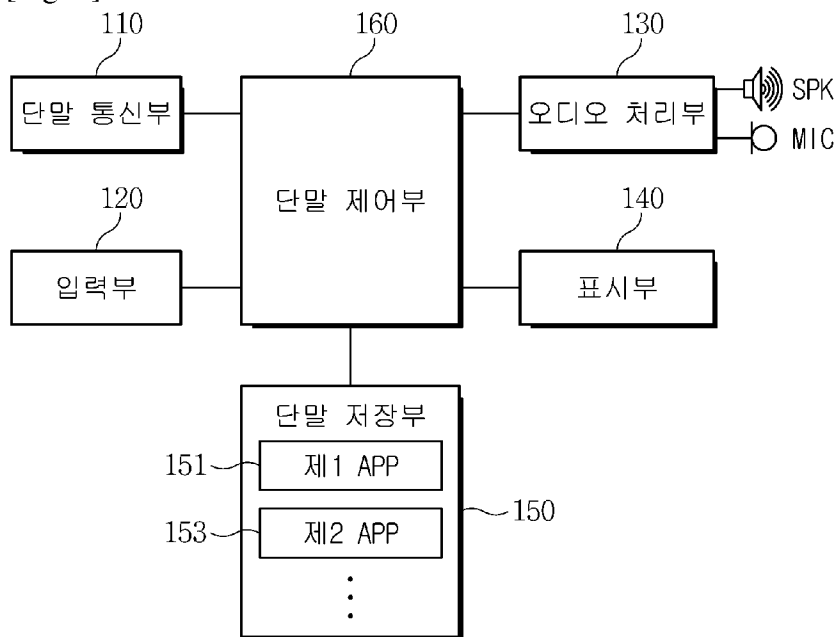
[청구항 26]

제21항 및 제25항 중 어느 한 항에 기재된 방법을 실행하는 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체.

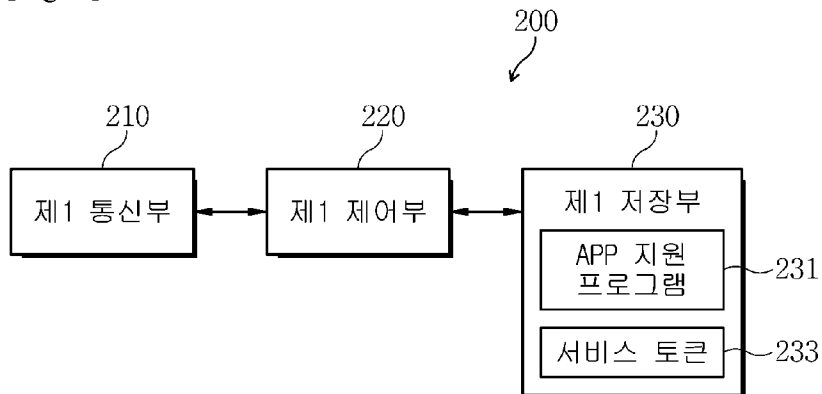
[Fig. 1]



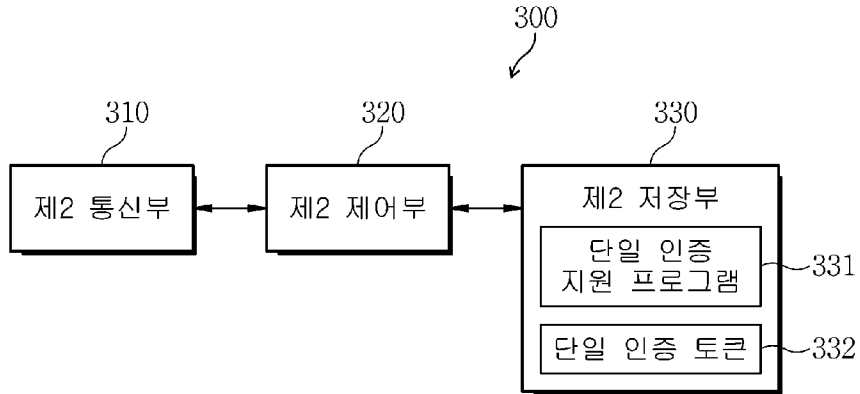
[Fig. 2]



