(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2013 년 5 월 2 일 (02.05.2013)

WIPO | PCT

(10) 국제공개번호
WO 2013/062394 A1

(51) 국제특허분류:
H04W 12/06 (2009.01)

(21) 국제출원번호: PCT/KR2012/008950

(22) 국제출원일: 2012 년 10 월 29 일 (29.10.2012)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
61/552,684 2011 년 10 월 28 일 (28.10.2011) US

(71) 출원인: **삼성전자 주식회사 (SAMSUNG ELECTRONICS CO., LTD.)** [KR/KR]; 443-742 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR).

(72) 발명자: **서경주 (SUH, Kyung Joo)**; 135-090 서울시 강남구 삼성동 104-10 삼성래미안 1 차 아파트 101-1102, Seoul (KR).

(74) 대리인: **윤동열 (YOON, Dong Yol)**; 153-803 서울시 금천구 가산디지털 1 로 226 에이스 하이엔드타워 5 차 3 층 윤앤리 특허 법률 사무소, 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, KM, KN, KP, KR, 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.

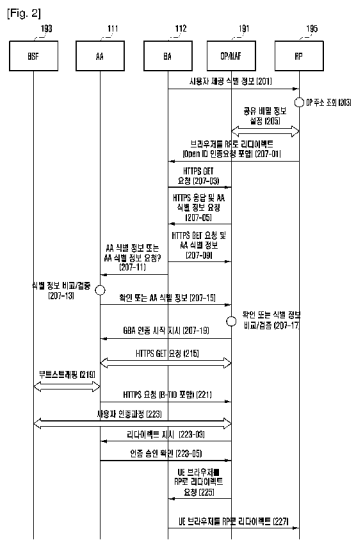
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE,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

[다음 쪽 계속]

(54) **Title**: METHOD AND APPARATUS FOR SINGLE SIGN-ON IN A MOBILE COMMUNICATION SYSTEM

(54) **발명의 명칭** : 이동 통신 시스템에서 단일 사용 승인 방법 및 장치

[Fig. 2]



201 ... Provide user-supplied identifier
203 ... Inquire into an OP address
205 ... Set shared confidential information
207-01 ... Re-direct a browser to RP (including a request for an open ID authentication)
207-03 ... Request for HTTPS GET
207-05 ... Response to HTTPS and request for AA identifier
207-09 ... Request for HTTPS GET and AA identifier
207-11 ... AA identifier or a request for AA identifier?
207-13 ... Compare/verify identifiers
207-15 ... Confirmation or AA identifier
207-17 ... Compare/verify confirmations or identifiers
207-19 ... Indicate starting of GBA authentication
215 ... Request for HTTPS GET
219 ... Bootstrapping
221 ... Request for HTTPS (including B-TID)
223 ... User authentication procedure
223-03 ... Indicate re-direct
223-05 ... Confirm authentication authorization
225 ... Request for re-directing UE browser to RP
227 ... Re-direct the UE browser to RP

(57) **Abstract**: The present invention relates to a method and an apparatus for single sign-on in a mobile communication system. A method in which a browsing agent performs single sign-on in a mobile communication system according to the present invention comprises: a step of transmitting user-supplied identifier to a relay party (RP); a step of receiving, from said RP, a message indicating that a browser should be re-directed to said RP; a step of transmitting an identifier of an authentication agent to an open ID provider (OP)/network application function (NAF); and a step of transmitting, to the authentication agent, the identifier of the authentication agent or a message that triggers to make an inquiry into the identifier of the authentication agent. According to the present invention, a single sign-on procedure may be performed in a safer manner.

(57) **요약서**: 본 발명은 이동 통신 시스템의 단일 사용 승인 방법 및 장치에 관한 것으로, 본 발명의 실시예에 따른 이동 통신 시스템에서 브라우징 에이전트(Browsing Agent)의 단일 사용 승인 방법은, 사용자 제공 식별 정보(User supplied identifier)를 RP(Relaying Party)로 전송하는 단계, 상기 RP 로부터 브라우저(browser)를 상기 RP 로 리다이렉트(redirect) 할 것을 지시하는 메시지를 수신하는 단계, 인증 에이전트(Authentication Agent)의 식별 정보(identifier)를 OP(Open ID Provider)/NAF(Network Application Function)로 전송하는 단계 및 상기 인증 에이전트의 식별 정보 또는 상기 인증 에이전트의 식별 정보를 조회하도록 트리거링(triggering)하는 메시지를 인증 에이전트로 전송하는 단계를 포함하는 것을 특징으로 한다. 본 발명에 따르면, 보다 안전하게 단일 사용자 승인 절차를 수행할 수 있다.

WO 2013/062394 A1

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))

명세서

발명의 명칭: 이동 통신 시스템에서 단일 사용 승인 방법 및 장치

기술분야

[1] 본 발명은 이동 통신 시스템의 단일 사용 승인 방법 및 장치에 관한 것으로, 특히, 단일 사용자 승인 절차를 수행하는 과정을 효율적으로 지원하기 위한 방법 및 장치에 관한 것이다.

배경기술

[2] 이동통신 네트워크에서 단일 사용 승인(Single Sign-ON, 이하 SSO로 표기)은 사용자가 네트워크에 한 번 로그온(log on)하여, 허가된 모든 자원에 접근할 수 있도록 하는 승인 방법이다. SSO을 이용하는 경우, 하나의 사용자 아이디와 암호를 이용하여 적절한 모든 서버에 자동적으로 로그온 할 수 있다.

[3] 종래의 기술에 따른 SSO는 승인을 위하여 전송되는 식별자 및 검증 과정에 보안 상의 취약점 존재한다. 따라서, 이러한 보안 상의 취약점을 이용한 피싱 공격 (pishing attack) 등에 취약하다는 문제점이 있다.

발명의 상세한 설명

기술적 과제

[4] 본 발명은 상기와 같은 문제점을 해결하기 위하여 안출된 것으로서, 인증 과정을 브라우징 에이전트(Browsing Agent)와 인증 에이전트(Authentication Agent)에서 분리하여 수행하도록 하여 단일 사용자 승인 과정을 수행함으로써 단일 사용자 승인 과정에서 발생할 수 있는 보안 문제를 해결하는데 그 목적이 있다.

과제 해결 수단

[5] 상기와 같은 문제점을 해결하기 위한 본 발명의 실시예에 따른 이동 통신 시스템에서 브라우징 에이전트(Browsing Agent)의 단일 사용 승인 방법은, 사용자 제공 식별 정보(User supplied identifier)를 RP(Relaying Party)로 전송하는 단계, 상기 RP로부터 브라우저(browser)를 상기 RP로 리다이렉트(redirect) 할 것을 지시하는 메시지를 수신하는 단계, 인증 에이전트(Authentication Agent)의 식별 정보(identifier)를 OP(Open ID Provider)/NAF(Network Application Function)로 전송하는 단계 및 상기 인증 에이전트의 식별 정보 또는 상기 인증 에이전트의 식별 정보를 조회하도록 트리거링(triggering)하는 메시지를 인증 에이전트로 전송하는 단계를 포함하는 것을 특징으로 한다.

[6] 또한, 본 발명의 다른 실시예에 따른 이동 통신 시스템에서 인증 에이전트(Authentication Agent)의 단일 사용 승인 방법은, 브라우징 에이전트(Browsing Agent)로부터 인증 에이전트의 식별 정보(identifier)를 수신하는 단계, 수신한 인증 에이전트의 식별 정보가 사용자 제공 식별 정보(User supplied identifier)와 동일한지 여부를 판단하는 단계 및 상기 인증

에이전트의 식별 정보가 사용자 제공 식별 정보와 동일한 경우, 확인 메시지를 OP(Open ID Provider)/NAF(Network Application Function)로 전송하는 단계를 포함하는 것을 특징으로 한다.

[7] 또한, 본 발명의 또다른 실시예에 따른 이동 통신 시스템에서 인증 에이전트(Authentication Agent)의 단일 사용 승인 방법은, 브라우징 에이전트(Browsing Agent)로부터 인증 에이전트의 식별 정보(identifier)를 조회하도록 트리거링(triggering)하는 메시지를 수신하는 단계 및 사용자 제공 식별 정보(User supplied identifier)를 OP(Open ID Provider)/NAF(Network Application Function)로 전송하는 단계를 포함하는 것을 특징으로 한다.

[8] 본 발명의 실시예에 따른 이동 통신 시스템에서 브라우징 에이전트(Browsing Agent)의 단일 사용 승인 장치는, 사용자 제공 식별 정보(User supplied identifier)를 RP(Relaying Party)로 전송하고, 상기 RP로부터 브라우저(browser)를 상기 RP로 리다이렉트(redirect) 할 것을 지시하는 메시지를 수신하며, 인증 에이전트(Authentication Agent)의 식별 정보(identifier)를 OP(Open ID Provider)/NAF(Network Application Function)로 전송하고, 상기 인증 에이전트의 식별 정보 또는 상기 인증 에이전트의 식별 정보를 조회하도록 트리거링(triggering)하는 메시지를 인증 에이전트로 전송하도록 제어하는 제어부를 포함하는 것을 특징으로 한다.

[9] 또한, 본 발명의 다른 실시예에 따른 이동 통신 시스템에서 인증 에이전트(Authentication Agent)의 단일 사용 승인 장치는, 브라우징 에이전트(Browsing Agent)로부터 인증 에이전트의 식별 정보(identifier)를 수신하고, 수신한 인증 에이전트의 식별 정보가 사용자 제공 식별 정보(User supplied identifier)와 동일한지 여부를 판단하며, 상기 인증 에이전트의 식별 정보가 사용자 제공 식별 정보와 동일한 경우 확인 메시지를 OP(Open ID Provider)/NAF(Network Application Function)로 전송하도록 제어하는 제어부를 포함하는 것을 특징으로 한다.

[10] 또한, 본 발명의 또다른 실시예에 따른 이동 통신 시스템에서 인증 에이전트(Authentication Agent)의 단일 사용 승인 장치는, 브라우징 에이전트(Browsing Agent)로부터 인증 에이전트의 식별 정보(identifier)를 조회하도록 트리거링(triggering)하는 메시지를 수신하고, 사용자 제공 식별 정보(User supplied identifier)를 OP(Open ID Provider)/NAF(Network Application Function)로 전송하도록 제어하는 제어부를 포함하는 것을 특징으로 한다.

발명의 효과

[11] 본 발명에 따르면, 보다 안전하게 단일 사용자 승인 절차를 수행할 수 있다.

도면의 간단한 설명

[12] 도 1은 본 발의 일 실시예에 따른 이동 통신 시스템 환경하에서의 단일 사용자 승인(Single Sign-On) 환경을 도시한 블록도이다.