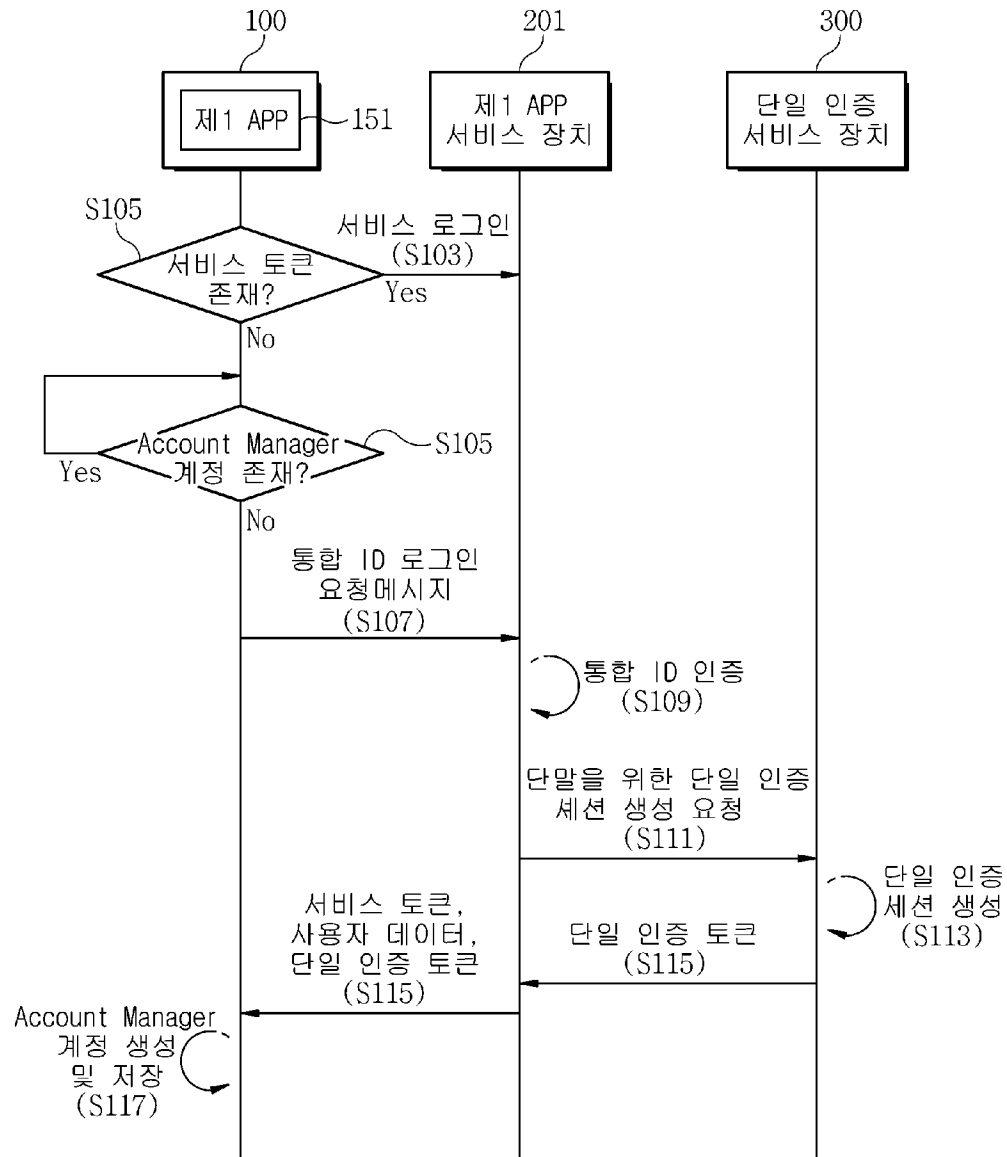
[Fig. 3]



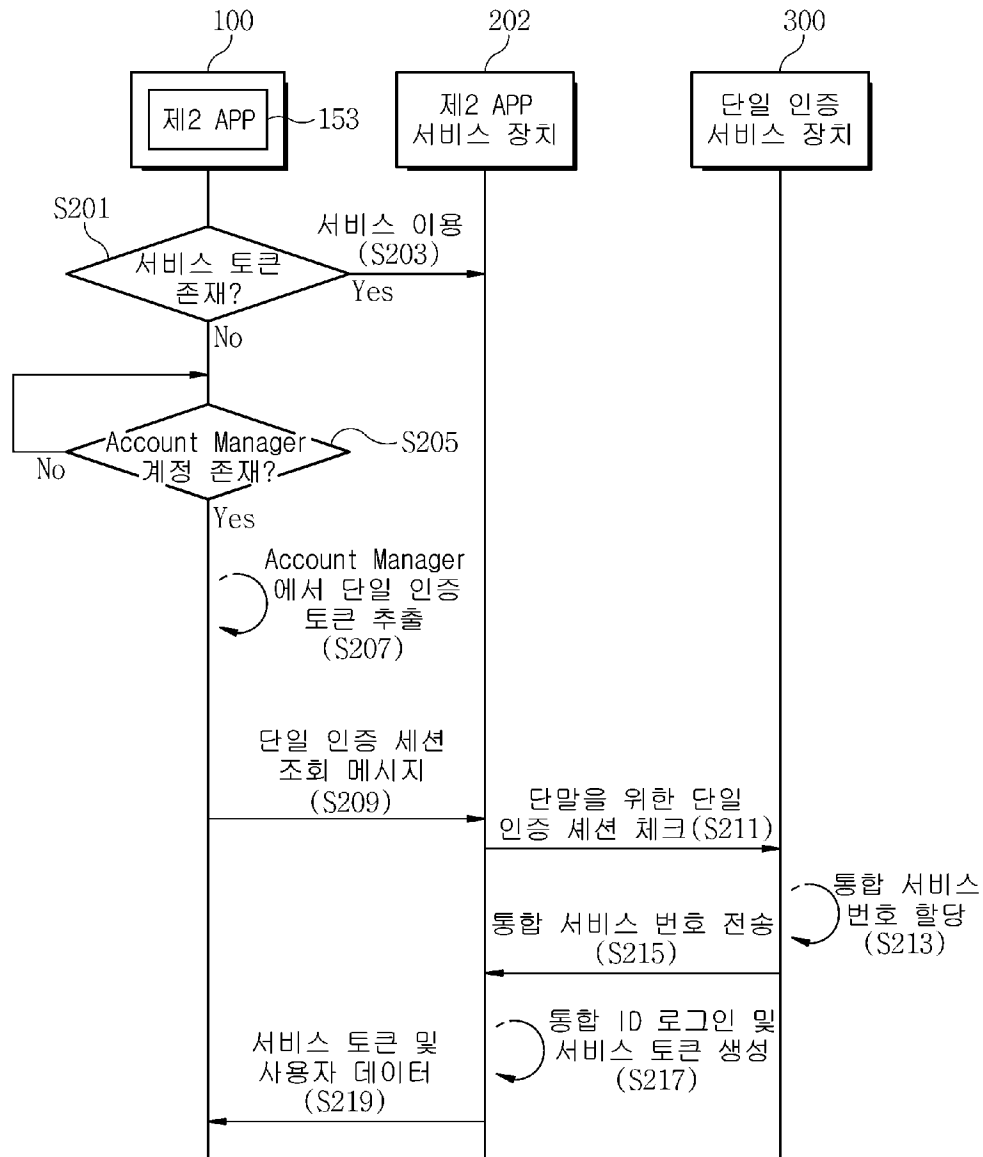
[Fig. 4]



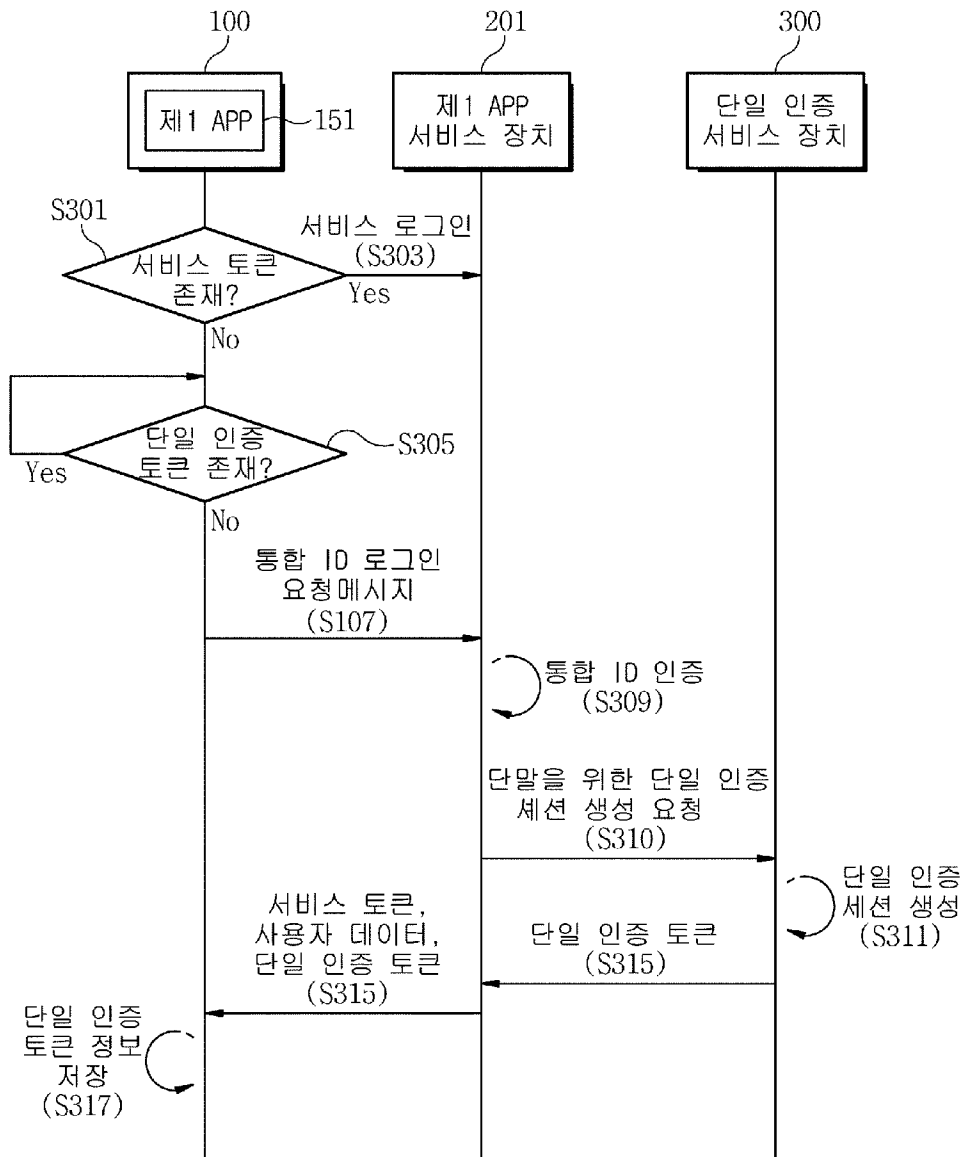
[Fig. 5]