[13] 도 2는 본 발명의 일 실시예에 따른 단일 사용자 승인 과정의 절차를 나타낸 순서도이다.

발명의 실시를 위한 형태

[14] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시 예들을 상세히 설명한다. 이 때, 첨부된 도면에서 동일한 구성 요소는 가능한 동일한 부호로 나타내고 있음에 유의해야 한다. 또한 본 발명의 요지를 흐리게 할 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략할 것이다.

[15] 본 발명은 이동 통신 시스템 환경하에서 단말이 단일 사용 승인을 함에 있어서 보다 안전한 단일 사용 승인 절차를 설명하는 것이다. 이하 본 발명을 구체적으로 설명하는데 있어, 3GPP 를 기반으로 하는 EPS(Evolved Packet System), UTRAN(Universal Terrestrial Radio Access Network: 이하 UTRAN), EUTRAN(Evolved Universal Terrestrial Radio Access Network: 이하 EUTRAN), GERAN(GSM/EDGE Radio Access Network: 이하 GERAN)을 이용할 것이며, 다만, 이에 한정되지 않고 다른 이동 시스템에서도 적용 가능할 것이다. 한편 본 발명에서는 단말을 단일 사용 승인 환경에 적합하도록 관련 정보를 처리하는 과정에 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다.

[16] 또한, 본 발명은 3GPP EPS 를 비롯한 진화된 이동 통신 시스템에서 일반 부트스트래핑 아키텍처 (Generic Bootstrapping Architecture) 및 관련 프로토콜과 기타 보안 관련 프로토콜, 그리고 Open ID 를 위한 지원하는 경우, 단말이 네트워크와 통신하는 과정에 있어서, 단일 사용자 승인 과정을 설명하는 것이다. 이 역시, 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능하다.

[17] 도 1은 본 발의 일 실시예에 따른 이동 통신 시스템 환경하에서의 단일 사용자 승인(Single Sign-On) 환경을 도시한 블록도이다.

[18] 도 1은 본 발명의 바람직한 실시 예에 따른 이동 통신 시스템 환경하에서의 단일 사용자 승인 (single Sign-on) 환경을 도시한 블록도이다.

[19] 여기에서는 일 예로서 3GPP EPS 시스템 구조를 도시하였다. 본 발명의 경우 EUTRAN 을 중심으로 기술하였으며, 이러한 방법은 유사한 다른 이동 통신 시스템에서도 사용할 수 있다.

[20] 도 1을 참조하면, 단말(User Equipment: 이하 단말 혹은 UE 라 칭함)(110)은 기지국과 무선 접속을 설정하고 통신을 수행할 수 있다. UE(110)는 서빙 게이트웨이(Serving Gateway: 이하 Serving GW, 또는 SGW라 칭함)를 통해 인터넷과 같은 패킷 데이터 네트워크에 접속할 수 있다.

[21] UE(110)는 모바일 장비(Mobile Equipment: 이하 ME) 및 SIM(Subscriber Identification Module)을 포함할 수 있다. 상기 모바일 장비는 사용자나 네트워크와 연동하여 통신을 위해 동작을 수행할 수 있다.

[22] 또한 상기 SIM은 사용자의 가입자 관련 정보 및 보안 정보 등의 저장, 관리 등에 관련되는 동작을 수행할 수 있다.

[23] 본 발명의 일 실시예에 따른 UE(110)는 단일 사용자 승인을 위하여 2개의 엔티티를 포함할 수 있다. 즉, UE(110)는 인증 에이전트(Authentication Agent, 이하 AA)(111)와 브라우징 에이전트(Browsing Agent, 이하 BA)(112)를 포함할 수 있다. 이 때, AA(111)와 BA(112)는 물리적으로 동일한 엔티티에 포함되지 않을 수도 있다. 즉, AA(111)는 UE(110)에 포함되어 ME에 존재하고, BA(112)는 물리적으로 별개의 엔티티에 존재할 수도 있다.

[24] 홈 구독자 서버(Home Subscriber Server: 이하 HSS)(121)는 사용자와 단말에 대한 인증정보 및 서비스 정보를 관리할 수 있다. HSS(121)은 홈 위치 등록 서버(Home Location Register: 이하 HLR), AUC(인증센터: Authentication Center)를 포함할 수 있다.

[25] 부트스트래핑 서버 기능(Bootstrapping Server Function: 이하 BSF)(193)은 일반 부트스트래핑 아키텍처를 구성하기 위하여 부트스트래핑 절차에 관여할 수 있다.

[26] 네트워크 어플리케이션 기능(Network Application function: 이하 NAF)(191)은 어플리케이션을 수행할 수 있다. NAF(191)은 오픈 아이디 제공자(OpenID Provider: 이하 OP)를 포함할 수 있다.

[27] 또한, 릴레잉 파티(Relaying Party: 이하 RP)(195)는 단일 사용자 승인 절차에 관여하는 엔티티이다. RP(195)는 사용자가 식별자(identifier)를 사용하는지에 대한 증거를 원하는 웹 어플리케이션(application)을 포함한다.

[28] 또한 상기 OP 는 오픈 아이디 인증 서버 기능을 수행하는 엔티티이다.