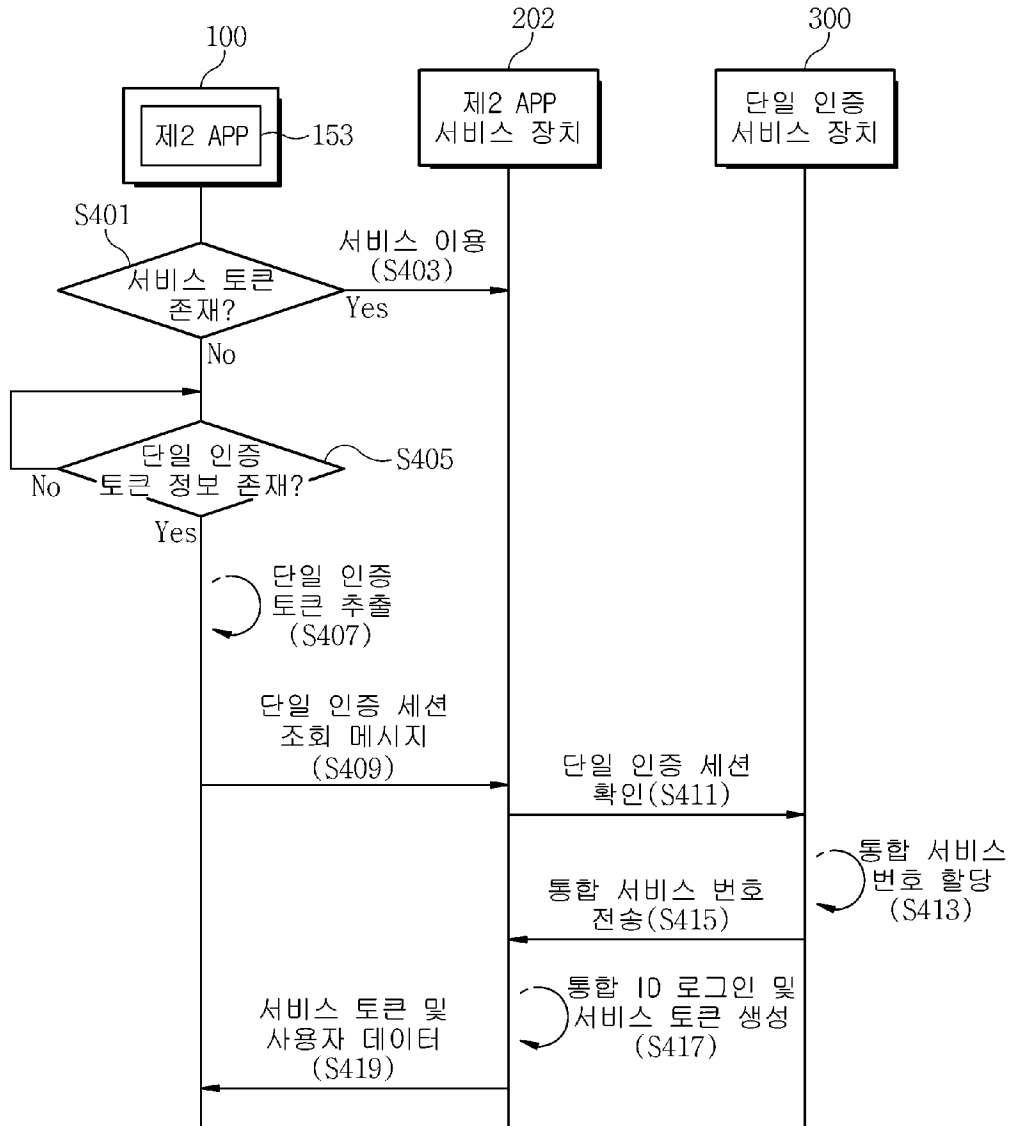
[Fig. 6]



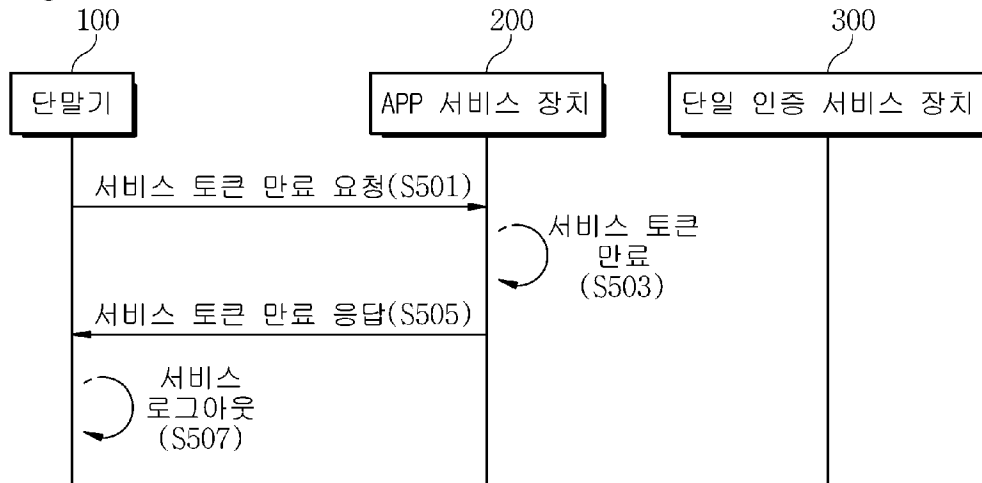
[Fig. 7]