[29] 따라서, 본 실시예에서는 이동 통신 및 인터넷 통신에서 사용되는 프로토콜을 기반으로 UE(110), AA(111), BA(112), HSS (121), BSF (193), NAF/OP(191), RP(195) 등 기타 네트워크 엔티티가 사용자의 단일 사용 승인을 좀더 안전하게 동작할 수 있는 방안을 제안하는 것이다.

[30] UE(110), AA(111), BA(112), HSS (121), BSF (193), NAF/OP(191), RP(195)는 각각 다른 구성요소와 데이터를 송수신 할 수 있는 송수신부 및 상기 송수신부를 통해 수신된 데이터를 기반으로 판단하고, 상기 판단 결과에 따른 결과 값을 상기 송수신부를 통해 송수신 할 수 있는 제어부를 포함한다.

[31] 한편 본 발명의 도 1에서 보는 바와 같이 도 1에 따른 본 발명의 실시예는 본 발명의 기본 목적인 단말이 EUTRAN 혹은 3GPP 환경하에서 단말이 단일 사용 승인 하는 방법을 제기한 것으로 이러한 방법은 유사한 기술적 배경 및 채널 형태, 혹은 네트워크 구조(architecture) 또는 유사한 프로토콜 혹은 프로토콜은 상이하나 유사한 동작을 하는 프로토콜을 가지는 여타의 이동통신 시스템에서도 본 발명의 범위를 크게 벗어나지 아니하는 범위에서 약간의 변형으로 적용 가능하며, 이는 본 발명의 분야에서 숙련된 기술적 지식을 가진 자의 판단으로 가능할 것이다.

[32] 도 2는 본 발명의 일 실시예에 따른 단일 사용자 승인 과정의 절차를 나타낸 순서도이다.

[33] 도 1 및 도 2를 참조하면, 먼저, 201 단계에서 BA(112)는 브라우저를 통해서 RP(195)로 사용자 제공 식별 정보(user provided identifier)를 포함하는 신호를 전송할 수 있다. 그 후, 203 단계에서 RP(195)는 단계 201에서 수신한 신호를 기반으로 OP(191)의 주소를 조회할 수 있다. 상기 OP(191)는 NAF를 포함할 수 있다, 나아가, 단계 205에서는 RP(195)는 상기 203 단계에서 조회된 OP/NAF(191) 사이에서 공유 비밀 (shared secret) 정보를 설정할 수 있다.

[34] 207-01 단계 내지 207-19 단계에서 AA(111)와 BA(112)를 통한 단일 사용자 승인과정과 사용자 인증 과정 절차를 설명한다.

[35] 207-01 단계에서, RP(195)가 BA(112)로 205 단계에서 공유 비밀 OP(191)로 BA(112)의 브라우저를 리다이렉트(redirect) 하도록 지시하는 정보를 포함한 메시지를 전송할 수 있다. 상기 메시지는 Open ID 인증 요청 (Open ID authentication request)를 포함할 수 있다. 이때, Open ID 동작에 대한 지시자(indicator)도 함께 전송될 수도 있으며, 이러한 지시자는 이후 BA(112)가 적절한 OP/NAF를 선택하는 과정이나 OP/NAF의 동작 과정에서 활용될 수 있다.

[36] BA(112)는 리다이렉트(redirect) 할 것을 지시하는 메시지를 수신 후, 207-03 단계에서, HTTPS GET 요청(request) 메시지를 OP/NAF(191)로 전송할 수 있다. HTTPS GET 요청 메시지를 수신한 OP/NAF(191)는 그에 대한 응답으로 207-05 단계에서, AA(111)의 식별자(identifier)를 요청하는 HTTPS 응답(response)을 BA(112)로 전송할 수 있다. 그 후, 207-09 단계에서 BA(112)는 OP/NAF(191)로 AA(111)의 식별 정보와 함께 HTTPS GET 요청을 전송할 수 있다.

[37] 207-11 단계 내지 207-19 단계에서 다양한 실시예에 따른 인증 과정을 설명한다.

[38] 본 발명의 제1 실시예에 따르면, 207-11 단계에서 BA(112)는 AA 식별 정보를 AA(111) 전송할 수 있다. 이때, 사용되는 식별 정보로는 사용자 제공 식별자(user supplied identifier)가 사용될 수 있다. AA(111)는 207-13 단계에서, 207-11 단계에서 BA(112)로부터 수신한 AA 식별 정보가 201 단계에서 BA(112)가 RP(195)로 전송한 사용자 제공 식별 정보와 맞는지 비교(compare) 혹은 검증(verification)하여 인증을 하게 된다. 이때, BA(112)가 AA(111)와 물리적으로 별도의 엔티티인 경우, 207-11 단계 이전에 BA(112)가 AA(111)로부터 사용자 제공 식별 정보를 제공받을 수도 있다. 인증에 성공한 경우, 207-15 단계에서 AA(111)는 OP/NAF(191)로 확인(confirm)하는 메시지를 전송할 수 있다.

[39] 본 발명의 제2 실시예에 따르면, 207-11 단계에서 BA(112)는 인증 에이전트의 식별 정보(identifier)를 조회하도록 트리거링(triggering)하는 메시지를 AA(111) 전송할 수 있다. 207-15 단계에서 AA(111)는 AA의 식별 정보로써 사용자 제공 식별 정보 (User spllied identifier)를 OP/NAF(191)로 전송할 수 있다. OP/NAF(191)는 207-17 단계에서, 수신한 AA 식별 정보를 BA(112)로부터 수신한

AA의 식별 정보와 비교 또는 검증하여 인증하는 과정을 수행할 수 있다.

[40] 본 발명의 제3 실시예에 따르면, 207-11 단계에서 BA(112)는 인증 에이전트의 식별 정보(identifier)를 조회하도록 트리거링(triggering)하는 메시지를 AA(111) 전송할 수 있다. 207-15 단계에서 AA(111)는 AA의 식별 정보 중 브트스트래핑 트랜젝션에 사용되는 B-TID (bootstrapping transaction identifier) 또는 사용자 제공 식별 정보 중 어느 하나 이상을 OP/NAF(191)로 전송할 수 있다. OP/NAF(191)는 207-17 단계에서, 수신한 AA 식별 정보 또는 B-TID를 BA(112)로부터 수신한 AA의 식별 정보와 비교 또는 검증하여 인증하는 과정을 수행할 수 있다.

[41] 본 발명의 제4 실시예에 따르면, 207-11 단계에서 BA(112)는 인증 에이전트의 식별 정보(identifier)를 조회하도록 트리거링(triggering)하는 메시지를 AA(111) 전송할 수 있다. 207-15 단계에서 AA(111)는 AA의 식별 정보 중 Mobile Station Integrated Services Digital Number (MSISDN) 또는 사용자 제공 식별 정보 중 어느 하나 이상을 OP/NAF(191)로 전송할 수 있다. OP/NAF(191)는 207-17 단계에서, 수신한 AA 식별 정보 또는 Mobile Station Integrated Services Digital Number (MSISDN)를 BA(112)로부터 수신한 AA의 식별 정보와 비교 또는 검증하여 인증하는 과정을 수행할 수 있다.

[42] 207-19 단계에서는 OP/NAF(191)가 AA(111)로 일반 브트스트래핑 아키텍처 (Generic Bootstrapping Architecture, GBA)를 이용하는 인증 과정을 시작(initiation) 하기 위한 동작을 수행할 수도 있다.

[43] 215 단계에서 AA(111)는 OP(191)로 HTTPS GET 메시지를 송신하고, 217 단계에서 NAF는 215 단계에서 수신한 HTTPS GET 메시지를 기반으로 UE 인증 과정(authneticaiton request)을 시작할 수 있다.

[44] 219 단계에서 AA(111)는 BSF(193)와 부트스트래핑 과정을 수행하게 되고, 이후 221 단계에서 AA(111) 는 부트스트래핑 트랜젝션에 사용되는 B-TID (bootstrapping transaction identifier) 를 포함하는 HTTPS request 메시지를 OP/NAF(191) 로 전송할 수 있다.

[45] 이후, 223 단계에서 OP/NAF(191) 와 BSF(193)는 211 단계에서 전송된 메시지를 기반으로 사용자 인증을 위한 과정을 할 수 있다. 223-03 단계에서 NAF/OP(191)는 브라우징 에이전트(Browsing Agent)를 통해 브라우저를 RP(Relaying Party)(195)로 리다이렉트 하겠다는 것을 알리는 메시지를 AA(111)로 전송할 수 있다. 그 후, 223-05 단계에서 AA(111)는 OP/NAF(191)로 인증 승인 확인(confirm) 메시지를 전송할 수 있다.

[46] 225 단계에서 OP/NAF(191)는 브라우저를 RP(195)로 리다이렉트 할 것을 지시하는 메시지를 BA(112)로 전송할 수 있다. 이때, 인증 승인 메시지를 함께 전송할 것을 지시하는 메시지를 포함하여 전송할 수 있다. 227 단계에서 BA(112)는 브라우저를 RP(195)로 리다이렉트 할 수 있으며, 이때, 인증 승인 메시지를 함께 전송할 수도 있다.

[47] 한편 본 발명의 상세한 설명에서는 구체적인 실시예에 관해 설명하였으나, 본

발명의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 그러므로 본 발명의 범위는 설명된 실시예에 국한되지 않으며, 후술되는 특허청구의 범위뿐만 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

청구범위

[청구항 1] 이동 통신 시스템에서 브라우징 에이전트(Browsing Agent)의 단일 사용 승인 방법에 있어서,
사용자 제공 식별 정보(User supplied identifier)를 RP(Relaying Party)로 전송하는 단계;
상기 RP로부터 브라우저(browser)를 상기 RP로 리다이렉트(redirect) 할 것을 지시하는 메시지를 수신하는 단계;
인증 에이전트(Authentication Agent)의 식별 정보(identifier)를 OP(Open ID Provider)/NAF(Network Application Function)로 전송하는 단계; 및
상기 인증 에이전트의 식별 정보 또는 상기 인증 에이전트의 식별 정보를 조회하도록 트리거링(triggering)하는 메시지를 인증 에이전트로 전송하는 단계를 포함하는 것을 특징으로 하는 방법.

[청구항 2] 제1항에 있어서,
상기 OP/NAF로부터 상기 브라우저를 상기 RP로 리다이렉트 할 것을 지시하는 메시지를 수신하는 단계; 및
상기 브라우저를 상기 RP로 리다이렉트 하는 단계를 더 포함하는 것을 특징으로 하는 방법.