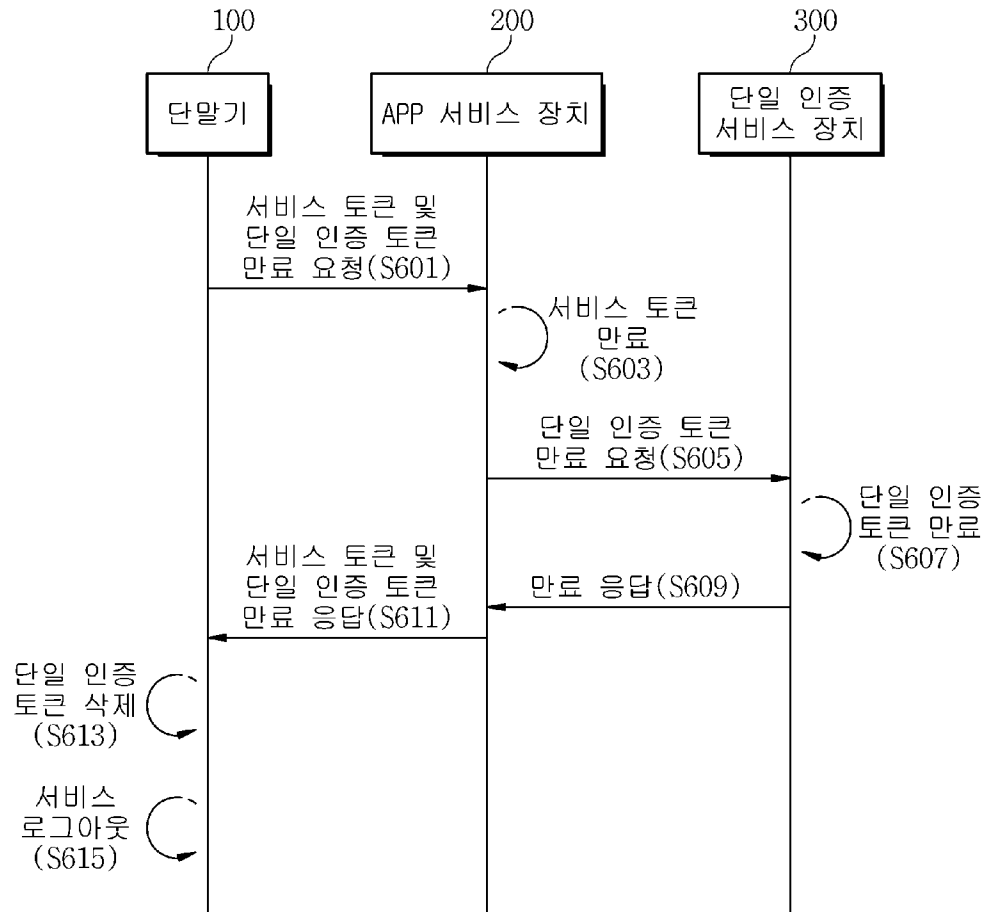
[Fig. 8]



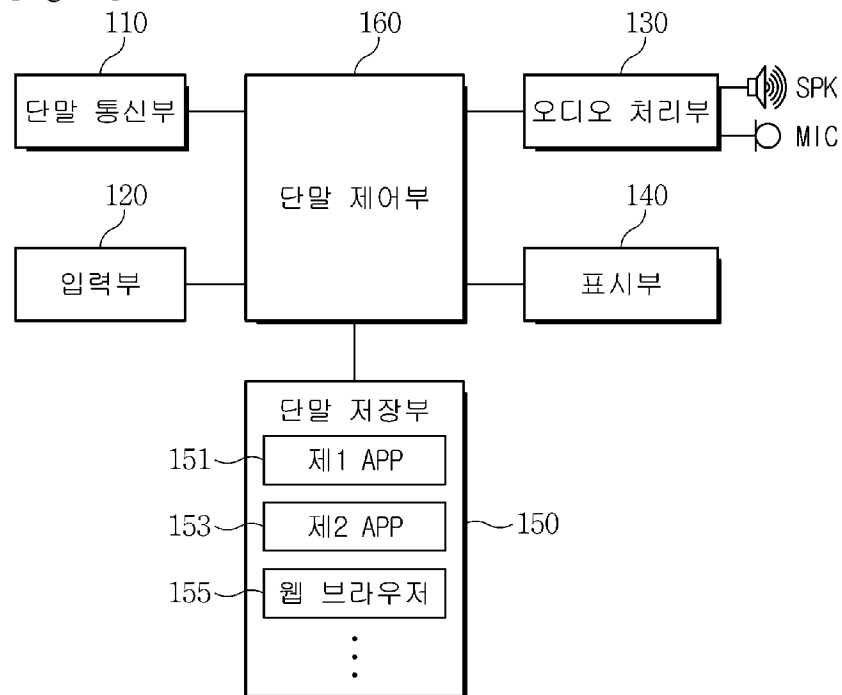
[Fig. 9]