[청구항 3] 제1항에 있어서,
상기 인증 에이전트의 식별 정보를 OP/NAF로 전송하는 단계는,
HTTPS GET 요청(request)을 상기 OP/NAF로 전송하는 단계;
상기 OP/NAF로부터 상기 HTTPS GET 요청(request)에 대한 응답으로, 상기 인증 에이전트의 식별 정보를 요청하는 HTTPS 응답(response)를 수신하는 단계; 및
상기 인증 에이전트의 식별 정보와 HTTP GET 요청을 상기 OP/NAF로 전송하는 단계를 포함하는 것을 특징으로 하는 방법.

[청구항 4] 이동 통신 시스템에서 인증 에이전트(Authentication Agent)의 단일 사용 승인 방법에 있어서,
브라우징 에이전트(Browsing Agent)로부터 인증 에이전트의 식별 정보(identifier)를 수신하는 단계;
수신한 인증 에이전트의 식별 정보가 사용자 제공 식별 정보(User supplied identifier)와 동일한지 여부를 판단하는 단계; 및
상기 인증 에이전트의 식별 정보가 사용자 제공 식별 정보와 동일한 경우, 확인 메시지를 OP(Open ID Provider)/NAF(Network Application Function)로 전송하는 단계를 포함하는 것을 특징으로 하는 방법.

[청구항 5] 제4항에 있어서,

상기 OP/NAF로부터 상기 브라우징 에이전트(Browsing Agent)를 통해 브라우저를 RP(Relaying Party)로 리다이렉트 하겠다는 것을 알리는 메시지를 수신하는 단계; 및
인증 승인 확인(confirm) 메시지를 상기 OP/NAF로 전송하는 단계를 더 포함하는 것을 특징으로 하는 방법.

[청구항 6] 제5항에 있어서,
상기 사용자 제공 식별 정보는,
상기 브라우징 에이전트가 상기 RP로 전송한 사용자 제공 식별 정보인 것을 특징으로 하는 방법.

[청구항 7] 이동 통신 시스템에서 인증 에이전트(Authentication Agent)의 단일 사용 승인 방법에 있어서,
브라우징 에이전트(Browsing Agent)로부터 인증 에이전트의 식별 정보(identifier)를 조회하도록 트리거링(triggering)하는 메시지를 수신하는 단계; 및
사용자 제공 식별 정보(User supplied identifier)를 OP(Open ID Provider)/NAF(Network Application Function)로 전송하는 단계를 포함하는 것을 특징으로 하는 방법.

[청구항 8] 제7항에 있어서,
상기 OP/NAF로부터 부트스트래핑 아키텍처(Bootstrapping Architecture)를 이용하는 인증과정을 시작(initiation)할 것을 지시하는 메시지를 수신하는 단계를 더 포함하는 것을 특징으로 하는 방법.

[청구항 9] 제7항에 있어서,
상기 OP/NAF로부터 상기 브라우징 에이전트(Browsing Agent)를 통해 브라우저를 RP(Relaying Party)로 리다이렉트 하겠다는 것을 알리는 메시지를 수신하는 단계; 및
인증 승인 확인(confirm) 메시지를 상기 OP/NAF로 전송하는 단계를 더 포함하는 것을 특징으로 하는 방법.

[청구항 10] 제7항에 있어서,
상기 사용자 제공 식별 정보를 OP/NAF로 전송하는 단계는,
B-TID(Bootstrapping Transaction Identifier) 또는 사용자 제공 식별 정보 중 적어도 하나 이상을 상기 OP/NAF로 전송하는 것을 특징으로 하는 방법.

[청구항 11] 제7항에 있어서,
상기 사용자 제공 식별 정보를 OP/NAF로 전송하는 단계는,
MSISDN(Mobile Station Integrated Serviced Digital Number) 또는 사용자 제공 식별 정보 중 적어도 하나 이상을 상기 OP/NAF로 전송하는 것을 특징으로 하는 방법.

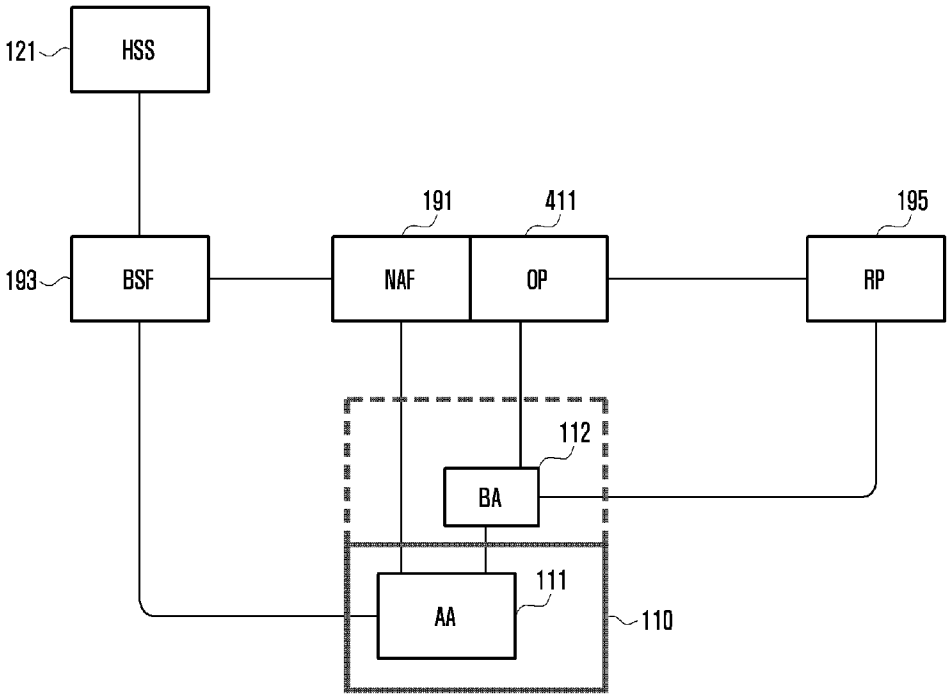
[청구항 12] 제7항에 있어서,
상기 사용자 제공 식별 정보는,
상기 브라우징 에이전트가 상기 RP로 전송한 사용자 제공 식별 정보인 것을 특징으로 하는 방법.

[청구항 13] 이동 통신 시스템에서 브라우징 에이전트(Browsing Agent)의 단일 사용 승인 장치에 있어서,
사용자 제공 식별 정보(User supplied identifier)를 RP(Relaying Party)로 전송하고, 상기 RP로부터 브라우저(browser)를 상기 RP로 리다이렉트(redirect) 할 것을 지시하는 메시지를 수신하며, 인증 에이전트(Authentication Agent)의 식별 정보(identifier)를 OP(Open ID Provider)/NAF(Network Application Function)로 전송하고, 상기 인증 에이전트의 식별 정보 또는 상기 인증 에이전트의 식별 정보를 조회하도록 트리거링(triggering)하는 메시지를 인증 에이전트로 전송하도록 제어하는 제어부를 포함하는 것을 특징으로 하는 장치.

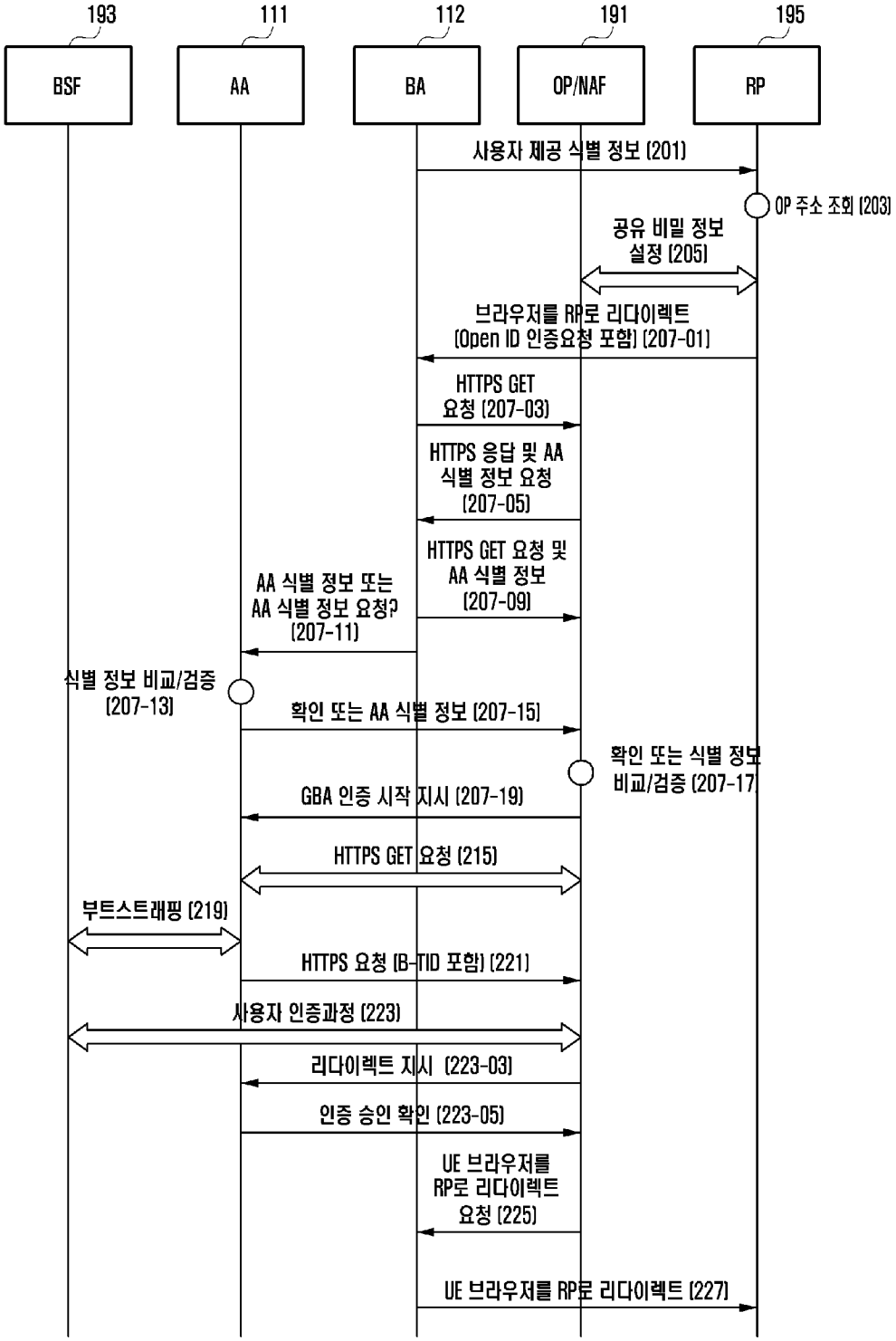
[청구항 14] 이동 통신 시스템에서 인증 에이전트(Authentication Agent)의 단일 사용 승인 장치에 있어서,
브라우징 에이전트(Browsing Agent)로부터 인증 에이전트의 식별 정보(identifier)를 수신하고, 수신한 인증 에이전트의 식별 정보가 사용자 제공 식별 정보(User supplied identifier)와 동일한지 여부를 판단하며, 상기 인증 에이전트의 식별 정보가 사용자 제공 식별 정보와 동일한 경우 확인 메시지를 OP(Open ID Provider)/NAF(Network Application Function)로 전송하도록 제어하는 제어부를 포함하는 것을 특징으로 하는 장치.