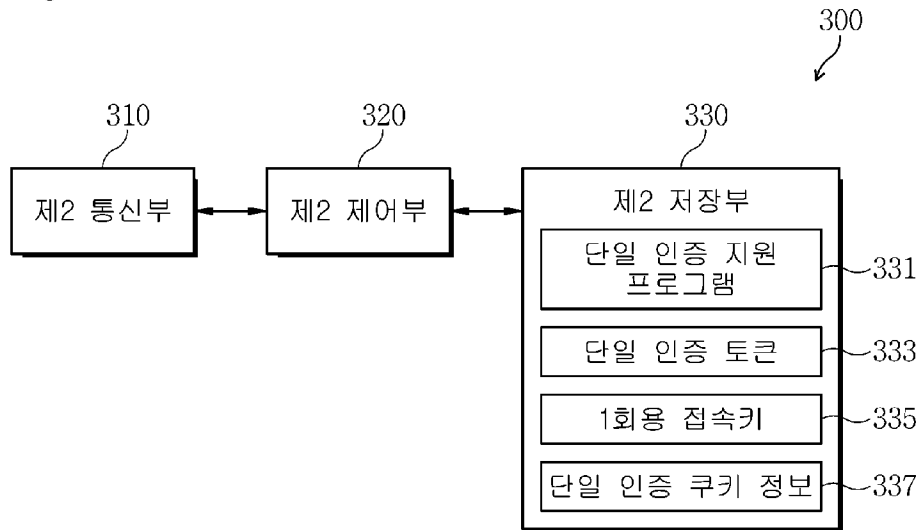
[Fig. 10]



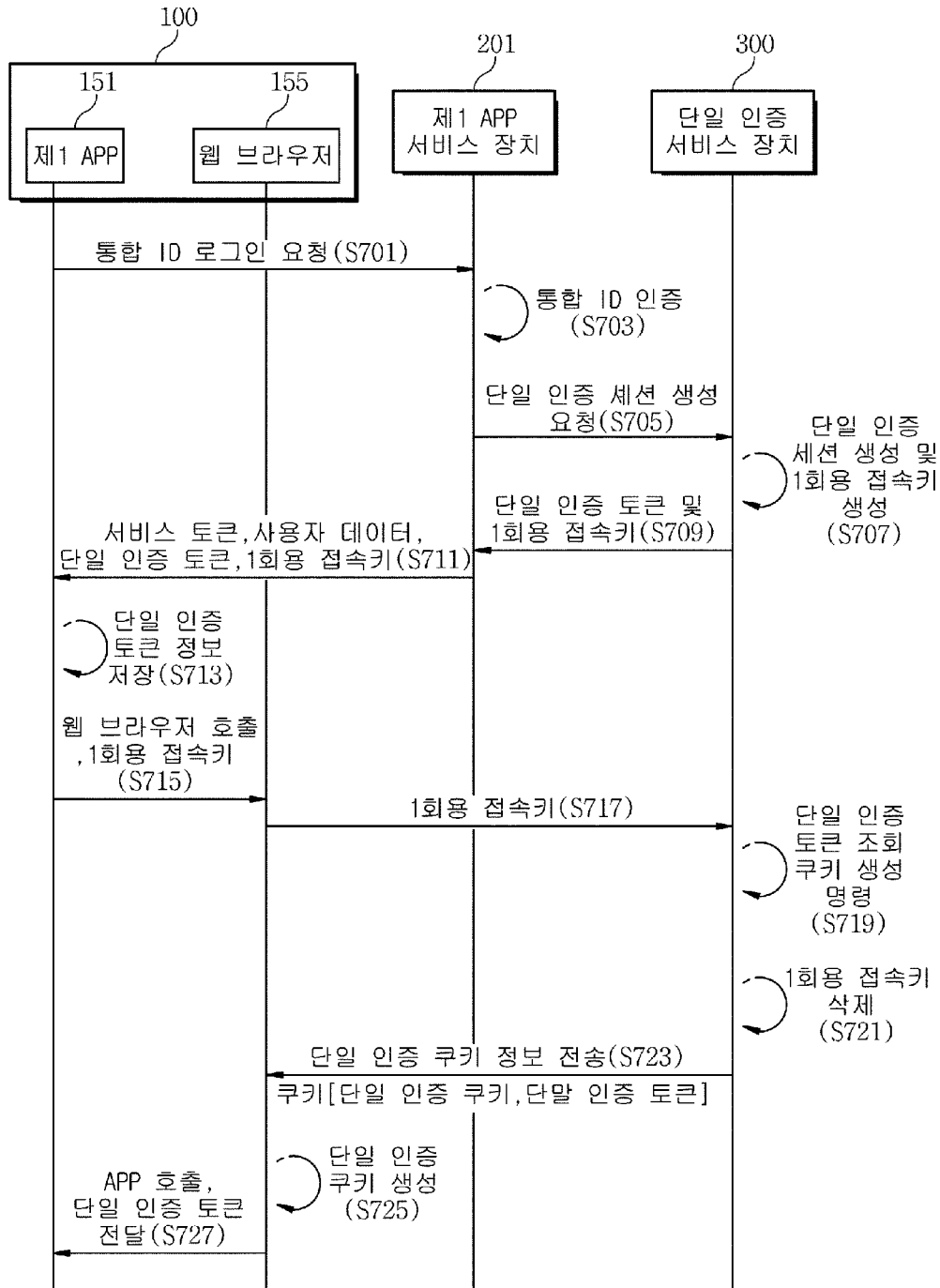
[Fig. 11]



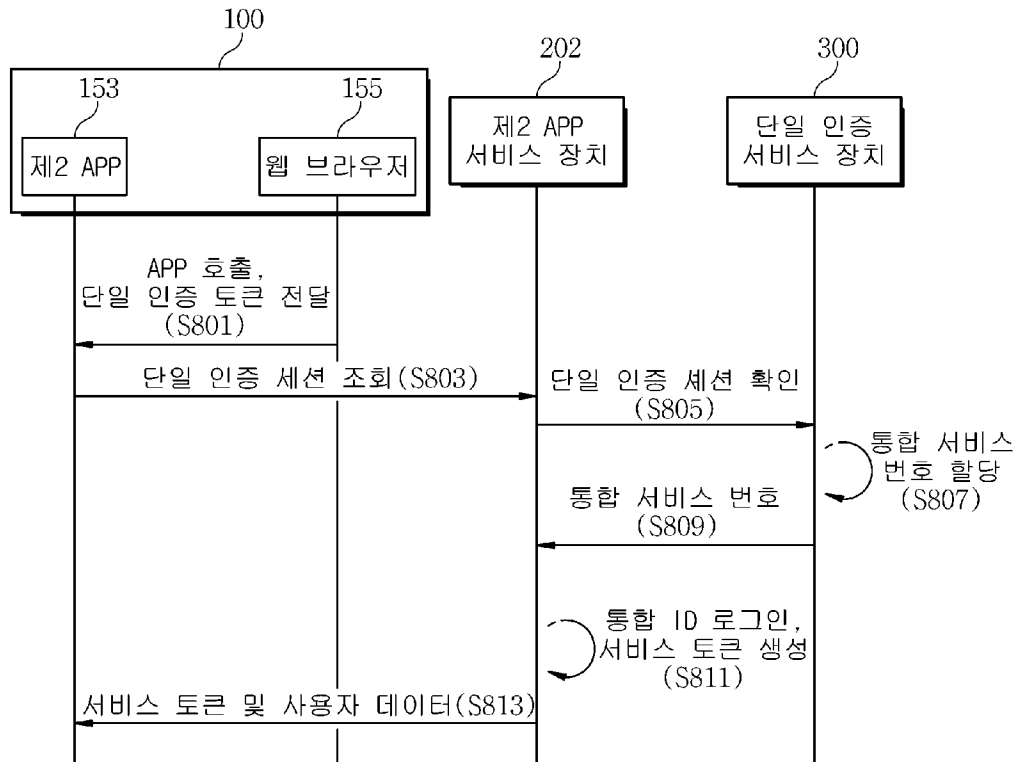
[Fig. 12]