[청구항 15] 이동 통신 시스템에서 인증 에이전트(Authentication Agent)의 단일 사용 승인 장치에 있어서,
브라우징 에이전트(Browsing Agent)로부터 인증 에이전트의 식별 정보(identifier)를 조회하도록 트리거링(triggering)하는 메시지를 수신하고, 사용자 제공 식별 정보(User supplied identifier)를 OP(Open ID Provider)/NAF(Network Application Function)로 전송하도록 제어하는 제어부를 포함하는 것을 특징으로 하는 장치.

[Fig. 1]



[Fig. 2]


193
111
112
191
195
BSF
AA
BA
OP/NAF
RP
사용자 제공 식별 정보 (201)
OP 주소 조회 (203)
공유 비밀 정보 설정 (205)
브라우저를 RP로 리다이렉트 (Open ID 인증요청 포함) (207-01)
HTTPS GET 요청 (207-03)
HTTPS 응답 및 AA 식별 정보 요청 (207-05)
HTTPS GET 요청 및 AA 식별 정보 (207-09)
AA 식별 정보 또는 AA 식별 정보 요청? (207-11)
식별 정보 비교/검증 (207-13)
확인 또는 AA 식별 정보 (207-15)
확인 또는 식별 정보 비교/검증 (207-17
GBA 인증 시작 지시 (207-19)
HTTPS GET 요청 (215)
부트스트래핑 (219)
HTTPS 요청 (B-TID 포함) (221)
사용자 인증과정 (223)
리다이렉트 지시 (223-03)
인증 승인 확인 (223-05)
UE 브라우저를 RP로 리다이렉트 요청 (225)
UE 브라우저를 RP로 리다이렉트 (227)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2012/008950

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; H04W 88/02; H04L 9/32; H04L 29/06; G06F 21/00

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(Single Sign-On, SSO), authentication, identification, Browsing(Browsing)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2011-0048038 A (KT CORPORATION) 09 May 2011 See paragraphs [0047]-[0077]; [0116]-[0124]; claims 1-3 and figures 3,8-9.	1-15
A	WO 2011-100331 A1 (INTERDIGITAL PATENT HOLDINGS, INC et al.) 18 August 2011 See paragraphs [0154]-[0159] and figures 4-5.	1-15
A	KR 10-2007-0083345 A (SAMSUNG ELECTRONICS CO., LTD.) 24 August 2007 See abstract; claims 1-2 and figures 2-3.	1-15

☐ 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	Date of mailing of the international search report
27 FEBRUARY 2013 (27.02.2013)	**27 FEBRUARY 2013 (27.02.2013)**

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
Government Complex-Daejeon, 139 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/KR2012/008950

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2011-0048038 A	09.05.2011	CA 2753846 A1	02.09.2010
		KR 10-1094577 B1	19.12.2011
		US 2011-0314531 A1	22.12.2011
		WO 2010-098534 A1	02.09.2010
		WO 2010-098534 A4	02.09.2010
WO 2011-100331 A1	18.08.2011	EP 2534810 A1	19.12.2012
		KR 10-2012-0120955 A	02.11.2012
		US 2012-072979 A1	22.03.2012
KR 10-2007-0083345 A	24.08.2007	NONE	

국 제 조 사 보 고 서

국제출원번호
PCT/KR2012/008950

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04W 12/06(2009.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
H04W 12/06; H04W 88/02; H04L 9/32; H04L 29/06; G06F 21/00

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: 단일 사용 승인(Single Sign-On, SSO), 인증, 식별, 브라우징(Browsing)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2011-0048038 A (주식회사 케이티) 2011.05.09 식별기호 [0047]-[0077]; [0116]-[0124]; 청구항 1-3 및 도면 3,8-9 참조.	1-15
A	WO 2011-100331 A1 (INTERDIGITAL PATENT HOLDINGS, INC 외 6명) 2011.08.18 식별기호 [0154]-[0159] 및 도면 4-5 참조.	1-15
A	KR 10-2007-0083345 A (삼성전자주식회사) 2007.08.24 요약; 청구항 1-2 및 도면2-3 참조.	1-15

☐ 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

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

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

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

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

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

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

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

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2013년 02월 27일 (27.02.2013)	**2013년 02월 27일 (27.02.2013)**

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 82-42-472-7140

심사관
복상문
전화번호 82-42-481-8345

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2012/008950

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2011-0048038 A	2011.05.09	CA 2753846 A1	2010.09.02
		KR 10-1094577 B1	2011.12.19
		US 2011-0314531 A1	2011.12.22
		WO 2010-098534 A1	2010.09.02
		WO 2010-098534 A4	2010.09.02
WO 2011-100331 A1	2011.08.18	EP 2534810 A1	2012.12.19
		KR 10-2012-0120955 A	2012.11.02
		US 2012-072979 A1	2012.03.22
KR 10-2007-0083345 A	2007.08.24	없음	