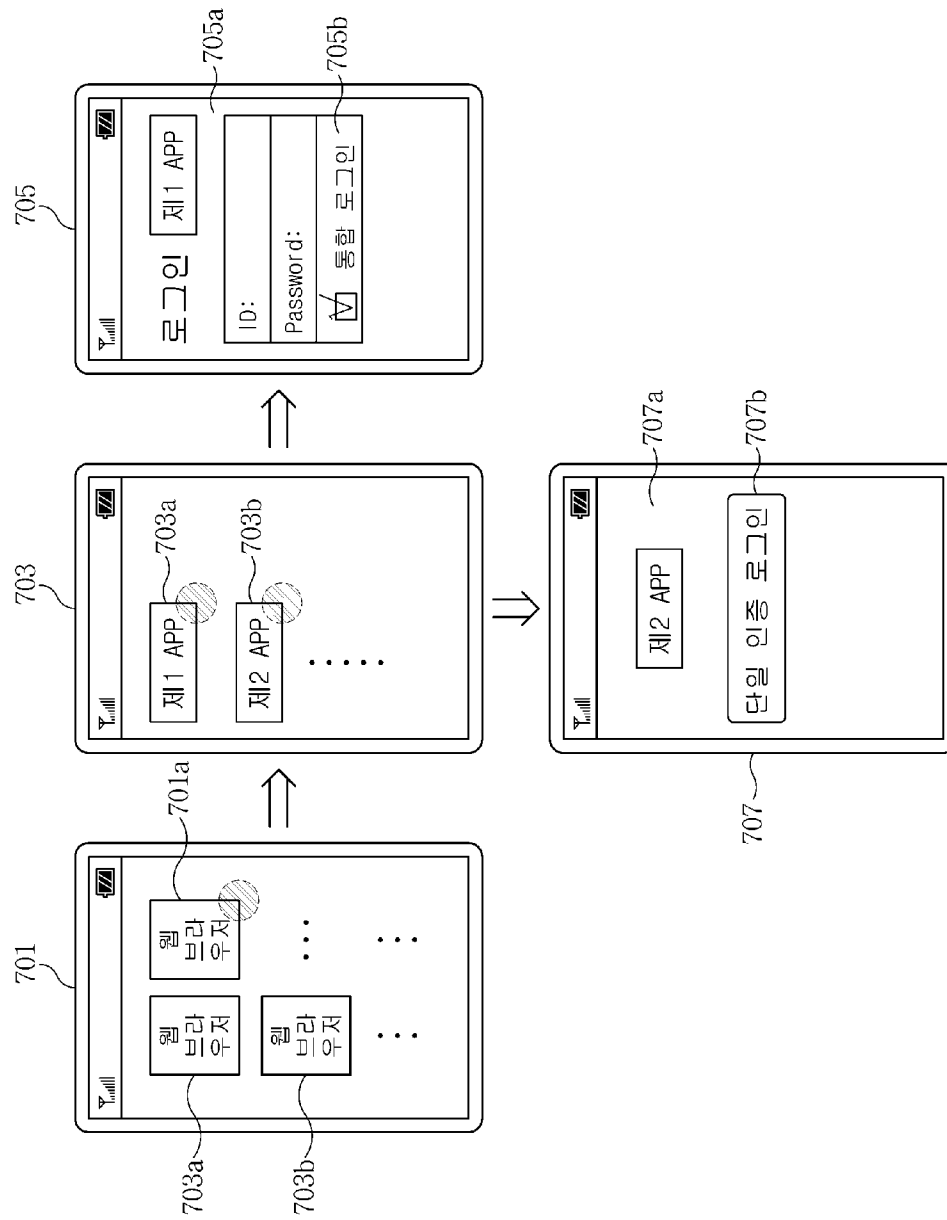
[Fig. 13]



[Fig. 14]



[Fig. 15]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2013/005859**A. CLASSIFICATION OF SUBJECT MATTER*****H04W 12/06(2009.01)i***

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W 12/06; G06F 15/16; G06F 21/20; H04L 9/32; G06F 21/00; G06F 7/04

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models: IPC as above

Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: single sign-on|unity certification|SSO| (single sign on), token|token ,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2010-0066907 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 18 June 2010 See abstract, claims 1-7 and figures 5-6	1-26
A	KR 10-2009-0102924 A (GENICS ASSOCIATES CO., LTD. et al.) 01 October 2009 See abstract, claims 1-2 and figure 2	1-26
A	US 2011-0264913 A1 (NIKANDER, Pekka et al.) 27 October 2011 See abstract, claim 1 and figure 6	1-26
A	WO 2011-063014 A1 (SECUREAUTH CORPORATION et al.) 26 May 2011 See abstract, claim 1 and figure 3	1-26



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

25 OCTOBER 2013 (25.10.2013)

Date of mailing of the international search report

28 OCTOBER 2013 (28.10.2013)

Name and mailing address of the ISA/KR



Korean Intellectual Property Office
Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2013/005859

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2010-0066907 A	18/06/2010	NONE	
KR 10-2009-0102924 A	01/10/2009	NONE	
US 2011-0264913 A1	27/10/2011	WO 2011-128183 A2 WO 2011-128183 A3	20/10/2011 05/01/2012
WO 2011-063014 A1	26/05/2011	US 2011-0119747 A1	19/05/2011

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04W 12/06(2009.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04W 12/06; G06F 15/16; G06F 21/20; H04L 9/32; G06F 21/00; G06F 7/04

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 단일인증|통합인증|SSO|(single sign on), 토큰|token ,

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2010-0066907 A (한국전자통신연구원) 2010.06.18 요약, 청구항 1-7 및 도면 5-6 참조	1-26
A	KR 10-2009-0102924 A ((주)제닉스어소시에츠 외 2명) 2009.10.01 요약, 청구항 1-2 및 도면 2 참조	1-26
A	US 2011-0264913 A1 (NIKANDER PEKKA 외 5명) 2011.10.27 요약, 청구항 1 및 도면 6 참조	1-26
A	WO 2011-063014 A1 (SECUREAUTH CORPORATION 외 2명) 2011.05.26 요약, 청구항 1 및 도면 3 참조	1-26

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

“A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2013년 10월 25일 (25.10.2013)

국제조사보고서 발송일

2013년 10월 28일 (28.10.2013)

ISA/KR의 명칭 및 우편주소

 대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-472-7140

심사관

장상배

전화번호 +82-42-481-8201



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2010-0066907 A	2010/06/18	없음	
KR 10-2009-0102924 A	2009/10/01	없음	
US 2011-0264913 A1	2011/10/27	WO 2011-128183 A2 WO 2011-128183 A3	2011/10/20 2012/01/05
WO 2011-063014 A1	2011/05/26	US 2011-0119747 A1	2011/05/19